PODER EXECUTIVO
MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE COMPUTAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

UM CONJUNTO DE TÉCNICAS DE INSPEÇÃO ORIENTADO À AVALIAÇÃO DE PRIVACIDADE EM REDES SOCIAIS ONLINE

ANDREY ANTONIO DE OLIVEIRA RODRIGUES

Manaus – Amazonas
Fevereiro de 2019

ANDREY ANTONIO DE OLIVEIRA RODRIGUES

UM CONJUNTO DE TÉCNICAS DE INSPEÇÃO ORIENTADO A AVALIAÇÃO DE PRIVACIDADE EM REDES SOCIAIS ONLINE

Dissertação de Mestrado submetida ao corpo docente do Programa de Pós-Graduação em Informática da Universidade Federal do Amazonas (PPGI-UFAM) como requisito para obtenção do título de mestre em Informática.

Orientador: Prof. Eduardo Luzeiro Feitosa, D.Sc.
Coorientadora: Profª. Natasha Malveira Costa Valentim, D.Sc.

Manaus – Amazonas
Fevereiro de 2019

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

R696u

Rodrigues, Andrey Antonio de Oliveira
Um Conjunto de Técnicas de Inspeção Orientado à Avaliação de Privacidade em Redes Sociais Online / Andrey Antonio de Oliveira Rodrigues. 2019
194 f.: il. color; 31 cm.

Orientador: Eduardo Luzeiro Feitosa
Coorientadora: Natasha Malveira Costa Valentim
Dissertação (Mestrado em Informática) - Universidade Federal do Amazonas.

1. Privacidade do Usuário. 2. Avaliação de Privacidade. 3. Inspeção de Privacidade. 4. Rede Social. 5. Estudo Empírico. I. Feitosa, Eduardo Luzeiro II. Universidade Federal do Amazonas III. Título

PODER EXECUTIVO
MINISTÉRIO DA EDUCAÇÃO
INSTITUTO DE COMPUTAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

UFAM

FOLHA DE APROVAÇÃO

Um Conjunto de Técnicas de Inspeção Orientado à Avaliação de Privacidade em Redes Sociais Online"

ANDREY ANTONIO DE OLIVEIRA RODRIGUES

Dissertação de Mestrado defendida e aprovada pela banca examinadora constituída pelos Professores:

Prof. Eduardo Luzeiro Feitosa - PRESIDENTE

Prof. Cristiano Maciel - MEMBRO INTERNO

Profa. Raquel Oliveira Prates- MEMBRO INTERNO

Manaus, 01 de Março de 2019

“Alguns homens veem as coisas como são, e dizem ‘Por quê?’ Eu sonho com as coisas que nunca foram e digo ‘Por que não?’”

(George Bernard Shaw).

AGRADECIMENTOS

Agradeço, em primeiro lugar, a Deus que tem iluminado meu caminho durante esta jornada, concedendo-me luz, força e sabedoria para que eu conseguisse seguir até aqui. Tenho certeza que sem Ele nada disso seria possível.

A minha mãe e a minha avó que, de forma especial e carinhosa, me dão força e coragem apoiando todas as minhas decisões. A realização deste sonho não seria possível sem o amor e cuidado que sempre tiveram comigo. Em todos os momentos de dificuldades, penso nelas e no quanto eu quero que elas sintam orgulho de mim.

Agradeço ao meu orientador, professor Eduardo Feitosa, que vem me auxiliando em todos os momentos desta caminhada, por estar sempre disposto a colaborar, por ser além de tudo, um excelente orientador que sempre concede incentivos durante as orientações e por sempre acreditar em mim e confiar no meu trabalho. Obrigado professor pela paciência e pela amizade.

Agradeço a minha coorientadora Natasha Valentim, a quem admiro não só por colaborar com o meu trabalho, mas pela pessoa maravilhosa e generosa que sempre foi. Muito obrigado pelo apoio constante, pelo voto de confiança e amizade. Agradeço por sempre me mostrar o caminho certo, me incentivar e, acima de tudo, por aumentar meu conhecimento.

Agradeço a uma pessoa muito especial, minha orientadora de TCC na graduação e amiga eterna Fabiane Clemente. Obrigado por ter me treinado para o mestrado, por ter feito eu amar a pesquisa, por sempre acreditar em mim, pela confiança e pelo apoio constante. Obrigado por ser essa pessoa incrível que sempre me apoiou. Estarei sempre ao seu lado.

Aos professores Raquel Prates e Cristiano Maciel por aceitarem o convite para participar da minha banca. Uma honra poder contar com a participação de duas grandes referências as quais eu sempre admirei. Espero segui-los como exemplo e ser um grande profissional.

Obrigado a minha família e aos meus grandes amigos que torcem muito por mim, me passando as melhores vibrações e energias positivas. Um agradecimento especial as minhas amigas da UFAM: Karla e Patricia pelas muitas demonstrações de carinho e amizade.

À CAPES pelo apoio financeiro. À UFAM, ao IComp, por prover a infraestrutura.

Por fim, também agradeço a todos que participaram dos estudos conduzidos neste trabalho, pela colaboração, paciência e contribuições.

RESUMO

A crescente discussão sobre a privacidade dos usuários em Redes Sociais Online (RSOs) tem incentivado a adoção de boas práticas de design e avaliação para garantir a aceitabilidade social e qualidade de uso destas aplicações. Desta forma, a privacidade em uma RSO tornou-se um dos fatores determinantes de qualidade, uma vez que mecanismos de privacidade discrepantes podem influenciar negativamente a adoção destas aplicações por parte do usuário. Atualmente, diversos pesquisadores vêm apresentando tecnologias para tratar aspectos de privacidade em RSOs. Parte das tecnologias apresentam soluções alternativas para serem aplicadas em tempo de design. Outra parte destas tecnologias disponibilizam controles de acesso e modelos para gerenciamento de informações pessoais. No entanto, estas tecnologias não se propõem em detectar problemas reais que possam comprometer a interação do usuário com o cenário de privacidade fornecido por estas aplicações. Uma forma alternativa de apoiar a avaliação de privacidade para detectar possíveis problemas é através de inspeção. Os métodos de inspeção destacam-se pelo fato de serem interessantes não apenas por serem de baixo custo, mas também por serem adequados para garantir a qualidade de uso. Nesse sentido, este trabalho propõe um conjunto de técnicas de avaliação orientado à inspeção de privacidade no contexto de RSOs. As técnicas propostas foram desenvolvidas a partir da condução de um mapeamento sistemático da literatura que apontou a carência de tecnologias que apoiassem a inspeção de privacidade no ambiente em questão. As técnicas foram avaliadas e evoluídas por meio de estudos experimentais que identificaram sua viabilidade como técnicas de inspeção. Os resultados indicam que o emprego das técnicas é potencialmente útil para a detecção de defeitos reais de privacidade devido ao caráter exploratório e reflexivo das mesmas. Desse modo, espera-se contribuir para promover a melhoria da qualidade de privacidade em aplicações sociais, de modo que o conjunto de técnicas possa ser usado para assegurar a disponibilização das funcionalidades necessárias e ao mesmo tempo garantir a privacidade dos dados do usuário.

Palavras-chave: Privacidade do Usuário, Avaliação de Privacidade, Inspeção de Privacidade, Rede Social, Estudo Empírico.

ABSTRACT

The growing discussion on user privacy in Online Social Networks (OSNs) has encouraged the adoption of good design and evaluation practices to ensure the social acceptability and quality of use of these applications. In this way, privacy in an OSN has become one of the determining factors of quality, since discrepant privacy mechanisms can negatively influence the adoption of these applications by the user. Currently, several researchers have been presenting technologies to address privacy issues in OSNs. Some of the technologies present alternative solutions to be applied at design time. Another part of these technologies provides access controls and models for managing personal information. However, these technologies are not intended to detect real problems that could compromise user interaction with the privacy scenario provided by these applications. An alternative way of supporting privacy assessment to detect potential problems is through inspection. Inspection methods stand out because they are interesting not only because they are inexpensive, but also because they are adequate to guarantee the quality of use. In this sense, we propose a set of evaluation techniques oriented to privacy inspection in the context of OSN. The proposed techniques were developed from a systematic mapping of the literature that pointed to the lack of technologies that would support the privacy inspection in the environment in question. The techniques were evaluated and evolved through experimental studies that identified their feasibility as inspection techniques. The results indicate that the use of the techniques is potentially useful for the detection of real privacy defects due to their exploratory and reflexive nature. In this way, we hoped to contribute to promote the improvement of the quality of privacy in social applications, so that the set of techniques can be used to ensure the availability of the necessary functionalities and at the same time guarantee the privacy of the user data.

Keywords: User Privacy, Privacy Evaluation, Privacy Inspection, Social Network, Empirical Study.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

CAPÍTULO 1 – INTRODUÇÃO

Este capítulo apresenta a introdução a esta dissertação de mestrado. Além de contextualizar esta pesquisa, são apresentados: a definição do problema, os objetivos, a metodologia e a organização do trabalho.

1.1 CONTEXTO

O avanço das tecnologias de informação e, principalmente, o advento da Internet possibilitaram o emergir de novas ferramentas de interação que coletam, processam e transmitem diversos tipos de informações na Web. Dentre estas, as Redes Sociais Online (RSOs) são as que mais se destacam na atualidade, pois mudaram o modo de interagir e pensar sobre a realidade, tornando-se importantes meios de socialização e informação (BOYD e ELLISON, 2008).

Uma rede social pode ser definida como uma aplicação social da Web cuja finalidade é conectar um grupo de indivíduos autônomos que podem construir um perfil público ou semipúblico e compartilharem ideias e interesses em comum em um mesmo ambiente social (RECUERO, 2009). Com a crescente popularidade destas aplicações e suas diferentes formas de interação e exploração das dinâmicas de relacionamento, seu uso tem incentivado o emprego de boas práticas de design e avaliação para garantir sua aceitabilidade social e qualidade de uso (ROMERO *et al.,* 2013; EPSTEIN *et al.,* 2015; VILLELA e PRATES, 2015).

De acordo com Netter *et al.* (2013), não é exagero afirmar que a privacidade em uma RSO tornou-se um dos fatores determinantes de qualidade de uso nestas aplicações, uma vez que mecanismos ou interfaces de privacidade discrepantes podem influenciar negativamente a interação do usuário com estes sistemas. Ainda que mecanismos sejam implementados para permitir um gerenciamento eficaz da privacidade por parte do usuário, disparidades têm sido observadas entre o que o sistema oferece e o que usuário precisa no que diz respeito à privacidade (LIU *et al.,* 2011; NETTER *et al.,* 2013). Esta disparidade reflete o *gap* sociotécnico apresentado por Ackerman (2000), como sendo a distância entre o que é viável construir tecnicamente e o que é preciso apoiar socialmente.

Dificuldades em encontrar a opção desejada ou a impossibilidade de executar determinadas ações de privacidade nem sempre ocorrem como um gerenciamento inadequado por parte do usuário. Ao invés disso, tais disparidades podem ser resultado do sistema se

basear em um modelo ou mecanismo restrito por regras que não conseguem atingir as necessidades e intenções do usuário (VILLELA e PRATES, 2015), gerando problemas indesejados de privacidade.

Nesse sentido, algumas ferramentas têm sido propostas visando apoiar o design e avaliação de RSOs com foco na privacidade do usuário, de forma que as soluções apresentadas por tais abordagens possam ser facilmente articuladas e aplicadas pelos próprios designers e avaliadores destas aplicações (FONG *et al.*, 2009; LEDERER *et al*., 2004; PANG e ZHANG, 2015; VILLELA e PRATES, 2015). Considera-se este parâmetro importante para o contexto da área de Interação Humano-Computador (IHC), uma vez que a avaliação e o design de privacidade são requisitos relevantes para apoiar a qualidade de uso de uma determinada aplicação.

Aumentar a qualidade de uso de sistemas interativos apresenta vários benefícios para a experiência pessoal do usuário em decorrência do uso e, consequentemente, para a sua vida (NORMAN, 1988; RUBIN, 1994; BIAS e MAYHEW, 2005). Nesse contexto, gerar interações sociais mais personalizadas e produtivas, que focam nos objetivos e tarefas do usuários referentes à privacidade, torna-se um fator preponderante, ainda que desafiador, para manter a segurança e garantir a qualidade da privacidade para o usuário.

1.2 DEFINIÇÃO DO PROBLEMA

Conforme apresentado, nota-se que existe uma ampla importância em avaliar a privacidade de um sistema de rede social online, principalmente por ser um ambiente de grande utilização. Nesta direção, diversos pesquisadores têm apresentado abordagens técnicas e conceituais para tratar aspectos específicos de privacidade em interfaces de RSOs visando aumentar a flexibilidade de uso que estes sistemas oferecem ao usuário durante o processo de interação com a aplicação (BESMER e LIPFORD, 2010; MAZZIA *et al*., 2012; MALANDRINO *et al*., 2013; GAO e BERENDT, 2013; WANG e ZHOU, 2015).

Muitas das abordagens já existentes foram desenvolvidas para tratar questões específicas de privacidade como, por exemplo, o gerenciamento de fotos e informações, controle de acesso e compartilhamento de dados (SHEHAB *et al*., 2010; GAO e BERENDT, 2013; JAMIL, 2017). No entanto, tais abordagens não possuem um foco abrangente para tratar questões gerais de privacidade e detectar problemas reais que possam comprometer a interação e experiência do usuário com o cenário de privacidade fornecido pelas RSOs. Um problema ou defeito de privacidade, nesse sentido, pode ser qualquer condição ou situação

que poderia levar o sistema a se comportar de maneira indesejada e representar um risco para a privacidade do usuário.

Para diagnosticar problemas que possam comprometer a interação do usuário com o design de privacidade destas aplicações, sugere-se o uso de inspeção. Os métodos de inspeção destacam-se principalmente por permitirem ao avaliador (ou inspetor) detectar possíveis problemas que os usuários podem vir a ter quando interagirem com um determinado sistema. Além disso, os métodos de avaliação por inspeção costumam ser mais rápidos e de custo de execução mais baixo do que métodos de investigação e de observação, pois estes não gastam tempo com recrutamento e sessões de coleta de opiniões (BARBOSA e SILVA, 2010).

Para proceder uma avaliação por inspeção existem diversas técnicas que focam em critérios de qualidade de uso específicos como, por exemplo, a Avaliação Heurística derivada da observação empírica, sendo um método amplamente difundido de avaliação de problemas de usabilidade (NIELSEN, 1994). Outro exemplo é o Método de Inspeção Semiótica (MIS), proposto pela Engenharia Semiótica, para avaliar a comunicabilidade de artefatos computacionais (DE SOUZA *et al*., 2006). No entanto, através de um mapeamento sistemático da literatura, foi identificado que não existem técnicas de inspeção que avaliem, especificamente, o critério de privacidade em sistemas de redes sociais online.

Diante disso, torna-se importante propor tecnologias[1] que possam ser aplicadas pelos próprios profissionais envolvidos no projeto e avaliação de uma RSO, de modo que tais tecnologias possam ser facilmente aplicadas na inspeção de privacidade destas aplicações. Os principais benefícios em utilizar este tipo de técnica são: (i) apoiar profissionais novatos, não especialistas, a aprenderem sobre inspeção de privacidade; (ii) garantir a qualidade da privacidade de uma aplicação social, e (iii) proporcionar uma avaliação efetiva com ênfase no baixo custo, rapidez e facilidade de aplicação.

Nesta visão, a questão de pesquisa deste trabalho é: "*Como melhorar a qualidade da privacidade de RSOs utilizando tecnologias que sejam fáceis de aprender e utilizar, que tenham um bom nível de eficiência e eficácia e que tenham uma boa relação custo/benefício?*". Para responder essa questão foram definidos objetivos, os quais serão apresentados a seguir.

---

[1] O termo "tecnologia" é utilizado como generalização para procedimentos, ferramentas, técnicas, metodologias, modelos e outras tipos de propostas elaboradas na área de Engenharia de Software e Interação Humano-Computador (SANTOS *et al*., 2012) .

1.3 OBJETIVOS

O objetivo central desta dissertação consiste em propor um conjunto de técnicas de avaliação que apoie a inspeção de privacidade em RSOs, visando a qualidade da privacidade destas aplicações. Para atingir este propósito geral, buscou-se dividi-lo nos seguintes objetivos específicos:

- Identificar características gerais de privacidade a partir da contribuição de propostas já existentes na literatura científica;
- Estabelecer um conjunto de recursos que apoie a aplicação das técnicas como: capacitação para o uso das tecnologias e recursos de apoio às inspeções;
- Avaliar o conjunto de técnicas por meio de diferentes avaliações experimentais.

O propósito final é que o conjunto de técnicas, apoiado pelo conjunto de recursos, possa ser empregado pelos próprios profissionais envolvidos no projeto e avaliação destas aplicações, buscando evidências que indiquem se as metas de design de privacidade foram alcançadas e se a RSO possui uma qualidade de uso desejada quanto aos seus aspectos de privacidade. Para tal, o conjunto de tecnologias deve atender os seguintes requisitos:

- **Ser fácil de aprender e utilizar (pouco tempo necessário para aprender e aplicar as técnicas) –** Os profissionais que realizarão as inspeções de privacidade em RSOs devem se tornar aptos a aplicar o conjunto de técnicas em um curto período de tempo, ainda que estes profissionais não sejam especialistas em privacidade ou avaliação de interfaces. Nesta visão, eles devem ser capazes de aplicar as técnicas sem treinamento ou após um treinamento que dure poucos minutos.
- **Apresentar bom nível de eficácia (razão entre o número de defeitos detectados e o número de defeitos existentes) –** O conjunto de técnicas deve apoiar os inspetores a identificarem um bom número de problemas de privacidade em RSOs. Comparativamente a outras abordagens de avaliação de privacidade, as técnicas devem apresentar um nível de eficácia equivalente ou superior.
- **Apresentar bom nível de eficiência (razão entre o número de defeitos e o tempo de inspeção)** – O conjunto de técnicas deve apoiar os inspetores na detecção de problemas de privacidade com o menor esforço (homem-hora) possível. Em comparação a outras abordagens de avaliação, as técnicas devem apresentar um nível de eficiência equivalente ou superior.

- **Oferecer uma boa relação custo-benefício na sua aplicação (esforço homens-hora empregados na inspeção) –** O benefício resultante do uso do conjunto de técnicas concebido deve superar seus custos. O maior componente do custo de uso de uma tecnologia é o esforço (homens-hora). O esforço (homem-hora) de inspeção deve representar um percentual baixo em comparação com o esforço total durante o desenvolvimento.

É importante destacar que esses requisitos, segundo Bolchini e Garzotto (2007), são atributos relevantes que podem contribuir para aceitação e adoção de tecnologias. Com isso, espera-se que o conjunto de técnicas definido possa ser empregado na avaliação de privacidade de uma RSO, permitindo a identificação de um maior número de defeitos com esforço reduzido.

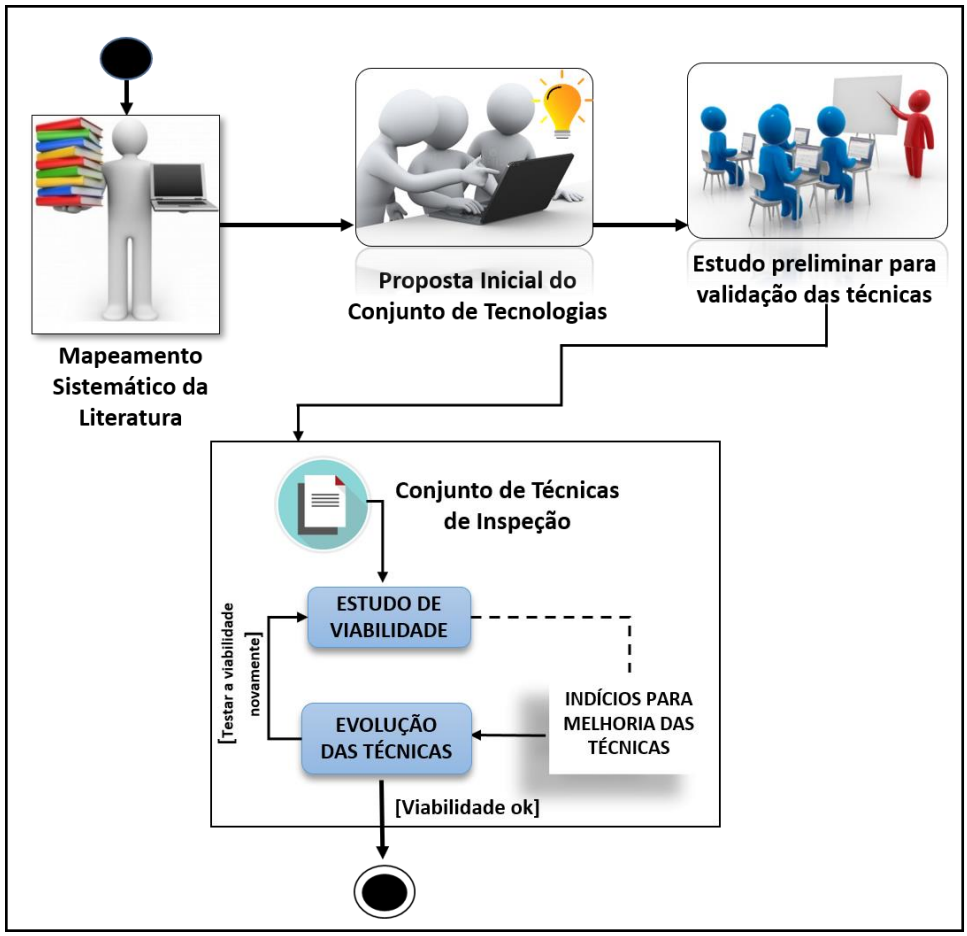
Embora sejam tecnologias de avaliação, as mesmas também podem ser aplicadas em tempo de design, podendo auxiliar em uma avaliação formativa e buscando verificar se as metas de design de privacidade foram alcançadas e se a RSO possui uma qualidade de privacidade desejada. Com isso, almeja-se contribuir para que designers e avaliadores de RSOs, ao utilizarem as técnicas, possam refletir sobre a situação atual do sistema referente à privacidade, suas informações ou elementos discrepantes e necessidades e oportunidades de melhoria.

1.4 METODOLOGIA DE PESQUISA

A metodologia da pesquisa representa o caminho do pensamento a ser seguido, ocupando um lugar central na teoria, tratando, basicamente, dos métodos a serem adotados para construir um conhecimento. Este processo de construção de conhecimento deve envolver a utilização de experimentos para testar modelos e hipóteses assegurando que o entendimento atual do campo é correto (MINAYO, 2003; MENDES, 2005). Desta forma, torna-se relevante a utilização de estudos empíricos para testar se o que está sendo proposto é válido. Com isso, avaliações empíricas devem ser executadas e repetidas para testar a expressividade da tecnologia, aprofundando assim uma melhor compreensão e análise sobre a construção da realidade (SHULL *et al.,* 2001).

Nesse sentido, a pesquisa realizada neste trabalho configurou-se como: (1) do tipo exploratória-descritiva; e (2) com abordagem qualitativa e quantitativa. Para apoiar esta pesquisa sobre a definição do conjunto de técnicas de inspeção de privacidade, utilizou-se o percurso metodológico ilustrado na Figura 1. Esta metodologia destina-se a cumprir os objetivos específicos estabelecidos neste trabalho e é composta pelas etapas listadas a seguir:

Figura 1. Visão ilustrativa da metodologia



Fonte: Próprio autor.

- **Mapeamento Sistemático da Literatura (MSL)** – esta etapa consiste na coleta de evidências na literatura sobre as principais lacunas não cobertas pelas tecnologias existentes, fornecendo os principais indícios para a concepção das novas tecnologias. Para conduzir o processo específico em torno da execução do MSL, foram utilizados os instrumentos apresentados no *guideline* de Kitchenham e Charters (2007), tal como apresentado no capítulo 3.
- **Proposta Inicial do Conjunto de Tecnologias –** com base no conhecimento adquirido através das evidências coletadas na fase anterior, esta etapa possibilitou obter o arcabouço inicial do conjunto de técnicas de inspeção de privacidade para RSOs.
- **Estudo Preliminar para Validação das Técnicas –** nesta etapa, um estudo preliminar é executado com a finalidade de fortalecer os procedimentos de validade e confiabilidade do conjunto de técnicas proposto. Este estudo foi conduzido com

estudantes universitários que indicaram a sua percepção em relação ao conjunto de tecnologias através da aplicação de questionário. Tal questionário foi elaborado com base nos indicadores do modelo TAM (*Tecnology Acceptance Model*), o que permitiu medir o grau de aceitação dos participantes em relação as tecnologias. Além disso, este questionário também coletou dados qualitativos através de perguntas abertas. Esta análise forneceu indícios relevantes para o refinamento das técnicas propostas.

- **Estudo de Viabilidade –** foram realizados dois estudos de viabilidade com o propósito de testar se o conjunto de tecnologias era viável e se o tempo empregado para executar sua proposta era bem utilizado. Estes estudos foram realizados com estudantes universitários que indicaram a sua percepção, em relação ao uso das técnicas, através de um questionário. Este questionário também continha perguntas elaboradas com base nos indicadores do modelo TAM e perguntas abertas para coletar as oportunidades de refinamento. Os dados qualitativos obtidos no questionário foram analisados com base nos procedimentos sugeridos pelo método *Grounded Theory* – GT. Além disso, análises estatísticas também foram efetuadas usando teste de normalidade, paramétricos e não paramétricos. Todo o planejamento, execução e análise destes estudos podem ser vistos no capítulo 6.
- **Evolução das Técnicas –** com base nos indícios coletados para a melhoria das técnicas, obtidos através dos resultados dos estudos de viabilidade, esta etapa permitiu a evolução das técnicas para aprimorar sua estrutura e realizar refinamentos.

1.5 ORGANIZAÇÃO DO TEXTO

Esta dissertação de mestrado está organizada em cinco (07) capítulos, incluindo este introdutório que apresentou a contextualização, a definição do problema, os objetivos e a metodologia de pesquisa inerente ao trabalho. Os conteúdos serão detalhados ao longo dos próximos capítulos. Ademais, este trabalho está organizado segundo a estrutura descrita abaixo:

Capítulo 2 – Fundamentação Teórica: descreve a contextualização bibliográfica acerca do fenômeno de interesse deste trabalho, onde serão abordados os conceitos sobre privacidade e técnicas de inspeção.

Capítulo 3 – Revisão da Literatura sobre Tecnologias que apoiam o Projeto e Avaliação de Privacidade em Redes Sociais Online: apresenta a condução de um mapeamento sistemático realizado com o propósito de identificar as tecnologias existentes

que melhoram a privacidade no contexto de redes sociais online, bem como os trabalhos relacionados com o tema em foco.

Capítulo 4 – Conjunto de Técnicas de Inspeção de Privacidade: apresenta a proposta do conjunto de técnicas para auxiliar na avaliação de privacidade em RSOs visando a qualidade de uso das aplicações.

Capítulo 5 – Estudo Preliminar com o Conjunto de Técnicas PIT-OSN: apresenta a condução de um estudo preliminar realizado para validar as técnicas propostas.

Capítulo 6 – Avaliação de Evolução das Técnicas PIT-OSN através de Estudos de Viabilidade: descreve dois estudos de viabilidade executados para avaliar empiricamente e aperfeiçoar a viabilidade prática das técnicas concebidas.

Capítulo 7 – Considerações Finais e Trabalhos Futuros: contém as considerações finais, contribuições do trabalho, além de apresentar as perspectivas futuras incluindo um cronograma.

CAPÍTULO 2 – FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta a contextualização bibliográfica acerca do fenômeno de interesse deste trabalho, onde serão abordados os conceitos sobre privacidade e suas características, bem como as definições sobre inspeção e suas tecnicalidades.

2.1 INTRODUÇÃO

A busca pela garantia de privacidade em sistemas digitais é um esforço que move diversas áreas da Computação, inclusive a área de IHC com o design e avaliação de sistemas. De acordo com Iachello e Hong (2007), a área de IHC possui boas práticas de design e avaliação para melhorar a qualidade da privacidade do usuário em sistemas computacionais, pois muitas das ameaças e vulnerabilidades associadas à privacidade, originam-se principalmente das falhas na etapa de design e avaliação das aplicações reais.

Um exemplo da importância de IHC para a melhoria de privacidade é que, no Brasil, a CEIHC (Comissão Especial de Interação Humano-Computador) gerou o relatório 'Grandes Desafios de Pesquisa em IHC no Brasil - GranDIHC-BR 2012-2022', que dividiu os desafios em cinco (05) grandes categorias. Uma delas, denominada como 'G4 – Valores Humanos', trata como um dos desafios a "Privacidade no Mundo Conectado".

Nesse sentido, a questão de privacidade é, de fato, um desafio internacional, uma vez que esta mudança do uso de tecnologias e integração entre elas está acontecendo em todo o mundo. Contudo, também tem um forte componente nacional, já que a privacidade é um valor cultural de uma sociedade (BARANAUSKAS *et al.*, 2012). Para melhor caracterizar o tema em questão, a próxima seção apresenta os principais conceitos e definições relacionados à privacidade, considerando a perspectiva do usuário no contexto de RSOs.

2.2 TEORIAS RELACIONADAS À PRIVACIDADE

De acordo com a teoria de regulação de privacidade apresentada por Altman (1975), o termo privacidade é definido como um controle seletivo de acesso ao indivíduo. O autor explica que a privacidade é um processo dialético e dinâmico de regulação de limites em que as pessoas aumentam ou diminuem seus controles de acesso de acordo com o nível de privacidade desejado em um determinado contexto.

Na perspectiva de Altman (1975), os termos dialético e dinâmico possuem definições distintas quanto ao processo de regulação de limites. Segundo o autor, o termo “dialético” diz respeito a um determinado indivíduo dar abertura ou fechamento quanto à interação social com outras pessoas em um dado contexto. Já o termo “dinâmico”, por sua vez, indica que a privacidade pode variar em diferentes circunstâncias, ou seja, que o processo de abertura e fechamento em relação à interação social pode mudar de acordo com diferenças culturais e individuais do indivíduo.

Villela (2016) interpretou a definição de Altman (1975) e identificou três características de privacidade a serem posteriormente consideradas na concepção de um modelo de privacidade proposto pela autora. Tais características são*: controle, estado (nível) e contexto de privacidade*. O controle está relacionado ao processo de regulação de limites de acesso ao indivíduo. O nível de privacidade é visto como resultado do aumento ou diminuição destes limites de acesso. Tais características enunciadas serão melhor explanadas nos parágrafos seguintes.

O **controle de privacidade** está associado ao processo de regulação de limites de acesso tal como abordado na teoria de privacidade de Altman (1975). Além disso, outros teóricos como DeCew (1997) e Westin (2003) também corroboram a visão de Altman em que o controle é o ponto central no sentido de manter a privacidade do indivíduo. Segundo Villela (2016), no mundo físico, este tipo de controle é normalmente óbvio, uma vez que um determinado indivíduo sabe com quem está dialogando e como poderá controlar a sua informação. Entretanto, controlar estes limites de acesso em uma ambiente de RSO pode ser mais complexo, devido as características específicas destas aplicações.

Embora possa acontecer uma violação de privacidade no mundo físico, em ambientes de RSOs a possibilidade da privacidade do indivíduo ser comprometida pode ser ainda maior, uma vez que informações sobre tal indivíduo podem ser compartilhadas por outros usuários e ou até mesmo pelo próprio sistema, sem seu conhecimento ou consentimento. Além disso, até mesmo quando a informação é compartilhada voluntariamente pelo próprio indivíduo, problemas de privacidade podem surgir, caso o mesmo não seja capaz de controlar efetivamente a audiência da informação ou o uso que pode ser feito dela (JOINSON e PAINE, 2007; VILLELA, 2016).

O **nível de privacidade** também relacionado à teoria de Altman, refere-se à possibilidade de um determinado indivíduo aumentar ou diminuir os seus limites de acesso para alcançar o seu estado desejado de privacidade. Para Altman (1975), a principal finalidade

da regulação de limites é possibilitar que o indivíduo atinja o seu estado desejado de privacidade a partir de um espectro que varia desde um ponto total de abertura até um ponto total de fechamento dado por um indivíduo a outras pessoas. Isto indica que pode haver um ponto contínuo de níveis de privacidade que podem ser alcançados pelo indivíduo, variando desde um nível de privacidade baixo (mínimo), onde todas as informações ficam acessíveis para uma ampla audiência, até o nível de privacidade alto, onde nenhuma informação é compartilhada pelo indivíduo.

O contexto de privacidade não será tratado como uma característica específica de privacidade em nossa proposta, uma vez que esta diz respeito ao dinamismo sobre o qual os níveis e controles de privacidade são modificados. Desta forma, a diferença entre os contextos é interessante no sentido de possibilitar que diferentes aspectos e considerações relacionados à privacidade sejam analisados, tendo em vista que o contexto é um fator determinante em decisões de privacidade (ALTMAN, 1975; VILLELA, 2016).

A teoria apresentada por Altman caracteriza inúmeros aspectos que são importantes no que tange a privacidade. No entanto, tal princípio não considera de forma explícita alguns elementos de interações relacionados ao compartilhamento de informações, que estão atualmente inseridos em contextos mediados. Nesse sentido, Petronio (2002) realizou uma extensão da teoria de Altman (1975), inserindo o elemento "colaboração" no processo de regulação de limites. Tal abordagem chamada "Gerenciamento da Privacidade da Comunicação" entende a perspectiva de privacidade como um processo de negociação entre pessoas, ou seja, há uma espécie de pacto entre ambas as partes que estão se comunicando durante o compartilhamento de informações.

Essa perspectiva de nível de privacidade vai ao encontro com a abordagem utilizada na construção do Modelo de Design de Privacidade (MDP), proposto por Villela e Prates (2015), onde as autoras do modelo consideram que as RSOs podem permitir que seus usuários atinjam diferentes níveis de privacidade, dependendo de diferentes elementos envolvidos no compartilhamento de suas informações. Estes elementos estão relacionados a quem compartilha, o que é compartilhado e para quem, em que local e por quanto tempo a informação fica disponível, além dos efeitos gerados por tal compartilhamento. Tal abordagem considera o emissor e o receptor desta comunicação, referentes ao compartilhamento de informação pessoal, como corresponsáveis pela privacidade do indivíduo ao qual a informação se refere.

Nesta direção, este modelo serviu como uma das principais referências para a concepção do conjunto de tecnologias proposto neste trabalho. Uma explanação sobre esta abordagem será apresentada na seção a seguir.

2.3 MODELO DE DESIGN DE PRIVACIDADE

O Modelo de Design de Privacidade (MDP) trata-se de uma ferramenta epistêmica para apoiar o projeto e avaliação do compartilhamento de informações pessoais em RSOs, com foco em privacidade. Como ferramenta epistêmica, o modelo não se propõe a fornecer diretamente uma solução para tratar questões de privacidade em RSOs, mas sim proporcionar uma melhor compreensão ao designer sobre como comunicar a ideia de privacidade e compará-las entre si nestas aplicações (VILLELA e PRATES, 2015).

De acordo com Villela (2016), o MDP é um modelo descritivo que considera o compartilhamento de informações pessoais em RSOs como uma comunicação entre usuários mediada pelo sistema. Tal comunicação pode ocorrer tanto na forma direta (quando o próprio usuário compartilha informações sobre si mesmo no sistema) quanto na forma indireta (quando outro usuário compartilha informações sobre um determinado indivíduo). Tal modelo consiste em uma ferramenta que permite ao designer expressar o seu modelo conceitual referente ao compartilhamento de informações pessoais dentro do sistema, ajudando-o na reflexão sobre o impacto desse compartilhamento na privacidade dos usuários.

O MDP usa como base o espaço de design da Engenharia Semiótica (de SOUZA, 2005) para estruturar o espaço de compartilhamento de informações pessoais em RSOs e fundamenta-se na teoria de privacidade de Altman (1975) para derivar as características de privacidade a serem consideradas no compartilhamento destas informações pessoais. O modelo é estruturado por meio de dimensões de privacidade que refletem diferentes aspectos que impactam a privacidade dos usuários e sobre os quais os designers devem refletir.

As dimensões de privacidade que estruturam o MDP são: **fonte de informação**, que diz respeito a quem pode determinar como, quando e em que extensão a informação pessoal do indivíduo será compartilhada no sistema; **espaço de comunicação**, que se refere ao local onde a informação sobre o indivíduo é compartilhada dentro do sistema; **informação do indivíduo**, composta pelas subdimensões *expressão* (forma como a informação é expressa no sistema) e *conteúdo* (refere-se ao teor da informação sobre o indivíduo que está sendo compartilhada, classificado de acordo com o seu nível de pessoalidade); **persistência temporal**, que diz respeito ao período de tempo durante o qual a informação sobre o indivíduo fica acessível à sua audiência, dentro do sistema; **audiência**, que se refere a quem

terá acesso à informação sobre o indivíduo, compartilhada no sistema; **notificação para o indivíduo**, que diz respeito ao sistema informar adequadamente ao indivíduo quando uma informação sobre ele é divulgada ou acessada por outros usuários e de que forma isso acontece; **discurso do sistema**, relacionada ao sistema tomar a iniciativa de gerar compartilhamentos de informações do indivíduo; e **disseminação da informação**, relacionada à audiência ser capaz de (re)compartilhar informação pessoal do indivíduo dentro do sistema.

Cada uma destas dimensões supracitadas pode assumir diferentes valores que remetem a diferentes níveis de privacidade e podem ser atribuídos às dimensões através de um determinado controle. Tal controle pode ser definido em tempo de design, pelo próprio designer, ou em tempo de uso, pelo usuário ou pelo sistema. Segundo Villela e Prates (2015), com o MDP é possível analisar as redes sociais online visando identificar os **níveis de privacidade** que estas oferecem a seus usuários e não as "opções de privacidade oferecidas a seus usuários".

Rodrigues *et al.* (2017) realizaram um estudo com o propósito de avaliar o MDP, a partir da análise da compreensão e percepção de potenciais usuários do mesmo, sobre o seu uso como ferramenta de apoio à avaliação de privacidade em RSOs. A partir da aplicação do modelo realizada na função *stories* de três RSOs (*Instagram Stories, Facebook Stories e WhatsApp Status),* escolhidas como objeto de estudo, foi possível diferenciar a aceitação dos participantes. Em relação à facilidade de uso observou-se que, de um modo geral, os participantes não acharam o modelo fácil de utilizar. No entanto, tal dificuldade não representa um problema, mas sim uma oportunidade em propor novas pesquisas no sentido de possibilitar uma melhor compreensão sobre o contexto de uso do modelo e/ou adaptar sua estrutura para ser usada em outras tecnologias de privacidade. No que se refere à utilidade percebida, observou-se que a mesma gerou indicadores positivos em relação ao uso do modelo como ferramenta analítica. Tal questão demonstra que o MDP é útil como uma tecnologia de apoio a avaliação de privacidade em RSOs.

Além disso, o estudo realizado aponta também que o MDP foi capaz de expressar clareza e compreensão para a maioria dos participantes do estudo como ferramenta de apoio à avaliação de privacidade em redes sociais online. Com isso, os resultados identificados evidenciam a relevância da aplicação do modelo como uma ferramenta analítica, mostrando também sua importância para apoiar a reflexão dos designers durante o processo de (re)design após uma avaliação executada com o mesmo.

Após as definições gerais sobre privacidade apresentadas nesta seção, a próxima seção aborda os conceitos relacionados à inspeção de software, mais especificamente no que diz respeito à classificação e organização de técnicas de inspeção.

2.4 INSPEÇÃO DE SOFTWARE

A inspeção, no contexto computacional, foi introduzida por Michael Fagan em 1976, inspirado pelos métodos estatísticos de qualidade utilizados na manufatura de hardware. Fagan basicamente formalizou em um processo a prática de questionar a um colega de trabalho se tudo estava ocorrendo de forma correta em um projeto de software (PETERSSON, 2002).

Nesse contexto, enquanto desenvolvia seu trabalho em uma empresa, Fagan criou a inspeção visando aumentar a qualidade de software e melhorar a produtividade dos programadores. Este tipo de método inicialmente centrou o foco na localização de defeitos na estrutura e códigos de programas. Posteriormente, a inspeção foi ampliada para aplicação em outros artefatos de software como documento de requisitos, arquiteturas, modelos, interfaces, entre outros (FAGAN, 1986).

A área de Interação Humano-Computador define a inspeção como um tipo específico de método de avaliação que permite ao avaliador examinar (ou inspecionar) uma solução de IHC para tentar antever as possíveis consequências de certas decisões de design sobre as experiências de uso. Ao inspecionar uma interface, os avaliadores tentam se colocar no lugar de um usuário com determinado perfil, para tentar encontrar problemas que estes teriam, e também para julgar como problemáticos pontos que causariam dificuldades aos usuários durante a interação em um dado sistema (BARBOSA e SILVA, 2010).

2.4.1 Classificação de defeitos

A literatura científica aponta diversas classificações de defeitos para inspeção de sistemas conforme o tipo de artefato que está sendo inspecionado. Um exemplo é a categorização sugerida por Kirner e Abib (1998) e Lanubile *et al.* (1998) adaptada da classificação de Porter e Votta (1994) para identificação de defeitos em requisitos de software. Esta categorização organiza os defeitos em duas classes: omissões e inadequações (*comission*). Uma omissão pode ser categorizada de acordo com o tipo de informação ausente na documentação: falta de funcionalidade, falta de desempenho, falta de ambiente ou falta de interface. Já os defeitos apontados como inadequações podem ser classificados em:

informação ambígua, informação inconsistente, informação incorreta ou seção incorreta. A Tabela 1 apresenta os conceitos relacionados a esta classe de defeitos.

Outra categorização de defeitos é a apresentada por Parnas e Weiss (1985) destinada a inspeção de modelos. Esta categorização classifica os defeitos como: inconsistências ou ineficiências (ocorre quando parte do modelo impõe barreiras para programação ou utilização do próprio modelo) e ambiguidades ou inflexibilidades (quando a parte do modelo que é considerada defeituosa não proporciona a acomodação de mudanças). De acordo com de Mello (2011), este tipo de classificação compreende como defeitos fatores nos quais estão estritamente relacionados a critérios de qualidade como manutenibilidade e reusabilidade do modelo que podem ser considerados subjetivos por não dependerem de um oráculo para comparação. A próxima seção aborda os tipos de técnicas de inspeção existentes na literatura.

Tabela 1. Classe de Defeitos

Classe	Tipo	Descrição
OMISSÃO	Funcionalidade Omitida	Alguma informação, relativa à descrição do comportamento esperado do sistema, não aparece no documento.
	Performance Omitida	Alguma informação, relativa à descrição da performance desejada, não aparece no documento, ou aparece de forma inaceitável.
	Ambiente Omitido	Alguma informação, relativa à descrição do hardware, do software, do banco de dados e do pessoal envolvido, não aparece no documento.
	Interface Omitida	Alguma informação, relativa à forma como o sistema interagirá ou se comunicará com componentes que estão fora do escopo do sistema, não aparece no documento.
INADEQUAÇÃO	Informação Ambígua	Um termo importante, uma frase ou uma sentença, essenciais para o entendimento do sistema não foi definido no documento, ou foi definido de forma que possa causar confusão.
	Informação Inconsistente	Duas sentenças contradizem-se mutuamente ou expressam ações de que não estão corretas ou não podem ser executadas.
	Funcionalidade Incorreta	Alguma sentença expressa um fato que não pode ser verdade de acordo com as condições especificadas.
	Seção Incorreta	Alguma informação está em um local errado dentro do documento.
OUTROS		Defeitos que não se enquadrem nos tipos acima

2.4.2 Técnicas de Inspeção

Um dos fatores decisivos no planejamento e nos resultados da inspeção de um sistema é a definição da técnica de inspeção que será utilizada. Para proceder a inspeção de um artefato de software, o inspetor (profissional que realiza a inspeção) pode utilizar diferentes técnicas de inspeção, tais como: *ad hoc, checklist* e técnicas de leitura.

A inspeção *ad hoc,* como o nome indica, baseia-se exclusivamente na experiência do avaliador, não havendo nenhuma tecnologia, direção ou foco sobre como proceder ou o que deve ser verificado especificamente durante a atividade de inspeção (PETERSSON, 2002). De acordo com Chen *et al.* (2002), um dos principais problemas inerentes a este tipo de técnica está relacionado a habilidade, conhecimento e experiência do inspetor no que tange a atividade de identificação de defeitos.

A inspeção baseada em *checklists* recebe uma estrutura em que questões do tipo "sim/não" devem ser respondidas pelos avaliadores enquanto inspecionam um determinado artefato (LAITENBERGER *et al*., 2001). Em linhas gerais, a técnica *checklist* utiliza uma lista de perguntas, cujas respostas auxiliam o inspetor na identificação de defeitos (KALINOWSKI *et al.*, 2004),

A técnica de inspeção baseada em leitura surgiu como forma de melhorar o processo de inspeção no que diz respeito à atividade de detecção de defeitos (MAFRA e TRAVASSOS, 2005). Tais técnicas podem ser definidas como uma série de procedimentos que podem ser adotados por um avaliador para obter um entendimento do artefato sob inspeção, provendo um guia sistemático para a identificação de defeitos (WONG, 2006). Segundo Shull (1998), o termo "leitura" foi escolhido de forma a enfatizar as similaridades com o processo mental que as pessoas utilizam quando tentam entender o significado de algum texto.

He e Carver (2006) notam que, enquanto as inspeções *ad hoc* e via *checklists* são intuitivas e baseadas em procedimentos não sistemáticos, as técnicas de leitura possuem procedimentos explícitos e sistemáticos. Uma técnica de leitura é constituída de dois componentes principais: procedimentos para orientar o avaliador nos objetivos específicos da inspeção e questões que levem o avaliador a refletir sobre a situação discrepante, de modo a encontrar defeitos (SHULL *et al.*, 2003). Os componentes das técnicas de leitura aumentam a eficiência dos avaliadores individuais (TRAVASSOS, 2002; DE MELLO, 2011).

De acordo com Basili (1997), as técnicas de leitura necessitam ser dependentes de contexto, bem definidas e orientadas a objetivos para apoiar o aprendizado e execução de seus procedimentos. Nesta ótica, Mafra e Travassos (2005) estabeleceram os principais requisitos para a concepção de uma técnica de inspeção baseada em leitura:

i. Estar associada a um tipo de artefato (como uma interface por exemplo) e a notação na qual o artefato é descrito (como língua portuguesa);
ii. Ser adaptável de acordo com as características intrínsecas da aplicação;
iii. Ser detalhista, fornecendo um processo de inspeção bem definido;
iv. Ser avaliada experimentalmente para determinar sua viabilidade e seu grau na efetividade quanto a detecção de defeitos.

O uso de heurísticas é uma opção alternativa que também pode ser inserida em técnicas de inspeção baseadas em leitura e *checklists*, tal como empregadas por Conte *et al.* (2009) que desenvolveram uma técnica de inspeção denominada WDP (*Web Design Perspectives-based Usability)* com o propósito de avaliar a usabilidade em projetos Web sob a perspectiva conceitual, navegacional, estrutural e de apresentação, utilizando as heurísticas de avaliação de usabilidade de Nielsen (1994) para a concepção da técnica em questão, conforme mostrado na Tabela 2.

Tabela 2. Heurísticas da WDP relacionadas à perspectiva de Navegação

#	HEURÍSTICAS
H5	***Prevenção de erros***
	Avalie se a interface previne erros de navegação, ou seja, se as opções disponíveis definem claramente quais resultados ou estados serão alcançados
H7	***Flexibilidade e eficiência de uso***
	Avalie se a interface provê formas diferentes de acessar as principais tarefas.
	Avalie se a interface provê teclas de aceleração ou atalhos quando o usuário realiza as tarefas principais
	Avalie se os acessos providos pela interface minimizam o esforço físico do usuário
H9	***Reconhecimento, diagnóstico e recuperação de erros***
	Avalie se o sistema mostra como acessar soluções alternativas quando são apresentadas mensagens de erro
H10	***Ajuda e Documentação***
	Avalie se a interface provê um modo fácil de acessar ajuda e documentação de uma tarefa específica

Fonte: Conte *et al.,* 2009.

Conforme o tipo de técnica a ser aplicada, uma inspeção pode variar no seu custo e na sua eficácia. Estudos sugerem que a adoção de técnicas de leitura apontam melhores resultados do que a aplicação de *checklists* (PORTER *et al*., 1995; LAITENBERGER *et al*.,

2001; HE e CARVER, 2006), todavia, ressalta-se que não há unanimidade (SABALIAUSKAITE *et al*., 2003).

2.5 CONSIDERAÇÕES SOBRE O CAPÍTULO

Este capítulo teve como principal objetivo apresentar o aporte teórico acerca do fenômeno de interesse abordado neste trabalho, onde foram apresentados os conceitos sobre privacidade e suas características, bem como as definições sobre inspeção de software e suas tecnicalidades.

Nesse sentido, este capítulo apresentou uma visão geral sobre as principais teorias relacionadas à privacidade que estão interligadas com a temática foco deste trabalho, como a teoria de regulação de limites proposta por Altman (1975) e a teoria que considera a privacidade como comunicação de Petronio (2002). Também foi apresentada uma visão sobre um Modelo de Design e Avaliação de Privacidade (MDP) que fundamentou suas características estruturais nestas teorias mencionadas, e que serviu como uma das principais bases referenciais para a concepção do conjunto de técnicas proposto neste trabalho.

Além disso, uma visão geral sobre o processo tradicional de inspeção foi apresentada, abordando fatores que podem influenciar na qualidade de inspeções. Dentre estes fatores, estão as técnicas de inspeção que podem ser identificadas na literatura apoiando a identificação de defeitos em diversos tipos de artefatos de sistemas, sendo tipicamente estruturadas como *ad hoc*, *checklists* e técnicas de leitura. Com isso, torna-se viável mapear possíveis casos de discrepâncias no artefato sob inspeção, utilizando-se destas técnicas. Ademais, é importante considerar a categorização de defeitos a ser seguida que pode variar conforme as perspectivas que devem ser observadas durante o processo de inspeção.

CAPÍTULO 3 – REVISÃO DA LITERATURA SOBRE TECNOLOGIAS QUE APOIAM O PROJETO E AVALIAÇÃO DE PRIVACIDADE EM REDES SOCIAIS ONLINE

Este capítulo apresenta a condução e os resultados de uma revisão da literatura cujo objetivo consistiu em identificar e caracterizar as tecnologias que apoiam o projeto e avaliação de privacidade no contexto de RSOs. Desta forma, é apresentado a condução de um mapeamento sistemático da literatura, bem como os trabalhos relacionados com o tema.

3.1 INTRODUÇÃO

A área de Interação Humano-Computador (IHC) investiga o "projeto (design) e avaliação de sistemas computacionais interativos para uso humano, juntamente com os fenômenos associados a este uso" (HEWETT *et al.*, 1992). De acordo com Prates e Barbosa (2007), os estudos relacionados ao **projeto** de IHC referem-se a como construir interfaces com alta qualidade. Para tal, são definidos métodos, modelos, diretrizes, entre outros. Os estudos relacionados à **avaliação** de IHC, por sua vez, buscam avaliar a qualidade de um projeto de interface, tanto ao longo do processo de desenvolvimento como quando o software está pronto.

Para construir tecnologias que apoiem o projeto e avaliação de privacidade em RSOs, torna-se necessário caracterizar as tecnologias já existentes na literatura especializada, com o propósito de conhecer as suas propostas e funcionamento e em que estágios (projeto ou avaliação) tais tecnologias podem ser empregadas. Deste modo, decidiu-se aprofundar conhecimentos a partir de um levantamento na literatura das tecnologias que tratam questões de privacidade voltadas para o projeto e avaliação de RSOs. Por esta razão, realizou-se um Mapeamento Sistemático da Literatura (MSL).

De acordo com Kitchenham e Charters (2007), um MSL é um tipo de Revisão Sistemática podendo ser utilizado para prover uma ampla visão de uma determinada área e estabelecer se existem evidências de pesquisas em um determinado tópico. Ao contrário das revisões tradicionais da literatura, onde o pesquisador não segue um processo definido para sua condução, um MSL é executado de maneira formal obedecendo um protocolo pré-definido. Em comparação com revisões tradicionais da literatura, os mapeamentos sistemáticos requerem maior rigor na sua execução. Em compensação, seus resultados tendem a ser mais confiáveis, visto que estes fazem uso de uma metodologia rigorosa e passível de

auditagem, tornando-a capaz de ser repetida e reduzindo a influência do viés dos pesquisadores.

Nesse contexto, um MSL foi executado com o propósito de identificar (a) qual a principal contribuição das tecnologias de privacidade investigadas e (b) em que estágio (projeto e/ou avaliação) estas tecnologias podem ser aplicadas. Em vista disso, este capítulo apresenta a condução do mapeamento, os principais resultados alcançados e um resumo das tecnologias identificadas. Nesta direção, almeja-se também fornecer um levantamento sistemático que sirva como base e direcionamento para profissionais e pesquisadores que buscam projetar e/ou avaliar aspectos de privacidade no contexto de redes sociais online.

3.2 PROTOCOLO DO MAPEAMENTO SISTEMÁTICO

O protocolo de um mapeamento especifica os instrumentos que foram utilizados para conduzir o processo específico em torno da execução do MSL e este diminui a possibilidade de viés do pesquisador (KITCHENHAM e CHARTERS, 2007). O protocolo deste mapeamento foi embasado no *guideline* apresentado em Kitchenham e Charters (2007), o qual será apresentado a seguir.

3.2.1 Objetivo

A descrição do objetivo deste MSL conforme o paradigma GQM (*Goal-Question-Metric*), proposto por Basili e Rombach (1998), é apresentado na Tabela 3.

Tabela 3. Objetivo do MSL segundo o paradigma GQM de Basili e Rombach (1998)

Analisar	as tecnologias de IHC que apoiam o projeto e avaliação de privacidade em redes sociais online (RSOs)
Com o propósito de	caracterizá-las
Em relação a	ao projeto e avaliação de privacidade em RSOs
Do ponto de vista dos	pesquisadores de IHC
No contexto	fontes primárias disponíveis no mecanismo de busca da SCOPUS, ACM e IEEE

Fonte: Próprio autor.

3.2.2 Questão de Pesquisa

A questão de pesquisa principal que permeou este mapeamento foi: ***"Quais tecnologias de IHC que apoiam o projeto e avaliação de privacidade em RSOs são relatadas na literatura científica?"***. Além desta questão de pesquisa, foram definidas um conjunto de subquestões com o intuito de responder questionamentos específicos sobre a aplicabilidade de cada tecnologia, conforme apresentadas na Tabela 4.

Tabela 4. Suquestões de pesquisa do MSL

Subquestões de Pesquisa	Objetivo
SQ1. Tipo de tecnologia	Descobrir se a tecnologia apoia o projeto ou avaliação de privacidade em Redes Sociais Online
SQ1.1 Tipo de avaliação da tecnologia	Descobrir quais são os tipos de tecnologias de avaliação de privacidade
SQ2. Tipo de contribuição	Descobrir a principal contribuição das fontes primárias da tecnologia
SQ3. Apoio Ferramental	Investigar quais tecnologias necessitam de apoio ferramental
SQ4. Estudos empíricos	Descobrir quais tecnologias têm sido empiricamente avaliadas
SQ4.1 Instrumentos de coletas de dados	Descobrir quais são os tipos de instrumentos de coletadas de dados utilizados em relação a tecnologia
SQ4.2 Tipo de dados coletados	Descobrir se os dados coletados pela tecnologia tem sido analisado de maneira quantitativa ou qualitativa
SQ4.3 Tipo de análise	Descobrir se os dados coletados foram analisados de forma preditiva, interpretativa ou experimental
SQ4.4 Ambiente de avaliação	Investigar quais tecnologias têm sido validadas em ambientes acadêmicos e/ou industrial
SQ5. Contexto da tecnologia	Descobrir quais tecnologias identificadas são específicas ou genéricas

Fonte: Próprio autor.

Estas subquestões de pesquisa possibilitaram categorizar e resumir a percepção e os conhecimentos atuais sobre o tema em foco. Com isso, foi possível identificar lacunas na pesquisa atual e recomendar áreas para investigação futura, além de viabilizar conhecimentos úteis para os profissionais que pesquisam sobre privacidade no contexto de RSOs. As possíveis respostas a cada subquestão de pesquisa são explicadas em mais detalhes a seguir.

Na **SQ1** (Tipo de tecnologia), a tecnologia pode ser categorizada nos seguintes tipos:

a. Projeto de Privacidade: foram consideradas tecnologias de projeto aquelas usadas para apoiar o design (projeto) de soluções de interface para RSOs com foco em privacidade.
b. Avaliação de Privacidade: foram consideradas tecnologias de avaliação aquelas usadas para apoiar a avaliação de aspectos de interface em RSOs com foco em privacidade.
c. Ambas: se a tecnologia é utilizada para projeto e avaliação de privacidade em RSO.

Dentro da SQ1, há uma subquestão chamada SQ1.1 (Tipo de avaliação da tecnologia) direcionada para tecnologias de avaliação. Sobre a **SQ1.1**, as tecnologias foram classificadas

com base nos tipos de avaliação de IHC apresentados por Dix *et al.* (2003) e Barbosa e Silva (2010) e podem ser dos seguintes tipos:

a. Investigação: esse método permite ao avaliador ter acesso, interpretar e analisar concepções, opiniões, expectativas e comportamentos do usuário relacionados com sistemas interativos. São frequentemente utilizadas nas etapas iniciais do processo de design ou também são usados para avaliar a introdução de uma nova tecnologia. Diferencia-se do método de observação, porque não é obrigatório que um usuário utilize um sistema interativo durante a coleta de dados.
b. Inspeção: permite ao avaliador examinar (ou inspecionar) uma solução de IHC para tentar antever as possíveis consequências de certas decisões de design sobre as experiências de uso. Em outras palavras, tenta identificar problemas que os usuários podem vir a ter quando interagem com o sistema.
c. Observação: fornece dados sobre situações em que os usuários realizam suas atividades com apoio de sistemas interativos. Através do registro dos dados observados, esses métodos permitem identificar problemas *reais* que os usuários enfrentaram durante sua experiência de uso da tecnologia sendo avaliada.

O objetivo da **SQ2** (Tipo de Contribuição) é identificar a principal contribuição do artigo. O tipo de contribuição refere-se à determinação do tipo de intervenção sendo estudada (PETERSEN *et al.*, 2015), que pode ser uma ferramenta, métodos, métricas, modelos, diretrizes, entre outros.

Sobre a **SQ3** (Apoio ferramental), a tecnologia pode ser classificada em uma das seguintes respostas:

a. Sim: a tecnologia requer algum suporte de ferramenta específico.
b. Não: a tecnologia não requer suporte de ferramentas específico.

Sobre a **SQ4** (Estudos empíricos), a tecnologia pode ser avaliada através dos estudos empíricos, onde os mesmos contam com a participação dos usuários para relatar experiências de uso vivenciadas ou permitir a observação de experiências reais de uso com a solução de IHC avaliada e/ou projetada (BARBOSA e SILVA, 2010). Nesse sentido, a tecnologia pode ser categorizada em uma das seguintes respostas:

a. Sim: existe uma avaliação empírica da tecnologia proposta descrita no artigo.
b. Não: não há avaliação empírica da tecnologia proposta descrita no artigo.

Dentro da SQ4, existem subquestões chamadas SQ4.1 (Instrumento de coleta de dados), SQ4.2 (Tipo de dados coletados), SQ4.3 (Tipo de análise) e SQ4.4 (Ambiente de avalia-

ção). Provas de conceitos e exemplos ilustrativos não foram considerados nesta subquestão, uma vez que não apresentam evidência empírica. Para **SQ4.1**, os instrumentos de coleta de dados foram classificados de acordo com as definições apresentadas por (COURAGE e BAXTER, 2005; BARBOSA e SILVA, 2010) e podem ser dos seguintes tipos:

a. Entrevista: trata-se de uma conversa guiada por um roteiro de perguntas ou tópicos na qual um entrevistador busca obter informação de um entrevistado;
b. Questionário: trata-se de um formulário impresso ou on-line com perguntas que os usuários e demais participantes devem responder, a fim de fornecer os dados necessários em uma pesquisa, análise ou avaliação;
c. Grupos de foco: diversas pessoas (geralmente entre três e dez) são reunidas por uma ou duas horas numa espécie de discussão ou entrevista coletiva, guiada por um moderador experiente;
d. Classificação de cartões: é utilizada principalmente para informar ou guiar o projeto da arquitetura de informação de um produto;
e. Estudo de campo: é entender o comportamento natural do usuário final no contexto do seu próprio ambiente de atuação;
f. Registro de uso: coletar informações sobre como os usuários usam o sistema através de registros feitos durante o uso.

Sobre a **SQ4.2**, os dados coletados em um estudo podem ser classificados em um dos seguintes tipos:

a. Qualitativo: a análise do estudo da tecnologia foi conduzida de forma qualitativa, ou seja, dados que representam conceitos que não são representados numericamente. Além dos dados nominais, também são dados qualitativos as respostas livres coletadas em questionários e entrevistas, tais como expectativas, explicações, críticas, sugestões e outros tipos de comentários (PRATES e BARBOSA, 2007).
b. Quantitativos: a análise do estudo da tecnologia foi realizada de forma quantitativa, ou seja, representam numericamente uma quantidade, uma grandeza resultante de uma contagem ou medição, tais como: o tempo e número de passos necessários para alcançar determinado objetivo; o número de erros cometidos durante uma sessão de uso, entre outros (WIXON e WILSON, 1997).
c. Ambas: a análise do estudo da tecnologia foi conduzida de forma quantitativa e qualitativa.

Sobre a **SQ4.3**, os avaliadores podem analisar os dados coletados em um dos seguintes tipos (PRATES e BARBOSA, 2007):

a. Análise preditiva: é realizada quando os avaliadores, ao analisarem os dados coletados de especialistas, tentam prever que tipo de problemas os usuários enfrentarão;
b. Análise interpretativa: é realizada quando, ao analisarem os dados coletados a partir da interação do usuário com o sistema, os avaliadores procuram explicar os fenômenos que ocorrem durante essa interação;
c. Análise experimental: os dados coletados em ambientes controlados, como laboratórios, precisam ser analisados em função das variáveis sendo observadas.

Em **SQ4.4**, o ambiente onde a tecnologia foi avaliada pode ser categorizado em um dos seguintes tipos:

a. Ambiente acadêmico com alunos: se a tecnologia foi utilizada ou avaliada em um ambiente acadêmico com os alunos;
b. Ambiente de laboratório com profissionais: se a tecnologia foi utilizada ou avaliada em laboratório (com profissionais ou especialistas);
c. Ambiente de laboratório com usuários: se a tecnologia foi utilizada ou avaliada com usuários reais; ou
d. Misto: se a tecnologia foi utilizada ou avaliada em laboratório e em ambientes acadêmicos.

Na **SQ5** (Contexto da tecnologia), a tecnologia pode ser categorizada em uma das seguintes respostas:

a. Específico: a tecnologia foi utilizada ou avaliada em um contexto específico, isto é, limitada a um tipo específico de rede social (por exemplo, rede social móvel, rede social acadêmica, entre outros), ou;
b. Genérico: se a tecnologia foi utilizada ou avaliada em um contexto geral, isto é, não limitado a um tipo específico de rede social.

3.2.3 Estratégia utilizada para a pesquisa dos estudos primários

Para montar a estratégia de busca deste mapeamento foram definidos: o escopo da pesquisa, o idioma considerado, os termos utilizados, a *string* de busca, os critérios de seleção de artigos e os procedimentos adotados para a execução do MSL.

- **Escopo da pesquisa**

A pesquisa foi executada em três bibliotecas digitais através de seus mecanismos de busca avançada. A Tabela 5 mostra as fontes consideradas no escopo desta pesquisa:

Tabela 5. Fontes utilizadas no MSL

Nome da Fonte	Link	Tipo de Pesquisa
Scopus	http://www.scopus.com/home.url	Máquina de Busca
ACM	https://dl.acm.org/	Máquina de Busca
IEEE	http://ieeexplore.ieee.org	Máquina de Busca

Fonte: Próprio autor

Estas bibliotecas foram selecionadas porque: (1) permitem uma boa operação e escopo de seus mecanismos de busca; (2) são bases referenciais para o acesso a informações de publicações que auxiliam pesquisadores no desenvolvimento de pesquisa na academia. A *Scopus* é uma das maiores bases de dados que indexa resumos e citações, além de ter uma ferramenta que permite avaliar o desempenho das pesquisas (medição de produção científica – bibliometria). ACM também indexa algumas publicações da *Springer*, *Link*, *Science Direct* e muitas publicações relacionadas a área de IHC. Por fim, a IEEE é uma das maiores bibliotecas que fornece acesso a conteúdo científico e técnico de algumas das publicações mais citadas do mundo em Ciência da Computação. Apesar de cada mecanismo apresentar suas particularidades para compor a *string* de busca, foi possível defini-la de acordo com o desejado (KITCHENHAM e CHARTERS, 2007).

- **Idioma dos artigos**

Decidiu-se que seriam selecionados apenas os artigos que foram escritos na língua inglesa ou portuguesa. Inglês por ser o idioma adotado pela maioria das conferências, periódicos internacionais e editoras relacionadas com o tema, listadas no Portal de Periódicos da CAPES. E português por ser a língua nativa do pesquisador.

- **Termos utilizados na pesquisa (palavras-chave)**

Com a finalidade de melhorar e estruturar a busca nas bibliotecas digitais selecionadas, utilizou-se neste mapeamento sistemático o PICOC (KITCHENHAM e CHARTERS, 2007), o qual foi aplicado da seguinte forma:

  - **Population (P)**: Redes Sociais Online
  - **Intervention (I)**: Tecnologias de IHC que apoiam o projeto e avaliação de privacidade em RSOs.

- **Comparison (C)**: Não se aplica, pois, o objetivo não é fazer uma comparação entre tecnologias, mas caracterizá-las.
- **Outcome (O)**: Melhorias de privacidade em RSOs através de tecnologias que projetam/avaliam tais RSOs.
- **Context (C)**: Não se aplica, pois, como não há comparação, não é necessário determinar um contexto.

Na Tabela 6 são apresentados os termos e a *string* de busca em inglês e na Tabela 7 são mostrados os termos e a *string* de busca em português utilizados durante a pesquisa. Os termos estão agrupados em três partes: a primeira parte representa a população, ou seja, as publicações que fazem referência a redes sociais online (RSOs); a segunda representa a intervenção: o que se planeja encontrar; e a terceira representa os resultados: o que se deseja melhorar, avaliar ou projetar.

Tabela 6. Termos e String de busca em inglês

***String* de busca em inglês**		
População	("online social network" OR "social network" OR “social networking” OR "social network site")	AND
Intervenção	("tool" OR "framework" OR "technique" OR "method" OR “mecha-nism” OR "model" OR "guideline" OR "approach*" OR "inspection" OR "aspect" OR "heuristic")	AND
Resultados	("privacy design" OR "privacy evaluation" OR "privacy assessment" OR "privacy improvement" OR “privacy control” OR “privacy analy-sis” OR "privacy assurance")	

Fonte: Próprio autor.

Tabela 7. Termos e String de busca em português

***String* de busca em português**		
População	("redes sociais online" OR "rede social" OR "site de rede social”	AND
Intervenção	("ferramenta" OR "framework" OR "técnica" OR "método" OR “me-canismo” OR "modelo" OR "diretrizes" OR "abordagem" OR "inspe-ção" OR "aspectos" OR "heurísticas")	AND
Resultados	("projeto de privacidade" OR "avaliação de privacidade" OR "melhoria de privacidade" OR “controle de privacidade” OR "garantia de priva-cidade")	

Fonte: Próprio autor.

3.2.4 Critérios de Seleção de Artigos e Procedimentos

Com o objetivo de filtrar apenas os artigos que possuíam realmente alguma relação com a temática foco deste MSL, foram estabelecidos critérios de inclusão (CI) e exclusão (CE), cuja aplicação foi feita sobre a análise do título, resumo e palavras-chaves de cada artigo identificado nas máquinas de busca. Antes do processo de seleção, o pesquisador

delimitou um entendimento consistente dos critérios de inclusão e exclusão, os quais estão listados na Tabela 8.

Tabela 8. Critérios de inclusão e exclusão definidos

Critérios	Descrição
Inclusão	[CI1] Publicações que apresentam tecnologias de IHC que apoiam o projeto ou avaliação de privacidade em redes sociais online
	[CI2] Publicações onde são apresentadas ferramentas que apoiam tecnologias de IHC que projetam e/ou avaliam a privacidade de redes sociais online
	[CI3] Publicações onde são descritos estudos empíricos de tecnologias de IHC que apoiam o projeto ou avaliação de privacidade em redes sociais online
	[CI4] Publicações que discutam aspectos relacionados a tecnologias de IHC que apoiam o projeto ou avaliação de privacidade em redes sociais online
Exclusão	[CE1] Não serão selecionadas publicações que não atendam aos critérios
	[CE2] Não serão selecionadas publicações que não têm disponibilidade de conteúdo para leitura e análise dos dados (especialmente em casos onde os estudos são pagos ou não disponibilizados pela máquina de busca)
	[CE3] Não serão selecionadas publicações que descrevam e/ou apresentam "*keynote speech*", anais, tutoriais, cursos e similares
	[CE4] Não serão selecionadas publicações que possuem linguagem diferente de Inglês e Português

Fonte: Próprio autor.

3.2.5 Processo de seleção dos artigos

- Processo de seleção preliminar (1º filtro): O pesquisador avaliou o título, o resumo e as palavras-chaves de cada artigo de acordo com os critérios de inclusão e exclusão e os artigos selecionados que estariam dentro do escopo da questão de pesquisa. O pesquisador manteve qualquer artigo para a próxima etapa do processo de seleção se não conseguiu decidir se incluí-lo ou descartá-lo com base apenas em seu título, resumo e palavras-chaves.
- Processo de seleção final (2º filtro): Efetuada a seleção dos artigos, iniciou-se a segunda filtragem dos mesmos. Como a estratégia de leitura de somente três informações (título, *abstract* e palavras-chaves) não é suficiente para identificar se o estudo é realmente relevante, torna-se necessário realizar a leitura completa dos artigos que restaram do 1° filtro. Dessa forma, no segundo filtro, o pesquisador realizou uma leitura completa dos artigos selecionados do primeiro filtro. O pesquisador usou os critérios de seleção para julgar se os artigos deveriam ser finalmente incluídos ou não.

3.2.6 Procedimento de Extração dos Dados

A estratégia de extração de dados empregada neste mapeamento foi baseada em fornecer o conjunto de possíveis respostas para cada subquestão de pesquisa definida anteriormente. Esta estratégia assegura a aplicação dos mesmos critérios de extração de dados para todos os artigos selecionados e facilita a sua classificação. Os dados extraídos foram registrados em um documento, conforme apresentado na Tabela 9, para posterior análise e síntese.

Tabela 9. Formulário para extração de dados.

Referência (autor, ano). Nome do artigo	
Descrição da tecnologia	Descrição da tecnologia proposta
Tipo de tecnologia	Verifica qual é o tipo da tecnologia: • Avaliação (é usada para apoiar a avaliação de aspectos de interface em RSOs com foco em privacidade); • Projeto (a tecnologia é usada para apoiar o projeto de soluções de interface em RSOs com foco em privacidade);
Tipo de avaliação da tecnologia	Os tipos de avaliação da tecnologia podem ser de: • Investigação • Inspeção • Observação
Baseia-se em alguma tecnologia existente? Qual?	Utiliza como base para formulação da proposta alguma tecnologia existente? Se sim, qual? • Sim • Não
A tecnologia é específica ou é genérica?	A tecnologia pode ser: • Específica (a tecnologia foi utilizada ou avaliada em um contexto específico, isto é, limitada a um tipo específico de rede social, por exemplo, rede social móvel, rede social acadêmica, entre outros) • Genérica (se a tecnologia foi utilizada ou avaliada em um contexto geral, isto é, não limitado a um tipo específico de rede social)
Qual é o resultado da pesquisa?	O resultado da pesquisa pode ser: • Ferramenta • Framework • Técnica • Método • Mecanismo • Modelo • Diretrizes • Abordagem • Inspeção • Nenhum
A tecnologia tem apoio ferramental? Qual?	Alguma ferramenta foi desenvolvida para dar suporte a tecnologia proposta? Se sim, qual? É gratuita ou paga? • Sim • Não

A tecnologia possui avaliação empírica?	O estudo realizado no artigo foi analisado empiricamente: • Sim • Não
Detalhes do estudo	
Descrição do estudo realizado	Resumo do estudo experimental efetuado
Qual o tipo de instrumento de coleta de dados utilizado?	O tipo de instrumento de coleta de dados pode ser: • Entrevista; • Questionário; • Grupos de foco, • Classificação de cartões; • Estudo de campo • Registro de uso
Qual foi o ambiente onde a tecnologia foi aplicada?	Ambiente em que foi aplicada a tecnologia: • Indústria • Academia • Laboratório • Mista
Os dados coletados são de que tipo?	Os dados coletados podem ser: • Qualitativo • Quantitativo • Ambos
A análise do estudo é de que tipo?	A análise do estudo poder ser: • Preditiva • Interpretativa • Experimental
A tecnologia tem limitações? Qual?	Há limitações encontradas na aplicação da tecnologia e na análise dos estudos? Se sim, qual? • Sim • Não

Fonte: Próprio autor.

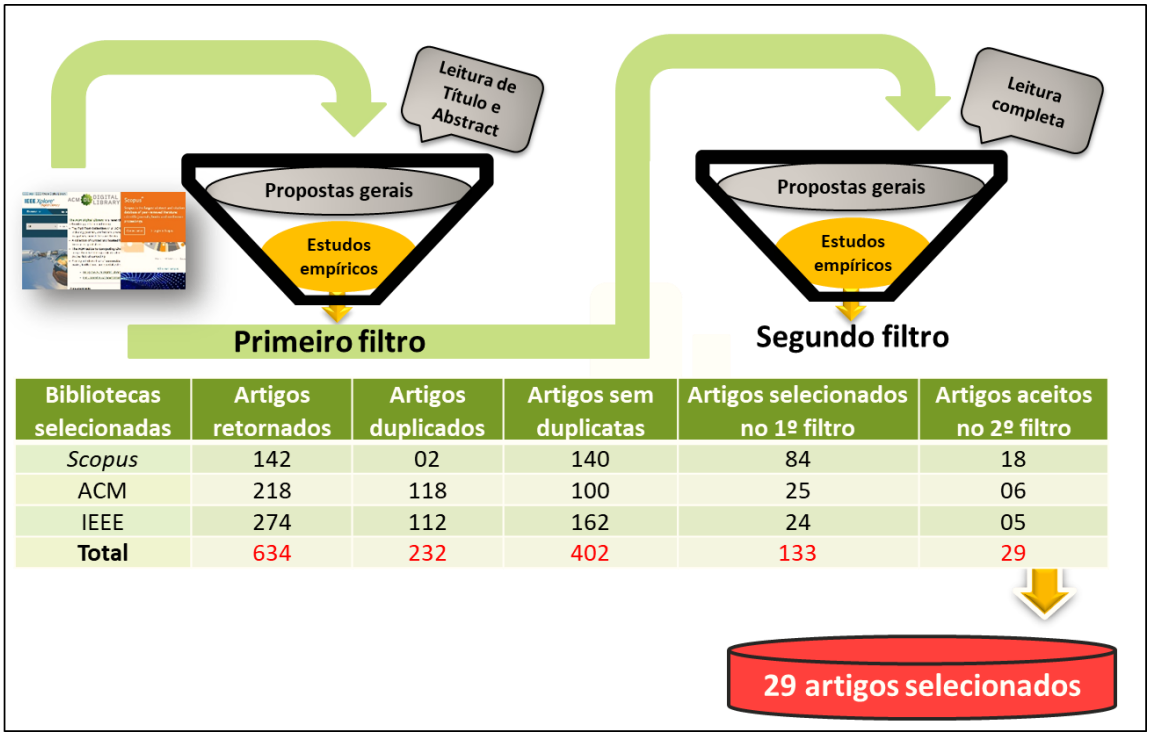
3.3 RESULTADOS DO MAPEAMENTO SISTEMÁTICO

A execução nas máquinas de busca ocorreu entre outubro de 2017 a janeiro de 2018. Conforme ilustrado na Figura 2, foram retornados 643 artigos inicialmente após a execução do primeiro filtro nas bases de dados. Entretanto, haviam repetições, ou seja, destas referências, apenas 402 eram distintas e foram contabilizadas como oficialmente retornadas nas bases de dados neste mapeamento. Destes 402 artigos, 133 foram pré-selecionados após a aplicação do primeiro filtro, com base nos critérios de inclusão definidos (ver subseção 3.2.4). Por fim, um total de 29 artigos foram selecionados após a execução do segundo filtro.

Com base nos resultados da pesquisa, observou-se que diversos artigos retornados neste mapeamento, que apresentam propostas de tecnologias de IHC para apoiar o projeto e avaliação de privacidade em RSOs, foram publicados em diferentes conferências e periódicos

não só relacionados com a área de IHC, mas também em diferentes comunidades, incluindo a área Rede de Computadores e Segurança da Informação.

Figura 2. Visão geral dos artigos retornados no MSL



Bibliotecas selecionadas	Artigos retornados	Artigos duplicados	Artigos sem duplicatas	Artigos selecionados no 1º filtro	Artigos aceitos no 2º filtro
Scopus	142	02	140	84	18
ACM	218	118	100	25	06
IEEE	274	112	162	24	05
Total	634	232	402	133	29

Fonte: Próprio autor.

A Tabela 10 lista os artigos selecionados neste mapeamento. Os artigos estão identificados com os códigos (A1, A2...) que representam a ordem de numeração dos mesmos. No final do título de cada artigo é apresentada a máquina de busca a qual o mesmo foi identificado.

Tabela 10. Artigos selecionados no Mapeamento Sistemático

Código	Referência	Título do artigo
[A1]	(TELES *et al.* 2017)	Situation-based privacy autonomous management for mobile social networks **[SCOPUS]**
[A2]	(WISNIEWSKI *et al.* 2017)	Making privacy personal: Profiling social network users to inform privacy education and nudging **[SCOPUS]**
[A3]	(LOPES *et al.* 2016)	Privacy Design Model Application on Sharing Pictures Apps **[SCOPUS]**
[A4]	(ALQARNI e SAMPALLI 2016)	Privacy-Enhancing of User's Behaviour Toward Privacy Settings in Social Networking Sites [**SCOPUS]**
[A5]	(COELHO e DUARTE 2016).	A literature survey on older adults' use of social network services and social applications. **[SCOPUS]**
[A6]	(VAN DER VALK *et al.* 2016)	Feeling Safe? Privacy controls and Online Disclosure Behavior **[SCOPUS]**
[A7]	(NAGARAJ e BRYANT 2016).	Factors in Building Transparent, Usable and Comprehensive User Privacy Policy System **[SCOPUS]**

Código	Referência	Título do artigo
[A8]	(MOUSAVIZADEH, e KIM 2015)	A study of the effect of privacy assurance mechanisms on self-disclosure in social networking sites from the view of protection motivation theory. **[SCOPUS]**
[A9]	(ZLATOLAS *et al.* 2015)	Privacy antecedents for SNS self-disclosure: The case of Facebook **[SCOPUS]**
[A10]	(ANTHONYSAMY *et al.* 2014)	A method for analysing traceability between privacy policies and privacy controls of online social networks **[SCOPUS]**
[A11]	(HEYMAN *et al.* 2014)	Evaluating social media privacy settings for personal and advertising purposes. *Info*, 16(4), 18-32. **[SCOPUS]**
[A12]	(KOOPS *et al.* 2013)	Open-source intelligence and privacy by design **[SCOPUS]**
[A13]	(MASOUMZADEH e JOSHI 2013).	Privacy settings in social networking systems: What you cannot control. **[SCOPUS]**
[A14]	(CHRISTIN *et al.* 2013)	Share with strangers: Privacy bubbles as user-centered privacy control for mobile content sharing applications **[SCOPUS]**
[A15]	(TIERNEY *et al.* 2013)	Cryptagram: Photo privacy for online social media **[SCOPUS]**
[A16]	(SHI *et al.* 2012)	See Friendship: Interpersonal Privacy Management in a Collective World. **[SCOPUS]**
[A17]	(ANTHONYSAMY *et al.* 2012)	Collaborative privacy management for third-party applications in online social networks **[SCOPUS]**
[A18]	(GURSES *et al.* 2008)	Privacy design in online social networks: Learning from privacy breaches and community feedback **[SCOPUS]**
[A19]	(FANG e LEFEVRE 2010)	Privacy wizards for social networking sites **[ACM]**
[A20]	(JAMIL 2017).	Using stratified privacy for personal reputation defense in online social networks **[ACM]**
[A21]	(UR e WANG 2013)	A cross-cultural framework for protecting user privacy in online social media **[ACM]**
[A22]	(SHEHAB *et al.* 2010)	Learning based access control in online social networks **[ACM]**
[A23]	(BESMER *et al.* 2009)	Social applications: exploring a more secure framework **[ACM]**
[A24]	(EMANUEL et al. 2013)	What does your profile really say about you?: privacy warning systems and self-disclosure in online social network spaces **[ACM]**
[A25]	(RAFIQ *et al.* 2017)	Learning to share: engineering adaptive decision-support for online social networks **[IEEE]**
[A26]	(YU *et al.* 2006).	A privacy assessment approach for serviced oriented architecture application **[IEEE]**
[A27]	(LICHTENSTEIN 2003)	Adding value to online privacy for consumers: Remedying deficiencies in online privacy policies with an holistic approach **[IEEE]**
[A28]	(KOST *et al.* 2011)	Privacy verification using ontologies **[IEEE]**
[A29]	(CHEN e RAHMAN 2008)	Analyzing privacy designs of mobile social networking applications **[IEEE].**

Fonte: Próprio autor.

Dos 29 artigos selecionados neste MSL, o trabalho de Coelho e Duarte (2010) apresenta um estudo secundário (revisão da literatura ou mapeamento sistemático ou revisão sistemática). Não foi realizada uma análise específica deste estudo secundário porque a intenção, nesse momento, não é executar uma revisão terciária. Portanto, considerou-se neste MSL apenas 28 artigos.

Com base na contagem das tecnologias identificadas e extraídas neste mapeamento, a **Erro! Fonte de referência não encontrada.** Tabela 11 apresenta numericamente os resultados gerais referentes a cada uma das respostas às subquestões de pesquisa investigadas.

Tabela 11. Resultados gerais para cada subquestão do MSL

Subquestão de Pesquisa	Possíveis Respostas	Resultados	
		Tecnologias	Porcentagem (%)
SQ1. Tipo de tecnologia	Projeto	16	57,14%
	Avaliação	11	39,29%
	Ambas	1	3,57%
SQ1.1 Tipo de avaliação da tecnologia	Investigação	11	91,67%
	Inspeção	0	0,00%
	Observação	1	8,33%
SQ3. Apoio ferramental	Sim	9	32,14%
	Não	19	67.86%
SQ4. Avaliação empírica	Sim	16	57,14%
	Não	12	42,86%
SQ4.1 Instrumento de coleta de dados	Entrevista	0	0,00%
	Questionário	11	68,75%
	Grupos de foco	0	0,00%
	Classificação de cartões	0	0,00%
	Estudo de campo	5	31,25%
	Registro de uso	0	0,00%
SQ4.2 Tipo de dados coletados	Qualitativos	3	18,75%
	Quantitativos	5	31,25%
	Ambos	8	50,00%
SQ4.3 Tipo de análise	Preditiva	2	12,50%
	Interpretativa	9	56,25%
	Experimental	5	31,25%
SQ4.4 Ambiente de avaliação	Academia	4	25,00%
	Laboratório com profissionais	4	25,00%
	Laboratório com usuários	8	50,00%
	Misto	0	0,00%
SQ5. Contexto da tecnologia	Específico	05	17,86%
	Genérico	23	82,14%

Fonte: Próprio autor.

Este MSL identificou 28 tecnologias que apoiam o projeto e avaliação de privacidade em RSOs. Pode-se observar que das 28 tecnologias identificadas, apenas uma direciona a sua proposta para auxiliar o projeto e avaliação. Nota-se também que a SQ2 (Tipo de contribuição) foi omitida da Tabela 11 devido às diversas respostas que a mesma contempla.

Ressalta-se ainda que a SQ1.1 é exclusiva para tecnologias de avaliação (12 tecnologias). Além disso, do total, os resultados indicam que 16 tecnologias foram avaliadas empiricamente. Com isso, a SQ4 e suas respectivas subquestões são específicas para a análise destas 16 tecnologias. Uma análise específica sobre tais artigos foi realizada e é apresentada de forma detalhada no Apêndice A. A seguir serão apresentadas as principais contribuições do mapeamento.

3.3.1 Características de privacidade consideradas pelas tecnologias existentes

Com base na análise das tecnologias identificadas a partir da realização deste mapeamento, observou-se que três principais características são sistematicamente enfatizadas quanto à estrutura de privacidade em uma RSO, a saber: o **nível** e o **controle** de privacidade, corroborando a teoria de Altman (1975) e a **política** de privacidade, a qual é um critério de qualidade que não é considerado no contexto da teoria do autor supracitado, mas foi uma característica identificada com base nas análises realizadas no mapeamento sistemático. A Tabela 12 apresenta os artigos identificados no mapeamento, indicando quais características tais fontes consideram como foco de trabalho.

Tabela 12. Características de privacidade consideradas pelas tecnologias existentes

Código do Artigo	Referência	Características de Privacidade		
		Níveis	**Controles**	**Políticas**
[A1]	(TELES *et al.* 2017)		X	
[A2]	(WISNIEWSKI *et al.* 2017)		X	
[A3]	(LOPES *et al.* 2016)	X		
[A4]	(ALQARNI e SAMPALLI 2016)		X	
[A6]	(VAN DER VALK *et al.* 2016)		X	
[A7]	(NAGARAJ e BRYANT 2016).			X
[A8]	(MOUSAVIZADEH, e KIM 2015)		X	
[A9]	(ZLATOLAS *et al.* 2015)		X	
[A10]	(ANTHONYSAMY *et al.* 2014)		X	X
[A11]	(HEYMAN *et al.* 2014)		X	
[A12]	(KOOPS *et al.* 2013)		X	X
[A13]	(MASOUMZADEH e JOSHI 2013).		X	X
[A14]	(CHRISTIN *et al.* 2013)		X	
[A15]	(TIERNEY *et al.* 2013)		X	
[A16]	(SHI *et al.* 2012)		X	
[A17]	(ANTHONYSAMY *et al.* 2012)		X	
[A18]	(GURSES *et al.* 2008)		X	
[A19]	(FANG e LEFEVRE 2010)		X	
[A20]	(JAMIL 2017).		X	
[A21]	(UR e WANG 2013)		X	
[A22]	(SHEHAB *et al.* 2010)		X	X
[A23]	(BESMER *et al.* 2009)		X	
[A24]	(EMANUEL et al. 2013)		X	

Código do Artigo	Referência	Características de Privacidade		
		Níveis	Controles	Políticas
[A25]	(RAFIQ *et al.* 2017)		X	
[A26]	(YU *et al.* 2006).			X
[A27]	(LICHTENSTEIN 2003)			X
[A28]	(KOST *et al.* 2011)		X	
[A29]	(CHEN e RAHMAN 2008)		X	

Fonte: Próprio autor.

3.3.2 Aspectos de privacidade considerados pelas tecnologias existentes

A Tabela 13 apresenta um resumo dos aspectos considerados pelo conjunto de tecnologias identificado a partir da execução do mapeamento. A coluna 1 apresenta o código do artigo o qual a tecnologia foi encontrada. A coluna 2 representa a categoria de privacidade a qual a tecnologia está inserida. A coluna 3 apresenta a principal contribuição dos artigos analisados, ou seja, a determinação do tipo de intervenção sendo estudada, que pode ser uma ferramenta, métodos, métricas, modelos, diretrizes, entre outros. A coluna 4 demonstra os aspectos considerados pelas tecnologias. Por fim, a coluna 5 denota se tipo de tecnologia apresentada é para projeto e/ou avaliação de privacidade em RSOs.

Tabela 13. Aspectos considerados pelas tecnologias identificadas no MSL

Código	Categoria	Tipo de contribuição	Aspectos de privacidade considerados	Tipo de tecnologia
[A1]	Controles	Mecanismo	Configurações de privacidade	Projeto
[A2]	Controles	Framework	Gerenciamento de privacidade	Projeto
[A3]	Níveis	Modelo	Compartilhamento de informações	Projeto e Avaliação
[A4]	Controles	Modelo	Configurações de privacidade	Avaliação
[A6]	Controles	Modelo	Comportamento das divulgações online	Avaliação
[A7]	Políticas	Framework	Transparência de dados	Projeto
[A8]	Controles	Modelo	Proteção de dados	Avaliação
[A9]	Controles	Método	Autopromoção e dinâmica de privacidade	Projeto
[A10]	Controles e Políticas	Método e Taxonomia	Gerenciamento de privacidade	Avaliação
[A11]	Controles	Abordagem	Autopromoção e divulgação a terceiros	Avaliação
[A12]	Controles e Políticas	Abordagem	Conformidade legal de privacidade	Projeto
[A13]	Controles e Políticas	Framework	Proteção de dados	Avaliação
[A14]	Controles	Abordagem	Gerenciamento de fotos e localização	Projeto
[A15]	Controles	Modelo	Gerenciamento de fotos	Projeto
[A16]	Controles	Heurísticas	Gerenciamento de privacidade	Projeto
[A17]	Controles	Framework	Gerenciamento de aplicativos de terceiros	Avaliação

Código	Categoria	Tipo de contribuição	Aspectos de privacidade considerados	Tipo de tecnologia
[A18]	Controles	Heurística	Violações de privacidade	Projeto
[A19]	Controles	Modelo	Configurações de privacidade	Projeto
[A20]	Controles	Modelo	Gerenciamento da reputação pessoal	Projeto
[A21]	Controles	Framework	Questões legais, culturais e pessoais de privacidade	Avaliação
[A22]	Controles e Políticas	Abordagem	Controle de acesso	Projeto
[A23]	Controles	Modelo	Gerenciamento de aplicativos de terceiros	Projeto
[A24]	Controles	Modelo	Feedback de privacidade	Avaliação
[A25]	Controles	Arquitetura	Monitoramento de privacidade	Projeto
[A26]	Políticas	Abordagem	Conformidade de privacidade	Avaliação
[A27]	Políticas	Framework	Risco de privacidade	Projeto
[A28]	Controles	Ontologia	Controle de acesso	Projeto
[A29]	Controles	Framework	Feedback de privacidade	Avaliação

Fonte: Próprio autor.

A partir das propostas identificadas com base na realização deste mapeamento, observou-se que todas as tecnologias focam em aspectos específicos de privacidade, como o controle de acesso e gerenciamento de informações pessoais por exemplo. No entanto, estas tecnologias não focam em aspectos gerais, ou seja, questões amplas de privacidade que podem ser consideradas em projetos e/ou avaliações de RSOs.

Em relação as contribuições identificadas nos artigos, ressalta-se que todos as propostas foram classificadas de acordo com as nomenclaturas dadas pelos próprios autores dos artigos. Desta forma, nota-se que a maioria das tecnologias propostas são modelos. Outras tecnologias empregam o uso de frameworks em sua proposta. Por exemplo, Anthonysamy *et al*. (2012) propuseram o *Collaborative Privacy Management* (CPM), um framework que torna explícito para o usuário todas as informações e dados que podem ser acessados por aplicativos de terceiros (*Third Party Applications - TPAs*) dentro das RSOs. Com isso, os resultados indicam que a maioria das contribuições identificadas nos artigos deste MSL são modelos e frameworks.

3.4 DISCUSSÃO DOS RESULTADOS

Este mapeamento sistemático teve como objetivo central investigar quais tecnologias para projeto e avaliação de privacidade, em RSOs, são relatadas pela literatura científica. Os resultados obtidos revelaram que existem diversos estudos propondo tecnologias aplicadas para apoiar o design de avaliação de RSOs, com foco na privacidade do usuário. No entanto,

ainda existem algumas lacunas não cobertas pelas tecnologias existentes, o que pode ser relevante para a introdução de novas tecnologias. As principais lacunas identificadas indicam que:

- Muitas das tecnologias já existentes foram desenvolvidas para tratar questões específicas de privacidade. No entanto, tais tecnologias não possuem um foco abrangente para considerar questões gerais de privacidade e, sobretudo, não se propõem a detectar problemas reais de privacidade que possam comprometer a interação do usuário com uma determinada RSO.
- Quando se trata do tipo de contribuição mais utilizado, nota-se que há uma tendência de pesquisadores em proporem modelos e frameworks. No entanto, com base nas análises efetuadas, observou-se que muitas das tecnologias identificadas necessitam de treinamentos com especialistas para serem executadas, consequentemente aumentando o potencial de esforço e custo de aplicação. Nesse sentido, outras abordagens podem ser propostas, de modo que a aplicação destas seja focalizada em um baixo custo, rapidez e facilidade de uso.
- Em relação as tecnologias de avaliação, observa-se que a maioria utiliza a observação ou a investigação como instrumentos de avaliação. Todavia, nenhuma tecnologia propôs utilizar a inspeção como forma de avaliação. Nesse sentido, torna-se importante propor tecnologias de avaliação por inspeção, uma vez que a inspeção pode promover a melhoria da qualidade de privacidade através da identificação de problemas que possam comprometer a privacidade do usuário em uma determinada aplicação.
- Em relação as características de privacidade, nota-se que a maioria das tecnologias direcionam o foco em controles ou políticas de privacidade, sendo que apenas uma tecnologia focaliza em níveis de privacidade. Desta forma, torna-se relevante propor tecnologias que consideram as três características identificadas com base no mapeamento, uma vez que estas denotam que toda a estrutura de privacidade de uma RSO está ancorada a níveis, controles e políticas de privacidade.

A partir das análises realizadas neste mapeamento sistemático, novas ideias surgiram sobre os principais pontos mão cobertos pelas tecnologias atuais, fornecendo indícios para a concepção de novas tecnologias. Uma das principais contribuições do mapeamento foi a identificação das categorias de privacidade que, além de nortear como um sistema de rede social é estruturado em relação à privacidade, formaram a base para a proposta do conjunto de

técnicas proposto neste trabalho, conforme demonstrado no Capítulo 4. A seguir serão apresentados outros trabalhos relacionados identificados com base na revisão da literatura.

3.5 TRABALHOS RELACIONADOS

Nem todas as tecnologias atualmente propostas para o projeto e avaliação de privacidade em RSOs puderam ser coletadas pelo mapeamento sistemático realizado. Há propostas bem divulgadas no ambiente acadêmico, sobre as quais a pesquisa não coletou nenhum artigo devido à limitação em algumas fontes de pesquisa. Por exemplo, alguns artigos relevantes estão disponíveis no repositório da ACM, mas não foram retornados no mapeamento provavelmente por algum problema na execução das strings ou no próprio mecanismo de busca da biblioteca. Por esta razão, também foram incluídos outros trabalhos relacionados que não foram identificados especificamente com base no MSL. Como as técnicas propostas nesta dissertação são tecnologias de avaliação, buscamos apresentar trabalhos que realizaram avaliações de privacidade e que estão diretamente relacionados com esta pesquisa.

Kimura *et al.* (2012) realizaram uma avaliação de usabilidade das funcionalidades assíncronas de privacidade do Facebook. Para atingir esta finalidade, os autores utilizaram a avaliação heurística de Nielsen (1994) e todo o processo de inspeção indicado pelo método, evidenciando os principais problemas referentes às funcionalidades de privacidade da aplicação. Um conjunto de especialistas examinaram o sistema e fizeram um diagnóstico dos problemas de usabilidade e das barreiras que os usuários provavelmente encontrariam durante a interação com as configurações de privacidade da rede social usada como objeto de inspeção. A pesquisa mostrou a importância em se realizar uma avaliação por inspeção e identificar possíveis problemas que podem criar barreiras aos usuários na utilização das configurações de privacidade de um sistema de RSOs.

Nesta mesma visão, Rodrigues *et al*. (2012) aplicaram um conjunto de 08 métodos e instrumentos de avaliação empíricos e analíticos para avaliar aspectos de privacidade sob a ótica da usabilidade, acessibilidade e de respostas emocionais dos usuários. Os resultados da aplicação desses instrumentos forneceram indícios de que os usuários enfrentavam problemas de usabilidade e acessibilidade na realização de tarefas relacionadas à privacidade na rede social investigada. Tal questão produzia um impacto direto sobre as respostas emocionais acerca da interação. Além disso, a pesquisa mostrou que a rede social avaliada fornecia proteção inadequada quanto aos aspectos de privacidade avaliados no sistema.

Com o propósito de identificar falhas de comunicabilidade sobre as Configurações de Privacidade de uma rede social alvo, Carvalho *et al.* (2012) aplicaram o Método de Inspeção Semiótica (MIS) e o Método de Avaliação de Comunicabilidade (MAC) propostos pela Engenharia Semiótica (DE SOUZA, 2005) para proceder esta avaliação. Tanto a inspeção executada pelo MIS, quanto a avaliação realizada através do MAC foram bastante eficazes em demonstrar falhas de comunicabilidade nas questões de privacidade do Facebook. A partir da aplicação dos métodos, os autores identificaram diversos problemas relacionados às atividades de privacidade. A inspeção procedida através do MIS demonstrou que seria necessária uma reformulação de alguns pontos importantes das configurações de privacidade para manter a correspondência entre a metalinguagem e os sinais estáticos e dinâmicos existentes no sistema.

Gürses *et al.* (2008) propuseram heurísticas de privacidade direcionadas para domínios específicos de RSOs, com foco no design de privacidade destas aplicações. Desta forma, os autores desenvolveram um framework conceitual que abrange diretrizes relevantes para serem usadas de forma sistemática durante a engenharia de controles de privacidade em uma aplicação de rede social. A proposta é baseada em características extraídas de trabalhos já existentes na literatura e feedbacks online sobre violações de privacidade. O framework é estruturado por meio de categorias interdependentes que destacam diferentes aspectos de privacidade que podem impactar em violações e representar um risco para a privacidade do usuário. Tais heurísticas podem ser utilizadas em tempo de design servindo como um aporte para auxiliar projetistas e desenvolvedores a refletirem sobre aspectos específicos de privacidade.

Anthonysamy *et al.* (2014) desenvolveram uma proposta para avaliar o grau de rastreabilidade entre políticas e controles de privacidade de uma RSO. Os autores destacam que com a complexidade das políticas de privacidade e a variedade de controles de privacidade, torna-se difícil avaliar se tais controles disponibilizados operam adequadamente conforma descritos nas políticas. Desta forma, o artigo apresenta, primeiramente, uma taxonomia para classificar o grau de conformidade de uma política de privacidade de RSOs. E, posteriormente, um método que fornece através de uma escala, o nível de confiança sobre a relação entre políticas e controles, estabelecendo assim o que os autores chamam de grau de rastreabilidade entre esses dois aspectos.

Com base nestes trabalhos relacionados apresentados acima, nota-se que vários autores buscaram abranger questões específicas de privacidade no contexto de RSOs. No plano técnico e conceitual, as propostas apresentadas por Gürses *et al.* (2008) e Anthonysamy *et al.* (2014) abrangem soluções alternativas para tratar questões de privacidade nestas aplicações, de modo a auxiliar projetistas e desenvolvedores de RSOs a refletirem sobre diferentes pontos que impactam a natureza contextual de privacidade do usuário nestas aplicações e, além disso, sobre o tipo de conhecimento a ser obtido com a base na proposta metodológica apresentada por estes autores referenciados.

Em uma perspectiva analítica, observa-se que alguns autores buscaram utilizar métodos de avaliação investigando atividades ou funcionalidades referentes a privacidade em RSOs, porém, com foco geral em avaliar critérios de qualidade relacionados a usabilidade, acessibilidade e comunicabilidade. Ainda que estes trabalhos destaquem o aspecto de privacidade como objetivo central de suas avaliações, os métodos usados como instrumentos de avaliação destinam a sua proposta a outros critérios de qualidade. Com isso, percebe-se que há uma carência de técnicas de avaliação, principalmente, no que diz respeito a técnicas de avaliação de privacidade através de inspeção, que possuem um foco abrangente para tratar questões amplas de privacidade e detectar possíveis problemas que possam comprometer as interações e experiência do usuário com o cenário de privacidade fornecido pelas RSOs.

3.6 CONSIDERAÇÕES SOBRE O CAPÍTULO

Os principais resultados apontam que há um maior número de tecnologias direcionadas para apoiar o design de privacidade, do que a avaliação de privacidade em RSOs. Com a aplicação de tecnologias de projeto e/ou avaliação, a privacidade pode ser considerada como critério de qualidade de uso em um sistema, buscando evidências que indiquem se as metas de design de privacidade foram alcançadas, ou seja, se a RSO possui os níveis de qualidade de uso desejados quanto à privacidade. Além disso, este MSL revelou indícios sobre lacunas de pesquisas que podem ser supridas por profissionais e pesquisadores de IHC, tais como: (a) criação de novas tecnologias que apoiem ambos estágios, ou seja, tecnologias que apoiem tanto o projeto como a avaliação de privacidade podem fornecer mais base e direcionamento para o design e avaliação de RSOs; e (b) a criação de tecnologias de avaliação por meio de inspeção.

Nesse contexto, os resultados deste MSL apresentam influências relevantes para os pesquisadores que estão planejando propor novas tecnologias de projeto e/ou avaliação de privacidade em RSOs ou que estão dispostos a realizar novos estudos com as tecnologias

identificadas; e para os profissionais que trabalham na proteção e melhoria da privacidade de informações e dados pessoais do usuário em RSOs e gostariam de integrar tecnologias de privacidade em seus processos de trabalho de forma eficaz. Para os pesquisadores seria relevante propor novas tecnologias com base nas lacunas mencionadas neste MSL, pois há uma necessidade de conceber tecnologias de avaliação por meio de inspeção. Para os profissionais, torna-se importante conhecer em que etapas do ciclo de construção de redes sociais online, as tecnologias poderiam ser melhor empregadas.

Por fim, o capítulo mostrou os principais trabalhos de avaliação relacionados com esta pesquisa, onde foi possível observar uma limitação de técnicas de avaliação, principalmente, no que diz respeito a técnicas de avaliação por inspeção. Após a realização destas análises, o próximo capítulo apresenta a proposta do conjunto de técnicas desenvolvido neste trabalho.

CAPÍTULO 4 – PROPOSTA DO CONJUNTO DE TÉCNICAS PIT-OSN

Este capítulo apresenta a proposta do conjunto de tecnologias que apoiam a inspeção de privacidade em RSOs. Este conjunto de tecnologias objetiva melhorar a qualidade de privacidade das aplicações com esforço reduzido.

4.1 INTRODUÇÃO

As contribuições identificadas nos trabalhos relacionados presentes na literatura e no mapeamento sistemático executado neste trabalho não exploram as possibilidades de outros recursos, como a inspeção, que podem ser aplicados durante a avaliação de privacidade de uma RSO. Através das análises realizadas com base no aporte teórico desta pesquisa, identificou-se a oportunidade do desenvolvimento de um conjunto de técnicas de inspeção orientado a avaliação de privacidade no contexto de RSOs.

Nesse sentido, este conjunto de técnicas de inspeção é apoiado por um conjunto de recursos que podem ser empregados pelos próprios profissionais envolvidos no projeto e avaliação de RSOs. Para atingir esta finalidade, o conjunto de técnicas proposto deve atender os seguintes requisitos: ser fácil de aprender e utilizar; apresentar um bom nível de eficiência e eficácia; além de proporcionar uma boa relação custo-benefício em sua aplicação. Com isso, almeja-se também que o conjunto de técnicas de inspeção seja:

1. Independente de ferramenta: não se limita a disponibilidade de um apoio ferramental, além de ser distribuído de forma gratuita;
2. Independente do estágio do desenvolvimento: não se limita especificamente a um determinado estágio, podendo também ser aplicada em tempo de design, pois é necessário realizar avaliações de IHC durante diferentes estágios do ciclo de desenvolvimento (BLOMKVIST, 2005);
3. Abrangente: não se limita a uma determinada rede social ou tipo de ambiente;
4. Usado por profissionais com pouco conhecimento em avaliação de privacidade: auxilia profissionais novatos a aprenderem sobre inspeção de privacidade, ou seja, profissionais não especialistas em avaliação de interfaces.

4.2 CONJUNTO DE TÉCNICAS PIT-OSN

A PIT-OSN (*Privacy Inspection Technique for Online Social Network)* é um conjunto de técnicas de inspeção, baseado em leitura, destinado a apoiar o processo de inspeção de privacidade em interfaces de redes sociais online. Por serem técnicas de leitura as mesmas ajudam a melhorar o desempenho do processo de inspeção no que se refere à atividade de detecção de defeitos.

Para direcionar a elaboração da proposta do conjunto de técnicas de inspeção, buscou-se coletar evidências de propostas já existentes identificadas a partir da execução de um mapeamento sistemático, realizado neste trabalho, e de outras abordagens já existentes na literatura. Esta análise permitiu identificar quais características de privacidade tais propostas focalizavam.

Conforme já apresentado nos resultados do mapeamento, observou-se que três principais características eram sistematicamente enfatizadas quanto à estrutura de privacidade em uma RSO: níveis, controles e políticas de privacidade, as quais denominamos de categorias de privacidade para o contexto deste trabalho. Considerando estas categorias enunciadas, o conjunto de técnicas proposto nesta dissertação direciona o foco de sua inspeção nestas três diferentes categorias:

(1) **Níveis de Privacidade** – que representam o comportamento da rede social em relação à adequação, distribuição das informações e publicações do usuário relacionadas à privacidade;

(2) **Controles de Privacidade** – que representam o que a rede social disponibiliza em termos de opções, recursos e ferramentas que auxiliam o usuário a controlar a sua privacidade;

(3) **Políticas de Privacidade** – que representam os termos e condições de uso para garantir a privacidade das informações do usuário.

O conjunto de técnicas proposto possui itens de verificação agrupados em dimensões de privacidade. Estes itens foram elaborados com base no conhecimento adquirido na literatura e da identificação, na prática, de diversos problemas de privacidade relacionados as dimensões referidas. Os itens são empregados como um guia para interpretar as dimensões das técnicas, ajudando os inspetores a refletirem sobre a situação discrepante do sistema, de modo a diagnosticarem os problemas de privacidade. A Figura 3 apresenta uma ilustração desta abordagem e suas categorias para inspeção de privacidade.

Figura 3. Visão geral do Conjunto de Técnicas PIT-OSN

Fonte: Próprio autor.

Para a realização da inspeção de privacidade com o apoio do conjunto de técnicas propostas, sugere-se contar com a participação de no mínimo dois avaliadores, pois, segundo Rocha e Baranauskas (2003), uma única pessoa nunca é capaz de encontrar todos os possíveis problemas existentes em um avaliação de interface. Nas próximas seções, cada técnica de inspeção será apresentada em detalhes.

4.2.1 Técnica PIT-OSN 1

A técnica PIT-OSN 1 direciona a sua inspeção para os **níveis de privacidade** de uma RSO. O nível de privacidade refere-se ao compartilhamento de informações. Com isso, um determinado indivíduo pode aumentar ou diminuir os seus limites de acesso para alcançar o seu nível desejado de privacidade em relação a um determinado compartilhamento de informação. Isto indica que pode haver um ponto contínuo de níveis de privacidade que podem ser alcançados pelo indivíduo, variando desde de um nível de privacidade baixo (mínimo), no qual todas as informações ficam acessíveis para uma ampla audiência compartilhar, ou até o nível de privacidade alto, onde nenhuma informação é compartilhada pelo indivíduo (ALTMAN, 1975; VILLELA, 2016).

Nesse contexto, ao utilizar esta técnica, os avaliadores têm a oportunidade de detectar problemas de privacidade quanto ao comportamento da aplicação em relação à adequação e disseminação das informações e publicações pessoais do usuário, a partir de um espectro que varia desde um ponto total de abertura até um ponto total de fechamento dado por um indivíduo a outras pessoas para o compartilhamento de informações. Com base nas dimensões apresentadas pelo MDP (VILLELA e PRATES, 2015), que foca amplamente na questão dos níveis em RSO, foram originados os itens de verificação que são empregados como um guia para interpretar as dimensões e diagnosticar possíveis defeitos nos níveis de privacidade fornecidos ao usuário pelo sistema. A Tabela 14 apresenta uma descrição das dimensões utilizadas na concepção da técnica.

Tabela 14. Dimensões da técnica PIT-OSN 1.

Nº	Dimensão	Explicação	Referência base
1	**Fonte de informação**	refere-se a quem é o responsável pelo compartilhamento de informações sobre o indivíduo dentro do sistema, ou seja, quem pode determinar como, quando e em que extensão tal informação será compartilhada.	Villela e Prates (2015)
2	**Espaço de comunicação**	refere-se ao local onde a informação sobre o indivíduo será compartilhada no sistema, relacionado à autonomia, concedida ou não ao indivíduo, para controlar o acesso ao espaço onde ocorre o compartilhamento de informações	
3	**Domínio, expressão e conteúdo dos dados**	refere-se ao tipo de informação sobre o indivíduo que será compartilhada no sistema, levando em consideração a forma como tal informação é expressa e o nível de pessoalidade que a mesma possui.	
4	**Persistência temporal**	refere-se ao tempo em que um conteúdo publicado fica disponibilizado à sua audiência, dentro do sistema. Assim, quanto mais tempo o conteúdo fica disponível, maior a chance dele ser acessado dentro do sistema, levando a um menor nível de privacidade.	
5	**Audiência**	refere-se à quantidade de pessoas que vão ter acesso a um conteúdo compartilhado. Assim, quanto mais ampla (e desconhecida) é a audiência, menor o nível de privacidade.	
6	**Notificação**	refere-se ao sistema informar adequadamente ao indivíduo quando alguma informação sobre ele é divulgada ou acessada por outros usuários e de que forma. Assim, quanto mais o usuário é notificado, maior é a chance dele ser mais restritivo em relação às informações que ele compartilha ou com suas configurações de privacidade.	

Nº	Dimensão	Explicação	Referência base
7	**Discurso do sistema**	refere-se ao compartilhamento que o sistema faz de informações sobre o indivíduo. Assim, quanto mais amplo tal compartilhamento, no que tange ao escopo dos conteúdos compartilhados, menor é o nível de privacidade	Villela e Prates (2015)
8	**Disseminação da informação**	refere-se ao controle que o indivíduo tem sobre a sua informação, em relação ao momento em que ela foi inicialmente compartilhada. Assim, quanto menor for tal controle, menor é o nível de privacidade.	

Fonte: Próprio autor.

A partir das definições das dimensões foram criados os itens que apontam o que deve ser verificado em cada dimensão da técnica proposta. Ao avaliar a privacidade sob a perspectiva dos *níveis*, o inspetor deve se preocupar com a possibilidade de um determinado indivíduo aumentar ou diminuir os seus limites de acesso através dos níveis de privacidade concedidos pela RSO ao usuário. Portanto, a "pergunta-chave" para nortear a categoria em foco é: "*O usuário consegue atingir o seu nível desejado de privacidade?"*. Na Tabela 15 são listadas as dimensões e seus respectivos itens de verificação da PIT-OSN 1 (versão 1).

Tabela 15. Extrato da PIT-OSN 1 (versão 1)

Dimensões e itens de verificação da PIT-OSN 1	
1A. Fonte de Informação	
1A1	Verifique se outro usuário (um amigo ou seguidor) tem autonomia para compartilhar conteúdos publicados por um determinado indivíduo dentro do sistema.
1A2	Verifique se outras fontes, como aplicativos ou sites de terceiros, têm autonomia para compartilhar informações de um determinado usuário
1B. Espaço de Comunicação	
1B1	Verifique se um conteúdo publicado por um determinado usuário pode ser compartilhado em um outro espaço de publicação sem a sua permissão.
1B2	Verifique se um conteúdo publicado por um determinado indivíduo pode ser acessado através de um espaço público (como em mecanismos de busca por exemplo) fora do sistema.
1C. Domínio, Expressão e Conteúdo dos dados	
1C1	Verifique se a rede social coleta dados cujo significado é definido pelo sistema, mas o valor é definido pelo usuário (como nome ou data de nascimento por exemplo).
1C2	Verifique se a rede social coleta e compartilha dados pessoais como habilidade profissional, atividade física, biometria, localização, fotos, músicas, culinária, entre outros.
1D. Persistência temporal	
1D1	Verifique se a rede social permite que um determinado conteúdo publicado no sistema fique sempre acessível para a sua audiência, não dando a possibilidade para o usuário compartilhar conteúdos curtos, que desapareçam depois de um determinado período de tempo.

Dimensões e itens de verificação da PIT-OSN 1	
1D. Persistência temporal	
1D2	Verifique se a rede social permite ao usuário que, ao aceitar a solicitação de um determinado indivíduo, este tenha acesso apenas as informações que forem compartilhadas a partir do momento em que tal usuário começou a fazer parte da audiência (tempo presente) e não tenha acesso as publicações antigas (tempo passado).
1E. Audiência	
1E1	Verifique se a rede social permite fazer publicações que ficam visíveis somente para o próprio usuário.
1E2	Verifique se a rede social permite compartilhar conteúdos, seletivamente, com pessoas específicas.
1E3	Verifique se rede social permite que uma audiência desconhecida (como amigos de amigos) possa visualizar determinadas ações do indivíduo no sistema, como o que o usuário curtiu ou comentou por exemplo.
1F. Notificação	
1F1	Verifique se a rede social notifica o indivíduo apenas sobre uma parte das interações de outros usuários com sua publicação.
1F2	Verifique se rede social não fornece ao indivíduo nenhuma informação sobre as interações de outros usuários com sua informação que é compartilhada no sistema.
1G. Discurso do sistema sobre o indivíduo	
1G1	Verifique se a rede social toma a iniciativa de gerar novos conteúdos sobre o usuário sem a sua permissão, com base no processamento de uma ou mais informações pessoais já compartilhadas (retrospectivas e scores, por exemplo).
1G2	Verifique se a rede social toma a iniciativa de recomendar o perfil do indivíduo para outros usuários sem a sua permissão (sugestões de amizade ou de seguir, por exemplo).
1H. Disseminação da Informação	
1H1	Verifique se a rede social permite à audiência (re)compartilhar ou (re)postar com outras pessoas uma publicação de um determinado usuário sem a sua permissão.
1H2	Verifique se a rede social permite que uma determinada Informação sobre o usuário seja compartilhada por sua audiência sem a sua permissão, porém de uma maneira restrita, apenas para uma audiência adicional limitada (amigos em comum, por exemplo).
1H3	Verifique se a rede social permite que uma informação sobre um determinado usuário seja compartilhada pela sua audiência sem nenhuma restrição

Fonte: Próprio autor.

4.2.2 Técnica PIT-OSN 2

A PIT-OSN 2, por sua vez, destina o foco da inspeção para os **controles de privacidade** disponibilizados pelas RSOs. O controle de privacidade está associado ao processo de regulação de limites de acesso tal como abordado na teoria de privacidade de Altman (1975). Um ponto importante a ser ressaltado é que os controles fornecidos pelas aplicações geralmente estão elencados através de informações ou representados através de elementos que indicam como funcionam estes determinados controles de privacidade.

Nesta direção, a técnica auxilia os inspetores a encontrarem possíveis problemas nas opções, recursos ou ferramentas de privacidade fornecidos pelo sistema, que podem não ter sido bem definidos ou representados, através da interface, ocasionando defeitos de

privacidade. Através de recomendações e indicadores técnicos identificados através da literatura, foram definidas as dimensões e os itens de verificação que guiam o inspetor a detectar prováveis problemas nos controles do sistema. Destaca-se que, diferente da PIT-OSN 1, as dimensões da técnica PIT-OSN 2 não tinham uma nomenclatura formada. Desta forma, o nome destas bem como as definições foram adaptadas a partir da visão do autor deste trabalho. Uma explanação sobre as dimensões da técnica PIT-OSN 2 é descrita na Tabela 16.

Tabela 16. Dimensões da técnica PIT-OSN 2 e referências base

Nº	Dimensão	Explicação	Referências base
1	**Direito de privacidade**	diz respeito ao sistema disponibilizar a opção de denunciar um perfil ou conteúdo impróprio tais como nudez, contas *fakes* ou violações de propriedade intelectual, por exemplo.	Yamauchi *et al.* (2016)
2	**Usabilidade e privacidade**	diz respeito ao sistema empregar, nas opções de privacidade, a facilidade necessária para os usuários aprenderem a manipular com eficiência e satisfação os controles de privacidade disponibilizados pelo sistema.	Nagaraj e Bry (2016) Ur e Wang (2013)
3	**Transparência de dados**	diz respeito ao sistema disponibilizar ao usuário a opção de acessar ou rever todo o seu histórico de publicações e interações na aplicação.	Gurses *et al.* (2008) Shi *et al.* (2012)
4	**Aplicativos de terceiros**	diz respeito ao sistema fornecer ao usuário a opção de tornar os dados informados mais protegidos, permitindo excluir aplicativos, mudar a privacidade destas aplicações e evitar ter suas informações compartilhadas em sites de terceiros.	Wisniewski *et al.* (2017) Anthonysamy *et al.* (2012)
5	**Solicitações de amizade**	diz respeito ao sistema prover mecanismos que permitam ao usuário controlar toda a propriedade relacionada à pedidos de amizade ou de seguidores.	Wisniewski *et al.* (2017)
6	**Bloqueio**	diz respeito ao sistema apresentar opções que permitam ao usuário impedir todas as comunicações ou interações de pessoas ou aplicativos inconvenientes por exemplo	Rodrigues *et al.* (2016) Wisniewski *et al.* (2017)
7	**Privacidade na busca**	diz respeito ao sistema fornecer ao usuário a opção de restringir ou impedir que outras fontes de informação encontrem seu perfil sem a sua permissão	Rodrigues *et al.* (2016
8	**Negociação de privacidade**	diz respeito ao sistema dispor de um controle de reputação, que permite ao usuário retirar ou solicitar a remoção de publicações indesejadas em seu nome.	Gurses *et al.* (2008) Wisniewski *et al.* (2017)
9	**Separação interna de identidades**	diz respeito ao sistema fornecer ao usuário a opção de fazer publicações de forma seletiva, através de listas personalizadas para a audiência.	Gurses *et al.* (2008) Wisniewski *et al.* (2017)
10	**Gerenciamento de informações do perfil**	diz respeito ao sistema disponibilizar ao usuário a opção de controlar ou limitar os dados pessoais fornecidos no perfil.	Wisniewski *et al.* (2017)

Nº	Dimensão	Explicação	Referências base
11	**Confidencialidade**	diz respeito ao sistema dispor de recursos que possibilitem ao usuário ocultar ou arquivar publicações compartilhadas na aplicação, sem que esta seja apagada definitivamente, ficando acessível para o usuário de forma privada.	Gurses *et al.* (2008) Shi *et al.* (2012) Wisniewski *et al.* (2017)
12	**Curtidas ou comentários**	diz respeito ao sistema disponibilizar ao usuário a opção de controlar quem pode curtir ou comentar suas publicações ou mesmo restringir comentários impróprios em publicações.	Rodrigues *et al.* (2016)
13	**Controle de localização**	diz respeito ao sistema fornecer ao usuário a opção de controlar os serviços de localização ou evitar que a aplicação utilize a sua localidade sem a permissão concedida.	Christin *et al.* (2013) Rodrigues *et al.* (2016)
14	**Legado digital pós-morte**	a privacidade pode ser violada também após o falecimento de dado usuário, uma vez que seu perfil pode ficar ativo nas redes sociais e ser usado indevidamente. Desta forma, as redes sociais devem disponibilizar funcionalidades para pré-configurar aspectos volitivos. Algumas RSOs já disponibilizam alguns controles como a designação de um herdeiro, transformando a conta em um memorial digital, ou a exclusão da conta. Assim, nesta dimensão, são propostos itens de verificação para que, antecipadamente, o usuário possa tomar tais decisões que terão efeitos futuros.	Maciel e Pereira (2013) Pereira e Prates (2017)

Fonte: Próprio autor.

Com base nestas definições, foram originados os itens que indicam o que deve ser verificado em cada dimensão no diz respeito ao foco geral desta categoria. Ao avaliar a privacidade sob a perspectiva dos *controles*, o inspetor deve checar se um determinado indivíduo teria a possibilidade de regular adequadamente os seus limites de acesso através das opções, recursos ou ferramentas de privacidade fornecidos pela RSO. Portanto, a "pergunta-chave" para nortear esta categoria é: "*O usuário consegue ter um controle adequado sobre a sua privacidade?"*. Na Tabela 17 são listadas as dimensões e os respectivos itens de verificação da PIT-OSN 2.

Tabela 17. Extrato da PIT-OSN 2

Dimensões e itens de verificação da PIT-OSN 2	
2A. Direito de Privacidade	
2A1	Verifique se rede social permite ao usuário solicitar a remoção de uma informação, imagem ou vídeo que viola os seus direitos de privacidade.
2A2	Verifique se há uma opção que permite denunciar uma conta que está se passando por um usuário (conta *fake*).
2A3	Verifique se a rede social permite denunciar uma publicação de conteúdos que violem os direitos de propriedade intelectual do usuário, como direitos autorais e de marca comercial.

2B. Usabilidade e Privacidade	
2B1	Verifique se há atalhos de privacidade que forneçam acesso rápido a algumas das configurações e ferramentas de privacidade mais relevantes da rede social.
2B2	Verifique se o usuário tem a opção de um mecanismo de ajuda que facilite a localização de um determinado controle de privacidade.
2B3	Verifique se em algum controle de privacidade aparecem informações escritas em um idioma diferente do utilizado eventualmente pelo usuário
2C. Transparência de dados	
2C1	Verifique se há uma opção que permite ao usuário solicitar acesso aos dados pessoais armazenados na rede social.
2C2	Verifique se o usuário tem a opção de acessar um registro ou histórico de atividades realizados na rede social.
2D. Aplicativos de terceiros	
2D1	Verifique se a rede social permite ao usuário visualizar os aplicativos ou sites de terceiros ativos em sua conta.
2D2	Verifique se o usuário tem a opção de editar ou atualizar as informações que os aplicativos ou sites de terceiros podem ter acesso na sua conta.
2D3	Verifique se a rede social permite ao usuário remover os aplicativos ou sites de terceiros que não desejam mais ter acesso ou utilizar.
2D4	Verifique se a rede social permite ao usuário denunciar um aplicativo ou site de terceiros
2E. Solicitações de amizade	
2E1	Verifique se a rede social permite editar quem pode seguir ou enviar solicitação de amizade para um determinado usuário.
2E2	Verifique se há uma opção para cancelar uma amizade ou remover um amigo ou seguidor da rede social.
2E3	Verifique se a rede social permite que uma solicitação de amizade fique com status pendente caso o usuário opte por não aceitar imediatamente.
2F. Bloqueio	
2F1	Verifique se o usuário tem a opção de bloquear uma pessoa que está na rede social.
2F2	Verifique se o usuário tem a opção de desbloquear um indivíduo.
2G. Privacidade na busca	
2G1	Verifique se há uma opção que restringe a indexação pública do perfil do usuário por outros mecanismos de busca fora da rede social.
2G2	Verifique se a rede social permite restringir quem pode procurar pelo usuário usando informações pessoais do contato, como o endereço de e-mail ou o número de telefone.
2H. Negociação de Privacidade	
2H1	Verifique se a rede social permite ocultar ou remover uma marcação de uma publicação ao qual o usuário foi marcado.
2H2	Verifique se o usuário tem a opção de solicitar para uma determinada pessoa que o marcou ou o mencionou em uma publicação indesejada, que remova o post.
2H3	Verifique se o usuário tem a opção de analisar marcações que as pessoas adicionam às suas publicações antes de serem exibidas no perfil do indivíduo na rede social.
2I. Separação interna de identidades	
2I1	Verifique se a rede social permite ao usuário definir direitos de visibilidade (como o uso de seletor de público por exemplo) para uma determinada publicação.
2I2	Verifique se a rede social permite ao usuário criar listas de amigos personalizadas para que o indivíduo possa compartilhar as postagens em grupos específicos de amigos.
2I3	Verifique se o usuário tem a opção de selecionar quem pode visualizar a sua lista de amigos ou seguidores na rede social.

2J. Gerenciamento de informações do perfil	
2J1	Verifique se a rede social permite ao usuário controlar quem pode visualizar informações biográficas ou informações de contato em seu perfil.
2J2	Verifique se o usuário tem a opção de alterar o seu nome ou informações de seu login na rede social.
2J3	Verifique se o usuário tem a opção de desativar a sua conta temporariamente ou permanentemente na rede social.
2L. Confidencialidade	
2L1	Verifique se o usuário tem a opção de ocultar ou arquivar uma publicação compartilhada por ele em seu perfil.
2L2	Verifique se o usuário tem a opção de escolher se deseja exibir novamente em seu perfil uma publicação ocultada ou arquivada.
2L. Confidencialidade	
2L3	Verifique se há uma opção que permita o usuário limpar o seu histórico de busca na rede social.
2M. Curtidas ou Comentários	
2M1	Verifique se o usuário tem a opção de controlar quem pode comentar sua publicação no sistema
2M2	Verifique se o usuário tem a opção de denunciar um comentário, tanto em sua publicação pessoal quanto na publicação de outro indivíduo, que contenha conteúdo impróprio
2M3	Verifique se o usuário tem a opção de ativar um filtro de palavras-chave para ocultar comentários que contenham palavras, frases, números ou emojis considerados inapropriados ou ofensivos
2N. Controle de localização	
2N1	Verifique se o usuário tem a opção de ativar ou desativar os serviços de localização na rede social.
2N2	Verifique se o usuário tem a opção de editar ou remover a sua localização em uma determinada publicação na rede social.
2O. Legado Digital Pós-Morte	
2O1	Verifique se o usuário tem a opção de escolher indicar um contato herdeiro para gerenciar a sua conta caso o mesmo venha a falecer
2O2	Verifique se a rede social permite transformar a conta de um usuário falecido em memorial digital
2O3	Verifique se a rede social permite solicitar que a conta de um usuário falecido seja permanentemente removida do sistema.

Fonte: Próprio autor.

4.2.3 Técnica PIT-OSN 3

A PIT-OSN 3, por fim, remete a sua inspeção para as **políticas de privacidade** de RSOs. Para auxiliar na obtenção de políticas de privacidade mais claras e coerentes, a PIT-OSN 3 dispõe de itens de verificação que auxiliam os inspetores a detectar possíveis problemas de privacidade neste cenário. Com base nas análises realizadas no mapeamento, considerou-se as políticas como a última categoria a ser tratada no conjunto de técnicas proposto neste trabalho. Tal como a PIT-OSN 2, algumas dimensões da técnica PIT-OSN 3 não tinham uma nomenclatura formada e estas foram criadas e/ou adaptadas com base na

visão do autor deste trabalho. A Tabela 18 descreve as dimensões que estão endereçadas na estrutura da técnica PIT-OSN 3.

Tabela 18. Dimensões da técnica PIT-OSN 3 e referências base

Nº	Dimensão	Explicação	Referências base
1	**Coleta de dados**	diz respeito às políticas informarem adequadamente ao usuário sobre o tipo de dados que está sendo coletado, o método de coleta e a finalidade para a qual os dados são coletados.	Yu *et al.* (2006) Anthonysamy *et al.* (2014) Yamauchi *et al.* (2016)
2	**Uso e divulgação dos dados**	diz respeito às políticas de privacidade explicitarem, de forma clara, como utilizam os dados do usuário e como compartilham ou divulgam suas informações.	Yu *et al.* (2006) Lichtenstein (2003) Anthonysamy *et al.* (2014) Yamauchi *et al.* (2016)
3	**Armazenamento de dados**	diz respeito às políticas especificarem de que maneira armazenam os dados do usuário e por quanto tempo tais conteúdos podem ficar guardados na aplicação.	Yu *et al.* (2006) Lichtenstein (2003)
4	**Clareza**	diz respeito à aplicação apresentar o conteúdo das políticas de privacidade de maneira clara, coerente, direta e em uma linguagem que facilite a leitura e compreensão do usuário.	Yu *et al.* (2006) Lichtenstein (2003) Yamauchi *et al.* (2016)
5	**Contato online**	diz respeito às políticas de privacidade especificarem algum meio para o usuário entrar em contato com a rede social em casos de dúvidas ou reclamações.	Yu *et al.* (2006)
6	**Anonimato em transações**	diz respeito às políticas especificarem como fazem uso das informações pessoais do usuário que são fornecidas em transações financeiras e se a aplicação garante o sigilo e proteção dos dados do usuário em tais transações.	Yu *et al.* (2006)
7	**Dados confidenciais**	diz respeito às políticas especificarem em que circunstâncias podem divulgar informações confidenciais do usuário, como em casos exigidos por lei, por exemplo.	Yu *et al.* (2006) Lichtenstein (2003)
8	**Garantia**	diz respeito às políticas declararem e garantirem aos usuários que estão seguindo suas regras de privacidade na prática.	Lichtenstein (2003)
9	**Restrição de idade**	diz respeito às políticas detalharem como tratam o envolvimento de crianças ou menores de idade na aplicação.	Lichtenstein (2003) Anthonysamy *et al.* (2014)

Nº	Dimensão	Explicação	Referências base
10	**Legislação vigente**	diz respeito às políticas estabelecerem o regulamento ou norma do país em que a aplicação está em uso.	Yamauchi *et al.* (2016)

Fonte: Próprio autor.

A partir destas definições foram formulados os itens que determinam o que deve ser verificado em cada dimensão referente ao foco geral da categoria. Ao avaliar a privacidade sob a visão das *políticas,* o inspetor deve checar se o conteúdo das políticas contém informações claras, coerentes e diretas e ao mesmo tempo informações adequadas que garantem a privacidade dos usuários. Portanto, a "pergunta-chave" para nortear esta categoria é: "*O usuário tem um documento que apresenta informações específicas que garantem a sua privacidade?"*. Um conjunto de 24 itens de verificação integra a versão inicial da PIT-OSN 3 e estão agregados nas dimensões caracterizadas acima. Na Tabela 19 são apresentadas as dimensões e seus respectivos itens de verificação que compõem PIT-OSN 3.

Tabela 19. Extrato da técnica PIT-OSN 3

Dimensões e itens de verificação da PIT-OSN 3	
3A. Coleta de dados	
3A1	Verifique se há alguma informação detalhada sobre os tipos de dados que estão sendo coletados do usuário.
3A2	Verifique se a política de privacidade especifica qual o meio que a rede social utiliza para coletar dados do usuário (se é através do cadastro de conta, se através de informações de compras ou comentários por exemplo).
3B. Uso e divulgação dos dados	
3B1	Verifique se a política de privacidade especifica como a rede social pode utilizar e manipular as informações fornecidas pelo usuário.
3B2	Verifique se a política de privacidade especifica com quem (parceiros, provedores ou outros usuários) a rede social pode divulgar as informações fornecidas pelo usuário.
3B3	Verifique se há declarações informando em que circunstâncias que a rede social pode divulgar informações do usuário a terceiros, como em casos de razões legais por exemplo.
3B4	Verifique se há alguma declaração informando sobre o que acontece com as informações do usuário no caso de uma alteração de controle (como venda ou transferência da rede social para outra empresa).
3C. Armazenamento de dados	
3C1	Verifique se há declarações sobre como a rede social armazena e processa (se em banco de dados ou nuvem por exemplo) os dados coletados do usuário.
3C2	Verifique se há alguma declaração sobre quais informações são opcionais antes de conceder ao usuário acesso a rede social.
3C3	Verifique se a política de privacidade especifica por quanto tempo a rede social pode manter armazenado os dados do usuário, caso o indivíduo escolha desativar sua conta.

Dimensões e itens de verificação da PIT-OSN 3	
3A. Coleta de dados	
3C4	Verifique se as políticas de privacidade especificam como utilizam os cookies e outras tecnologias de armazenamento.
3D. Clareza	
3D1	Verifique se o documento estabelecido pela rede social é de fácil acesso e expressa claramente as políticas de privacidade.
3D2	Verifique se há alguma informação sobre possíveis modificações ou atualizações nas políticas de privacidade da rede social e se há formas adicionais de notificação de mudanças para o usuário.
3D3	Verifique se as políticas de privacidade possuem alguma informação escrita em outro idioma diferente do idioma do usuário.
3E. Contato online	
3E1	Verifique se as políticas de privacidade especificam algum meio para o usuário entrar em contato com a rede social
3F. Anonimato em transações	
3F1	Verifique se é especificada alguma medida para preservar informações financeiras do usuário disponibilizadas em transações na rede social (como conexão criptografada e proteção de hardware e software por exemplo).
3F2	Verifique se é especificada alguma informação sobre como a rede social atua em casos de atividades fraudulentas em transações feitas pelo usuário por meio da rede social.
3G. Dados confidenciais	
3G1	Verifique se as políticas de privacidade especificam as opções para obter o consentimento do usuário quando algumas informações confidenciais precisarem ser usadas ou divulgadas.
3G2	Verifique se as políticas de privacidade apresentam um relatório de transparência sobre as informações mais solicitadas em processos jurídicos ou sobre as ações do usuário na rede social.
3H. Garantia	
3H1	Verifique se as informações declaradas nas políticas de privacidade estão sendo cumpridas na prática
3I. Restrição de idade	
3I1	Verifique se as políticas de privacidade fornecem informações sobre o acesso e envolvimento de crianças na rede social.
3I2	Verifique se as políticas de privacidade especificam algum mecanismo de restrição de idade para preservar a participação de menores na rede social.
3J. Legislação vigente	
3J1	Verifique se as políticas de privacidade especificam se estão cumprindo ou seguindo a legislação vigente do país em que a rede social está em uso
3L. Serviços de publicidade	
3L1	Verifique se há informações sobre os serviços de publicidade e como eles atuam na rede social.
3L2	Verifique se as políticas de privacidade especificam informações sobre preferências publicitárias e como o usuário pode deixar de receber anúncios indesejados

Fonte: Próprio autor.

4.2.4 Finalidade de uso da PIT-OSN

A principal finalidade destas técnicas é oferecer uma prática que talvez não esteja sendo exercida pelos profissionais envolvidos (designers ou avaliadores, por exemplo) no

projeto de desenvolvimento de RSOs, que é a avaliação de privacidade através de inspeção. A PIT-OSN 1 tem como principal vantagem verificar se a rede social permite ou não o usuário atingir o seu nível desejado de privacidade a partir de dimensões que norteiam o avaliador examinar a qualidade dos níveis de privacidade do sistema. A PIT-OSN 2, por sua vez, tem como vantagem mostrar se a rede social permite o usuário ter um controle adequado sobre a sua privacidade a partir de dimensões holísticas que tratam sobre questões gerais e abrangentes relacionadas a opções, recursos ou ferramentas de privacidade. Já a PIT-OSN 3 tem como principal vantagem evidenciar se a rede social contém um documento que apresenta informações claras e coerentes que garantem a privacidade do usuário.

Além disso, as técnicas orientam os inspetores a diagnosticarem problemas de privacidade sem exigir que estes sejam especialistas em inspeção de interfaces. Ainda que sejam técnicas de avaliação, as mesmas também podem ser aplicadas em tempo de design, podendo funcionar como um guia de aspectos a serem considerados pelos inspetores, buscando evidências que indiquem se as metas de design de privacidade foram alcançadas e se a RSO possui uma qualidade de uso desejada quanto a sua estrutura de privacidade.

Uma das principais características destas técnicas é que são independentes de apoio ferramental, ou seja, não se limitam à disponibilidade de um sistema de apoio para proceder sua execução. Além disso, as técnicas podem ser utilizadas de forma independente. Por exemplo, quando o designer ou avaliador de uma RSO acredita que somente o cenário das políticas de privacidade pode estar fragmentado, a PIT-OSN 3 pode ser aplicada separadamente para melhorar este cenário em questão. Entretanto, ao serem executadas em conjunto melhores resultados serão encontrados, pois o inspetor avalia e interpreta a situação atual de privacidade a partir de um ponto de vista abrangente, o que contribui para enriquecer a identificação das necessidades e oportunidades de melhoria geral da privacidade da aplicação.

Espera-se que o conjunto de tecnologias seja fácil de aprender e utilizar, seja eficiente e eficaz e possa oferecer uma boa relação custo-benefício em sua aplicação. Evidencia-se, no entanto, que uma limitação das técnicas é o fato de serem aplicáveis apenas para o contexto de RSOs, não podendo serem executadas em outros tipos de sistemas. Além disso, ainda que o conjunto de tecnologias possa ser aplicado em tempo de design, esta aplicação só poderá ocorrer posterior a escolha das representações de interface, não podendo serem aplicadas em um modelo de tarefas por exemplo.

4.2.5 Taxonomia para a classificação de defeitos de privacidade

Para auxiliar o processo de inspeção de privacidade do conjunto de técnicas PIT-OSN, adotou-se uma taxonomia de classificação de defeitos, a qual foi adaptada para o contexto deste trabalho. Esta taxonomia foi obtida a partir das propostas de Porter e Votta (1994) e Kirner e Abib (1998).

A partir do auxílio da taxonomia, os defeitos identificados com as técnicas podem ser classificados em três classes: *omissão, inadequação ou disseminação.* Nota-se que a classe "disseminação" não está presente na categorização apresentada por Porter e Votta (1994), todavia, sentiu-se a necessidade de inserir esta nova proposição para ser testada no contexto deste trabalho, visto que em tempos de redes sociais online a disseminação de informações é comum. Além disso, até mesmo quando a informação é disseminada voluntariamente pelo próprio indivíduo problemas de privacidade podem surgir, caso o mesmo não seja capaz de controlar efetivamente a audiência da informação ou o uso que pode ser feito desta informação. A Tabela 20 apresenta uma descrição dos defeitos incorporados ao conjunto de tecnologias PIT-OSN.

Tabela 20. Taxonomia de defeitos da PIT-OSN

Classe	Tipo	Descrição
OMISSÃO	Funcionalidade Omitida	Ocorre quando uma informação ou descrição sobre alguma funcionalidade de privacidade deixou de ser informada ou **não existe** no sistema
	Feedback Omitido	Ocorre quando não é percebida ou compreendida a resposta dada pelo sistema para uma determinada ação em relação a privacidade (a ação foi realizada, mas está faltando a resposta)
	Interface Omitida	Ocorre quando se deseja achar alguma informação ou funcionalidade de privacidade **que existe** no sistema e não a consegue encontrar na interface
INADEQUAÇÃO	Informação Ambígua	Um elemento importante, uma frase ou uma sentença de não é bem definido (nos níveis, nos controles ou nas políticas da rede social) causando assim múltiplas interpretações
	Informação Inconsistente	Uma informação ou um elemento de privacidade é representado de maneira diferente em duas visões, ou seja, possuem o mesmo sentido, mas nomes distintos (sinônimos)

Classe	Tipo	Descrição
INADEQUA-ÇÃO	Funcionalidade Incorreta	Alguma funcionalidade de privacidade foi descrita ou representada de maneira incorreta
	Seção Incorreta	Alguma informação ou elemento de privacidade está em um local errado dentro do sistema
DISSEMINAÇÃO	Difusão por outro usuário	Ocorre quando o sistema permite a exposição de um determinado indivíduo por meio das ações de outros usuários ou de terceiros
	Difusão pelo sistema	Ocorre quando a própria rede social toma a iniciativa de divulgar informações do usuário no sistema ou em outros meios de comunicação

Fonte: Adaptado de Porter e Votta. 1994.

Ressalta-se, também, que o tipo de defeito “ambiente omitido” não foi inserido na taxonomia de classificação defeitos de privacidade, pois este busca procurar descrições sobre o hardware, software e banco de dados. A partir disso, definiu-se a omissão como um tipo de informação ou elemento ausente nas categorias de privacidade das técnicas e podem ser definidas como: funcionalidade omitida, feedback omitido ou interface omitida. Já os defeitos relacionados a inadequação podem ser classificados em: informação ambígua, informação inconsistente, funcionalidade incorreta ou seção incorreta. Por fim, os defeitos referentes à disseminação podem ser definidos como: exposição passiva ou difusão indevida. Nota-se que estes últimos defeitos citados também representam uma nova proposição relacionada à classe em questão, pois acredita-se que tanto a exposição como a difusão podem surgir através da disseminação de informações nas RSOs.

Com o auxílio da taxonomia proposta, os inspetores têm a oportunidade também de classificar os problemas detectados durante a atividade de inspeção de privacidade no sistema. Desta forma, os inspetores conseguem ter uma visão das informações ou itens discrepantes que comprometem a interação do usuário com as categorias de privacidade do sistema.

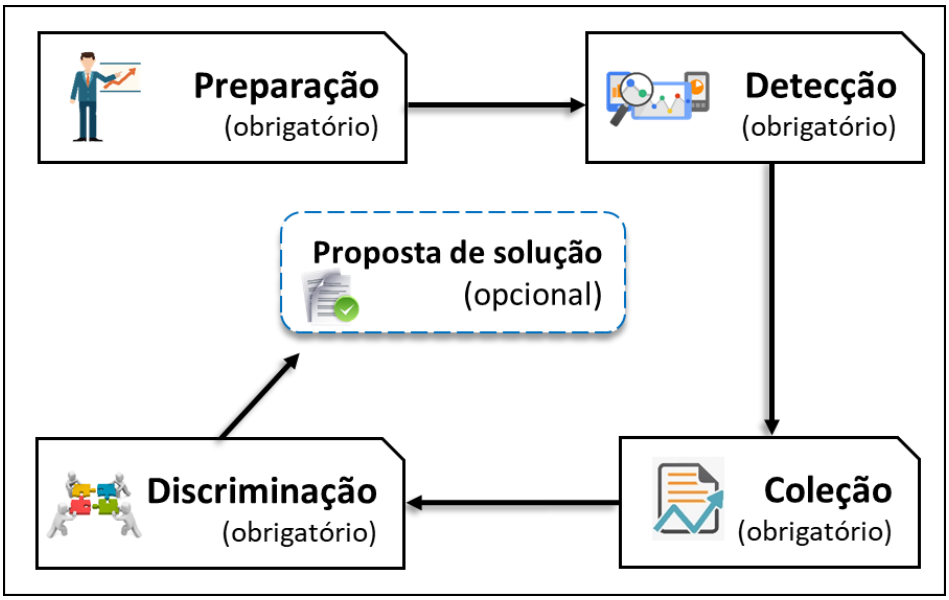
4.3 PROCESSO DE AVALIAÇÃO USANDO AS TÉCNICAS PIT-OSN

Ao aplicar o conjunto de técnicas PIT-OSN, sugere-se o uso de um processo de avaliação com o propósito de providenciar uma maior organização nas inspeções, conforme demonstrado na Figura 4. Para executar o processo de inspeção com o uso das técnicas, recomenda-se a participação de no mínimo duas pessoas, pois adicionar mais inspetores pode

aumentar a chance de encontrar novos defeitos. O processo de avaliação é composto por cinco etapas, as quais serão descritas a seguir:

- **Preparação**: Nesta etapa, o processo de inspeção é preparado e organizado. Uma pessoa, desempenhando o papel de moderador, seleciona os inspetores, define o contexto da inspeção, onde é feita uma breve apresentação sobre o conjunto de técnicas, e distribui os recursos das mesmas a serem aplicados.
- **Detecção de defeitos**: Nesta etapa, cada inspetor realiza sua inspeção individualmente reportando os itens de verificação que foram violados, descrevendo e classificando os possíveis defeitos de privacidade identificados em um relatório de discrepâncias. Uma discrepância representa um possível defeito detectado durante a inspeção, mas este só será julgado como um defeito real de privacidade na etapa de discriminação.
- **Coleção:** Nesta etapa, as listas individuais de discrepâncias (possíveis defeitos) produzidas pelos inspetores são integradas em uma única lista referente ao foco de cada técnica. Um dos inspetores pode ser o responsável por realizar esta integração. Após a geração das listas únicas, uma reunião é feita para a eliminação de discrepâncias repetidas, encontradas por mais de um inspetor, mantendo apenas um registro para cada discrepância. Esta eliminação de duplicatas facilita a etapa de discriminação, onde os inspetores terão que classificar as discrepâncias identificadas.
- **Discriminação**: Nesta etapa, os inspetores devem discutir sobre as discrepâncias detectadas. Durante esta discussão, algumas discrepâncias serão classificadas como falso-positivos e outras como um defeito real de privacidade. Os falsos positivos são descartados, pois representam os pontos que o inspetor pode ter reportado como um defeito, mas não é, seja porque ele não checou a rede social corretamente ou porque não entendeu completamente o que o item de verificação solicitava. Posteriormente, os problemas reais são registrados em uma única lista de defeitos gerando um relatório consolidado.
- **Proposta de solução:** Por fim, nesta etapa, os inspetores podem julgar a justificativa dos defeitos detectados e apontar recomendações de solução.

Figura 4. Processo de avaliação da PIT-OSN



Fonte: Baseado em Sauer *et al.* (2000).

4.4 CONSIDERAÇÕES SOBRE O CAPÍTULO

Este capítulo apresentou o conjunto de técnicas PIT-OSN proposto para apoiar a inspeção de privacidade em RSOs. Estas técnicas são estruturadas por meio de três categorias genéricas que descrevem diretrizes gerais relacionadas à privacidade. Nomeadas de itens de verificação, estas diretrizes são agrupadas em dimensões que guiam o inspetor a detectar um possível defeito de privacidade. A partir disso, foi apresentada a motivação que levou a construção das técnicas, bem como os recursos de apoio às inspeções do conjunto de técnicas de inspeção.

Para apoiar as inspeções de privacidade, o conjunto de técnicas PIT-OSN também disponibiliza uma taxonomia para a classificação dos defeitos detectados durante o processo de inspeção. Com o auxílio da taxonomia, os defeitos identificados com as técnicas podem ser classificados em três diferentes classes: omissão, inadequação ou disseminação. Estas classes permitem categorizar um determinado tipo de defeito durante a atividade de detecção, possibilitando ao inspetor obter um entendimento satisfatório sobre o tipo de defeito identificado nas inspeções.

A inspeção com o auxílio do conjunto de técnicas deve ser feita preferencialmente por, no mínimo, 2 inspetores que podem utilizar um processo de avaliação sugerido com o propósito de providenciar uma maior organização durante as inspeções. O conjunto de técnicas permite identificar problemas em caminhos alternativos de interação, revelando-se

especialmente útil na análise da privacidade com padrões de interação. Além disso, por serem técnicas genéricas, podem ser aplicadas em diversos contextos de RSOs, permitindo a geração de um diagnóstico de defeitos de privacidade sobre uma porção focal da interface da rede social sob inspeção.

As técnicas podem ser usadas em várias fases do ciclo de design. Podem ser aplicadas na avaliação formativa, desde que posterior a escolha das representações da interface, quanto na avaliação somativa. No entanto, as técnicas podem ser mais promissoras ao serem utilizadas em uma avaliação somativa, quando existir uma solução (parcial ou completa) de interação e de interface pronta, permitindo avaliar se a RSO possui os níveis de qualidade de privacidade desejados.

CAPÍTULO 5 – ESTUDO PRELIMINAR COM O CONJUNTO DE TÉCNICAS PIT-OSN

Este capítulo apresenta a condução de um estudo preliminar executado com o conjunto de tecnologias PIT-OSN. Este estudo foi realizado para validar as técnicas propostas.

5.1 INTRODUÇÃO

O conjunto de técnicas PIT-OSN foi inicialmente avaliado através de um estudo preliminar que teve como propósito realizar os procedimentos de validade e confiabilidade das tecnologias concebidas e coletar as oportunidades para o seu refinamento. A seguir será apresentado o detalhamento deste estudo, incluindo seu planejamento, a execução das atividades referentes ao processo de avaliação e os resultados alcançados.

5.2 PLANEJAMENTO DO ESTUDO

O planejamento do estudo foi realizado visando avaliar o conjunto inicial de tecnologias PIT-OSN em relação ao tipo de conhecimento gerado, tempo de aplicação, facilidade de uso e utilidade de cada técnica aplicada. Buscou-se, com isso, ganhar novos *insights* e perspectivas sobre a aplicação das tecnologias, buscando também obter as possibilidades para o seu refinamento.

As inspeções foram realizadas por três pesquisadores voluntários escolhidos por critérios de conveniência. Os três pesquisadores são doutorandos do programa de pós-graduação em Informática da Universidade Federal do Amazonas. Dois participantes relataram ter conhecimentos básicos sobre avaliação de interfaces adquiridos em uma disciplina de pós-graduação. Um participante declarou não ter experiência em avaliação de interfaces. Embora os participantes não sejam especialistas em inspeção, eles produzem e dominam o uso de tecnologias, ou seja, são inspetores prospectivos. Desta forma, este trabalho considerou o público-alvo com a perspectiva de um inspetor que está aprendendo sobre inspeção de privacidade e tem o potencial de mostrar como estes inspetores, que não conhecem o conjunto de técnicas concebido, entenderam a sua proposta e aplicação.

Considerando os aspectos éticos, um termo de consentimento livre e esclarecido (TCLE) assegurando a confidencialidade e a privacidade dos dados coletados foi estabelecido. Outros artefatos foram previamente definidos como um questionário de caracterização que continha perguntas sobre a experiência dos participantes referente a

avaliação de interfaces e outras perguntas referentes ao conhecimento sobre privacidade. Um questionário pós-estudo para coletar a opinião dos participantes em relação ao grau de aceitação sobre o conjunto de tecnologias propostas também foi estabelecido. Ademais, outros recursos foram definidos para a realização das inspeções de privacidade, tais como: as diretrizes para execução das inspeções, um documento contendo a taxonomia de defeitos para auxiliar na classificação dos problemas detectados e uma planilha para o relato e especificação das discrepâncias identificadas, este material pode ser visto no Apêndice C.

A rede social Instagram, em sua versão para dispositivos móveis, foi escolhida como objeto de inspeção. Esta escolha deu-se por dois critérios: expansão e mobilidade. No que diz respeito a expansão, nota-se o crescimento exponencial do Instagram como serviço de rede social, considerando a quantidade e diversidade de usuários. Em relação à mobilidade, a versão mobile do Instagram evidencia a tendência de uso dessas aplicações em smartphones, tornando-se relevante a avaliação por inspeção dessas tecnologias sociais móveis. A aplicação foi avaliada no mês de maio de 2018.

Como os participantes não eram especialistas em inspeção de privacidade, foi realizada uma apresentação para mostrar a ideia inicial do conjunto de técnicas. Esta apresentação serviu como a fase de **preparação** do processo de avaliação da PIT-OSN (ver seção 4.3). Nesta preparação, definiu-se os procedimentos da inspeção, os recursos das técnicas e as atividades a serem executadas durante a detecção de defeitos. Além disso, foi apresentado um conjunto de slides contendo toda a contextualização e exemplificação prática das técnicas. Esta apresentação foi feita para os três participantes. Para cada técnica de inspeção foi mostrado um possível problema de privacidade que ocorria em uma determinada RSO. A rede social escolhida como exemplo para ilustrar violações de privacidade durante a preparação, não foi a mesma escolhida como objeto de inspeção, descartando qualquer viés. Todas as eventuais dúvidas que surgiam quanto à explicação de algum ponto das técnicas eram imediatamente esclarecidas. O tempo total da preparação durou aproximadamente uma hora.

Como o propósito inicial deste estudo era validar o conjunto de técnicas proposto e coletar as oportunidades para o seu refinamento, não foi solicitado que os participantes realizassem uma inspeção utilizando as três técnicas em conjunto, ou seja, cada participante aplicou um tipo de técnica. Isto indica que, na prática, foi realizada apenas uma avaliação de cada técnica. Optou-se, a princípio, pela inspeção parcial para permitir que os participantes capturassem o máximo do potencial de resultados de cada técnica aplicada, de modo a

disponibilizar informações mais críticas e abrangentes e, sobretudo, analisar a plausibilidade e os processos interpretativos de cada técnica PIT-OSN. Após a preparação, iniciou-se a etapa de detecção de defeitos de privacidade a qual será apresenta a seguir.

5.3 EXECUÇÃO DO ESTUDO

O autor desta dissertação atuou como observador durante a condução do estudo, sendo o principal responsável por auxiliar em casos de dúvidas referente ao processo de aplicação das tecnologias, tomando a devida precaução para não influenciar na atividade de detecção de defeitos. Como o estudo contou com a atuação de três participantes, cada inspetor recebeu um tipo de técnica de inspeção estabelecida por meio de sorteio. A partir disso, os participantes foram classificados como P1, P2 e P3.

Com base no sorteio, o participante P1 foi designado para a técnica PIT-OSN 1 para inspecionar os níveis de privacidade. Já o participante P2, por sua vez, ficou com a PIT- OSN 2 para a inspeção dos controles de privacidade. Por fim, o participante P3 foi designado para a PIT- OSN 3 para proceder a inspeção das políticas de privacidade. Cada participante recebeu o material de apoio referente a sua técnica específica de inspeção. Procedeu-se a detecção de defeitos, onde os participantes usaram o seu próprio dispositivo móvel e sua própria rede social para executar a avaliação. Após a inspeção, um questionário pós-estudo foi aplicado.

Após a execução do estudo, as listas de discrepâncias produzidas pelos inspetores foram posteriormente revisadas na reunião de discriminação de defeitos. Ressalta-se que uma discrepância representa um possível defeito detectado durante a inspeção, mas este só é classificado na etapa de discriminação. A etapa de coleção foi descartada neste estudo, pois não haviam discrepâncias duplicadas devido as inspeções terem sido realizadas por apenas um inspetor para cada técnica. Os participantes do estudo poderiam ter realizado todas as etapas do processo de avaliação, no entanto, para evitar que o estudo ficasse prolongado e dispendioso, a etapa de discriminação foi realizada a parte por dois pesquisadores da área de IHC. A etapa de consolidação não foi executada nos estudos. A seguir serão apresentados os resultados obtidos com base neste estudo preliminar.

5.4 RESULTADOS DO ESTUDO PRELIMINAR

O conhecimento dos participantes quanto à avaliação de interfaces (S: Sim e N: Não) e os resultados gerais da avalição de cada inspetor são mostrados nas Tabelas 21, 22 e 23. A seguir, apresenta-se os resultados identificados através das técnicas de inspeção utilizadas.

5.4.1 Inspeção dos Níveis de Privacidade

Ao analisar a Tabela 21, pode-se observar que a PIT-OSN 1 cumpriu sua finalidade, auxiliando a detecção de problemas de privacidade relacionados aos níveis da aplicação utilizada como objeto de avaliação. O diagnóstico de defeitos gerou 7 pontos problemáticos em relação aos níveis de privacidade da RSO avaliada, sendo que o inspetor levou 1h32min na atividade de detecção. Ressalta-se que a discriminação, ou seja, a classificação dos defeitos como reais ou falso-positivos, foi realizada por duas pessoas, a parte, com conhecimento prévio sobre o conjunto de técnicas de inspeção.

Tabela 21. Resultados da inspeção realizada com a PIT-1

Part.	EAI	ND	FP	DE	T(h)	D(h)
P1	S	07	0	07	1,32	4,07
Legenda: **Part**. – Participante; **EAI** – Experiência em avaliação de interfaces; **ND**. – Número de discrepâncias; **FP** – Número de falso-positivo; **DE** – Número de defeitos; **T(h)** – Tempo em hora; **D(h)** – Defeito por hora.						

Fonte: Próprio autor.

Foram identificados quatro tipos de defeitos relacionados aos níveis de privacidade, os quais foram classificados pelo inspetor como: funcionalidade omitida, feedback omitido, difusão por outro usuário e difusão pelo sistema Os defeitos mais encontrados foram funcionalidade omitida e exposição passiva, evidenciando que muitas funções relativas aos níveis de privacidade não existem no sistema. Além disso, a rede social permite a exposição passiva de um determinado indivíduo através das ações de outros usuários, o que pode gerar problemas indesejados de privacidade. Um exemplo de dois defeitos identificados pelo inspetor na rede social avaliada é apresentado na Figura 5.

Figura 5. Exemplos de defeitos identificados com a PIT-OSN 1

Fonte: Instagram, 2018.

Com base na Figura 5, nota-se que, caso o indivíduo tenha a conta aberta, a rede social permite que outro usuário compartilhe uma publicação, sobre este indivíduo, em um outro espaço de comunicação que não pertence ao dono da postagem e provavelmente sem a sua permissão. Este outro espaço de publicação pode ser o *Instagram Direct*, tal como mostrado na Figura 5, que permite que a publicação seja diretamente enviada para amigos específicos ou grupos de amigos do usuário que compartilhou e, além disso, permite compartilhar em outros espaços fora da rede social como o Facebook e Messenger, por exemplo. Tal questão evidencia que a dimensão "Espaço de Comunicação" e um dos seus itens de verificação foram violados, revelando um defeito de difusão por outro usuário.

Além disso, ao permitir que outro usuário compartilhe uma publicação de um determinado indivíduo via *direct*, a rede social também viola a dimensão "Notificação" e um de seus itens de verificação, pois não é fornecida ao indivíduo (dono da postagem) nenhuma notificação, mesmo se a conta estiver pública ou privada, sobre esta divulgação feita por outro usuário através do recurso *direct*. Esta questão revela um defeito de funcionalidade omitida, pois o sistema não notifica o indivíduo sobre esta interação, ou seja, a função não existe no sistema. Este resultado pode representar um indício para tomar decisões de (re)design pois, para que o usuário tenha um nível de privacidade adequado, o sistema deve fornecer uma notificação completa de modo que este fique consciente sobre o que está sendo acessado, por outros usuários, sobre ele. Assim, a notificação ao usuário garante que ele esteja ciente da disseminação de informações sobre ele, permitindo que seja mais restritivo quando compartilha, caso queira aumentar sua privacidade..

5.4.2 Inspeção dos Controles de Privacidade

Observando a Tabela 22, nota-se que a técnica PIT-OSN 2 também cumpriu o seu propósito geral de apoiar o diagnóstico de defeitos nos controles de privacidade disponibilizados pela RSO inspecionada. Um total de 13 problemas de privacidade foram diagnosticados. O tempo gasto para a aplicação da técnica durou a 2h14min.

Tabela 22. Resultados da inspeção com a técnica PIT-2

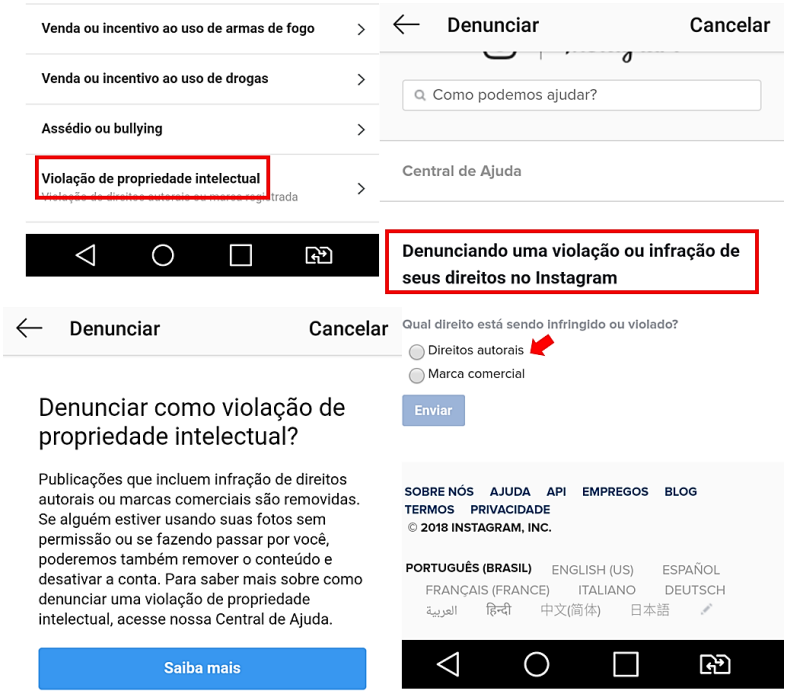
Part.	EAI	ND	FP	DE	T(h)	D(h)
P2	S	16	3	13	2,14	5,12

. **Legenda:**
Part. – Participante; **EAI** – Experiência em avaliação de interfaces; **ND**. – Número de discrepâncias; **FP** – Número de falso-positivo; **DE** – Número de defeitos; **T(h)** – Tempo por hora; **D(h)** – Defeito por hora;

Fonte: Próprio autor.

Foram identificados dois tipos de defeitos pelo inspetor que aplicou a PIT-OSN 2: funcionalidade omitida e seção incorreta. Com isso, observa-se que informações ou elementos de privacidade específicos para este domínio estão ausentes nos controles de privacidade do sistema. Além disso, o problema de seção incorreta demonstra também que algumas informações ou elementos de privacidade estão incorporados em uma localização incorreta na rede social inspecionada, ocasionando o tipo de defeito relatado, tal como mostrado na Figura 6.

Figura 6. Exemplo de defeito identificado com a PIT-2



Fonte: Instagram, 2018.

Ao inspecionar o Instagram a partir da dimensão “Direito de Privacidade” e de seu respectivo item de verificação 1A1 “*Verifique se a rede social permite denunciar uma publicação de conteúdos que violem os direitos de propriedade intelectual do usuário, como direitos autorais por exemplo*”, o inspetor detectou um defeito de seção incorreta. Apesar da rede social permitir que o usuário denuncie uma violação de propriedade intelectual, esta opção não será encontrada nas configurações de privacidade do sistema. Ao procurar esta opção, o usuário será direcionado para central de ajuda e terá que percorrer a interface em busca desta funcionalidade. Ou seja, o usuário precisa consultar a ajuda online para saber como denunciar esta questão. Tal caminho reflete um defeito, pois, considerando o perfil de

um usuário que não conhece bem o sistema, haveria uma dificuldade em encontrar esta opção desejada relacionada a uma ação de privacidade.

5.4.3 Inspeção das Políticas de Privacidade

Com base nos resultados da Tabela 20, pode-se observar que a técnica PIT-OSN 3 também cumpriu o seu propósito para identificar defeitos nas políticas do sistema. Um total de 10 defeitos foram detectados nas políticas de privacidade com o uso da técnica, tendo como duração 1h36min de aplicação.

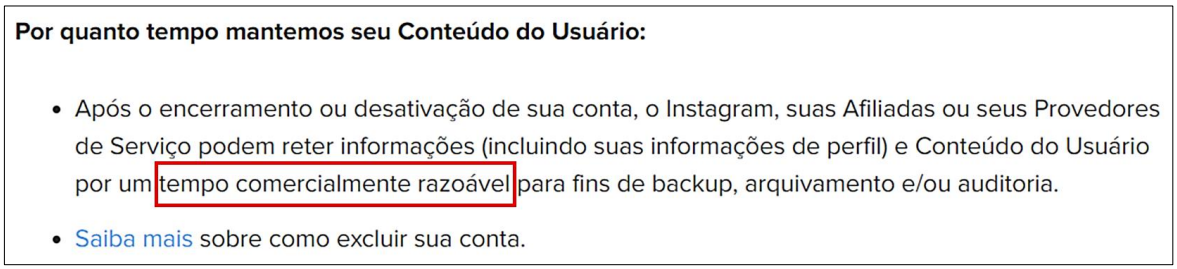
Tabela 23. Resultados da inspeção com a técnica PIT-OSN 3

Part.	EAI	ND	FP	DE	T(h)	D(h)
P3	N	11	1	10	1,36	5,68
Legenda: **Part**. – Participante; **EAI** – Experiência em avaliação de interfaces; **ND**. – Número de discrepâncias; **FP** – Número de falso-positivo; **DE** – Número de defeitos; **T(h)** – Tempo em hora; **D(h)** – Defeito por hora;						

Fonte: Próprio autor.

Foram identificados três tipos de defeitos pelo inspetor que aplicou a PIT-OSN 3: funcionalidade omitida, informação ambígua e seção incorreta. Os defeitos mais detectados foram funcionalidade omitida e informação ambígua. Com isso, nota-se que algumas funcionalidades da aplicação que deveriam ser descritas nas políticas do sistema não existiam no cenário em evidência. Além disso, algumas outras informações contidas nas políticas são ambíguas, ou seja, várias interpretações podem ser derivadas dos documentos de privacidade, levando o usuário a ter uma compreensão dúbia quanto ao que está sendo exposto para garantir sua proteção na interação com o sistema. Um exemplo de uma informação ambígua detectada pelo inspetor é mostrada na Figura 7.

Figura 7. Exemplo de defeito identificado com a técnica PIT-3



Fonte: Políticas de privacidade do *Instagram*, 2018.

Com base na Figura 7, nota-se que a rede social informa por quanto tempo mantém armazenado o conteúdo do usuário. No entanto, ao avaliar esta informação através da dimensão "*Armazenamento de dados*" e de seu item de verificação 3C2 "*Verifique se a política de privacidade especifica por quanto tempo a rede social pode manter armazenado os dados do usuário, caso o indivíduo escolha desativar sua conta*", percebe-se que há uma informação ambígua, pois não é informado especificamente ao usuário por quanto tempo sua informação será mantida caso o mesmo desative sua conta. A frase "tempo comercialmente razoável" não especifica de maneira clara o período de tempo do armazenamento de dados, causando assim variadas interpretações, revelando também um defeito nas políticas de privacidade.

5.4.4 Tipo de Conhecimento e Explicações Geradas com as Técnicas

Em termos de conhecimento necessário para a aplicação e interpretação dos itens de verificação do conjunto de técnicas, observou-se, ainda que preliminarmente, que a PIT-OSN dispensa o avaliador da necessidade de serem especialistas para identificar e listar problemas, tal como exposto em sua formulação. A qualidade da explicação dos problemas de privacidade diagnosticados pode ser um indicador de que o processo de inspeção das técnicas não depende necessariamente do conhecimento do avaliador em avaliação de interfaces.

Quanto ao tipo de conhecimento gerado, a PIT-OSN mostra-se adequada para contribuir tecnicamente para a melhoria da qualidade de privacidade em projetos e avaliações de RSOs. Podem ser usadas tanto para uma avaliação formativa, ou seja, para dar insumos para a qualidade de um (re)projeto de privacidade e comparar alterativas de design, e também em uma avaliação somativa, servindo de ferramentas para avaliar se a RSO possui os níveis de qualidade de uso desejados quanto aos seus aspectos de privacidade.

Considerando o tipo de explicação gerada, a PIT-OSN, por serem técnicas qualitativas e exploratórias, buscam fomentar a reflexão e interpretação do avaliador sobre os problemas de privacidade detectados. Ou seja, por terem itens de verificação vinculados à pratica, o conjunto de técnicas busca oferecer resultados que gerem explicações articuladas e consistentes sobre níveis, controles e políticas de privacidade de uma determina RSO.

5.4.5 Tempo de Aplicação

A PIT-OSN 1 mostrou um bom desempenho para detecção de defeitos encontrando cerca de 4,07 defeitos por hora e tendo um tempo de execução de 1h32min, destacando-se como o tempo mais ágil de aplicação do conjunto de tecnologias proposto. Com isso, pode-se

inferir que a PIT-OSN 1 apresenta indícios de que seu uso é viável para o diagnóstico de defeitos de níveis de privacidade em uma RSO em um curto período de tempo.

A PIT-OSN 2, por sua vez, identificou 5,12 defeitos por hora e teve um tempo de 2h14min de aplicação. Apesar de ter o maior tempo empregado para detectar os defeitos, a mesma cumpriu o seu propósito geral para detectar problemas referentes aos controles de privacidade da RSO utilizada como objeto de avaliação.

Por fim, a PIT-OSN 3 identificou 5,68 defeitos por hora e teve uma duração de 1h36min de execução. Com isso, a técnica também mostrou-se capaz de detectar informações discrepantes nas políticas de privacidade do sistema avaliado.

Nota-se que o tempo necessário às aplicações pode estar estritamente relacionado ao processo interpretativo que cada técnica gerou. A PIT-OSN 1 e 3, ao cumprirem suas finalidades técnicas, mostram-se como técnicas de inspeção relativamente ágeis e objetivas. Já a PIT-OSN 2, por conter a maior quantidade de itens de verificação do conjunto de técnicas, tende a ter um processo interpretativo mais prolongado, pois a quantidade de itens a serem verificados pode aumentar o tempo de inspeção. No entanto, este estudo não apresentou dados suficientes para comprovar esta suposição.

5.4.6 Análise da Aceitação das Tecnologias

Os participantes responderam seu grau de aceitação em relação ao conjunto de tecnologias através de um questionário pós-estudo. Este questionário foi elaborado com base nos indicadores do modelo TAM (*Tecnology Acceptance Model*) que tem sido amplamente utilizado em diversas pesquisas (VENKATESH e BALA, 2008). Davis (1989) propôs o TAM para avaliar o motivo de usuários aceitarem ou rejeitarem uma determinada tecnologia. Apesar do TAM ter sido proposto para o contexto de sistemas de informação, o mesmo também pode ser aplicado para avaliar a aceitação de modelos, técnicas, ferramentas, entre outros (CONTE *et al.,* 2018), Os indicadores utilizados para a avaliação do conjunto de técnicas foram: (i) facilidade de uso percebida; (ii) utilidade percebida; e (iii) intenção de uso futuro.

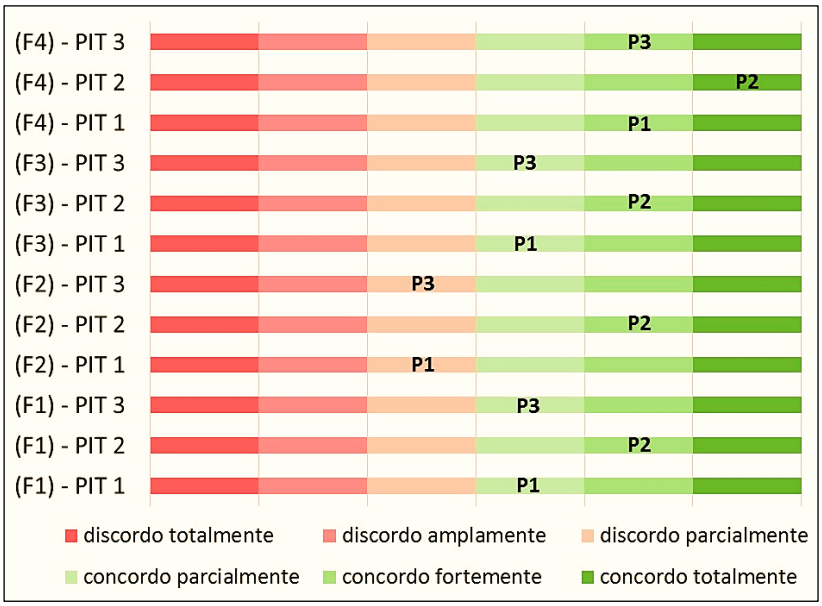
Facilidade de uso percebida. Define o grau em que uma pessoa acredita que usar uma tecnologia específica seria livre de esforço, através das seguintes questões: (F1) Minha interação com a PIT-OSN foi clara e compreensível, (F2) Utilizar a PIT-OSN não exige muito do meu esforço mental, (F3) Considero a PIT-OSN fácil de usar e (F4) Considero fácil de utilizar a PIT-OSN para fazer o que eu quero que ela faça, apoiar a avaliação de privacidade em redes sociais online através de inspeção.

Utilidade percebida. Define o grau em que uma pessoa acredita que a tecnologia poderia melhorar seu desempenho, através das seguintes questões: (U1) Usar a PIT-OSN melhorou o meu desempenho na inspeção de privacidade em redes sociais, (U2) Usar os itens de verificação da PIT-OSN melhorou a minha produtividade na inspeção de privacidade em redes sociais, (U3) Usar a PIT-OSN aumentou a minha eficácia na inspeção de privacidade em redes sociais e (U4) Eu considero a PIT-OSN útil para apoiar o processo de inspeção de privacidade em redes sociais.

Intenção de uso futuro. Define o grau em que uma pessoa acredita que utilizaria a tecnologia em projetos futuros, através das seguintes questões: (I1) Supondo que eu tenha acesso a PIT-OSN, eu pretendo usá-la e (I2) Levando em conta que eu tenho acesso a PIT-OSN eu prevejo que irei usá-la em outros momentos.

Os participantes forneceram suas respostas em uma escala de seis pontos, baseado no questionário aplicado por Lanubile *et al.* (2003). As possíveis respostas foram: concordo totalmente, concordo amplamente, concordo parcialmente, discordo parcialmente, discordo amplamente e discordo totalmente. Esta escala de respostas foi considerada adequada porque não há valor intermediário, ou seja, ela ajuda a evitar o viés da tendência central em classificações, forçando os participantes a julgar o resultado como adequado ou não adequado. A Figura 8 apresenta a percepção dos participantes quanto ao indicador *facilidade de uso percebida*.

Figura 8. Grau de aceitação em relação a facilidade de uso percebida da PIT-OSN

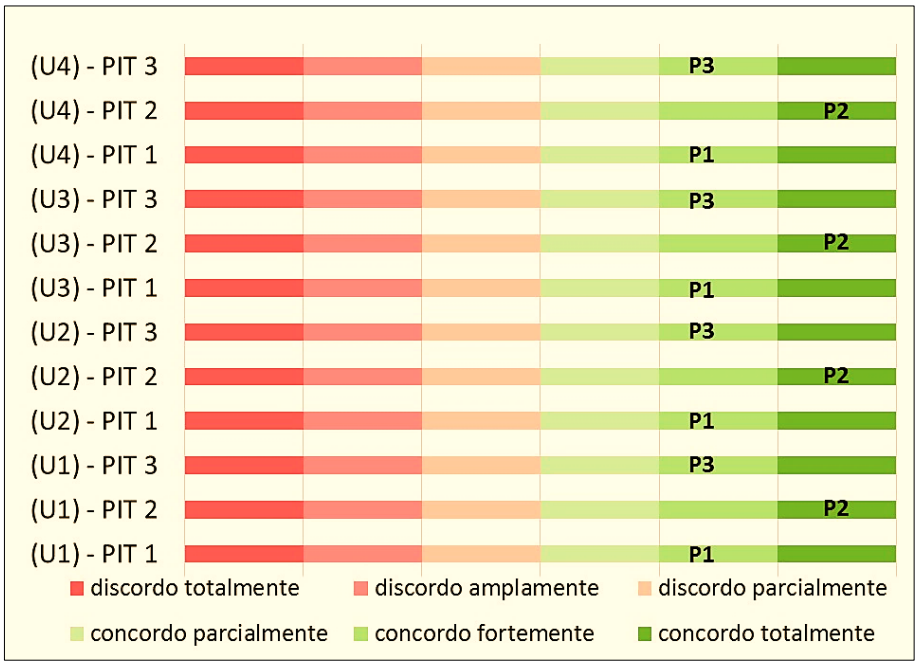


Fonte: Próprio autor.

O eixo vertical do gráfico acima representa às afirmativas do indicador em foco juntamente com o número da técnica e o eixo horizontal refere-se ao grau de aceitação dos participantes. Nas barras foram inseridos códigos que simbolizam os participantes (P1, P2 e P3) do estudo e sua respectiva avaliação.

Com base na visão que a Figura 8 fornece, nota-se que todos participantes concordaram com a afirmação (F3) "*Considero a PIT-ONS fácil de usar*" indicando que PIT-OSN possui facilidade de uso, na medida em que apresenta diretrizes simples, objetivas e genéricas, desvinculadas de conhecimentos sólidos do inspetor em avaliação de interfaces. No entanto, dois participantes discordaram parcialmente quanto a afirmativa F2, que destaca que usar a PIT-1 e PIT-3 não exige muito do esforço mental. Essa questão aponta a provável necessidade de uma investigação mais aprofundada sobre alguns pontos destas técnicas, a fim de buscar identificar o que pode estar causando esforço mental e o que pode ser simplificado para evitar possíveis dificuldades quanto à aplicação. A Figura 9 demonstra o grau de concordância dos participantes quanto ao indicador de utilidade percebida.

Figura 9. Grau de aceitação em relação a utilidade percebida da PIT-OSN



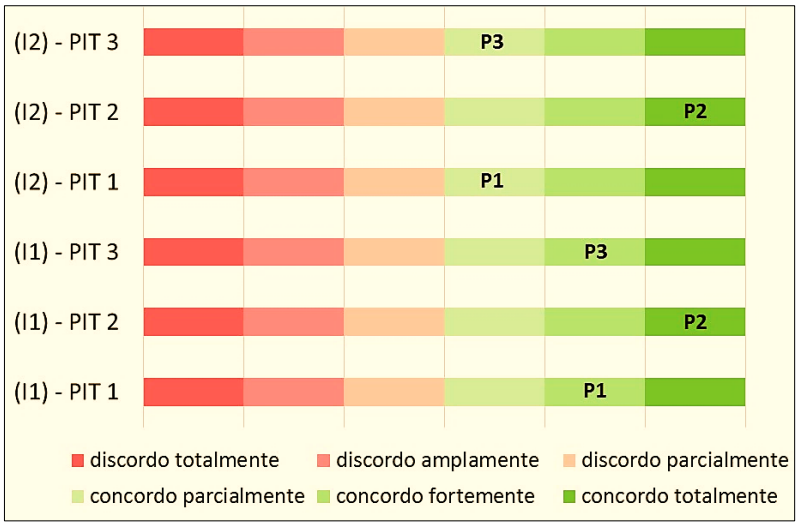
Fonte: Próprio autor.

A interpretação da Figura 9 é semelhante à interpretação descrita na figura anterior. Nesta ótica, a aplicação do conjunto de tecnologias PIT-OSN, neste estudo, revelou que as técnicas foram julgadas úteis para identificar problemas de privacidade durante a avaliação da aplicação utilizada. Este resultado pode estar relacionado com o tipo de conhecimento que as

técnicas geraram, pois, por estarem vinculadas a itens de verificação vigentes na prática e permitirem a discussão de resultados articulados, as técnicas acabam sendo consideradas potencialmente úteis para apoiar a geração do diagnóstico de problemas em RSOs.

Por fim, a Figura 10 aponta a percepção dos participantes em relação ao indicador intenção de uso futuro. Seguindo a mesma interpretação das figuras anteriores, a Figura 10 demonstra que os participantes consideram a PIT-OSN apropriada para ser utilizada em projetos futuros.

Figura 10. Grau de aceitação em relação a intenção de uso futuro da PIT-OSN



Fonte: Próprio autor.

5.4.7 Resultados Qualitativos e Melhorias

Adicionalmente, realizou-se uma análise em relação aos comentários dos participantes obtidos através de perguntas abertas contidas no questionário pós-estudo. Tal análise forneceu feedbacks relevantes sobre o uso do conjunto de técnicas PIT-OSN. No que diz respeito a aspectos positivos, destaca-se o comentário do participante P2 que afirma: "*[A técnica] é bem detalhista, trouxe abordagens atuais e permite de fato inspecionar a privacidade em redes sociais".* P3 salienta também que "*[A técnica permite] a análise de todos os pontos principais de privacidade e é fácil de identificar falhas de privacidade".* Com isso, pode-se inferir que a tecnologia proposta tem um bom nível de detalhes que forcem subsídios importantes para identificar problemas de privacidade, o que pode auxiliar os profissionais envolvidos na articulação de causas e explicações para tais problemas.

Quanto aos aspectos negativos e dificuldades envolvidas na aplicação das PIT-OSN, pode-se enfatizar o comentário do participante P1 que retrata: "*[Tive] dificuldade em entender alguns itens de verificação*". P3 também expressa sua dificuldade, mas não relacionada a utilidade da técnica especificamente, e sim ao conteúdo descrito pelas políticas: "*A técnica em si é de fácil utilização, a maior dificuldade está na questão de interpretação das informações fornecidas pela política de privacidade".* Esta questão reflete plenamente os problemas das políticas quanto à sua estrutura e adequação, que muitas das vezes contemplam textos extensos, com jargões técnicos, sem padrões de escrita e muito complexos.

P2, por sua vez, salientou a questão do tempo como um aspecto negativo: *"É uma inspeção demorada. Poderia padronizar e/ou reduzir os itens [de verificação] da técnica dos controles de privacidade.* No entanto, o tempo necessário para proceder as inspeções pode está estritamente relacionado a quantidade de itens de verificação que cada técnica apresenta. Em linhas gerais, as PIT-OSN 1 e PIT-OSN 3 tiveram um tempo de aplicação inferior ao da PIT-OSN 2, um dos fatores que pode ter influenciado este tempo de aplicação pode ter sido o número inferior de itens de verificação que estas, PIT-OSN 1 e 3, possuem. Por ter uma quantidade de diretrizes maior, a PIT-OSN 2 tende a ter um processo de inspeção mais longo. Desse modo, pode-se observar que há pontos que precisam ser mais investigados nas técnicas propostas para analisar se a quantidade de itens de verificação pode ser um fator que influencia ou não o tempo de aplicação.

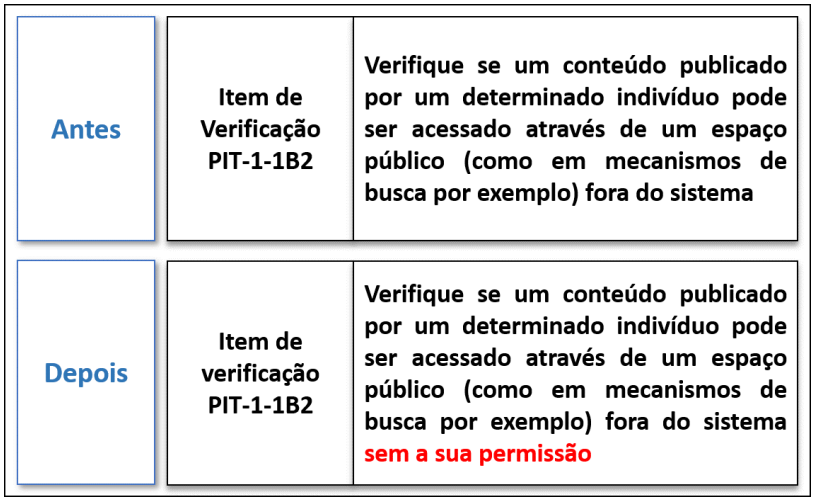
Pode-se observar que, após a execução do estudo preliminar, houve algumas dificuldades e uma delas precisa ser destacada: a compreensão em relação à descrição de alguns itens de verificação. Observamos que a definição de alguns itens não estava representada de maneira clara para detectar um possível problema de privacidade, o que pode ter causado dificuldades de aplicação.

Nesse contexto, analisamos a descrição de alguns itens de verificação como, por exemplo, do item 1B2 da técnica PIT-OSN 1, o qual o mesmo pede para verificar se um conteúdo publicado por um indivíduo pode ser acessado fora do sistema. Para que esta questão possa ser vista como um problema que aumenta a possibilidade da privacidade do indivíduo ser comprometida, o conteúdo sobre ele deve ser compartilhado fora do sistema sem o seu conhecimento ou consentimento. Essa questão caracteriza melhor um problema real relacionado à privacidade, pois se a rede social não solicita a permissão do usuário para que seu conteúdo seja compartilhado e acessado em um outro domínio, tem-se um potencial problema. Para que este item de verificação levasse em consideração o consentimento do

usuário, foi incluída a complementação "sem a sua permissão", conforme mostrado na Figura 11.

Além disso, outras adaptações foram realizadas na técnica PIT-OSN 1. Observou-se que a nomenclatura usada na dimensão 1C (*Domínio, expressão e conteúdo de dados)* não estava condizente com a descrição dos itens de verificação da mesma. A dimensão busca avaliar, em específico, o nível de privacidade sobre o conteúdo dos dados do usuário. Logo, retiramos os termos “domínio e expressão”, deixando-a somente com a nomenclatura “conteúdo dos dados”. Ademais, o item 1H3[1] foi retirado da dimensão “disseminação de informação”, pois este tinha uma semelhança com o item anterior (1H2)[2].

Figura 11. Item de verificação da PIT-OSN 1



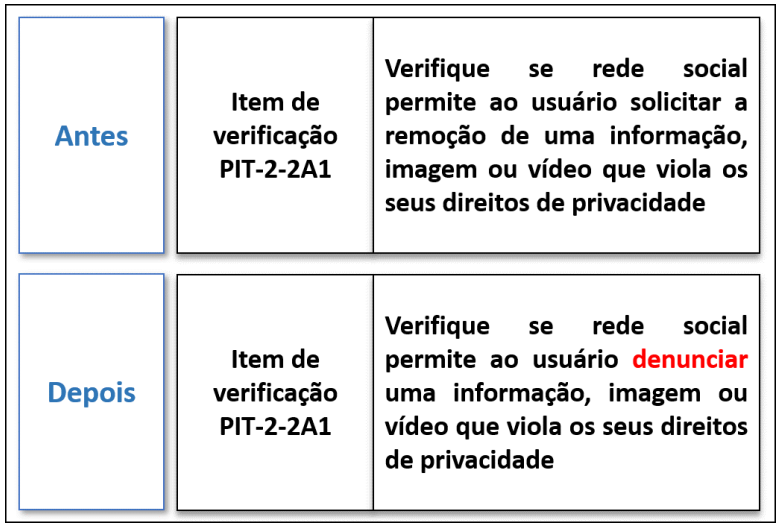
Fonte: Próprio autor.

Em relação à técnica PIT-2, observou-se que um dos itens de verificação poderia estar confuso quanto à sua interpretação. Trata-se do item 2A1 onde é requisitado que seja verificado se a RSO permite ao usuário solicitar a remoção de uma publicação que viola os seus direitos de privacidade. Observou-se que um controle específico para solicitar a remoção de uma determinada publicação seria um termo pouco usado nas interfaces existentes de RSOs. Com isso, modificamos a frase "solicitar remoção" por "denunciar", conforme mostrado na Figura 12. Nesse sentido, caso a rede social não disponibilize um controle para

[1] Item de verificação 1H3 – Verifique se a rede social permite que uma informação sobre um determinado usuário seja compartilhada pela sua audiência sem nenhuma restrição.
[2] Item de verificação 1H2 – Verifique se a rede social permite que uma determinada informação sobre o usuário seja compartilhada por sua audiência sem a sua permissão, porém de uma maneira restrita, apenas para uma audiência adicional limitada (amigos em comum, por exemplo).

denunciar publicações que violam os direitos de privacidade do usuário, tem-se um potencial problema.

Figura 12. Item de verificação da PIT-OSN 2



Fonte: Próprio autor.

Além disso, observou-se também a necessidade em se realizar outras melhorias na estrutura da PIT-OSN 2. O item 2E3[1] da dimensão "curtidas e comentários", o item 2F2[2] da dimensão "bloqueio" e o item 2L2[3] da dimensão "confidencialidade" foram retirados, pois observamos que estes não estavam qualificando um possível problema de privacidade, fugindo do propósito específico da técnica de inspeção. A dimensão 2J (*Gerenciamento de informações do perfil*) teve sua nomenclatura modificada para "Gerenciamento de conta" ficando mais adequada com a descrição dos seus itens de verificação.

Por fim, a PIT-3 também passou por melhorias após a execução do estudo preliminar. As principais adaptações realizadas na técnica foram remoções e ajustes na estrutura. A dimensão 3H (*Garantia*) e seu item de verificação foram retirados em razão de não estarem qualificando um potencial problema nas políticas de privacidade. O item 2A3 da dimensão "coleta de dados" também foi eliminado visto que este estava similar ao item 3B3 da dimensão "uso e divulgação de dados". O item 3C2[4] da dimensão "armazenamento de dados"

[1] Item de verificação 2E3 – Verifique se a rede social permite que uma solicitação de amizade fique com status pendente caso o usuário opte por não aceitar imediatamente.
[2] Item de verificação 2F2 – Verifique se o usuário tem a opção de desbloquear um indivíduo.
[3] Item de verificação 2L2 – Verifique se o usuário tem a opção de escolher se deseja exibir novamente em seu perfil uma publicação ocultada ou arquivada.
[4] Item de verificação 3C2 – Verifique se há alguma declaração sobre quais informações são opcionais antes de conceder ao usuário acesso a rede social.

também foi removido, dado que este não estava evidenciando um problema de privacidade no cenário das políticas.

5.5 LIMITAÇÕES DO ESTUDO PRELIMINAR

As limitações deste estudo preliminar estão relacionadas, principalmente, a três itens: (1) ao tamanho da amostra; (2) a rede social utilizada como objeto de inspeção; e (3) ao processo de inspeção parcial utilizado no estudo.

Em relação ao item 1, o pequeno número de participantes não é considerado o ideal do ponto de vista estatístico. Portanto, há limitação nos resultados, sendo estes considerados indícios e não conclusivos. Porém, este foi um estudo inicial para verificar a validade do conjunto de técnicas e coletar as oportunidades de melhorias para realização de estudos mais amplos. No que diz respeito ao item 2, a rede social utilizada como objeto de inspeção (*Instagram*) corresponde a um sistema real. No entanto, não é possível afirmar que a aplicação representa todos os tipos de redes sociais existentes. Por fim, em relação ao item 3, nota-se que com uma inspeção parcial, ganha-se insumos sobre a validade da proposta como técnica de inspeção a qual pode ser aplicada de forma independente. Ganha-se também o conhecimento necessário para a aplicação de cada técnica e o tempo gasto com as aplicações. No entanto, a principal limitação está relacionada a perda da opinião dos participantes sobre o potencial de benefícios que a inspeção integrada (com as três técnicas em conjunto) permitiria explorar.

5.6 CONSIDERAÇÕES SOBRE O CAPÍTULO

Este capítulo apresentou o planejamento, execução e resultados de um estudo preliminar realizado com o conjunto de técnicas PIT-OSN. Neste primeiro estudo, os resultados obtidos demonstram que as três técnicas foram capazes de cumprir os objetivos de avaliação as quais se propõem, considerando que estas foram aplicadas em um contexto de aplicação móvel (*Instagram*). Com isso, observa-se que a questão da mobilidade não serviu como barreira para proceder a inspeção, uma vez que os objetivos de detectar defeitos foram plenamente alcançados. Com base nos resultados deste estudo preliminar, foram realizados ajustes e melhorias gerais no conjunto de técnicas PIT-OSN. Desse modo, novas versões das técnicas foram elaboradas para serem testadas nos próximos estudos, conforme descrito no capítulo a seguir.

CAPÍTULO 6 – AVALIAÇÃO E EVOLUÇÃO DAS TÉCNICAS PIT-OSN ATRAVÉS DE ESTUDOS DE VIABILIDADE

Este capítulo descreve dois estudos de viabilidade executados para avaliar empiricamente e aperfeiçoar o conjunto de técnicas PIT-OSN. Os resultados desses estudos indicam a viabilidade das técnicas propostas.

6.1 INTRODUÇÃO

Estudos empíricos devem ser realizados e repetidos para melhorar a qualidade da proposta que está sendo desenvolvida, tornando público a outros pesquisadores o conhecimento utilizado na execução de uma avaliação empírica e possibilitando, desta forma, um melhor entendimento e análise do estudo realizado. A principal finalidade com a execução e repetição de estudos empíricos é construir um corpo de conhecimento baseado em experimentação que identifica as vantagens e os custos das diferentes técnicas e ferramentas propostas (SHULL *et al.*, 2004).

Este capítulo apresenta a execução de dois (02) estudos de viabilidade, conforme apresentado na metodologia do trabalho. Estes estudos testaram se a nova tecnologia era viável e se o tempo empregado para executar sua proposta foi bem utilizado, possibilitando assim verificar a possibilidade de uso e o aprimoramento das técnicas concebidas. A seguir serão descritos o planejamento, execução e resultados obtidos com os experimentos realizados.

6.2 1º ESTUDO DE VIABILIDADE COM A PIT-OSN

O propósito deste primeiro estudo de viabilidade foi responder a seguinte questão: "*O conjunto de técnicas PIT-OSN é viável em relação ao número de defeitos encontrados*?". Este estudo foi executado no período de Junho de 2018. O objetivo, conforme o paradigma GQM (BASILI e ROMBACH, 1988), é descrito a seguir:

Analisar	as técnicas PIT-OSN
Com o propósito de	caracterizá-las
Em relação à	viabilidade (número de defeitos detectados)
Do ponto de vista	dos pesquisadores das técnicas
No contexto de	uma inspeção de privacidade em uma RSO por alunos de graduação e pós-graduação

Após a definição do objetivo do estudo, serão descritas a seguir as etapas que compuseram o planejamento da avaliação de viabilidade.

a. Contexto

A rede social *Instagram*, em sua versão para dispositivos móveis, foi escolhida novamente como objeto de inspeção. Essa escolha foi feita por dois critérios: expansão e mobilidade. Em relação à expansão, podemos notar o crescimento exponencial do *Instagram* como serviço de rede social, considerando a quantidade e diversidade de usuários. Em relação à mobilidade, a versão mobile do *Instagram* evidencia a tendência de uso desses aplicativos em smartphones, tornando-se relevante a avaliação por inspeção dessas tecnologias sociais móveis. Além disso, uma avaliação mais ampla, com um número maior de inspetores, seria interessante no sentido de verificar se novos defeitos seriam detectados com o auxílio da nova versão das técnicas nesta rede social alvo.

b. Seleção dos participantes

Dezenove (19) participantes dos cursos de Ciência da Computação e Pós-Graduação em Informática (16 alunos de graduação e 3 alunos de pós-graduação), da Universidade Federal do Amazonas, foram selecionados. Esses participantes cursavam a disciplina de Segurança da Informação e foram escolhidos por critérios de conveniência. Estes participantes assinaram um Termo de Consentimento Livre e Esclarecido (TCLE) e preencheram um Formulário de Caracterização para identificar a experiência deles em avaliação de interface (AI) e a experiência no domínio da aplicação (EDA) escolhida como objeto de inspeção (*Instagram*).

c. Projeto experimental

Os participantes foram alocados em três grupos, um para cada PIT-OSN. Os grupos da PIT-OSN 1 e PIT-OSN 2 foram compostos por 06 participantes cada e o grupo da PIT-OSN 3 por 7 integrantes. Ressalta-se que os participantes foram designados para cada grupo de forma aleatória e balanceada, considerando o nível de experiência de cada participante e o conhecimento do domínio da aplicação.

d. Instrumentação

Diversos artefatos foram definidos para apoiar a execução do estudo, tais como: formulários de caracterização, termo de consentimento livre e esclarecido (TCLE), as diretrizes para a execução das inspeções, uma planilha para a anotação das discrepâncias identificadas, a taxonomia para a classificação de defeitos e um questionário pós-inspeção, os quais estão disponíveis no Apêndice C.

e. Preparação

Seguindo a primeira etapa de preparação do processo de avaliação da PIT-OSN, foram organizados os procedimentos das inspeções, os recursos das técnicas e as atividades a serem executadas durante a avaliação. Além disso, nesta etapa, foi realizada uma única apresentação para todos os participantes do estudo contendo toda a contextualização e exemplificação prática das técnicas. Para cada técnica de inspeção foi mostrado um possível problema de privacidade que ocorria em uma determinada RSO. Foram escolhidos como exemplos para ilustrar violações de privacidade durante a preparação, redes sociais diferentes da escolhida (*Instagram*) como objeto de inspeção, descartando qualquer viés. Todas as eventuais dúvidas que surgiram quanto à explicação de algum ponto das técnicas foram imediatamente esclarecidas. O tempo total da preparação durou aproximadamente 45 minutos.

6.2.1 Execução do 1º Estudo de Viabilidade

A segunda atividade do processo de avaliação usando a PIT-OSN é a detecção de defeitos, na qual cada inspetor procura defeitos de privacidade individualmente na RSO sob inspeção. No começo do estudo, um pesquisador (autor da dissertação) atuou como monitor, sendo responsável por acompanhar os grupos e passar as informações pertinentes à avaliação. Cada participante recebeu os artefatos descritos na seção 6.2 (instrumentação). Durante a inspeção, cada participante preencheu uma planilha reportando as discrepâncias detectadas juntamente com a classificação das mesmas e a justificativa sobre elas. Todos os participantes devolveram as planilhas contendo os possíveis defeitos e o tempo total gasto na inspeção. Eles também entregaram o questionário pós-inspeção preenchido. Durante a atividade de detecção, os inspetores não receberam qualquer ajuda do monitor do estudo e não conversaram entre si.

6.2.2 Coleção e Discriminação do 1º Estudo de Viabilidade

Os participantes do estudo poderiam ter realizado todas as etapas do processo de avaliação da PIT-OSN. No entanto, para evitar que o estudo ficasse prolongado e dispendioso, as etapas de coleção e discriminação foram realizadas à parte por outros pesquisadores.

A etapa de coleção foi realizada pelo autor desta dissertação e sua coorientadora, ambos especialistas nas técnicas. Após a detecção de defeitos, as listas de discrepâncias produzidas pelos inspetores foram integradas em listas únicas referentes à cada técnica (lista única de discrepâncias da PIT-OSN 1, PIT-OSN 2 e PIT-OSN 3).

A partir destas listas únicas, os pesquisadores realizaram a coleção, ou seja, a eliminação de discrepâncias repetidas (encontradas por mais de um inspetor) gerando uma lista de discrepâncias sem duplicatas para ser analisada na etapa de discriminação. Esta etapa durou aproximadamente 3 horas.

Outros dois pesquisadores, com conhecimento prático sobre as técnicas PIT-OSN, realizaram a etapa de discriminação. Ou seja, nesta etapa, as discrepâncias detectadas pelos inspetores (participantes do estudo) foram classificadas como falso-positivos ou como problemas de privacidade. Os falso-positivos foram descartados, pois estes representavam os pontos identificados que não eram defeitos de privacidade e os problemas reais de privacidade foram registrados em uma lista única de defeitos referente a cada técnica. Esta fase teve duração de 2 horas.

6.2.3 Resultados Quantitativos do 1º Estudo de Viabilidade

A Tabela 24 apresenta uma visão geral dos resultados das inspeções de privacidade na rede social selecionada como objeto de inspeção. O rótulo "P" e um número identificam cada participante, por exemplo, P01 identifica o participante 01. Os participantes P01 a P06 aplicaram a PIT-OSN 1. Os participantes P07 a P12 aplicaram a PIT-OSN 2 e os participantes P13 a P19 aplicaram a PIT-OSN 3.

Em relação à **PIT-OSN 1**, a inspeção com esta técnica resultou em um total de 53 discrepâncias identificadas. Após a reunião de coleção, foi verificado que 35 discrepâncias estavam repetidas e somente 18 eram discrepâncias únicas. Com base na reunião de discriminação, os pesquisadores identificaram que das 18 discrepâncias restantes, 6 eram falso-positivos e 12 eram defeitos reais relacionados aos níveis de privacidade da aplicação.

Pode-se observar também, através da Tabela 24, que os inspetores que aplicaram a PIT-OSN 1 encontraram entre 6 e 9 defeitos gastando em torno de 33 a 73 minutos. Os inspetores P01 e P02 não tinham experiência em avaliação de interface (mas conheciam o domínio de aplicação) e conseguiram detectar defeitos. Os inspetores P03, P04 e P06 tinham experiência em avaliação de interface (mas não conheciam o domínio da aplicação) e conseguiam diagnosticar defeitos. Portanto, pode-se notar que nem a experiência em AI e nem o conhecimento do domínio do sistema parecem ter influenciado a detecção de defeitos feita pelo inspetores com o uso da técnica PIT-OSN 1.

Tabela 24. Resultados das inspeções com as técnicas PIT-OSN

Part.	EAI	EDA	DS	FP	DF	Tempo (min)	Defeito /(hora)	Técnica
P01	Não	Sim	8	0	8	67	7,16	PIT-1
P02	Não	Sim	7	0	7	40	10,50	
P03	Sim	Não	10	2	8	41	11,71	
P04	Sim	Não	11	2	9	45	12,00	
P05	Sim	Sim	10	1	9	33	16,36	
P06	Sim	Não	7	1	6	73	4,93	
P07	Sim	Sim	14	6	8	69	6,96	PIT-2
P08	Não	Sim	8	4	4	56	4,29	
P09	Sim	Sim	11	0	11	54	12,22	
P10	Sim	Sim	9	7	2	50	2,40	
P11	Sim	Sim	7	2	5	59	5,08	
P12	Sim	Sim	14	3	11	52	12,69	
P13	Sim	Não	5	1	4	60	4,00	PIT-3
P14	Não	Não	3	0	3	27	6,67	
P15	Sim	Não	13	5	8	46	10,43	
P16	Sim	Não	4	1	3	33	5,45	
P17	Não	Não	7	1	6	45	8,00	
P18	Sim	Sim	3	2	1	29	2,07	
P19	Não	Sim	3	0	3	35	5,14	

Legenda:
Part.. - Participante; **AI** – Experiência em Avaliação de Interface; **EDA** – Experiência no Domínio da Aplicação; **DS** – Número de Discrepâncias; **FP** – Número de Falso-Positivos; **DF** – Número de Defeitos por hora;

Fonte: Próprio autor.

No que diz respeito à **PIT-OSN 2**, a inspeção com esta técnica possibilitou detectar, no geral, 63 discrepâncias. Destas, 22 estavam duplicadas e 41 eram discrepâncias únicas. Com base na reunião de discriminação foi identificado que, destas 41 discrepâncias, 22 eram falso-positivos e 19 eram defeitos reais referentes aos controles de privacidade da aplicação avaliada.

Os inspetores que utilizaram a PIT-OSN 2 encontraram entre 2 e 11 defeitos gastando cerca de 50 e 69 minutos. Todos os participantes que aplicaram a PIT-OSN 2 tinham experiência em avaliação de interface, exceto o participante P08 que não possuía experiência em AI, e conhecimento no domínio da aplicação. Os resultados indicam que os participantes P09 e P11 foram os que detectaram a maior quantidade de defeitos (11 defeitos) nos controles de privacidade em comparação aos outros inspetores.

Por fim, a inspeção com a **PIT-OSN 3** permitiu identificar um total de 38 discrepâncias. Após a execução da coleção, identificaram-se 19 discrepâncias duplicadas e 19 discrepâncias únicas. Destas 19 únicas, 10 foram classificadas como falso-positivos e 9 como defeitos reais pertinentes as políticas de privacidade da aplicação inspecionada.

Os inspetores que aplicaram a PIT-OSN 3 encontraram entre 1 a 8 defeitos gastando cerca de 27 e 60 minutos. Com base nos dados fornecidos pela Tabela 24, nota-se que o diagnóstico de defeitos produzido pelo participante P18 foi baixo (1 defeito). Ao observar o tempo de inspeção gasto pelo participante 18, nota-se que o mesmo levou 29 minutos na atividade de detecção. O inspetor P14, por sua vez, gastou 27 minutos na inspeção e produziu um diagnóstico de defeitos maior (3 defeitos). Desta forma, acredita-se que um dos fatores que pode ter ocasionado a detecção de um pequeno número de defeitos pelo inspetor 18, seria a falta de empenho deste participante durante a inspeção. Com isso, a PIT-OSN 3 foi a técnica que teve o menor tempo gasto no processo de inspeção comparado a PIT-OSN 1 e PIT-OSN 2.

A Tabela 25 apresenta os números totais obtidos a partir da inspeção com o conjunto de técnicas PIT-OSN. Com base nestes dados, nota-se que a PIT-OSN 1 e a PIT-OSN 3 foram as técnicas que fornecerem a menor quantidade de falso-positivos, totalizando 16 identificados por ambas, enquanto a PIT-OSN 2 detectou 22 falso-positivos. O baixo grau de falso-positivos pode ser explicado pelo fato de que a PIT-1 e PIT-3 fornecem uma quantidade menor de itens de verificação para detectar defeitos de privacidade. No entanto, a técnica PIT-OSN 2, por abranger a maior quantidade de itens de verificação, foi a técnica que gerou o maior diagnóstico de defeitos de privacidade do conjunto. Ou seja, uma quantidade maior de itens de verificação pode ser um fator que prolonga o tempo de inspeção, todavia, oferece como benefício a geração de um maior diagnóstico de defeitos buscando fomentar a reflexão e interpretação do inspetor.

Tabela 25. Dados gerais do 1º estudo de viabilidade

Dados Gerais	**Técnicas**		
	PIT-1	**PIT-2**	**PIT-3**
Total de discrepâncias detectadas	53	63	38
Total de defeitos (incluindo os duplicados)	47	41	28
Total de defeitos (sem duplicatas)	12	19	09
Total de Falso-Positivos	6	22	10
Tempo total gasto nas inspeções (min)	299	340	275

Fonte: Próprio autor.

Desta forma, os resultados deste primeiro estudo de viabilidade demonstram que todos os inspetores foram capazes de detectar defeitos, independentemente da experiência em avaliação de interfaces ou do conhecimento no domínio da aplicação. Isto pode ser um indicador de que o conjunto de técnicas PIT-OSN habilita inspetores com diferentes níveis de experiência a diagnosticar defeitos, reduzindo, portanto, a dependência da experiência dos avaliadores, tal como sugerido no estudo preliminar.

Com base nestes dados quantitativos, nota-se que o resultado obtido neste primeiro estudo de viabilidade foi positivo, mostrando que o conjunto de técnicas PIT-OSN atende seu objetivo geral de apoiar a detecção de defeitos, sendo, portanto, viável para uso em inspeções de privacidade. A partir da análise dos defeitos apontados por cada inspetor (dados quantitativos) uma questão de pesquisa foi levantada para posterior investigação.

Uma próxima questão a ser averiguada é se o custo-eficiência apresentado pelo conjunto de técnicas é equivalente ou superior ao custo-eficiência apresentado por outra abordagem, visto que este é um fator crítico de sucesso na adoção/utilização de uma técnica de inspeção. Nesse estudo, não foi possível estabelecer uma relação comparativa com outra técnica em termos de eficiência (razão entre o número de defeitos por tempo de inspeção) e eficácia (razão entre o número de defeitos detectados e o número total de defeitos) de inspeção. Por esse motivo, optou-se por não aplicar uma análise estatística dos dados quantitativos obtidos desse primeiro estudo. Decidiu-se realizar um novo estudo de viabilidade com o propósito de medir a viabilidade do conjunto de técnicas em relação aos indicadores de eficiência e eficácia em comparação com outra técnica, esse estudo será mostrado na seção 6.3.

6.2.4 Análise da Percepção dos Participantes do 1º Estudo de Viabilidade

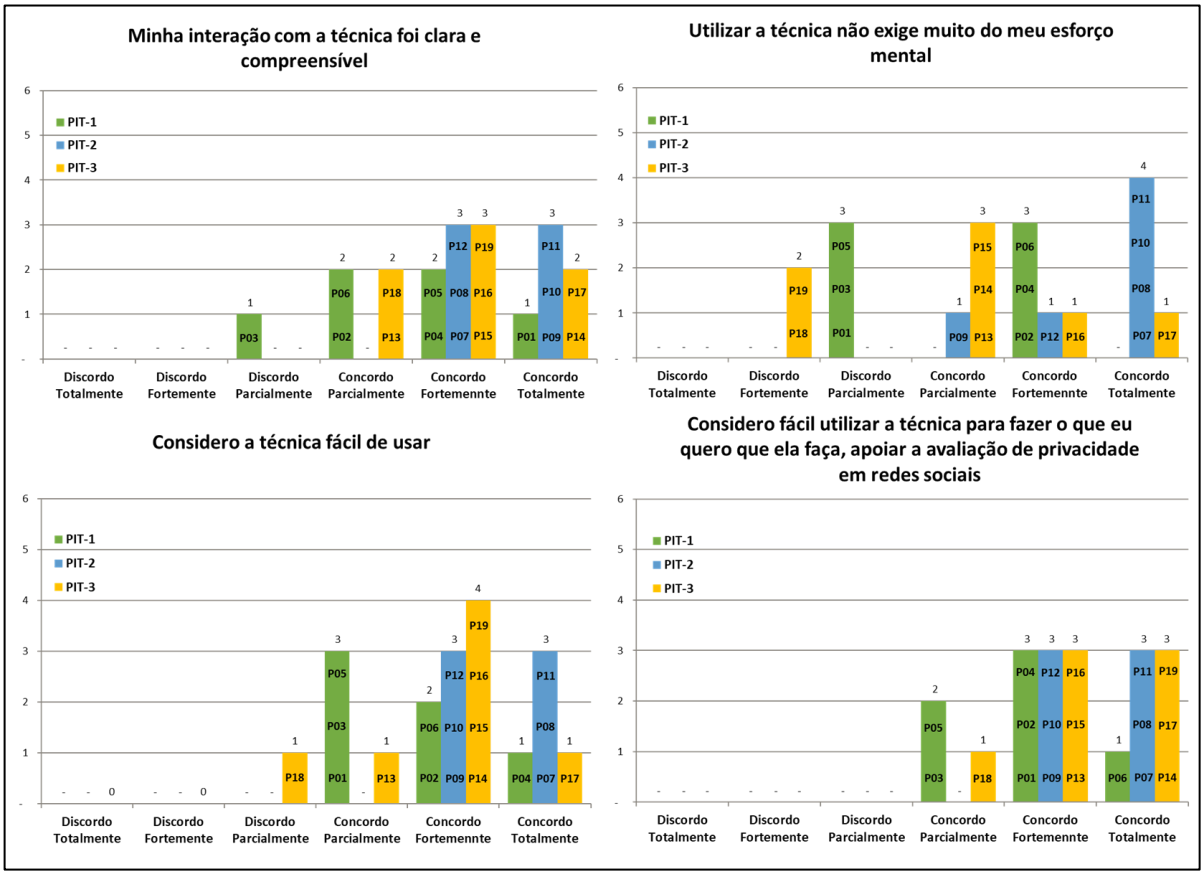
Os participantes responderam seu grau de aceitação em relação ao conjunto de tecnologias através de um questionário pós-inspeção. Este questionário também foi elaborado com base nos indicadores do modelo TAM (*Technology Acceptance Model*). Os indicadores utilizados foram: (i) facilidade de uso percebida; (ii) utilidade percebida; e (iii) intenção de uso futuro.

a. Facilidade de Uso Percebida

A Figura 13 apresenta a resposta dos participantes em relação ao indicador de facilidade de uso percebida. Cada participante reportou o seu grau de aceitação de acordo com

a técnica a qual aplicou durante o estudo. A percepção dos participantes está representada através de gráficos (Figura 13), em que o eixo vertical representa o número de participantes e eixo horizontal refere-se as possíveis respostas do questionário pós-inspeção. Nas barras foram inseridos códigos que simbolizam os participantes da Tabela 24.

Figura 13. Percepção sobre Facilidade de Uso – 1º Estudo de Viabilidade



Fonte: Próprio autor.

Ao analisar a Figura 13, pode-se observar que o participante P03, do grupo da PIT-OSN 1, discordou parcialmente em relação à afirmativa "*Minha interação com a técnica foi clara e compreensível*". Considerando os dados da Tabela 24, percebe-se que o participante P03 reportou não ter conhecimento sobre o domínio da aplicação inspecionada, o que pode ter influenciado para a discordância do participante em questão. No entanto, no contexto de uma avaliação em um projeto real, o mais comum seria o inspetor não conhecer o objeto de inspeção.

O participante P18, do grupo da PIT-OSN 3, discordou parcialmente da afirmativa "*Considero a técnica fácil de usar*", já o participante P13, do grupo da PIT-OSN 3, e os participantes P01, P03 e P05, do grupo da PIT-OSN 1, concordaram parcialmente com esta

mesma afirmativa supracitada. Tal questão pode ser um indicador de que alguns passos da PIT-OSN 1 e PIT-OSN 3 podem não ser tão fáceis de usar e precisam ser melhorados.

A afirmativa "*Usar a técnica não exige muito do meu esforço mental*" também obteve discordâncias entre os participantes da PIT-OSN 1 (P01, P03, P05) e entre os participantes da PIT-OSN 3 (P18, P19). Assim como no estudo preliminar, houve novamente discordâncias em relação a afirmativa em questão. Estes resultados sugerem as técnicas PIT-OSN 1 e PIT-OSN 3 podem exigir uma maior concentração por parte do inspetor. Por serem técnicas de leitura, as mesmas podem demandar um potencial esforço para ler e interpretar o que elas instruem o inspetor a fazer.

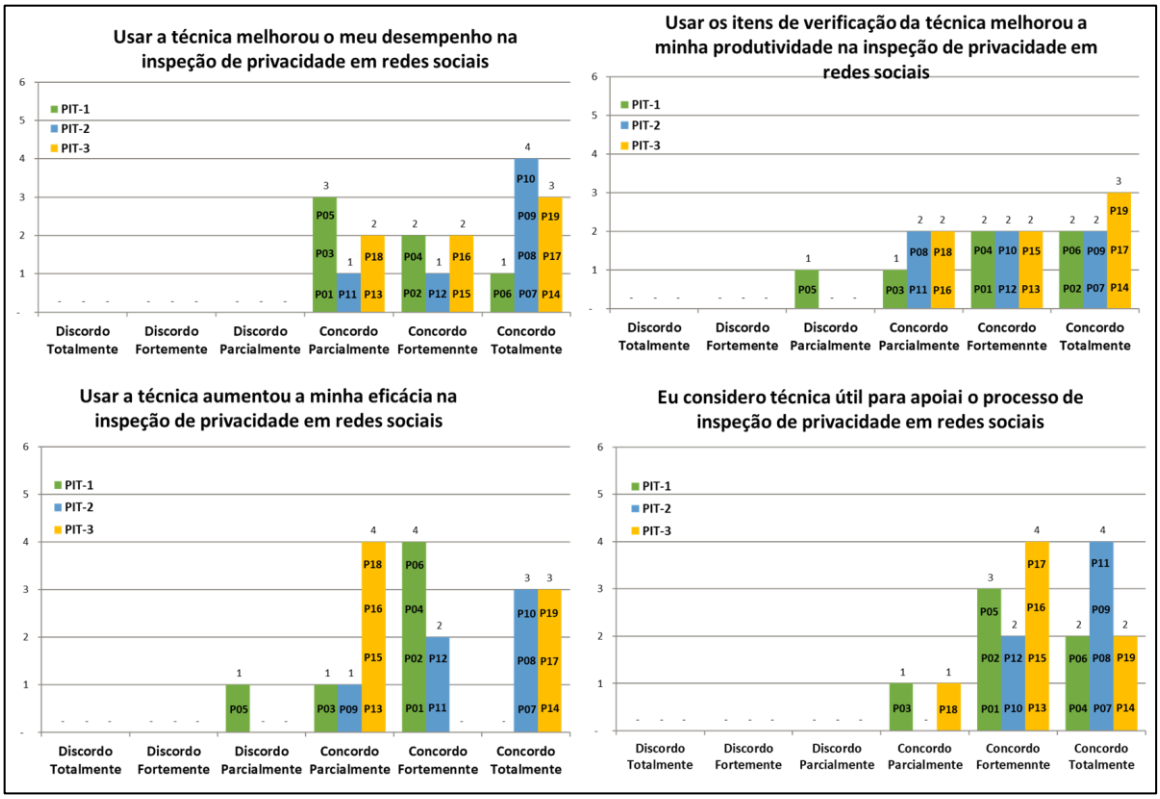
Em relação à afirmativa "*Considero fácil utilizar a técnica para fazer o que eu quero que ela faça, apoiar a avaliação de privacidade em RSOs"*, observa-se que não houveram discordâncias. Tal questão reflete um ponto positivo, pois evidencia que o conjunto de técnicas foi fácil de usar para cumprir o seu principal objetivo, apoiar a inspeção de privacidade em RSOs. Além disso, um outro ponto relevante a ser ressaltado é que nenhum participante do grupo da PIT-OSN 2 discordou das afirmativas do indicador em foco, demonstrando que houve facilidade de uso com a aplicação desta técnica.

b. Utilidade Percebida

A Figura 14 apresenta a percepção dos participantes em relação ao indicador utilidade para o conjunto de técnicas PIT-OSN.

A partir da visão fornecida pela Figura 14, percebe-se que somente o participante P05 do grupo da PIT-OSN 1 discordou parcialmente de duas afirmativas sobre a utilidade da técnica e justificou através do seguinte argumento "*Tive dificuldade para entender a ideia inicial da técnica"*. Isso indica que, em algum momento na etapa de preparação, o inspetor encontrou dificuldade quanto a proposta inicial da técnica a qual aplicou. No entanto, todos os demais participantes concordaram com as sentenças deste indicador, demonstrando que, no geral, as técnicas foram consideradas úteis para serem aplicadas em uma inspeção de privacidade de RSOs.

Figura 14. Percepção sobre Utilidade – 1º Estudo de Viabilidade

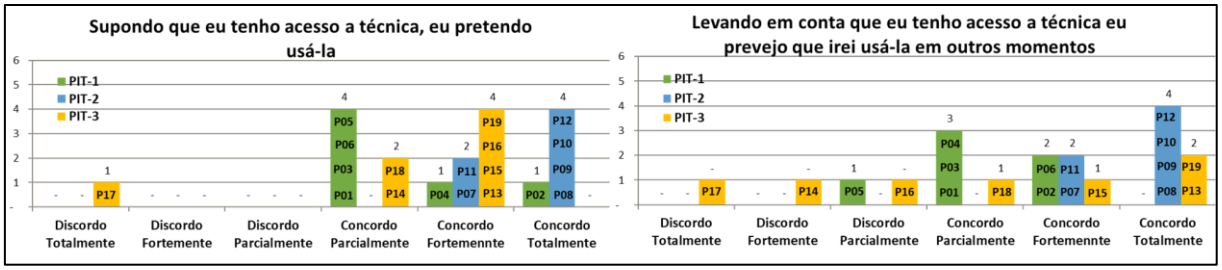


Fonte: Próprio autor.

c. Intenção de Uso

Por fim, a Figura 15 apresenta a percepção dos participantes em relação ao indicador intenção de uso futuro.

Figura 15. Percepção sobre Intenção de Uso – 1º Estudo de Viabilidade



Fonte: Próprio autor.

Nota-se que a técnica PIT-OSN 3 foi a que teve o maior número de discordâncias em relação às sentenças do indicador de intenção de uso futuro. Isto indica que alguns participantes do grupo da PIT-OSN 3 não presumem usar a técnica em projetos futuros. Algumas discordâncias também podem ser justificadas, pois caso o participante não pretenda trabalhar com projeto e avaliação de RSOs, provavelmente este não prever utilizar a técnica

em outros momentos. Nesse sentido, o grau de discordância pode estar mais relacionado com uma decisão de carreira e não pelo uso da técnica em si.

Em relação ao grupo da PIT-OSN 1 houve apenas uma discordância referente à uma afirmativa do indicador em questão, todavia, a maioria dos inspetores concordaram que usariam a técnica de níveis em momentos posteriores. Por fim, no grupo da PIT-OSN 2 não houveram discordâncias e todos os participantes concordaram que aplicariam a técnica de controles em projetos futuros.

6.2.5 Resultados Qualitativos do 1º Estudo de Viabilidade

Uma análise específica com relação aos comentários dos participantes (dados qualitativos) obtidos através de perguntas abertas contidas no questionário pós-inspeção foi realizada. Esta análise foi efetuada com base nos procedimentos sugeridos pelo método *Grounded Theory* - GT (CORBIN e STRAUSS, 2008).

A partir da aplicação do método GT foi possível analisar os dados qualitativos que foram extraídos dos questionários pós-inspeção usando um subconjunto de fases do processo de codificação sugerido por Corbin e Strauss (2008) para o método em questão. Este processo de codificação contém as seguintes fases: codificação aberta (primeira fase) e axial (segunda fase).

Para analisar as citações (trechos das respostas) foram criados códigos para todos os comentários dos participantes (conceitos importantes para entendimento da percepção sobre as técnicas e seus processos de aplicação) – codificação aberta (primeira fase). Em seguida, os códigos foram agrupados de acordo com suas propriedades, formando conceitos que representam categorias. Por fim, cada código criado foi relacionado a uma categoria – codificação axial (segunda fase). Uma vez que a intenção deste estudo não é criar uma teoria, não foi realizada a codificação seletiva (terceira fase do método GT). As fases de codificação aberta e axial foram suficientes para entender as causas de alguns problemas na aplicação do conjunto de técnicas. Os conceitos específicos relacionados ao método GT são apresentados em detalhes em Corbin e Strauss (2008).

O questionário pós-inspeção possuía questões abertas para coletar o ponto de vista dos participantes sobre os pontos positivos e negativos sobre a estrutura da técnica, dificuldades de uso com a técnica e sugestões de melhorias para a técnica, o que levou à identificação destas duas categorias: Dificuldade de Aplicação e Estrutura da Técnica. A categoria "Dificuldade de aplicação" representa os pontos que dificultaram o entendimento dos participantes no processo de aplicação das técnicas". Já a categoria "Estrutura da técnica"

representa os pontos positivos e negativos em relação à formulação e caracterização de todos os recursos das técnicas.

A seguir serão apresentadas as categorias geradas, bem como uma análise em relação aos códigos criados a partir dos comentários dos participantes do estudo. A apresentação destas análises é feita por técnica, conforme descrito abaixo.

a. Categoria 1 - Dificuldade de aplicação da PIT-OSN 1

Em relação à PIT-OSN 1, algumas das dificuldades que foram coletadas no que diz respeito à aplicação da técnica foram: um ponto negativo da PIT-OSN 1 é a necessidade de ter experiência na RSO inspecionada (ver citação de P02 abaixo); um ponto negativo da PIT-OSN 1 é que é um pouco trabalhosa (ver citação de P01 abaixo); alguns itens de verificação da PIT-OSN 1 permitem encontrar o mesmo defeito (ver citação de P06 abaixo); uma dificuldade foi a semelhança entre alguns tipos de defeitos encontrados (ver citação de P01);

"*É preciso fazer bastante exploração na rede social em questão ou ter muita experiência"* (Participante 2).

"*(...) é um pouco trabalhosa"* (Participante 1).

"*Alguns itens ficaram com defeitos iguais, sendo assim ficou difícil a compreensão da diferença de ambos*" (Participante 6).

"*A maior dificuldade é a semelhança entre alguns tipos de defeitos em alguns problemas encontrados*" (Participante 1).

A partir dessas análises, pôde-se compreender alguns pontos que ocasionaram alguma dificuldade de aplicação com a técnica PIT-OSN 1. Um dos pontos a ser destacado pode ser observado no discurso do participante P02, o qual reportou: "*Para realizar uma inspeção com a PIT-OSN 1, o inspetor deve fazer bastante exploração [no sistema] ou ter muita experiência na aplicação"*. Tal observação pode ser um indicador de que a PIT-OSN 1 pode não ser clara e compreensível para pessoas sem conhecimento sobre a aplicação a qual será inspecionada. Tal questão corrobora a suposição feita na análise do TAM, onde um participante discordou sobre uma sentença relacionada a clareza e compreensão da técnica em questão e este inspetor não tinha conhecimento do domínio do sistema.

Pode-se observar também que houveram outras dificuldades e uma delas precisa ser destacada: há itens de verificação que podem estar semelhantes ou ambíguos, fazendo com que o inspetor encontre o mesmo tipo de defeito com itens separados. Com isso, observamos que a relação entre alguns itens de verificação precisava ser revisada com o propósito de situar as redundâncias e reduzi-las.

b. Categoria 2 - Estrutura da PIT-OSN 1

A geração desta categoria revelou algumas inadequações quanto à estrutura da técnica PIT-OSN 1, tais como: há itens de verificação semelhantes (ver comentário de P06 abaixo). Além disso, foi dada uma sugestão para inserir exemplos para cada tipo de defeito com o propósito de facilitar a compreensão para identificar problemas. (ver comentário de P01 abaixo).

"*Poderia alterar a descrição de alguns itens como, por exemplo, 1A1 e 1H1, praticamente são iguais, está ambíguo*" (Participante 6).

"*Acredito que exemplos em cada tipo de problemas facilitaria a compreensão*" (Participante 1).

Em relação à sugestão fornecida, nota-se que se forem inseridos exemplos para facilitar na detecção de defeitos, a técnica pode ficar menos abrangente/genérica e muito específica. Ou seja, tal sugestão pode fazer com que o inspetor fique recluso aos exemplos de defeitos contidos no documento da técnica, ao invés de procurar por novos defeitos com base, exclusivamente, na descrição dos itens de verificação. Portanto, achamos que esta sugestão pode não ser viável para ser inserida na estrutura da técnica PIT-OSN 1.

Além disso, houve outra citação representando inadequação no tocante à estrutura da técnica, a saber: alguns itens foram identificados como similares na técnica. Tal citação provavelmente gerou dúvidas durante a utilização da PIT-OSN 1. Nesse sentido, algumas melhorias foram realizadas na PIT-OSN 1 e uma nova versão da técnica (versão 3) foi elaborada, conforme apresentado a seguir.

c. Melhorias na PIT-OSN 1

As análises qualitativas do primeiro estudo de viabilidade levaram à terceira versão da técnica PIT-OSN 1. As descrições de alguns itens de verificação foram modificadas com o objetivo de tornar mais clara a definição dos mesmos e reduzir as redundâncias. O primeiro ponto a ser revisado foi o item 1A1 da dimensão "fonte de informação" e 1H1 da dimensão "disseminação da informação", onde um participante relatou que as descrições estavam semelhantes, conforme destacado na categoria estrutura da PIT-OSN 1.

Em relação à dimensão fonte de informação, observou-se que quando informações pessoais sobre o indivíduo são compartilhadas por outros usuários na RSO, o indivíduo, não possui autonomia para controlar a disseminação da publicação contendo informações **sobre** ele, a partir do momento que esta informação é compartilhada por outro usuário.

Logo, para deixar o item mais claro, retiramos o "por um indivíduo" e inserimos o "sobre o indivíduo", uma vez que o contexto do item é saber se a rede social permite com que **outros usuários** compartilhem informações pessoais sobre um indivíduo e não por um indivíduo, conforme descrito na Tabela 26.

Tabela 26. Melhorias no item de verificação da PIT-OSN 1

1A. Fonte de Informação	
1A1 (versão 2)	Verifique se outro usuário (um amigo ou seguidor) tem autonomia para compartilhar conteúdos publicados por um determinado indivíduo dentro do sistema
1A1 (versão 3)	Verifique se outro usuário (um amigo ou seguidor) tem autonomia para compartilhar conteúdos publicados **sobre um determinado indivíduo** dentro do sistema

Fonte: Próprio autor.

Em relação à dimensão "disseminação de informação", o item 1H1 foi modificado para que não englobasse com o mesmo sentido do item 1A1 da dimensão "fonte de informação". Em linhas gerais, o item 1H1 tratava a questão da audiência ser capaz de re(compartilhar) uma informação do indivíduo no sistema, referindo-se a possibilidade da informação se espalhar através da rede gerando problemas indesejados de privacidade. Desse modo, o termo "re(compartilhar)" foi substituído por "repostar". Para mais, outro complemento foi inserido ao final do item de verificação: *"...sem a sua permissão, ou seja, sem nenhuma restrição*", conforme exposto na Tabela 27. Com isso, a descrição do item torna-se mais clara para detectar se a rede social permite um *repost*, pela audiência, sem qualquer restrição. Além disso, o item IH2[1] foi retirado da dimensão em questão, posto que o mesmo não estava remetendo a identificação de um potencial defeito de privacidade.

Tabela 27. Melhorias no item de verificação da PIT-OSN 1

1H. Disseminação da Informação	
1H1 (versão 2)	Verifique se a rede social permite à audiência (re)compartilhar ou (re)postar com outras pessoas uma publicação de um determinado usuário
1H1 (versão 3)	Verifique se a rede social permite à audiência **repostar** com outras pessoas uma publicação de um determinado usuário **sem a sua permissão, ou seja, sem nenhuma restrição**

Fonte: Próprio autor.

[1] Item de verificação IH2 - Verifique se a rede social permite que uma determinada Informação sobre o usuário seja compartilhada por sua audiência sem a sua permissão, porém de uma maneira restrita, apenas para uma audiência adicional limitada (amigos em comum, por exemplo).

Além disso, outras adaptações foram realizadas no sentido de tornar a descrição de outros itens de verificação, de outras dimensões, mais consistente. Na Tabela 28 são apresentados alguns ajustes efetuados em relação a alguns itens verificação da técnica PIT-OSN 1.

Tabela 28. Melhorias no item de verificação da PIT-OSN 1

1C. Conteúdo de Dados	
1C1 (versão 2)	Verifique se a rede social coleta dados pessoais (como nome, data de nascimento, habilidade profissional por exemplo) e expõe essas informações na própria rede social sem a permissão do usuário
1C1 (versão 3)	Verifique se a rede social coleta dados pessoais (como data de nascimento, **número de telefone, endereço de e-mail** por exemplo) e expõe essas informações na própria rede social sem a permissão do usuário
1E. Audiência	
1E1 (versão 2)	Verifique se a rede social permite fazer publicações que ficam visíveis somente para o próprio usuário - **item retirado, pois não remete um problema de privacidade**
1E1 (versão 3)	Verifique se a rede social permite que uma audiência desconhecida (como amigos em comum por exemplo) possa visualizar determinadas ações do indivíduo no sistema, sem fazer parte da lista de amigos
1E2 (versão 2)	Verifique se a rede social permite compartilhar conteúdos, seletivamente, com pessoas específicas
1E2 (versão 3)	Verifique se a rede social permite que outras pessoas, que não são usuários da rede, tenham acesso ao conteúdo compartilhado pelo indivíduo no sistema

Fonte: Próprio autor.

Após a exposição da avaliação e evolução da técnica PIT-OSN 1, apresenta-se a seguir as análises qualitativas referentes ao uso da técnica PIT-OSN 2. Serão também apresentadas as principais melhorias realizadas na técnica com base nos dados qualitativos extraídos e analisados do questionário pós-inspeção.

a. Categoria 1 - Dificuldade de aplicação da PIT-OSN 2

No que diz respeito à PIT-OSN 2, dificuldades também foram coletadas quanto à aplicação da técnica, tais como: a PIT-OSN 2 é trabalhosa (ver comentário de P10 abaixo); a aplicação da PIT-OSN 2 é cansativa (ver comentário de P08 abaixo); identificar o tipo de defeito na PIT-OSN 2 requer prática (ver comentário de P09 abaixo).

"*(...) trabalhosa e exaustiva".* (Participante 10).

"*(...) fica cansativo no momento de aplicar a técnica*" (Participante 8).

"*Identificar o tipo de defeito requer uma prática e é muito sensível a erros*" (Participante 9).

Nota-se que todas estas dificuldades apontadas em relação à aplicação da PIT-OSN 2 podem estar associadas à quantidade de conteúdo que a técnica fornece para apoiar a inspeção de controles de privacidade, podendo tornar o processo de avaliação mais cansativo. Tal dificuldade pode ser comprovada com base em algumas sugestões de melhorias fornecidas pelos próprios participantes, tais como: sugestão de reduzir a lista de itens de verificação da PIT-OSN 2 (ver comentário de P08 abaixo); sugestão de reduzir o esforço necessário de aplicação da PIT-OSN 2, reduzindo o tempo de aplicação da PIT-OSN 2 (ver comentário de P10 abaixo).

"*Talvez diminuir a listagens de itens*" (Participante 8).

"*Ter uma forma de deixar menos trabalhoso e que não gaste muito tempo"* (Participante 10).

b. Categoria 2 - Estrutura da PIT-OSN 2

Este estudo também revelou pontos na estrutura da PIT-OSN 2 que podem estar inadequados, indicando necessidades de melhorias. A PIT-OSN 2, por abranger a maior quantidade de itens de verificação do conjunto de técnicas, pode conter o procedimento de inspeção como sendo o mais prolongado. Tal suposição pode ser inferida a partir da análise dos seguintes códigos: os itens de verificação da PIT-OSN 2 podem influenciar o tempo de aplicação (ver comentário de P09 abaixo); a lista de itens de verificação da PIT-OSN 2 é um pouco extensa (ver comentário de P08 abaixo).

"*Já há passos listados o que torna a técnica fácil de seguir. Em compensação, isso pode deixar a técnica engessada no tempo*" (Participante 9).

"*Achei a lista um pouco extensa (...)"* (Participante 8).

Por ser a técnica mais ampla, em termos de itens de verificação, a PIT-2 pode necessitar de mais esforço mental, por parte do inspetor, para interpretar e desempenhar o que a mesma direciona a fazer. No entanto, se reduzirmos a técnica, eliminando alguns itens de verificação, a mesma pode não cumprir seu propósito central de apoiar uma completude sobre inspeções em controles de privacidade de RSOs. Não obstante, melhorias serão efetuadas buscando deixar a técnica mais clara e compreensível.

Além disso, este estudo também possibilitou observar que determinados itens de verificação da PIT-OSN 2 podem indicar um ponto problemático em uma determinada RSO, mas que pode ser uma característica desejável em outros contextos de RSOs. Tal reflexão ficou explícita com base no relato do participante P07, o qual relatou "*Algumas instruções [itens de verificação] não se aplicavam ao contexto do app avaliado, deveria ter uma*

abordagem para isto". Nesse sentido, um novo complemento foi inserido na estrutura do conjunto de técnicas, tal como demonstrado na subseção 6.2.6.

c. Categoria 3 – Sugestões de melhorias na PIT-OSN 2

As análises qualitativas em relação ao primeiro estudo de viabilidade levaram a revisão da técnica PIT-OSN 2, possibilitando efetuar as seguintes melhorias:

- O item 2A3[2] foi retirado da dimensão "direito de privacidade", posto que não estava evidenciando um potencial defeito relacionado a controles de privacidade.
- A dimensão "curtidas e comentários" teve a sua nomenclatura alterada para "comentários", visto que a mesma só retrata itens de verificiação relacionados a comentários.
- Um novo item de verificação foi inserido na dimensão "comentários", o qual permite inspecionar se uma determinada rede social possibilita criar um filtro avançado que bloqueia comentários impróprios que podem causar problemas de privacidade.

Por fim, serão apresentadas a seguir as análises qualitativas com relação à aplicação da técnica PIT-OSN 3.

a. Categoria 1 - Dificuldade de aplicação da PIT-OSN 3

Em relação à PIT-OSN 3, algumas dificuldades também foram coletadas quanto à aplicação da técnica, sendo que alguns participantes expressaram suas dificuldades sobre o procedimento de aplicação da técnica em questão:

> "*Revisar o documento se tornou um pouco cansativo depois de um tempo*" (Participante 15).
>
> "*Confundi quais seriam os itens certos* (...)" (Participante 18).
>
> "*Demora um pouco para saber/entender onde cada item inspecionado se encaixa*" (Participante 16).

Uma das principais dificuldades observadas quanto à aplicação da PIT-OSN 3 nas políticas da rede social avaliada, trata-se da interpretação quanto à estrutura e adequação do documento das políticas que, muitas das vezes, contemplam textos extensos com jargões técnicos, sem padrões de escrita e muito complexos de compreender. Embora os itens de verificação guiem o inspetor a detectar um potencial defeito neste cenário, o processo de

[2] Item de verificação 2A3 – Verifique se a rede social permite denunciar uma publicação de conteúdos que violem os direitos de propriedade intelectual do usuário, como direitos autorais e de marca comercial.

inspeção com a PIT-OSN 3 pode se tornar cansativo se o conteúdo das políticas estiver desordenado. Tal questão já representa um defeito quanto a representação do documento.

b. Categoria 2 - Estrutura da PIT-OSN 3

Por fim, esta categoria retrata os principais pontos extraídos relacionados à estrutura da técnica em questão, onde destacam-se os seguintes códigos:

Os itens de verificação da PIT-OSN 3 contemplam a identificação de todos os defeitos –"*Acredito que os [itens] já existentes estão contemplando a todos os defeitos encontrados"* (P13).

A PIT-OSN 3 permite inspecionar um documento de políticas de privacidade – "*Ler efetivamente sobre as políticas de privacidade*" (P17).

Os itens de verificação da PIT-OSN 3 conseguem direcionar o processo de inspeção –"*Pontos positivos é que o checklist direciona a inspeção*" (P15).

Para revisar um item de verificação da PIT-OSN 3 é necessário reler o documento das políticas de privacidade – "(...) *visto que para revisar o ponto solicitado no checklist é necessário reter o documento para encontrar o texto em questão*" (P15).

c. Categoria 3 – Sugestões de melhorias na PIT-OSN 3

Após as análises qualitativas, observou-se que poucos ajustes na estrutura da técnica PIT-OSN 3 seriam necessários, uma vez que nenhum participante reportou uma dificuldade quanto a um item de verificação específico. Portanto, somente a descrição de itens de verificação foram ajustadas com o propósito de melhorar sua explicação, conforme exposto na Tabela 29.

Tabela 29. Melhorias no item de verificação da PIT-OSN 3

3C. Armazenamento de Dados	
3C1 (versão 2)	Verifique se há declarações sobre como a rede social armazena e processa (se em banco de dados ou nuvem por exemplo) os dados coletados do usuário.
3C1 (versão 3)	Verifique se há declarações sobre como a rede social armazena e processa (se em bancos de dados **de outros países**) os dados coletados do usuário

Fonte: Próprio autor.

A partir dos resultados obtidos com esta análise qualitativa, foi possível explorar o entendimento e as principais dificuldades dos participantes do estudo ao empregar o conjunto de técnicas PIT-OSN em inspeções de privacidade. A categoria *Dificuldade de Aplicação* permitiu analisar as principais dificuldades que os participantes encontram ao aplicar as técnicas. Além disso, esta categoria também permitiu observar a justificativa para algumas

das discordâncias sobre as afirmativas de facilidade de uso e utilidade do TAM. Ademais, os códigos relacionados a esta categoria podem ser considerados como indícios que impactaram o tempo de aplicação que alguns participantes gastaram ao utilizar as técnicas.

6.2.6 Grau de severidade para o conjunto de técnicas PIT-OSN

Após as análises qualitativas e quantitativas realizadas no 1º estudo de viabilidade, verificou-se a necessidade de inserir um novo passo no conjunto de técnicas para atender algumas especificidades de domínios. Pode ser que determinados itens de verificação indiquem pontos problemáticos em uma determinada RSO, e pontos que podem ser características desejáveis em outros sistemas. Ou seja, pode haver itens que não sejam nem atendidos e nem violados. Desse modo, inseriu-se como uma etapa complementar o grau de severidade (ou gravidade) para que os avaliadores possam julgar os problemas detectados, analisando o contexto do domínio do sistema e o custo/correção dos mesmos. Este grau de severidade foi elaborado com base na escala sugerida por Nielsen (1994). A escala é representada através de um nível que varia de 0 a 5, sendo classificado como:

0. Não considero um problema de privacidade nesta rede social;
1. Somente um problema de privacidade cosmético – consertar apenas se houver tempo disponível;
2. Problema leve de privacidade – baixa prioridade para consertá-lo;
3. Problema grave de privacidade – alta prioridade para consertá-lo;
4. Problema catastrófico de privacidade – é imperativo consertá-lo.

Após a análise dos resultados obtidos neste primeiro estudo de viabilidade e da evolução do conjunto de técnicas proposto, um novo estudo foi planejado para explorar uma nova questão de pesquisa. A condução deste segundo estudo de viabilidade, bem como os resultados e discussões será apresentada na seção 6.3.

6.2.7 Limitações do 1º Estudo de Viabilidade

As limitações deste primeiro estudo de viabilidade estão relacionadas principalmente a três itens: (1) ao tamanho da amostra; (2) a rede social usada como objeto de inspeção; e (3) o processo de inspeção parcial utilizado no estudo. Em relação ao item 1, o número de participantes não é considerado ideal do ponto de vista estatístico. Portanto, há limitações nos resultados, que são considerados indícios e não conclusivos. Em relação ao item 2, a rede social inspecionada (*Instagram*) corresponde a um sistema real. No entanto, não é possível

afirmar que o aplicativo representa todos os tipos de redes sociais existentes. Por fim, com relação ao item 3, observa-se que, não foi solicitado que os participantes utilizassem todo conjunto de técnicas durante as inspeções, havendo limitações. Além disso, os participantes do estudo não seguiram todo o processo de avaliação sugerido pelo conjunto de técnicas PIT-OSN, sendo que somente as fases de preparação e detecção de defeitos foram executadas pelos inspetores, as demais atividades do processo foram efetuadas por outros pesquisadores, sendo esta também uma limitação do estudo.

6.3 2º ESTUDO DE VIABILIDADE COM A PIT-OSN

Como não foi possível estabelecer no primeiro estudo de viabilidade uma relação entre o número de defeitos detectados, o número total de defeitos existentes e o tempo gasto pelos inspetores comparados com outra abordagem, decidiu-se planejar e executar um segundo estudo de viabilidade, de cunho comparativo. Como não haviam técnicas para comparar com o conjunto de tecnologias PIT-OSN, decidiu-se utilizar uma técnica de inspeção *ad hoc* para que fosse possível estabelecer uma relação comparativa entre uma técnica com procedimentos para inspeção e outra sem procedimentos (*ad hoc*).

Este segundo estudo foi conduzido no período de Novembro de 2018 utilizando a terceira versão da PIT-OSN (v3) e teve como objetivo responder a seguinte questão de pesquisa: "*O conjunto de técnicas PIT-OSN é eficiente e eficaz para inspeções de privacidade?*". Desse modo, este segundo estudo de viabilidade teve como foco coletar os indicadores de eficiência e eficácia das técnicas em comparação a uma inspeção *ad hoc*. No contexto deste estudo, os termos eficiência e eficácia são definidos da seguinte forma:

- Eficiência – a razão entre o número de defeitos detectados e o tempo gasto no processo de inspeção;
- Eficácia – a razão entre o número de defeitos detectados e o número total de defeitos conhecidos.

A seguir será apresentado todo o detalhamento deste segundo estudo de viabilidade, incluindo a caracterização dos objetos do estudo, o planejamento do mesmo, a execução das atividades do processo de inspeção, os resultados obtidos e as melhorias realizadas no conjunto de técnicas.

6.3.1 Caracterização dos objetos de estudo

Para explorar a questão de pesquisa definida na seção anterior, optou-se por escolher novamente como objeto de estudo RSOs existentes. Esta escolha deu-se pois, ao avaliar a

privacidade de RSOs existentes, é possível garantir que estamos detectando defeitos de privacidade reais que o conjunto de técnicas PIT-OSN deveria ser capaz de detectar em uma determinada RSO.

Para proceder o processo de inspeção, buscou-se escolher RSOs que fossem amplamente utilizadas e que fossem voltadas para contextos distintos. A diferença entre os contextos é interessante no sentido de possibilitar que diferentes aspectos e considerações relacionados à privacidade fossem analisados, tendo em vista que o contexto é um fator determinante em questões de privacidade (NISSENBAUM, 2004).

Desse modo, foram selecionadas três diferentes RSOs. Para não haver repetição de defeitos entre as técnicas, cada RSO foi designada para ser inspecionada por uma técnica específica do conjunto. O Twitter, que é uma rede social para *microblogging*, foi escolhido para ser avaliado pela técnica de níveis de privacidade (PIT-1). O Facebook, que é uma RSO de propósito geral, foi selecionado para ser avaliado pela técnica de controles de Privacidade (PIT-2). Por fim, a ResearchGate, que é uma RSO que visa conectar pesquisadores e compartilhar conhecimento científico, foi escolhida para ser avaliada pela técnica de políticas de privacidade (PIT-3).

6.3.2 Planejamento do 2º estudo de viabilidade

A finalidade específica deste segundo estudo de viabilidade foi comparar a eficiência e a eficácia do conjunto de técnicas PIT-OSN v3 com a eficiência e eficácia de uma inspeção *ad hoc*. O objetivo, segundo o paradigma GQM (BASILI e ROMBACH, 1988), será apresentado a seguir.

Analisar	as técnicas PIT-OSN
Com o propósito de	caracterizá-las
Em relação à	sua eficiência e eficácia em comparação com uma técnica de inspeção *ad hoc*
Do ponto de vista	estudantes de graduação em Ciência da Computação
No contexto de	uma avaliação de privacidade em RSOs existentes por alunos de graduação

A partir da questão de pesquisa citada na seção 6.3, foram formuladas as seguintes hipóteses nulas (H01 e H02) e hipóteses alternativas correspondentes (HA1 e HA2):

- **H01:** Não há diferença entre a eficiência de inspeções de privacidade que aplicam a PIT-OSN e a eficiência de inspeções *ad hoc*.

- **HA1:** A eficiência de inspeções de privacidade que aplicam a PIT-OSN é maior que a eficiência de inspeções *ad hoc*.
- **H02:** Não há diferença entre a eficácia de inspeções de privacidade que aplicam a PIT-OSN e a eficácia de inspeções *ad hoc.*
- **HA2:** A eficácia de inspeções de privacidade que aplicam a PIT-OSN é maior que a eficácia de inspeções *ad hoc.*

Após a definição do objetivo do estudo, serão descritos a seguir as etapas que compuseram o planejamento da segunda avaliação de viabilidade.

- **Seleção dos participantes**

Vinte e seis (26) alunos do curso de Ciência da Computação da Universidade Federal do Amazonas foram selecionados dentre todos que se dispuseram a participar. Estes estudantes cursavam a disciplina de Segurança de Informação e foram escolhidos por critérios de conveniência. Ressalta-se que os estudantes deste estudo não eram os mesmos que participaram dos estudos executados anteriormente. Cada participante assinou um formulário de consentimento e preencheu um formulário de caracterização que mediu sua experiência em privacidade (EP) e avaliação de interface (AI).

O formulário de caracterização foi aplicado para categorizar a experiência dos participantes como: nenhuma, baixa, média ou alta experiência em privacidade. No diz respeito a esta classificação sobre a experiência em privacidade, utilizou-se como base o questionário de Valentim *et al* (2016) e considerou-se com:

- Alta experiência (A): participantes que tinham participado em mais de 5 projetos ou avaliação de privacidade na indústria;
- Média Experiência (M): participantes que tinham participado entre 1 e 4 projetos ou avaliação de privacidade na indústria;
- Baixa Experiência (B): participantes que participaram em pelo menos um projeto ou avaliação de privacidade em sala de aula.
- Nenhuma Experiência (N): participantes que não tinham conhecimento sobre privacidade ou que conheciam alguns conceitos de privacidade adquiridos em leituras/palestras mas sem nenhuma experiência prática.

- **Projeto Experimental**

Os participantes foram alocados em dois grupos: o grupo da PIT-OSN (grupo 1) e o grupo das inspeções *ad hoc* (grupo 2). O grupo 1 foi composto por 14 participantes e o grupo

2 foi composto por 12 integrantes. Como a PIT-OSN é um conjunto que dispõem de três técnicas e cada uma direciona o foco da sua inspeção considerando um aspecto específico de privacidade (níveis, controles e políticas), optou-se, neste estudo, que os participantes realizassem uma inspeção completa com todo o conjunto.

Primeiramente, o grupo 1 e o grupo 2 avaliaram os níveis de privacidade da rede social Twitter, sendo que o grupo 1 aplicou a PIT-OSN 1 e o grupo 2 realizaram inspeções *ad hoc*. Uma segunda avaliação sobre os controles de privacidade da rede social Facebook foi efetuada pelo grupo 1, que aplicou a técnica PIT-OSN 2, e pelo grupo 2 que aplicou uma inspeção *ad hoc*. Por fim, uma última avaliação foi realizada nas políticas de privacidade da rede social ResearchGate. Para proceder esta avaliação, o grupo 1 aplicou a PIT-OSN 3 e o grupo 2 realizou inspeções *ad hoc*.

- **Instrumentação**

Alguns artefatos para este estudo foram definidos no sentido de apoiar a condução do mesmo, tais como: um termo de consentimento livre e esclarecido (TCLE), um formulário de caracterização, uma especificação das técnicas PIT-OSN e das inspeções *ad hoc*, uma planilha para anotação das discrepâncias identificadas e um questionário pós-inspeção. Este material pode ser visto no Apêndice C. Vale ressaltar que todos estes artefatos foram validados em um estudo piloto para que não houvesse nenhum problema que inviabilizasse a execução do segundo estudo de viabilidade.

- **Preparação**

Seguindo a etapa de preparação do processo de avaliação da PIT-OSN, uma apresentação geral contendo conceitos e definições básicos sobre privacidade foi abordada para os dois grupos juntos, durando cerca de 15 minutos. Em seguida, os grupos foram alocados em salas separadas e os integrantes dos grupos não sabiam qual técnica iriam aplicar. Após serem separados, os grupos receberam uma apresentação específica sobre a técnica a qual iriam utilizar durante a avaliação.

Para os dois grupos foi demonstrado como os participantes deveriam proceder a atividade de detecção de defeitos. Além disso, exemplos para ilustrar violações de privacidade foram demonstrados, no entanto, os exemplos de problemas de privacidade foram de redes sociais diferentes das escolhidas como objeto de inspeção, descartando qualquer viés. O tempo total desta preparação durou aproximadamente 30 minutos.

6.3.3 Detecção de Defeitos do 2º Estudo de Viabilidade

A execução da etapa de detecção de defeitos foi realizada em dois dias. No primeiro dia, os participantes inspecionaram os controles de privacidade da rede social *Facebook*. No segundo dia, os participantes realizaram inspeções sobre os níveis de privacidade do *Twitter* e das políticas de privacidade do *ResearchGate*. Durante a atividade de detecção de defeitos, cada grupo realizou a inspeção em salas separadas acompanhados por dois monitores.

O grupo da PIT-OSN teve como monitor o autor da dissertação e o grupo das inspeções *ad hoc* teve o orientador do autor desta dissertação como monitor. Estes monitores ficaram a disposição durante as inspeções, para eliminar as eventuais dúvidas que poderiam ocorrer quanto a atividade de detecção de defeitos. Durante este acompanhamento, os estudantes não receberam qualquer auxílio dos monitores sobre à inspeção em si.

Desse modo, cada participante recebeu os artefatos do estudo, conforme descrito na subseção 6.3.2 (instrumentação), realizando a atividade de detecção de defeitos individualmente. Durante a inspeção, os participantes preencheram uma planilha com as discrepâncias (possíveis defeitos) identificadas. Todos os integrantes dos grupos entregaram ao final da atividade de detecção a planilha contendo todas as discrepâncias encontradas e a anotação do tempo total gasto na inspeção. Após isso, eles deveriam responder um questionário pós-inspeção para fornecer um feedback de uso sobre as inspeções realizadas.

6.3.4 Coleção e Discriminação do 2º Estudo de Viabilidade

As atividades de Coleção e Discriminação foram executadas de forma similar ao estudo anterior, seguindo o mesmo percurso. No entanto, na atividade de coleção deste estudo, as listas de discrepâncias produzidas pelos inspetores foram juntadas em uma única lista referente ao foco das técnicas. Por exemplo, a lista da PIT-OSN 1 foi juntada com a lista das inspeções *ad hoc* relacionadas aos níveis de privacidade, e o mesmo trabalho foi feito para as demais técnicas, eliminando as discrepâncias duplicadas, ou seja, identificadas por mais de um inspetor. Tal coleção foi efetuada pelo autor desta dissertação e sua coorientadora.

Por fim, foi realizada a atividade de discriminação de feitos por outros dois pesquisadores com conhecimento prévio sobre as técnicas. No entanto, neste estudo, durante a discriminação, os pesquisadores não sabiam se as discrepâncias listadas foram identificadas com o conjunto de técnicas PIT-OSN ou através das inspeções *ad hoc*. Desse modo, os pesquisadores realizaram a discriminação dos defeitos sem nenhum viés.

6.4 RESULTADOS DO 2º ESTUDO DE VIABILIDADE DA PIT-1

6.4.1 Resultados Quantitativos do 2º Estudo de Viabilidade da PIT-1

A Tabela 30 apresenta o resultado geral das inspeções de privacidade realizadas no Twitter por cada participante do 2° Estudo de Viabilidade. A primeira coluna (Part.) representa o código de cada participante (indicados por P01, P02,...). A segunda coluna (EP) indica a experiência dos participantes em privacidade. A terceira coluna (EAI) indica a experiência dos participantes em avaliação de interface. A quarta coluna (DS) representa o número de discrepâncias (possíveis defeitos) identificadas por participante. A quinta coluna (FP) demonstra o número de falso-positivos identificados. A sexta coluna (DF) revela o número de defeitos totais encontrados por participante. A sétima coluna (tempo) indica o tempo gasto por participante na inspeção. A oitava coluna (defeito/hora) sugere o número de defeitos/hora que cada participante identificou calculado como (número de defeito/tempo*60). A nona coluna indica a eficácia por participante calculada como o número de defeitos detectados por participante/número de defeitos conhecidos. O número de defeitos conhecidos detectados por cada técnica é mostrado na Tabela 31.

Tabela 30. Resultado das inspeções – 2º Estudo de Viabilidade PIT-OSN 1

Part.	EP	EAI	DS	FP	DF	Tempo (min)	Defeito /(hora)	Eficácia	Técnica
P01	Nenhuma	Sim	6	3	3	35	5,14	12,00%	PIT-OSN 1
P02	Nenhuma	Não	6	3	3	29	6,21	12,00%	
P03	Nenhuma	Sim	2	1	1	21	2,86	4,00%	
P04	Nenhuma	Sim	9	4	5	35	8,57	20,00%	
P05	Nenhuma	Sim	7	2	5	52	5,77	20,00%	
P06	Nenhuma	Não	5	3	2	45	2,67	8,00%	
P07	Nenhuma	Sim	9	3	6	23	15,65	24,00%	
P08	Nenhuma	Sim	8	5	3	38	4,74	12,00%	
P09	Nenhuma	Sim	4	1	3	27	6,67	12,00%	
P10	Nenhuma	Não	8	1	7	27	15,56	28,00%	
P11	Nenhuma	Sim	3	0	3	45	4,00	12,00%	
P12	Nenhuma	Sim	5	1	4	21	11,43	16,00%	
P13	Nenhuma	Não	4	1	3	43	4,19	12,00%	
P14	Nenhuma	Não	1	0	1	30	2,00	4,00%	
P15	Nenhuma	Sim	4	2	2	45	2,67	8,00%	AD HOC
P16	Nenhuma	Não	2	1	1	22	2,73	4,00%	
P17	Nenhuma	Não	4	0	4	27	8,89	16,00%	
P18	Nenhuma	Sim	3	2	1	21	2,86	4,00%	
P19	Nenhuma	Sim	4	2	2	35	3,43	8,00%	
P20	Nenhuma	Sim	2	2	0	23	0,00	0,00%	
P21	Nenhuma	Não	4	2	2	33	3,64	8,00%	
P22	Nenhuma	Sim	5	1	4	31	7,74	16,00%	
P23	Nenhuma	Sim	4	4	0	28	0,00	0,00%	

Part.	EP	EAI	DS	FP	DF	Tempo	Defeito	Eficácia	Técnica
P24	Baixa	Sim	2	2	0	23	0,00	0,00%	AD HOC
P25	Média	Sim	2	2	0	23	0,00	0,00%	
P26	Nenhuma	Sim	2	1	1	36	1,67	4,00%	
Legenda: **Part**.. - Participante; **EP** – Experiência em Privacidade; **EAI** – Experiência em Avaliação de Interface; **DS** – Número de Discrepâncias; **FP** – Número de Falso-Positivos; **DF** – Número de Defeitos;									

Fonte: Próprio autor.

Os participantes P01 a P14 aplicaram a PIT-OSN 1. Já os participantes P15 a P26 realizaram inspeções *ad hoc*. Pode-se observar que os inspetores que aplicaram a PIT-OSN 1 detectaram entre 1 a 7 defeitos gastando entre 21 a 52 minutos. Por outro lado, os inspetores que realizaram inspeções *ad hoc* gastaram entre 21 a 45 minutos, identificando entre 0 a 4 defeitos. Pode-se notar que a PIT-OSN 1 propiciou um diagnóstico de defeitos superior ao da inspeção *ad hoc*. No entanto, os inspetores levaram mais tempo aplicando a PIT-OSN 1 do que os inspetores que realizaram inspeções *ad hoc*.

No geral, as inspeções com as duas técnicas resultaram em um diagnóstico de 25 defeitos conhecidos (únicos). A Tabela 31 exibe a média da eficácia e eficiência. A eficiência foi calculada como o número total de defeitos detectados/tempo total gasto na inspeção*60, seguindo a definição do indicador. Já a eficácia foi calculada como a média entre número de defeitos detectados/número total de defeitos conhecidos (únicos) encontrados com as duas técnicas, seguindo também a definição do indicador.

Tabela 31. Eficiência e Eficácia – 2º Estudo de Viabilidade da PIT-OSN 1

Item analisado	Técnicas	
	PIT-1	**Ad hoc**
Total de discrepâncias detectadas	77	38
Total de defeitos detectados (incluindo os duplicados)	49	10
Total de defeitos conhecidos (únicos)	18	7
Total de Falso-Positivos	28	21
Média da eficácia	14,00%	5,67%
Tempo total dedicado as inspeções (min)	471	347
Eficiência	6,24	2,94

Fonte: Próprio autor.

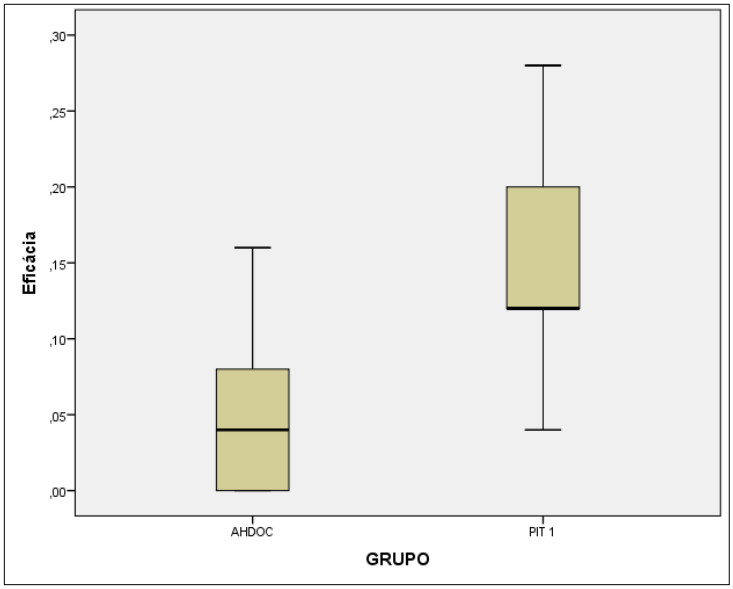
A partir desses dados, pode-se observar que a eficácia da técnica PIT-OSN 1 foi de 14% neste estudo. Relacionando esta medida com a eficácia do grupo das inspeções *ad hoc* (5,67%), verifica-se que a eficácia da técnica PIT-OSN 1 foi superior. Além disso, com base nos dados fornecidos pela Tabela 31, nota-se que uma inspeção *ad hoc* tende a fornecer um número inferior de falso-positivos (21 identificados) comparado a 28 encontrados na PIT-OSN 1. O número inferior de falso-positivos pode ser explicado pelo fato de uma inspeção *ad*

hoc possuir passos mais simples, intuitivos e baseados em procedimentos não-sistemáticos. Entretanto, a PIT-OSN 1 possibilitou um diagnóstico de defeitos de privacidade superior (49 incluindo os duplicados) comparativamente ao da inspeção *ad hoc* (10 defeitos incluindo os duplicados). O número superior de defeitos de privacidade detectados com a aplicação da PIT-OSN 1 pode sugerir que esta técnica é mais favorável para guiar os inspetores em uma atividade de detecção de defeitos de privacidade em RSOs.

Para analisar de forma mais específica a eficiência e eficácia dos grupos, análises estatísticas foram efetuadas usando o teste de normalidade de Shapiro-Wilk com α=0,05 para eficácia e eficiência. O teste de normalidade testa a hipótese de que os dados apresentam uma distribuição normal. No caso de amostras menores (<50 casos), o teste de Shapiro-Wilk é mais eficaz. Nestes testes, se a significância do teste de normalidade for menor que 0,05 então a distribuição em questão é não normal. Se for maior que 0,05, pode-se dizer que a distribuição da amostra é não significantemente diferente da distribuição normal, ou seja, é normal (LAZAR *et al.*, 2010). O teste de normalidade mostrou que a distribuição dos valores de eficácia é normal para ambos os grupos (com p=0,228 para PIT-OSN 1 e p=0,031 para ADHOC), e que a distribuição dos valores de eficiência não é normal (com p=0,021 para a PIT-1 e p=0,029 para ADHOC).

Segundo Lazar *et al.* (2010) se a distribuição dos valores da variável é normal, deve-se usar um teste paramétrico, caso a distribuição seja não normal usa-se um teste não paramétrico. De acordo com projeto do experimento deste estudo, tem-se um *between-group* com uma variável independente e 2 condições. As variáveis independentes são as técnicas de inspeção (PIT-OSN 1 e ADHOC) e as condições são os indicadores de eficiência e eficácia. A partir disso, o t-test, para amostras independentes, foi selecionado para avaliar a eficácia e o teste não paramétrico de Mann-Whitney foi selecionado para avaliar a eficiência.Para representar um resumo dos resultados destas análises foi utilizado o gráfico de *boxplot*. A análises foram executadas através do uso da ferramenta estatística SPSS V. 23, e α = 0,10. A escolha desta significância estatística foi motivada pelo pequeno tamanho da amostra usada neste estudo.

Figura 16. Boxplot comparando a eficácia da PIT-1 vs ADHOC

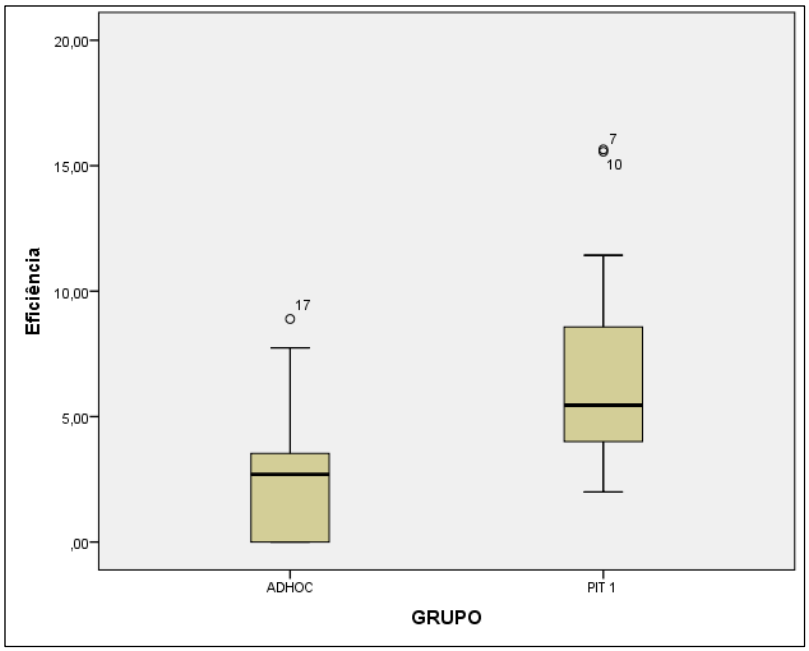


Fonte: Próprio autor.

A Figura 16 apresenta a análise aplicada para determinar se houve diferença estatística comparando o indicador de eficácia das duas técnicas na identificação de defeitos de privacidade. A partir da visão fornecida pelo gráfico de *boxplots*, com a distribuição da eficácia por técnica, nota-se que o grupo da PIT-OSN 1 teve uma eficácia muito mais elevada que o grupo da ADHOC para inspecionar os níveis de privacidade da rede social alvo. Além disso, o t-teste confirmou que a eficácia da PIT-OSN 1 foi significantemente superior que a eficácia da ADHOC (p = 0,003). Estes resultados apoiam a hipótese alternativa HA2 - "A eficácia de inspeções de privacidade que aplicam a PIT-OSN 1 é maior que a eficácia de inspeções *ad hoc*", consequentemente rejeitando a hipótese nula H02.

A mesma análise foi aplicada comparando a distribuição de eficiência por técnica. A Figura 17 apresenta os *boxplots* demostrando tal comparação. Com base na visão fornecida pelo gráfico de *boxsplot*, pode-se observar que ao relacionar as duas amostras usando o teste não paramétrico de Mann Whitney, também foi identificada diferença significativa entre os dois grupos (p = 0,008). Estes resultados indicam que a PIT-OSN 1 teve uma eficiência superior comparativamente a inspeção *ad hoc* quando utilizadas para inspecionarem os níveis de privacidade do Twitter. Logo, estes resultados apoiam a hipótese alternativa HA1 – "A eficiência de inspeções de privacidade que aplicam a PIT-OSN 1 é maior que a eficiência de inspeções *ad hoc*", e em razão disso rejeitam a hipótese nula H01.

Figura 17. Boxplot comparando a eficiência da PIT-1 vs ADHOC



Fonte: Próprio autor.

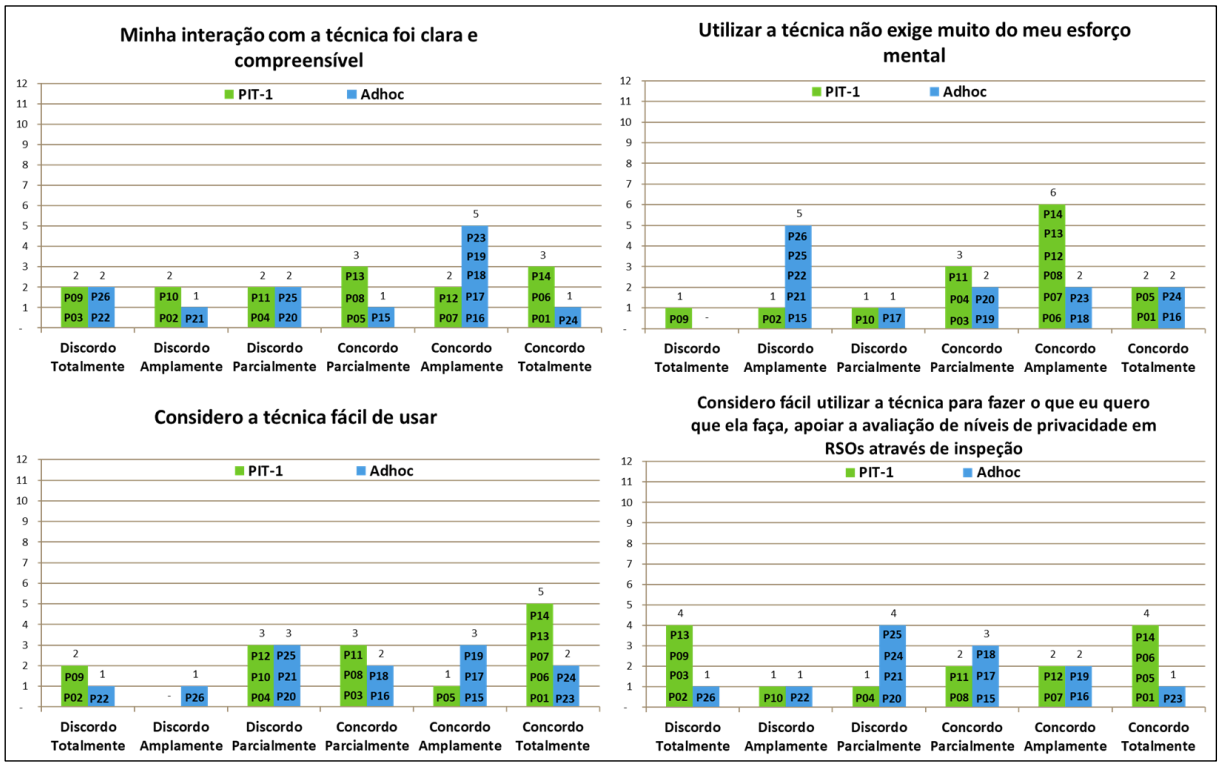
6.4.2 Análise da Percepção dos Participantes do 2º Estudo de Viabilidade da PIT-1

Após as análises quantitativas, os questionários pós-inspeção sobre a aceitação das técnicas PIT-OSN 1 e *Ad hoc* foram analisados. Seguindo a mesma direção do estudo anterior, o grau de aceitação dos participantes foi analisado com base nos indicadores do modelo TAM. No entanto, neste estudo, os participantes responderam um questionário pós-inspeção ao final da aplicação de cada técnica do conjunto. No geral, eles forneceram feedback de uso sobre cada técnica PIT-OSN. Os indicadores escolhidos para este estudo foram: (i) Facilidade de Uso Percebida; e (ii) Utilidade Percebida. Os resultados obtidos a partir das análises destes indicadores serão apresentados a seguir.

a. Facilidade de uso percebida

A Figura 18 aponta a visão dos participantes do estudo em relação à facilidade de uso da técnica percebida da PIT-OSN 1 e das inspeções *ad hoc*. Na representação gráfica ilustrada na Figura 18, o eixo horizontal apresenta o grau de concordância e discordância de cada participante e o eixo vertical indica o número de participantes do estudo. Nas barras foram inseridos códigos (P01, P02...) que simbolizam os participantes apresentados na Tabela 30**.**

Figura 18. Facilidade de uso percebida – 2º Estudo de Viabilidade



Fonte: Próprio autor.

Ao observar os dados fornecidos pelos gráficos contidos na Figura 18, nota-se que muitos dos participantes do grupo da PIT-OSN 1 concordaram com as quatro sentenças do indicador facilidade de uso percebida. No entanto, houve também algumas discordâncias sobre este indicador. Os participantes P02, P09 e P10 discordaram de todas as afirmativas do indicador em questão. Um deles (participante P02) justificou a sua discordância apontando o seguinte argumento "*Achei a técnica difícil de usar, muitos termos não ficaram claros e estão ambíguos*". Nesse sentido, nota-se que há pontos na técnica PIT-OSN 1 que ainda precisam ser aprimorados para que a tecnologia tenha uma facilidade de aplicação melhor e não seja considerada ambígua em tempo de uso.

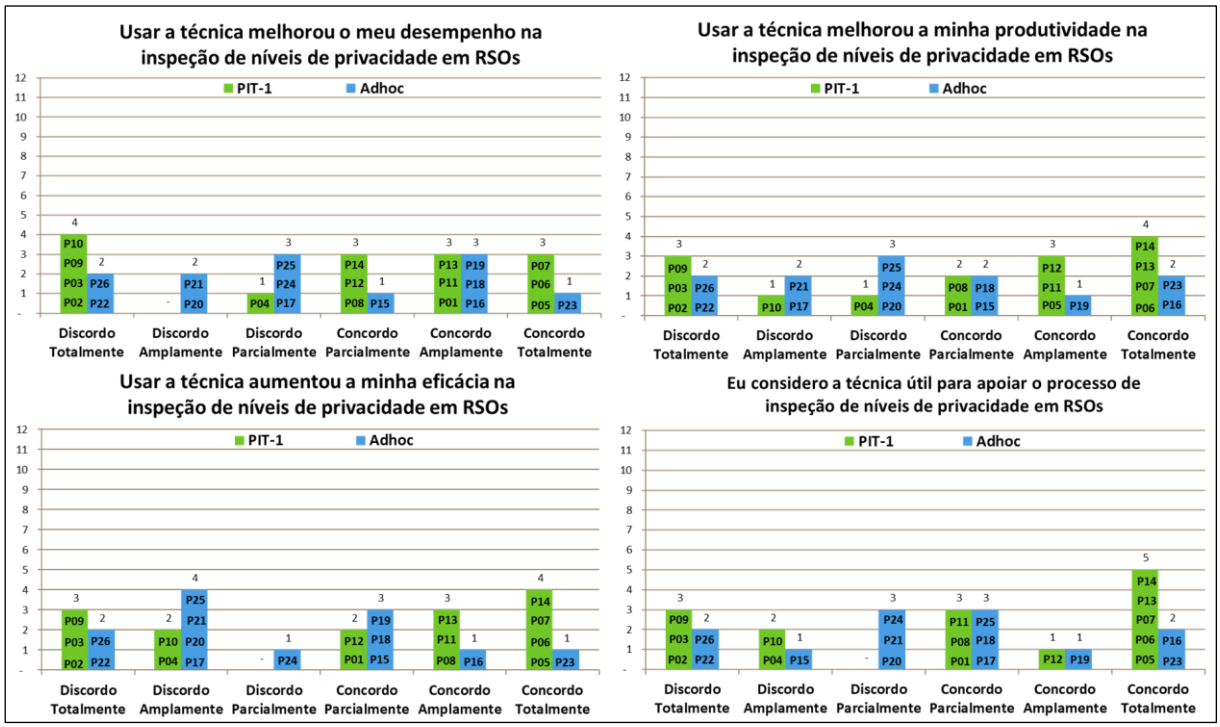
Em relação à percepção dos participantes sobre as inspeções *ad hoc*, observa-se que houve um pouco mais de discordâncias neste grupo que no grupo da PIT-OSN 1. O participante P15, do grupo das inspeções *ad hoc*, apresentou as principais razões que o fizeram discordar de algumas sentenças: "*...esta técnica requer muito esforço mental e se houver outras técnicas, a ad hoc não será uma escolha para mim".* Desse modo, nota-se que uma inspeção sem técnica (*ad hoc*) pode exigir mais esforço mental para executar um atividade de detecção de defeitos, pois o foco da inspeção reside na especialidade do inspetor.

Tal reflexão demonstra a importância em se ter técnicas com instruções concretas que guiam o inspetor na detecção de defeitos.

b. Utilidade percebida

A Figura 18 indica a visão dos participantes do estudo em relação à utilidade percebida da técnica PIT-OSN 1 e da inspeção *ad hoc*. Nota-se que a maioria dos participantes do grupo da PIT-OSN 1 concordaram com as sentenças que afirmam que a técnica é útil para apoiar uma atividade de inspeção de privacidade em RSOs, porém, discordâncias também foram apontadas. O participante P10, por exemplo, foi um dos inspetores que discordou de todas as afirmativas sobre o indicador em questão. No entanto, um ponto a ser destacado é que este participante foi o que detectou o maior número de defeitos no grupo da PIT-OSN 1 (07 defeitos) e gastando o menor tempo de inspeção (27 minutos.) Desse modo, nota-se que o desempenho do participante P10, bem como o tempo gasto na inspeção, foi relativamente bom, e apesar disso, este participante achou que a técnica PIT-OSN 1 não foi útil para detectar defeitos.

Figura 19. Percepção sobre Utilidade – 2º Estudo de Viabilidade



Fonte: Próprio autor.

Além disso, três participantes (P02, P03 e P09) discordaram totalmente de todas as sentenças do indicador em foco. Para analisar de forma mais específica tais discordâncias, buscamos observar os argumentos destes participantes. P09 discordou apontando o seguinte relato: "*...o uso [da técnica] é confuso e não me deixou satisfeito ao responder*". O argumento do participante P02 é o mesmo apontado para o indicador de facilidade de uso percebida, onde o participante afirma novamente que achou a técnica difícil de aplicar e muitos termos poderiam estar ambíguos. O relato destes dois participantes representam oportunidades de melhorias, indicando que ainda há itens na técnica PIT-1 que necessitam de ajustes gerais para melhorar sua compreensão e eliminar as ambiguidades.

Em relação à inspeção *ad hoc*, nota-se que também houve sentenças em que os inspetores concordaram e outras as quais discordaram. No geral, o nível de discordância no grupo das inspeções *ad hoc* foi um pouco maior que no grupo da PIT-OSN 1. Alguns participantes explicaram as principais razões sobre as quais os levaram a discordar da utilidade de uma inspeção *ad hoc.* O participante P22, por exemplo, relatou "*Discordei, porque além de eu não utilizar o twitter, também não tinha um roteiro para seguir e para estipular os níveis de privacidade*". Com esta mesma visão, o participante P26 argumentou "*Falta a capacidade de guiar o inspetor durante o processo*".

Nesse sentido, nota-se que uma inspeção *ad hoc* pode não ser útil para uma atividade de detecção de defeitos, devido a mesma depender exclusivamente da experiência do avaliador. Além disso, o fato de inspeções *ad hoc* não terem um roteiro para guiar o inspetor durante uma atividade de inspeção, esta carência pode influenciar negativamente o alcance de bons resultados ao ser comparada com uma técnica baseada em procedimentos sistemáticos.

6.4.3 Análise Qualitativa do 2º Estudo de Viabilidade da PIT-OSN 1

Uma análise específica dos dados qualitativos (comentários adicionais dos inspetores contidos nos questionários pós-estudo) foi realizada. Esta análise teve por base o método *Grounded Theory* (GT). Como o propósito da análise qualitativa era melhorar a técnica proposta (PIT-OSN 1), só foram realizadas análises referentes ao dados desta técnica.

Seguindo o mesmo percurso do estudo anterior, os dados qualitativos extraídos dos questionários foram analisados utilizando um subconjunto de fases do processo de codificação sugerido por Corbin e Strauss (1998) para o método GT – as codificações aberta (1ª fase) e axial (2ª fase). O processo de codificação produziu, no total, 69 códigos que foram associados à 3 categorias. O questionário pós-inspeção possuía questões abertas para coletar o ponto de vista dos participantes sobre os pontos positivos e negativos da técnica, dificuldades de uso

com a técnica e sugestões de melhorias para a técnica, o que levou à identificação destas três categorias: Dificuldade de Aplicação, Facilidade de Aplicação e Sugestões de Melhorias.

Entre os códigos criados na categoria “Dificuldade de Aplicação”, quatro deles apontam evidências de inadequação na técnica, tais como: “A PIT-OSN 1 é difícil de usar”, “A PIT-OSN 1 é ambígua”, “A PIT-OSN 1 não é clara”, “A PIT-OSN 1 exige esforço para entender”. Nota-se que estes códigos justificam algumas das discordâncias apontadas pelos participantes do estudo no questionário TAM, evidenciando que estas podem ser as principais razões que levaram os inspetores a discordarem de algumas sentenças sobre a utilidade da PIT-OSN 1. Além disso, estes códigos demonstram as dificuldades que os inspetores tiveram com algumas terminologias usadas pela técnica. Estes resultados podem sugerir que a técnica ainda possui alguns itens difíceis de entender para inspetores sem experiência, destacando a importância em aperfeiçoá-la, pois, uma técnica difícil de entender, possivelmente não será usada.

No entanto, não somente pontos negativos foram coletados através dos comentários dos participantes, a categoria “Facilidade de Aplicação” destacou os principais pontos positivos da técnica através dos seguintes códigos: “A PIT-OSN 1 é rápida”, “A PIT-OSN 1 é bem elaborada”, “A PIT-OSN 1 permite um maior e melhor conhecimento durante a inspeção”, “A PIT-OSN 1 é detalhada” e “A PIT-OSN 1 possui um fluxo fácil de ser seguido”.

Por fim, a categoria "Sugestões de Melhoria" identificou códigos que descrevem recomendações de melhorias na PIT-OSN 1. A maioria dos códigos mencionam questões referentes à tornar a técnica mais clara, tais como: “Sugestão em tornar a linguagem da PIT-OSN 1 mais clara” e “Sugestão em ser mais objetiva”, citados pelos participantes P06 e P04 respectivamente. Isto demonstra que a técnica PIT-OSN 1 pode não estar totalmente clara e pode ser melhorada para que seja positivamente útil para detectar problemas reais em níveis de privacidade em tempo de uso.

6.4.4 Melhorias na PIT-OSN 1

Os resultados obtidos com a análise qualitativa permitiram a identificação das causas para alguns pontos negativos resultantes na análise quantitativa. bem como apresentaram um importante retorno para melhorias adicionais na técnica PIT-OSN 1. Observou-se que um dos pontos mais destacados pelos participantes em relação à dificuldade de aplicação da PIT-OSN 1 foi a compreensão e clareza sobre a descrição de alguns itens de verificação, como pode ser observado nos seguintes códigos: “*Algumas descrições de itens de verificação são confusas*

de entender" (P13) e "*A PIT-OSN 1 não é clara*" (P09). Através da análise destes dados, revisões foram efetuadas e uma quarta versão (v4) da PIT-OSN 1 foi elaborada, o extrato completo da PIT-OSN 1 é descrito na Figura 20. A partir das análises foram feitas as seguintes melhorias:

- As descrições de alguns itens de verificações foram modificadas com o objetivo de torná-las mais claras e eliminar as redundâncias.
- O item 1E2[3] da dimensão de "audiência" foi retirado, pois este estava com o mesmo sentido do item 2I2[4] da dimensão de "separação interna de identidade" da técnica de controles de privacidade. Ou seja, o item IE2 estava verificando um aspecto de interface relacionado aos controles de privacidade e não diretamente ao níveis do sistema.
- O item 1F1[5] da dimensão de "notificação" foi retirado, pois a descrição estava confusa e o mesmo não remetia a identificação de um potencial problema nos níveis de privacidade de uma RSO.

Figura 20. Extrato completo da PIT-1 (versão 4).

INSPEÇÃO DOS NÍVEIS DE PRIVACIDADE	
1A. Fonte de Informação	
1A1	Verifique se outro usuário (um amigo ou seguidor) tem autonomia para compartilhar conteúdos publicados sobre um determinado indivíduo dentro do sistema sem permissão
1A2	Verifique se outras fontes, como aplicativos ou sites de terceiros, tem autonomia para compartilhar informações sobre um determinado usuário sem o seu consentimento ou conhecimento
1B. Espaço de Comunicação	
1B1	Verifique se um conteúdo publicado sobre um determinado usuário pode ser compartilhado em um outro espaço de publicação que não seja seu, provavelmente sem a sua permissão
1B2	Verifique se um conteúdo publicado sobre um determinado indivíduo pode ser acessado através de um espaço público fora do sistema (como em mecanismos de busca) sem a sua permissão
1C. Conteúdo dos dados	
1C1	Verifique se a rede social coleta dados pessoais (como data de nascimento, número de telefone, endereço de e-mail) e expõe essas informações na própria rede social sem a permissão do usuário

[3] Verifique se a rede social permite compartilhar conteúdos, seletivamente, com pessoas específicas.
[4] Verifique se a rede social permite ao usuário criar listas de amigos personalizadas para que o indivíduo possa compartilhar as postagens em grupos específicos de amigos.
[5] Verifique se a rede social notifica o indivíduo apenas sobre uma parte das interações de outros usuários com sua publicação.

1D. Persistência temporal	
1D1	Verifique se a rede social permite restringir a duração de um conteúdo publicado no sistema, possibilitando criar postagens curtas que desapareçam depois de um determinado período de tempo
1D2	Verifique se a rede social permite ao usuário que, ao aceitar a solicitação de um determinado indivíduo, este indivíduo tenha acesso apenas as informações que forem compartilhadas a partir do momento em que começou a fazer parte da audiência do usuário (tempo presente) e não tenha acesso as publicações antigas (tempo passado)
1E. Audiência	
1E1	Verifique se a rede social permite que uma audiência desconhecida (como amigos em comum por exemplo) possa visualizar determinadas ações do indivíduo no sistema sem fazer parte da lista de amigos
1F. Notificação	
1F2	Verifique se rede social não notifica o indivíduo sobre as interações de outros usuários com o seu conteúdo que é compartilhado no sistema
1G. Discurso do sistema sobre o indivíduo	
1G1	Verifique se a rede social toma a iniciativa de gerar novos conteúdos sobre o usuário sem a sua permissão, com base no processamento de uma ou mais informações pessoais já compartilhadas anteriormente (como retrospectivas e *scores* por exemplo)
1G2	Verifique se a rede social toma a iniciativa de recomendar o perfil do indivíduo para outros usuários sem a sua permissão (como as sugestões de pessoas por exemplo)
1H. Disseminação da Informação	
1H1	Verifique se a rede social permite à audiência repostar com outras pessoas uma publicação de um determinado usuário sem a sua permissão, ou seja, de maneira irrestrita

Fonte: Próprio autor.

6.5 RESULTADOS DO 2º ESTUDO DE VIABILIDADE DA PIT-OSN 2

6.5.1 Resultados Quantitativos do 2º Estudo de Viabilidade da PIT-OSN 2

A Tabela 32 apresenta o resultado geral das inspeções realizadas por participante nos controles de privacidade da rede social Facebook. Os participantes P01 a P14 aplicaram a PIT-OSN 2 e os participantes P15 a P26 realizaram inspeções *ad hoc*.

Tabela 32. Resultado das inspeções – 2º estudo de viabilidade com a PIT-2

Part.	EP	EAI	DS	FP	DF	Tempo (min)	Defeito /(hora)	Eficácia	Técnica
P01	Nenhuma	Sim	3	2	1	49	1,22	3,33%	PIT-OSN 2
P02	Nenhuma	Não	5	3	2	35	3,43	6,67%	
P03	Nenhuma	Sim	5	1	4	36	6,67	13,33%	
P04	Nenhuma	Sim	5	1	4	43	5,58	13,33%	
P05	Nenhuma	Sim	5	1	4	56	4,29	13,33%	
P06	Nenhuma	Não	3	2	1	55	1,09	3,33%	
P07	Nenhuma	Sim	5	2	3	41	4,39	10,00%	

Part.	EP	EAI	DS	FP	DF	Tempo	Defeito	Eficácia	Técnica
P08	Nenhuma	Sim	2	1	1	45	1,33	3,33%	PIT-OSN 2
P09	Nenhuma	Sim	4	2	2	35	3,43	6,67%	
P10	Nenhuma	Não	8	4	4	26	9,23	13,33%	
P11	Nenhuma	Sim	4	2	2	36	3,33	6,67%	
P12	Nenhuma	Sim	3	0	3	32	5,63	10,00%	
P13	Nenhuma	Não	7	4	3	43	4,19	10,00%	
P14	Nenhuma	Não	5	1	4	43	5,58	13,33%	
P15	Nenhuma	Sim	4	2	2	36	3,33	6,67%	AD HOC
P16	Nenhuma	Não	5	1	4	23	10,43	13,33%	
P17	Nenhuma	Não	1	1	0	48	0,00	0,00%	
P18	Nenhuma	Sim	3	0	3	51	3,53	10,00%	
P19	Nenhuma	Sim	6	3	3	48	3,75	10,00%	
P20	Nenhuma	Sim	1	0	1	50	1,20	3,33%	
P21	Nenhuma	Não	4	1	3	47	3,83	10,00%	
P22	Nenhuma	Sim	4	1	3	49	3,67	10,00%	
P23	Nenhuma	Sim	3	1	2	47	2,55	6,67%	
P24	Baixa	Sim	1	1	0	35	0,00	0,00%	
P25	Média	Sim	4	2	2	41	2,93	6,67%	
P26	Nenhuma	Sim	3	0	3	48	3,75	10,00%	

Legenda:
Part.. - Participante; **EP** – Experiência em Privacidade; **EAI** – Experiência em Avaliação de Interface; **DS** – Número de Discrepâncias; **FP** – Número de Falso-Positivos; **DF** – Número de Defeitos;

Fonte: Próprio autor.

Ao analisar a Tabela 32, verifica-se que os inspetores que aplicaram a PIT-OSN 2 detectaram entre 1 a 4 defeitos e tiveram o tempo de inspeção variando entre 26 a 56 minutos. Já os inspetores que efetuaram inspeções *ad hoc* gastaram entre 23 a 51 minutos na detecção, encontrando entre 0 a 4 defeitos.

Observa-se que alguns inspetores que realizaram as inspeções *ad hoc* conseguiram identificar apenas uma única discrepância, a qual não era um defeito real sobre os controles de privacidade e foi discriminada como um falso-positivo. Isto pode ser um indicador de que estes participantes tiveram dificuldades de criar um diagnóstico de defeitos de privacidade ao realizarem uma inspeção *ad hoc*, pois com o auxílio da PIT-OSN 2 pelo menos 1 defeito foi diagnosticado.

No geral, as inspeções com as duas técnicas produziram um diagnóstico de 30 defeitos conhecidos. A Tabela 33 exibe as médias para os indicadores de eficácia e eficiência sobre as técnicas em foco. A eficiência foi calculada como o número total de defeitos detectados/tempo total gasto na inspeção*60. Já a eficácia foi calculada como a média entre número de defeitos detectados/número total de defeitos conhecidos (únicos).

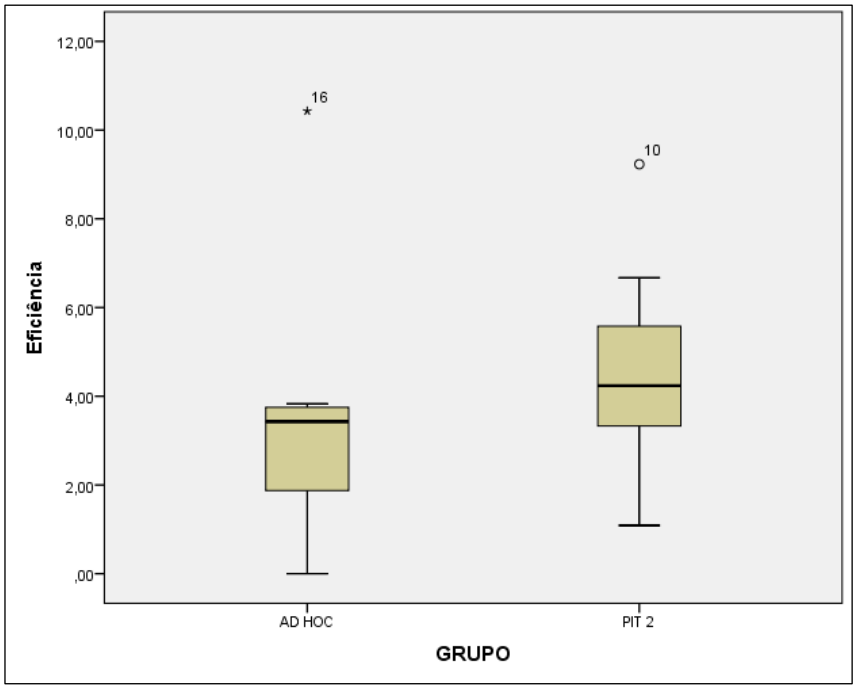
Tabela 33. Eficiência e Eficácia – 2º Estudo de Viabilidade da PIT-OSN 2

Item analisado	Técnicas	
	PIT-1	Ad hoc
Total de discrepâncias detectadas	60	39
Total de defeitos detectados (incluindo os duplicados)	38	26
Total de defeitos conhecidos (únicos)	16	14
Total de Falso-Positivos	26	13
Média da eficácia	9,05%	7,22%
Tempo total dedicado as inspeções (minutos)	575	523
Eficiência	3,97	2,98

Fonte: Próprio autor.

Para comparar de forma mais específica a eficiência e eficácia das duas amostras, utilizou-se novamente o teste de normalidade de Shapiro-Wilk com o nível de significância de α=0,05. O teste de normalidade mostrou que a distribuição dos valores de eficácia é não normal (com p=0,019 para PIT-1 e p=0,050 para ADHOC), e que a distribuição dos valores de eficiência é normal (com p=0,440 para a PIT-1 e p=0,006 para ADHOC). Com base nesses resultados, o t-test (teste paramétrico) para amostras independentes foi selecionado para avaliar a eficiência e o teste não paramétrico de Mann-Whitney foi selecionado para avaliar a eficácia. O resumo destas análises é apresentado em um gráfico de *boxsplot*. A análise estatística foi realizada através do software SPSS v. 23 com α=0,10, dado o tamanho limitado das amostras. A Figura 21 apresenta os *boxplots* comparando a distribuição de eficiência por técnica.

Figura 21. Boxplot comparando a eficiência por técnica do 2º estudo de viabilidade

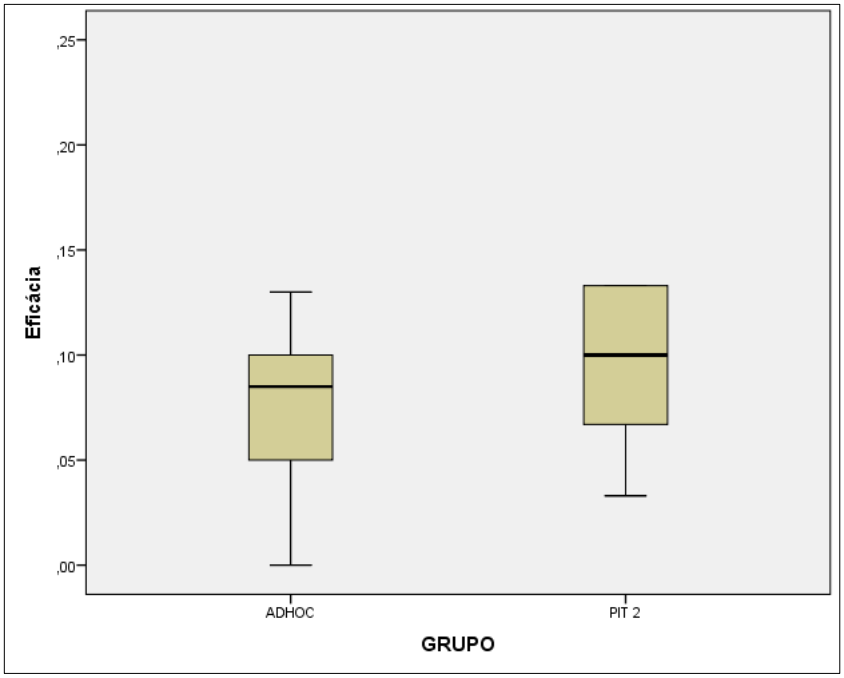


Fonte: Próprio autor.

Com base na visão fornecida pela Figura 21, pode-se observar que a mediana do grupo das PIT-OSN 2 está um pouco mais elevada que a mediana do grupo da *ad hoc*. No entanto, ao comparar as duas amostras usando o t-teste, não foi identificada diferença estatística significativa entre os dois grupos (p = 0,313). Tais resultados sugerem que o uso da PIT-OSN 2 e de uma inspeção *ad hoc* proveram eficiência similar quando utilizadas para inspecionar controles de privacidade em RSOs. Esta questão apoia a hipótese nula H01 - "Não há diferença entre a eficiência de inspeções de privacidade que aplicam a PIT-OSN 2 e a eficiência de inspeções *ad hoc",* e consequentemente rejeita a hipótese alternativa HA1.

A mesma análise foi efetuada para verificar se havia diferença significativa das duas amostras em relação ao indicador de eficácia na detecção de defeitos nos controles de privacidade. Os *boxplots* apresentados na Figura 22 demonstram que a mediana do grupo que aplicou uma inspeção *ad hoc* está um pouco mais elevada que a mediana do grupo que utilizou a PIT-OSN 2. No entanto, através do teste não paramétrico de Mann-Whitney não foi possível observar diferença estatística significativa entre os dois grupos (p = 0,322). Com isso, estes resultados denotam que a PIT-OSN 2 e o grupo da inspeção *ad hoc* apresentaram eficácia similar quando utilizadas para inspecionar controles de privacidade de RSOs neste estudo. Tal resultado apoia a hipótese nula HO2 - "Não há diferença entre a eficácia de inspeções de privacidade que aplicam a PIT-2 e a eficácia de inspeções ad hoc", e por esta razão rejeita a HA2.

Figura 22. Boxplot comparando a eficácia por técnica do 2º estudo de viabilidade



Fonte: Próprio autor.

6.5.2 Análise da Percepção dos Participantes do 2º Estudo de Viabilidade da PIT-2

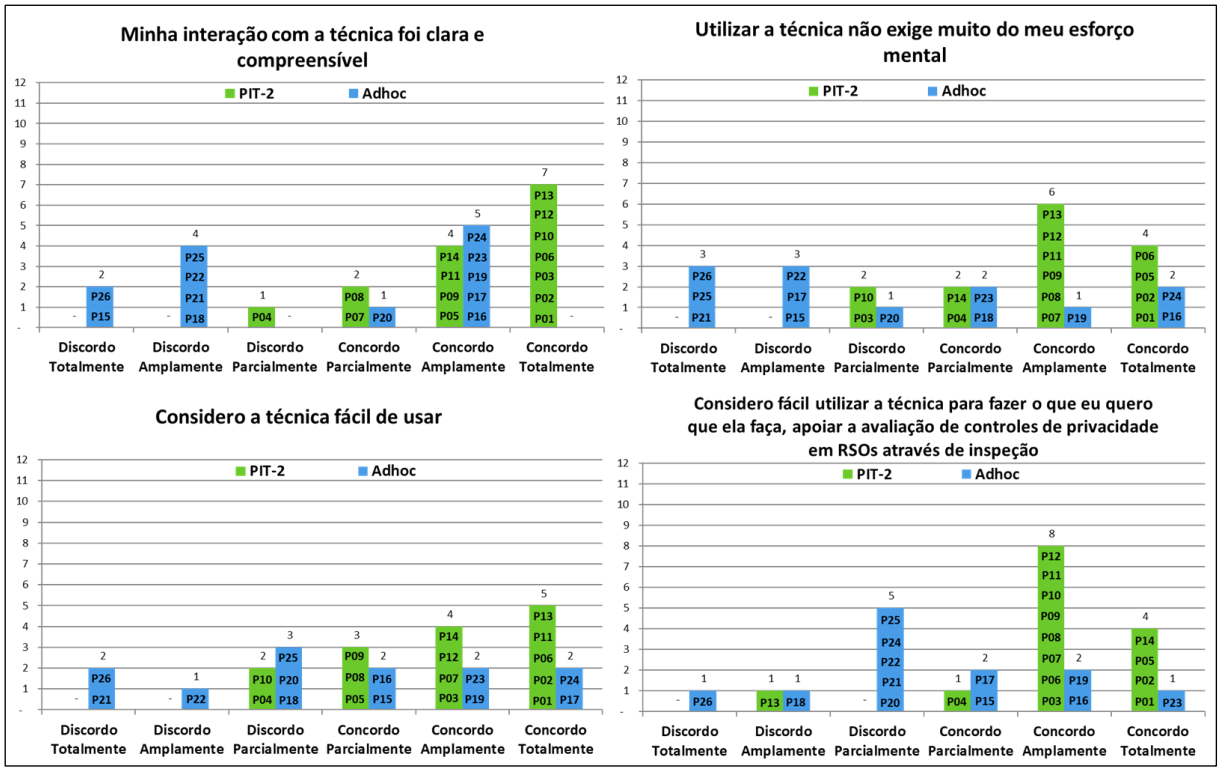
Para analisar a percepção dos participantes sobre o uso das técnicas, também foi utilizado o modelo de aceitação de tecnologia (*Technology Acceptance Model* – TAM). Os dois indicadores utilizados foram: (1) Facilidade de uso percebida e (2) Utilidade percebida. Uma discussão sobre os resultados obtidos a partir da análise de tais indicadores será abordada a seguir:

a. Facilidade de uso percebida

A Figura 23 exibe as respostas referentes à facilidade de uso percebida da PIT-OSN 2 e das inspeções *ad hoc*. A partir da visão fornecida pelos gráficos, pode-se destacar que a maioria dos inspetores que aplicaram a PIT-OSN 2 concordaram com todas as sentenças do indicador em questão. Houve também poucas discordâncias, mas, no geral, a PIT-2 foi considerada fácil de usar pelos participantes deste estudo.

Em relação à inspeção *ad hoc*, nota-se que o número de discordâncias foi superior ao comparar com a percepção dos inspetores que utilizaram a PIT-2. Isto pode ser um indicador de que houveram dificuldades em realizar uma inspeção sem técnica (*ad hoc*).

Figura 23. Facilidade de uso percebida – 2º estudo de viabilidade



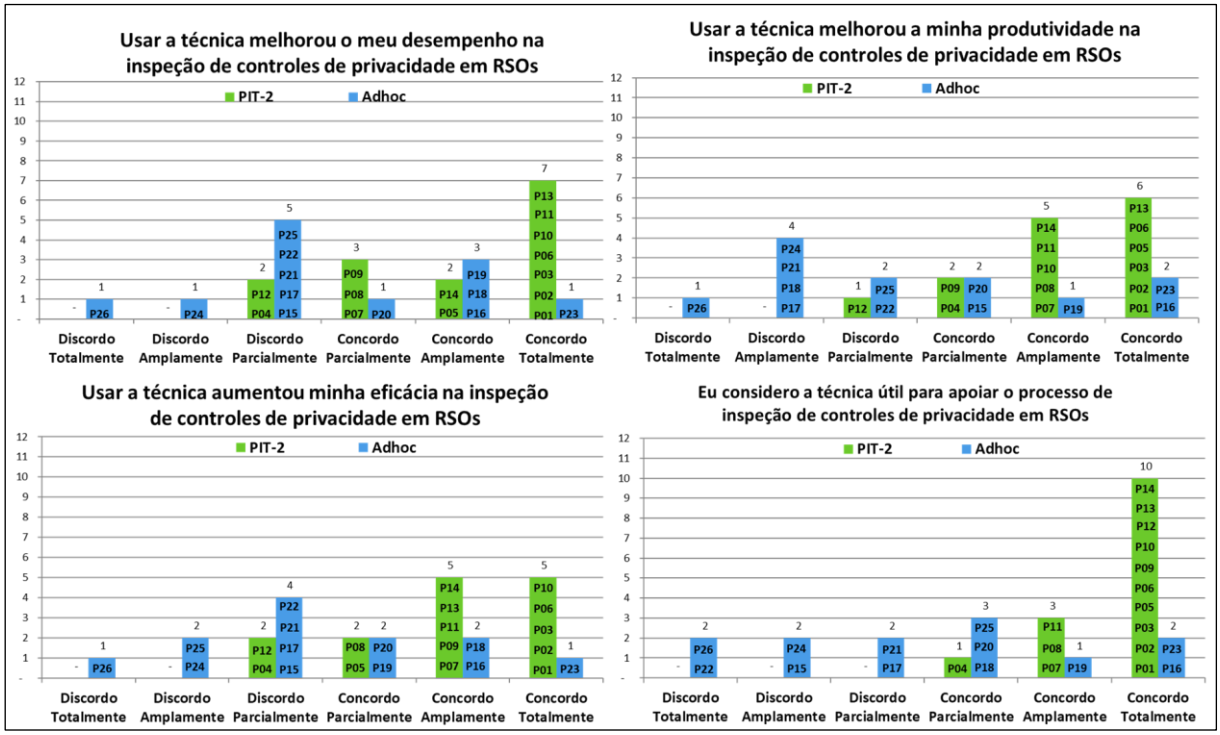
Fonte: Próprio autor.

b. Utilidade percebida

As respostas referentes à utilidade percebida das técnicas são apresentadas na Figura 24. As sentenças buscam investigar se a técnica ajuda a melhorar o desempenho, a produtividade e a eficácia na inspeção e se o inspetor a considera útil para inspeções de controles de privacidade. Observa-se que, no que diz respeito à PIT-OSN 2, o participante P12 discordou de três afirmativas da técnica em questão e justificou "*A tabela [de inspeção] não é necessariamente é fácil de lembrar, então não me vejo usando com grande eficácia em um primeiro instante*". Esta questão indica que em algum momento o usuário encontrou dificuldade de uso. No entanto, a maioria dos outros inspetores consideraram a PIT-OSN 2 útil para apoiar o processo de detecção de problemas nos controles de privacidade de RSOs.

Em relação à inspeção *ad hoc*, nota-se que houve algumas discordâncias. O participante P26, por exemplo, discordou totalmente de todas as afirmativas do indicador em foco, relatando o seguinte discurso "*eu discordei, pois creio que faltou orientação da técnica no sentindo de definir quais pontos atentar*". Tal questão demonstra que uma inspeção *ad hoc* pode não ser útil, pois não há uma orientação sobre como proceder ou o que procurar em uma atividade de detecção de defeitos.

Figura 24. Percepção sobre Utilidade – 2º Estudo de Viabilidade



Fonte: Próprio autor.

6.5.3 Resultados Qualitativos do 2º Estudo de Viabilidade da PIT-OSN 2

Realizou-se uma análise dos dados qualitativos (comentários adicionais dos participantes) contidos nos questionários pós-inspeção. Como o intuito é evoluir a PIT-OSN 2, foi realizada uma análise somente dos comentários feitos pelos inspetores que utilizaram esta técnica em questão.

Seguindo o mesmo percurso do estudo anterior, os dados qualitativos extraídos dos questionários foram analisados utilizando um subconjunto de fases do processo de codificação sugerido por Corbin e Strauss (1998) para o método GT – as codificações aberta (1ª fase) e axial (2ª fase). O processo de codificação produziu um total de 56 códigos que foram associados à 3 categorias. O questionário pós-inspeção possuía questões abertas para coletar o ponto de vista dos participantes sobre os pontos positivos e negativos da técnica, dificuldades de uso com a técnica e sugestões de melhorias para a técnica, o que levou à identificação destas três categorias: Dificuldade de Aplicação, Facilidade de Aplicação e Sugestões de Melhorias.

A categoria "Dificuldade de Aplicação" teve um total de 13 códigos produzidos, entre estes, alguns evidenciam as principais dificuldades com a aplicação da técnica e alguns pontos negativos em utilizá-la: "*A tabela de inspeção da PIT-OSN 2 não é fácil de lembrar*", "*Alguns itens de verificação da PIT-OSN 2 tornam difícil a busca por problemas*", "*A PIT-OSN 2 pode não ser rápida se as funcionalidades da rede social forem obscuras*", "*A tabela de inspeção da PIT-OSN 2 não é eficiente de início*" e "*Alguns itens de verificação da PIT-OSN 2 tem um certo grau de dificuldade de serem encontrados no app*".

O participante P01 realizou uma crítica sobre aplicação da PIT-OSN 2, destacando que a mesma não avalia informações sensíveis de privacidade, através do seguinte argumento "*Acredito que existem falhas mais críticas que poderiam ser avaliadas, como a frequência da coleta de localização, áudio ou imagem"*. No entanto, nem todas as redes sociais possuem compartilhamento de áudio e imagens e uma das premissas do conjunto de técnicas PIT-OSN é que o mesmo seja genérico e não específico. Portanto, focamos em questões geais sobre controles de privacidade para que a técnica possa ser aplicável em qualquer domínio.

A categoria "Facilidade de Aplicação" teve um total de 32 códigos produzidos, os quais destacam os principais pontos positivos da técnica, alguns destes códigos são: "*A técnica PIT-OSN 2 é fácil de utilizar*", "*A técnica não tem ambiguidades*", "*A técnica permite achar problemas nas redes sociais*", "*A técnica PIT-OSN 2 abrange os principais termos de*

privacidade", "*A técnica é completa*" e "*A técnica PIT-OSN 2 guia a melhoria da rede social sob inspeção*".

Por fim, a categoria "Sugestão de melhorias" teve 07 códigos produzidos que apontavam as principais sugestões sobre complementos para os itens de verificação e estrutura da técnica. Dentre estes códigos, dois sugerem que a técnica informe quais informações que o sistema coleta sem o consentimento do usuário: "*Sugestão em inserir itens que avaliam quais informações que são adquiridas pela rede sem o consentimento do usuário*" e "*Sugestão em incluir itens sobre quais permissões que a aplicação usa quando informações sensíveis são coletadas*". Estas sugestões são relevantes e já estão inseridas, mas não especificamente na técnica PIT-OSN 2, que trata sobre controles de privacidade, e sim na técnica PIT-OSN 3 que aborda diretamente sobre estas questões que devem estar contidas nas políticas de privacidade da aplicação. Com a aplicação da PIT-OSN 3 é possível avaliar esta coleta indevida de dados.

6.5.4 Melhorias na PIT-OSN 2

A análise dos dados qualitativos nos forneceu um retorno importante para melhorar alguns pontos da técnica PIT-OSN 2. Nenhum participante reportou um item específico que poderia ser um indício de inadequação. Logo, uma análise minuciosa foi realizada e observou-se que haviam poucos ajustes a serem efetuados na estrutura da técnica PIT-OSN 2, a qual contou com as seguintes melhorias:

- A descrição de alguns itens de verificação foi simplificada para tornar a leitura mais clara e concisa.
- O item 2H2 da dimensão "Negociação de privacidade" foi excluído, pois este não estava apontando um problema específico de controles de privacidade. Além disso, esta dimensão teve a sua nomenclatura alterada para "Controle de reputação".
- O item 2I1 da dimensão "Separação interna de identidades" foi retirado, pois este estava com o mesmo sentido no item 2I2 da mesma dimensão. Além disso, esta dimensão também teve sua nomenclatura alterada para "Publicação seletiva".
- Na dimensão "Solicitações de amizade", o termo amizade foi substituído pelo termo "relacionamentos" para deixar a dimensão com uma nomenclatura mais genérica, uma vez que este relacionamento pode ser de amizade (em redes sociais de propósito geral) ou profissional (em redes sociais de colaboração científica).

Estes refinamentos deram origem a uma nova versão da técnica PIT-OSN2 (v4). A Figura 25 apresenta o extrato completo da técnica em questão (versão 4).

Figura 25. Extrato completo da PIT-OSN 2 (versão 4)

Técnica PIT-OSN 2 - Inspeção dos Controles de Privacidade	
2A. Direito de Privacidade	
2A1	Verifique se rede social permite ao usuário denunciar uma informação, imagem ou vídeo que viola os seus direitos de privacidade
2A2	Verifique se há uma opção que permite denunciar uma conta que está se passando por um usuário (conta *fake*)
2B. Usabilidade e Privacidade	
2B1	Verifique se há atalhos de privacidade que forneçam acesso rápido a algumas das configurações e ferramentas de privacidade mais relevantes da rede social
2B2	Verifique se o usuário tem a opção de um mecanismo de ajuda que facilite a localização de um determinado controle de privacidade
2B3	Verifique se em algum controle de privacidade aparecem informações escritas em um idioma diferente do utilizado eventualmente pelo usuário
2C. Transparência de dados	
2C1	Verifique se há uma opção que permite ao usuário solicitar acesso aos dados pessoais armazenados na rede social
2C2	Verifique se o usuário tem a opção de acessar um registro ou histórico de atividades realizados na rede social
2D. Aplicativos de terceiros	
2D1	Verifique se a rede social permite ao usuário visualizar os aplicativos ou sites de terceiros ativos em sua conta
2D2	Verifique se o usuário tem a opção de editar as informações que os aplicativos ou sites de terceiros podem ter acesso na sua conta
2D. Aplicativos de terceiros	
2D3	Verifique se a rede social permite ao usuário remover os aplicativos ou sites de terceiros que não desejam mais ter acesso ou utilizar
2D4	Verifique se a rede social permite ao usuário denunciar um aplicativo ou site de terceiros que estejam comprometendo a sua privacidade
2E. Solicitações de relacionamento	
2E1	Verifique se a rede social permite editar quem pode seguir ou enviar solicitação de relacionamento para um determinado usuário
2E2	Verifique se há uma opção para remover alguém de sua lista de relacionamento da rede social
2F. Bloqueio	
2F1	Verifique se o usuário tem a opção de bloquear uma pessoa que esteja comprometendo a sua privacidade
2G. Privacidade na busca	
2G1	Verifique se há uma opção que restringe a indexação pública do perfil do usuário por outros mecanismos de busca fora da rede social
2G2	Verifique se a rede social disponibiliza um controle que possa restringir quem pode procurar pelo usuário usando informações pessoais do contato, como o endereço de e-mail ou o número de telefone
2H. Controle de reputação	
2H1	Verifique se a rede social permite ocultar do perfil do usuário uma publicação a qual o mesmo foi marcado ou mencionado sem a sua permissão
2H2	Verifique se o usuário tem a opção de analisar publicações que as pessoas o marcaram ou mencionaram antes de serem exibidas em seu perfil na rede social
2I. Publicação seletiva	
2I1	Verifique se a rede social permite o usuário criar listas personalizadas para que seja possível compartilhar as postagens com grupos específicos de amigos

Técnica PIT-OSN 2 - Inspeção dos Controles de Privacidade	
2J. Gerenciamento de informações sobre o usuário	
2J1	Verifique se o usuário tem a opção de alterar informações de seu login na rede social
2J2	Verifique se o usuário tem a opção de desativar a sua conta temporariamente ou permanentemente na rede social
2J3	Verifique se o usuário tem a opção de criar um filtro avançado para desativar as notificações de determinados usuários que deseja evitar
2J4	Verifique se o usuário tem a opção de selecionar quem pode visualizar a sua lista de amigos ou seguidores na rede social
2L. Confidencialidade	
2L1	Verifique se há uma opção que permita o usuário limpar o seu histórico de busca ou ações na rede social
2L2	Verifique se o usuário tem a opção de ocultar uma publicação compartilhada por ele em seu perfil
2M. Comentários	
2M1	Verifique se o usuário tem a opção de controlar quem pode comentar sua publicação no sistema
2M2	Verifique se o usuário tem a opção de denunciar um comentário, tanto em sua publicação pessoal quanto na publicação de outro indivíduo, que contenha conteúdo impróprio
2M3	Verifique se o usuário tem a opção de ativar um filtro de palavras-chave para ocultar para que ninguém veja comentários que contenham palavras, frases, números ou *emojis* considerados inapropriados ou ofensivos
2N. Controle de localização	
2N1	Verifique se o usuário tem a opção de desativar os serviços de localização na rede social
2N2	Verifique se o usuário tem a opção de editar ou remover a sua localização em uma determinada publicação na rede social
2O. Pós-Morte e Privacidade	
2O1	Verifique se o usuário tem a opção de escolher indicar um contato herdeiro para gerenciar a sua conta caso o mesmo venha a falecer
2O2	Verifique se a rede social permite transformar a conta de um usuário falecido em memorial digital
2O3	Verifique se a rede social permite solicitar que a conta de um usuário falecido seja permanentemente removida do sistema.

Fonte: Próprio autor.

6.6 RESULTADOS DO 2º ESTUDO DE VIABILIDADE DA PIT-OSN 3

6.6.1 Resultados Quantitativos do 2º Estudo de Viabilidade da PIT-OSN 3

A Tabela 34 apresenta o resultado geral das inspeções realizadas nas políticas de privacidade do ResearchGate. Os participantes P01 a P14 aplicaram a técnica PIT-OSN 3. Enquanto que os participantes P15 a P26 realizaram inspeções *ad hoc*. Pode-se observar que os inspetores que utilizaram a PIT-OSN 3 produziram um diagnóstico com 0 a 5 defeitos gastando em torno de 7 a 47 minutos de inspeção. Por outro lado, os inspetores que realizaram inspeções *ad hoc* levaram entre 16 a 48 minutos na atividade de detecção de defeitos, encontrando entre 0 a 7 defeitos.

Tabela 34. Resultado das inspeções – 2º Estudo de Viabilidade PIT-OSN 3

Part.	EP	EAI	DS	FP	DF	Tempo (min)	Defeito /(hora)	Eficácia	Técnica
P01	Nenhuma	Sim	3	1	2	24	5,00	9,52%	PIT-OSN 3
P02	Nenhuma	Não	5	2	3	20	9,00	14,29%	
P03	Nenhuma	Sim	3	2	1	11	5,45	4,76%	
P04	Nenhuma	Sim	4	4	0	7	0,00	0,00%	
P05	Nenhuma	Sim	5	3	2	23	5,22	9,52%	
P06	Nenhuma	Não	5	2	3	25	7,20	14,29%	
P07	Nenhuma	Sim	2	1	1	20	3,00	4,76%	
P08	Nenhuma	Sim	3	1	2	16	7,50	9,52%	
P09	Nenhuma	Sim	4	1	3	20	9,00	14,29%	
P10	Nenhuma	Não	5	2	3	16	11,25	14,29%	
P11	Nenhuma	Sim	4	3	1	25	2,40	4,76%	
P12	Nenhuma	Sim	6	1	5	22	13,64	23,81%	
P13	Nenhuma	Não	4	3	1	47	1,28	4,76%	
P14	Nenhuma	Não	2	1	1	34	1,76	4,76%	
P15	Nenhuma	Sim	5	3	2	25	4,80	9,52%	AD HOC
P16	Nenhuma	Não	2	2	0	45	0,00	0,00%	
P17	Nenhuma	Não	3	1	2	24	5,00	9,52%	
P18	Nenhuma	Sim	1	1	0	22	0,00	0,00%	
P19	Nenhuma	Sim	7	0	7	26	16,15	33,33%	
P20	Nenhuma	Sim	2	1	1	18	3,33	4,76%	
P21	Nenhuma	Não	4	4	0	48	0,00	0,00%	
P22	Nenhuma	Sim	5	2	3	46	3,91	14,29%	
P23	Nenhuma	Sim	1	1	0	20	0,00	0,00%	
P24	Baixa	Sim	1	1	0	22	0,00	0,00%	
P25	Média	Sim	2	2	0	16	0,00	0,00%	
P26	Nenhuma	Sim	4	3	1	27	2,22	4,76%	

Legenda:
Part.. - Participante; **EP** – Experiência em Privacidade; **EAI** – Experiência em Avaliação de Interface; **DS** – Número de Discrepâncias; **FP** – Número de Falso-Positivos; **DF** – Número de Defeitos;

Fonte: Próprio autor.

Nota-se que um dos participantes que aplicou a PIT-OSN 3 (participante P04) chegou a identificar 4 discrepâncias, no entanto, nenhuma destas eram defeitos reais de privacidade. Isso pode ter ocorrido devido este inspetor ter gastado somente 7 minutos na atividade de detecção de defeitos. Já no grupo das inspeções *ad hoc*, 6 (seis), dos 12 participantes, não identificaram defeitos nas políticas de privacidade da aplicação alvo. No geral, as inspeções com as duas técnicas resultaram em um diagnóstico com 21 defeitos conhecidos relacionados as políticas de privacidade inspecionada.

A Tabela 35 apresenta os dados gerais do 2º estudo de viabilidade, bem como os resultados para os indicadores de eficiência e eficácia das técnicas. A eficiência foi calculada como o número total de defeitos detectados/tempo total gasto na inspeção*60, seguindo a definição do indicador. A eficácia foi calculada como a média entre número de defeitos

detectados/número total de defeitos conhecidos (únicos) encontrados com as duas técnicas, seguindo também a definição do indicador.

Tabela 35. Eficiência e Eficácia – 2º Estudo de Viabilidade da PIT-3

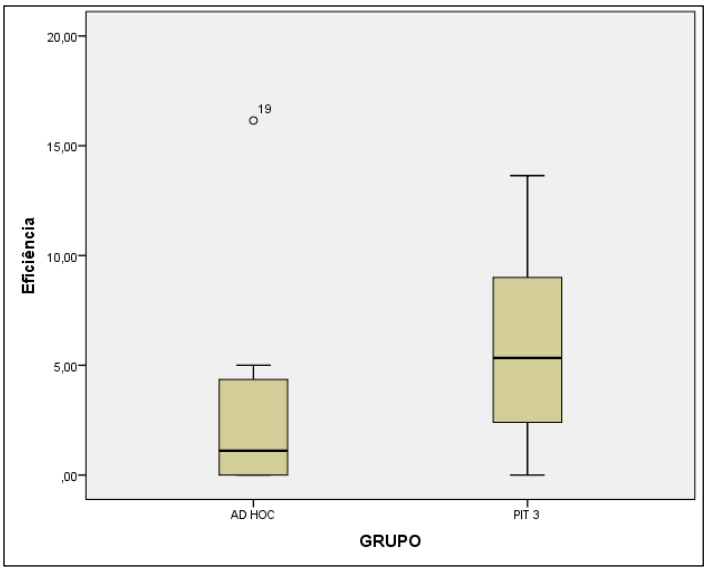
Item analisado	Técnicas	
	PIT-3	Ad hoc
Total de discrepâncias detectadas	55	37
Total de defeitos detectados (incluindo os duplicados)	28	16
Total de defeitos conhecidos (únicos)	9	12
Total de Falso-Positivos	27	21
Média da eficácia	9,52%	6,35%
Tempo total dedicado as inspeções (minutos)	310	339
Média da eficiência	5,42	2,83

Fonte: Próprio autor.

Seguindo a mesma direção das análises anteriores, uma análise específica usando o teste de normalidade de Shapiro-Wilk com nível de significância de α=0,05, para eficácia e eficiência, também foi realizada. O teste de normalidade mostrou que a distribuição dos valores de eficácia é normal (com p=0,134 para PIT-3 e p=0,001 para ADHOC), e que a distribuição dos valores de eficiência também é normal (com p=0,841 para a PIT-3 e p=0,001 para ADHOC). Desta forma, um teste paramétrico (t-teste) foi selecionado para avaliar a eficiência e eficácia dos grupos que aplicaram tais técnicas. Um resumo dos resultados destas análises é exibido através do gráfico de *boxplot*. As análises estatísticas foram executadas usando a ferramenta SPSS V. 23, com α = 0,10. A escolha desta significância estatística foi motivada pelo pequeno tamanho da amostra usada neste estudo. A Figura 26 apresenta o gráfico de *boxplot* com a distribuição da eficiência por técnica.

Com base na visão fornecida pela Figura 26, pode-se verificar que a mediana do grupo da PIT-OSN 3 está um pouco mais elevada que a mediana do grupo da *ad hoc*. No entanto, quando as duas amostras são comparadas usando o t-teste, não se encontra diferença significativa entre os dois grupos (p = 0,101). Nesta ótica, estes resultados apoiam a hipótese nula H01 que afirma que não há diferença entre a eficiência de inspeções de privacidade que aplicam a PIT-OSN 3 e a eficiência de inspeções *ad hoc*, rejeitando, portanto, a hipótese alternativa HA1. Esses resultados apontam que a PIT-OSN 3 e as inspeções *ad hoc* proveram eficiência similar quando utilizadas para inspecionar políticas de privacidade da ResearchGate.

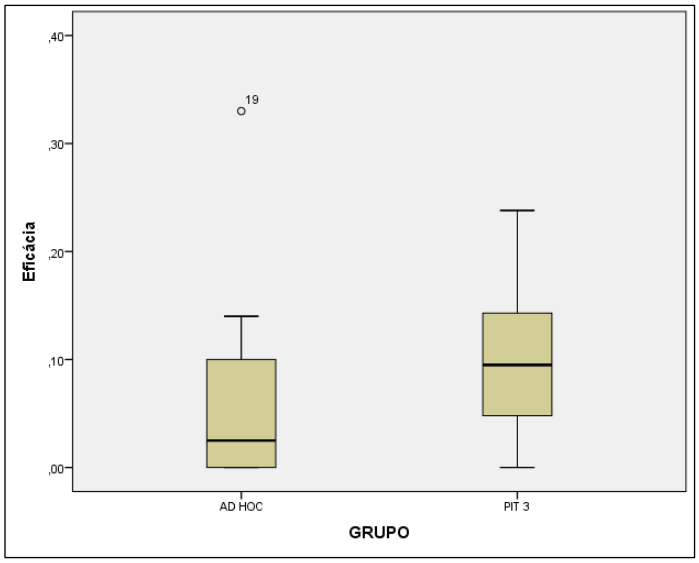
Figura 26. Boxplot comparando a eficiência por técnica do 2º estudo de viabilidade



Fonte: Próprio autor.

A mesma análise foi aplicada para determinar se havia alguma diferença significativa relacionando o indicador de eficácia das duas técnicas na detecção de defeitos em políticas de privacidade. O gráfico de *boxplots* com a distribuição da eficácia por técnica (ver Figura 27) aponta que o grupo da PIT-OSN 3 teve uma eficácia similar ao grupo da *ad hoc*. No entanto, quando se compara as duas amostras usando o t-teste, não se encontra diferença estatística significante entre os dois grupos (p = 0,332). Estes resultados apoiam a hipótese nula H02 – "Não há diferença entre a eficácia de inspeções de privacidade que aplicam a PIT-3 e a eficácia de inspeções *ad hoc*", e em razão disso rejeitam a hipótese HA2.

Figura 27. Boxplot comparando a eficácia por técnica do 2º estudo de viabilidade



Fonte: Próprio autor.

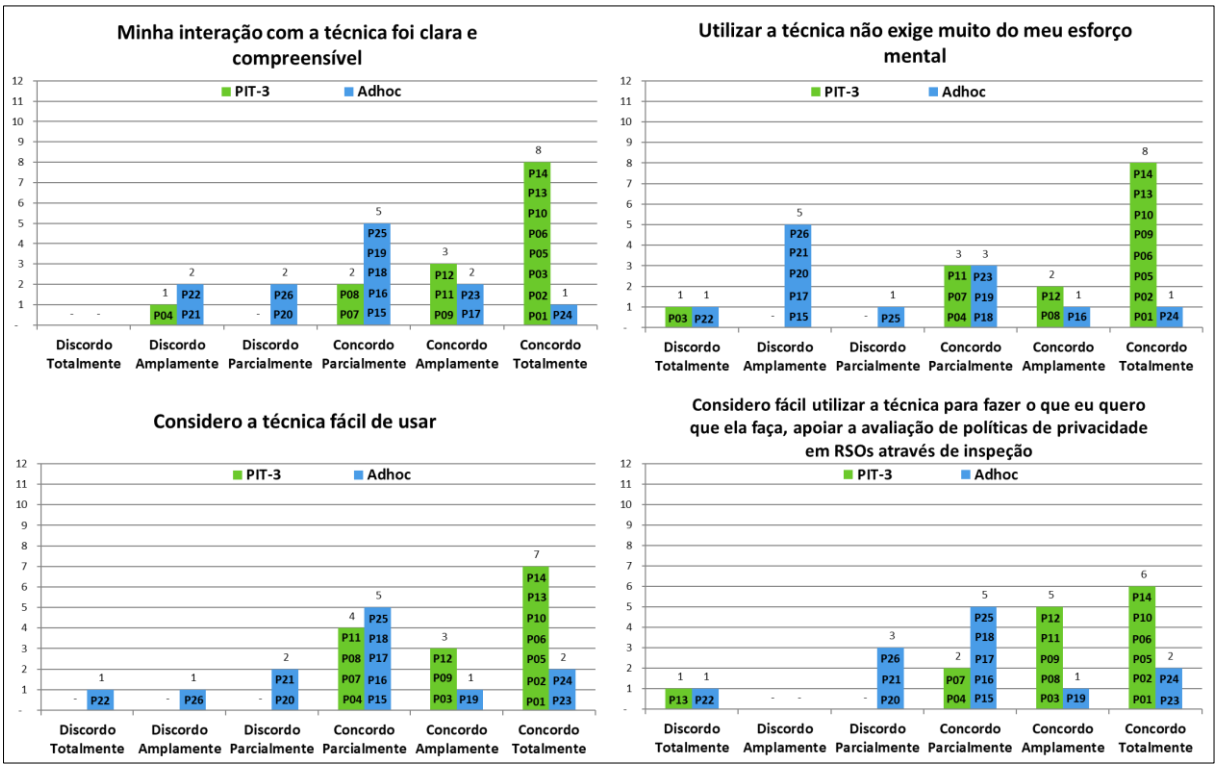
6.6.2 Análise da Percepção dos Participantes do 2º Estudo de Viabilidade da PIT-3

Os questionários pós-inspeção contendo o grau de aceitação dos participantes em relação as técnicas também foram analisados com base no modelo TAM (*Technology Acceptance Model* – TAM). Os dois indicadores utilizados foram (1) Facilidade de uso percebida e (2) Utilidade percebida. Uma discussão sobre os resultados obtidos a partir destes indicadores será abordada a seguir:

a. Facilidade de uso percebida

A Figura 28 exibe as respostas referentes à facilidade de uso percebida da PIT-OSN 3 e das inspeções *ad hoc*. Em relação à PIT-OSN 3, alguns inspetores destacaram diversos pontos positivos em relação à estrutura e ao conteúdo da técnica, tal como abordado no relato do participante P01, o qual destacou: "*Chama a atenção para algumas informações que eu ainda não tinha prestado atenção como: uso por menores, leis em diferentes países e uso de dados por terceiros...eu realmente gostei desta [técnica]*". O participante P02 também salientou um aspecto positivo "*achei a técnica bem completa*". Tais visões indicam que, no geral, a técnica foi considerada fácil de usar pelos participantes do estudo.

Figura 28. Percepção sobre Facilidade de Uso – 2º estudo de viabilidade PIT-3



Fonte: Próprio autor.

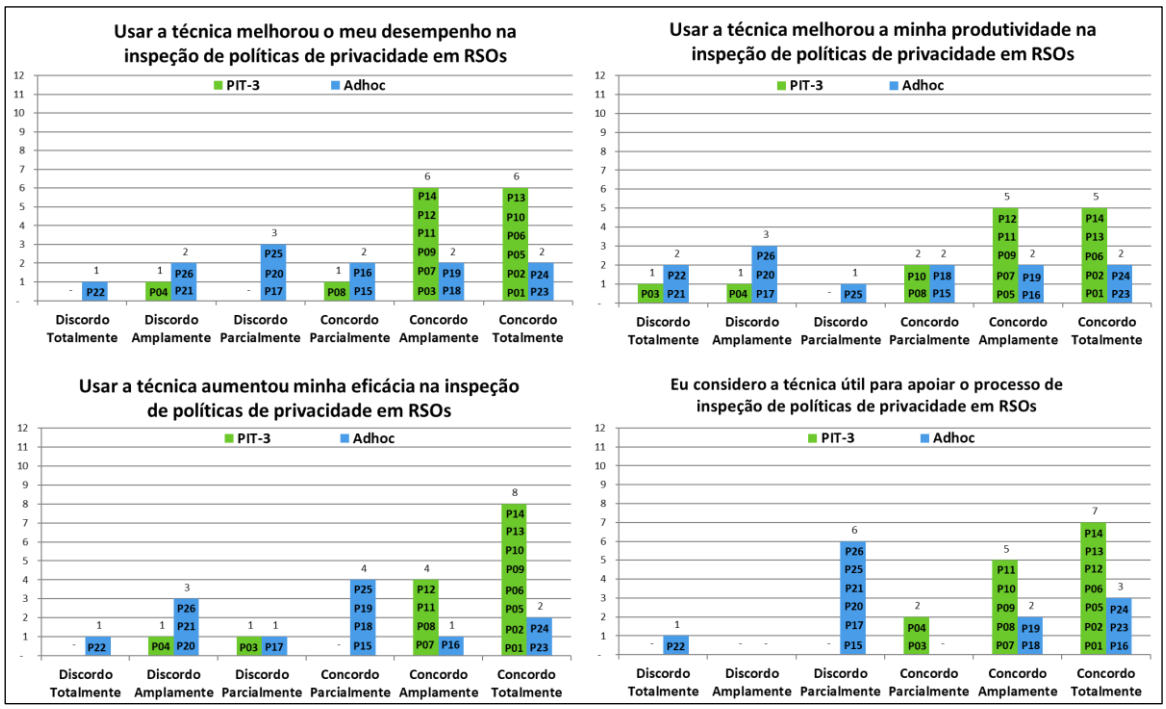
Em relação às inspeções *ad hoc*, houve graus de concordância e discordância sobre a facilidade de uso percebida da técnica em questão. Nota-se que a afirmativa "*Utilizar a técnica não exige muito do meu esforço mental*" foi a sentença a qual os participantes mais discordaram. O participante P15, por exemplo, argumentou: "*(...) meus pensamentos se afirmam quando digo que é uma técnica que requer muito esforço mental para conseguir resultados satisfatórios*". O participante P17 também justificou seu grau de discordância através do seguinte relato: "*[a técnica] falha por não ter instruções mais específicas*".

Desta forma, nota-se que estes resultados sugerem que uma inspeção sem técnica (*ad hoc*) pode exigir mais esforço do que uma técnica com procedimentos que guiam o inspetor durante a atividade de detecção de defeitos. Além disso, uma inspeção *ad hoc* acaba sendo dependente exclusivamente da experiência do avaliador, caso este não seja experiente no domínio do sistema, a técnica pode ser ineficaz. Ou seja, o custo/eficiência de uma inspeção *ad hoc* pode ser adequado quando inspetores possuem muita experiência.

b. Utilidade percebida

As respostas referentes à utilidade percebida das técnicas são apresentadas na Figura 29. As afirmativas buscam identificar a percepção do inspetor em relação a técnica ajudar a melhorar o desempenho, a produtividade e a eficácia na inspeção e se o inspetor a considera útil para inspeções de políticas de privacidade.

Figura 29. Percepção sobre Utilidade – 2º estudo de viabilidade PIT-3



Fonte: Próprio autor.

No que diz respeito a técnica PIT-OSN 3, nota-se que a maioria dos participantes que a aplicaram concordaram com as sentenças do indicador em questão, sugerindo que a técnica é potencialmente útil para apoiar a detecção de defeitos nos cenários das políticas de privacidade. No entanto, o participante P04 discordou de três afirmativas do indicador em foco e justificou: "*Discordei, pois há pontos negativos que podem ser melhorados"*. Nesse sentido, nota-se que ainda podem existir pontos que podem ser aprimorados para tornar a técnica mais útil.

6.6.3 Análise Qualitativa do 2º Estudo de Viabilidade da PIT-3

Uma análise dos dados qualitativos (comentários adicionais dos participantes) contidos nos questionários pós-inspeção foi efetuada. Como o intuito é evoluir a PIT-OSN 3, realizou-se uma análise somente dos comentários feitos pelos inspetores que utilizaram esta técnica.

Seguindo o mesmo percurso dos estudos anteriores, os dados qualitativos extraídos dos questionários foram analisados utilizando um subconjunto de fases do processo de codificação sugerido por Corbin e Strauss (1998) para o método GT – as codificações aberta (1ª fase) e axial (2ª fase).

Analisando os conteúdos produzidos nos questionários, verificou-se que as respostas apontavam um maior direcionamento em relação à estrutura, ao uso e às possíveis melhorias para a técnica PIT-OSN 3. O processo de codificação produziu no total 37 códigos que foram associados à estas três categorias: Estrutura da PIT-OSN 3, Facilidade de Aplicação e Sugestões de Melhorias.

A categoria "Estrutura da PIT-OSN 3" teve um total de 05 códigos produzidos, entre estes, alguns evidenciam pontos positivos e negativos quanto à estrutura da técnica, tais como: "Aplicar a PIT-OSN 3 em documentos longos pode ser demorado", "A PIT-OSN 3 não é tão eficaz". Em relação aos pontos positivos da técnica, destacam-se os seguintes códigos: "A PIT-OSN 3 permite uma leitura guiada dos termos das políticas de privacidade", e "As categorias de checagem da PIT-OSN 3 estão bem divididas".

A categoria "Facilidade de Aplicação" teve um total de 26 códigos produzidos, os quais destacam os principais pontos positivos da técnica, alguns destes códigos são: "A PIT-OSN 3 é clara", "A PIT-OSN 3 é completa", "A PIT-OSN 3 fornece uma boa linha de raciocínio durante a inspeção", "A PIT-OSN 3 é proveitosa para adquirir conhecimentos durante a inspeção", "A PIT-OSN 3 é prática" e "A PIT-OSN 3 identifica problemas de

maneira rápida". Por fim, a categoria de "Sugestões de Melhoria" produziu 3 códigos que destacam algumas sugestões que podem ajudar a técnica ser mais prática.

Nota-se que, no geral, poucas dificuldades de aplicação com a PIT-OSN 3 foram evidenciadas. Tal questão pode ser observada através dos códigos produzidos com base nos comentários dos participantes, onde não foi identificado um código específico que apontasse indícios de inadequação na técnica. Com base nestes resultados, uma revisão sucinta foi realizada sob a estrutura da técnica, conforme descrito na próxima subseção.

6.6.4 Melhorias na PIT-OSN 3

A análise dos dados qualitativos concedeu um retorno fundamental o qual demonstrou que a técnica PIT-OSN 3 está adequada para uso. Ainda assim, uma análise minuciosa foi realizada e observou-se que haviam poucos ajustes a serem efetuados na estrutura da técnica PIT-OSN 3, onde a principal melhoria realizada foi tornar a descrição de alguns itens de verificação mais simples para tornar a leitura do documento das políticas mais clara e concisa. A Figura 30 apresenta o extrato completo da PIT-OSN 3 (versão 4).

Figura 30. Extrato completo da PIT-3 (versão 4)

Técnica PIT-OSN 3 - Inspeção das Políticas de Privacidade	
3A. Coleta de dados	
3A1	Verifique se há alguma informação detalhada sobre os tipos de dados que estão sendo coletados do usuário
3A2	Verifique se a política de privacidade especifica qual o meio que a rede social utiliza para coletar dados do usuário (se é através do cadastro de conta, se através de informações de compras ou comentários por exemplo)
3B. Uso e divulgação dos dados	
3B1	Verifique se a política de privacidade especifica como a rede social pode utilizar e manipular as informações fornecidas pelo usuário
3B2	Verifique se a política de privacidade especifica com quem (parceiros, provedores ou outros usuários) a rede social pode divulgar as informações fornecidas pelo usuário
3B3	Verifique se há declarações informando em que circunstâncias que a rede social pode divulgar informações do usuário a terceiros, como em casos de razões legais por exemplo
3B4	Verifique se há alguma declaração informando sobre o que acontece com as informações do usuário no caso de uma alteração de controle (como venda ou transferência da rede social para outra empresa)
3C. Armazenamento de dados	
3C1	Verifique se há declarações sobre como a rede social armazena e processa (se em bancos de dados de outros países) os dados coletados do usuário
3C2	Verifique se a política de privacidade especifica por quanto tempo a rede social pode manter armazenado os dados do usuário, caso o indivíduo escolha desativar sua conta

Técnica PIT-OSN 3 - Inspeção das Políticas de Privacidade	
3C. Armazenamento de dados	
3C3	Verifique se as políticas de privacidade especificam como utilizam os cookies e outras tecnologias de armazenamento
3D. Clareza	
3D1	Verifique se a política apresenta alguma descrição visual (como vídeos breves ou ilustrações) que tornam o documento mais fácil de entender
3D2	Verifique se há alguma informação sobre possíveis modificações ou atualizações nas políticas de privacidade da rede social e se há formas adicionais de notificação de mudanças para o usuário (como lembretes regulares)
3D3	Verifique se as políticas de privacidade possuem alguma informação escrita em outro idioma diferente do idioma do usuário
3E. Ajuda online	
3E1	Verifique se as políticas de privacidade especificam algum meio para o usuário entrar em contato com a rede social
3F. Anonimato em transações	
3F1	Verifique se é especificada alguma medida para preservar informações financeiras do usuário disponibilizadas em transações na rede social (como conexão criptografada e proteção de hardware e software por exemplo)
3G. Dados confidenciais	
3G1	Verifique se as políticas de privacidade especificam as opções para obter o consentimento do usuário quando algumas informações confidenciais precisarem ser usadas ou divulgadas
3G2	Verifique se as políticas de privacidade apresentam um relatório de transparência sobre as informações mais solicitadas em processos jurídicos ou sobre as ações do usuário na rede social
Técnica PIT-OSN 3 - Inspeção das Políticas de Privacidade	
3I. Restrição de idade	
3H1	Verifique se as políticas de privacidade fornecem informações sobre o acesso e envolvimento de crianças na rede social
3H2	Verifique se as políticas de privacidade especificam algum mecanismo de restrição de idade para preservar a participação de menores na rede social
3J. Legislação vigente	
3I1	Verifique se as políticas de privacidade especificam se estão cumprindo ou seguindo a legislação vigente do país em que a rede social está em uso
3L. Serviços de publicidade	
3J1	Verifique se há informações sobre os serviços de publicidade e como eles atuam na rede social
3J2	Verifique se as políticas de privacidade especificam informações sobre preferências publicitárias e como o usuário pode deixar de receber anúncios indesejados

Fonte: Próprio autor.

6.7 LIMITAÇÕES DO 2º ESTUDO DE VIABILIDADE

As limitações deste segundo estudo de viabilidade estão relacionadas principalmente a três itens: (1) a divisão de grupos; (2) a inspeção parcial nas redes sociais e (3) o processo de avaliação parcial utilizado no estudo. Em relação ao item 1, grupo que aplicou a PIT-OSN tinha dois integrantes a mais que o grupo que realizou inspeções *ad hoc*. Portanto, há uma ameaça à validade neste contexto. Em relação ao item 2, foram realizadas inspeções em três diferentes RSOs, porém, estas avaliações foram executadas usando somente uma técnica do

conjunto para cada rede social. Desta forma, houve uma inspeção limitada. Por fim, nota-se que os participantes do estudo não seguiram todo o processo de avaliação sugerido pelo conjunto de técnicas PIT-OSN, sendo que somente as fases de preparação e detecção de defeitos foram realizadas pelos inspetores, as demais atividades do processo sugerido pelo conjunto de técnicas foram executadas por outros pesquisadores, sendo esta também uma limitação do estudo.

6.8 DISCUSSÃO DOS RESULTADOS

Os dados obtidos neste segundo estudo apoiaram a conclusão de que o conjunto de técnicas PIT-OSN é viável. Mesmo considerando a limitação dos estudos devido ao tamanho da amostra (ver seção 6.7), os resultados indicam que é possível produzir um bom diagnóstico de defeitos de privacidade com o auxílio das técnicas, sendo estas, portanto, viáveis para uso em inspeções de privacidade em RSOs. Tal observação apoia a primeira questão de pesquisa proposta no experimento: "*O conjunto de técnicas é viável em relação ao número de defeitos detectados"?*. Além disso, os resultados do segundo estudo de viabilidade não somente proveram uma resposta positiva para a primeira questão de pesquisa, como também forneceram um importante retorno para melhorias adicionais nas técnicas propostas.

Os resultados quantitativos foram utilizados para investigar detalhadamente o conjunto de técnicas PIT-OSN e seus itens de verificação de privacidade. A partir do estudo executado, foram calculados o número de discrepâncias (os itens apontados como possíveis defeitos pelos inspetores na atividade de detecção) e o número de defeitos reais (as discrepâncias que foram classificadas como defeitos reais na atividade de discriminação de defeitos). Com base nestes dados, foi possível observar que houve alguns erros durante as inspeções. Alguns destes erros eram resultados do julgamento incorreto dos inspetores durante a inspeção e outros eram erros oriundos da estrutura das técnicas. Realizando uma revisão criteriosa de cada item de verificação, foi possível identificar alguns itens que levavam a uma classificação incorreta e alguns pontos que tinham de ser melhorados quanto às características estruturais das técnicas. Estas análises conduziram a uma nova versão das técnicas (v4).

Além disso, os resultados quantitativos do segundo estudo de viabilidade mostraram que a técnica PIT-OSN 1 foi significativamente mais eficaz e eficiente do que inspeções *ad hoc*, apoiando a hipótese alternativa definida no projeto do experimento deste trabalho. Já os resultados com o uso das técnicas PIT-OSN 2 e PIT-OSN 3 apontaram que as mesmas proveram eficiência e eficácia similar ao de inspeções *ad hoc*, quando utilizadas para inspecionar a privacidade do *Facebook* e do *ResearchGate*. No entanto, vale ressaltar que

estes experimentos foram executados em apenas uma única rede social. Desta forma, novos estudos devem ser efetuados para testar se a eficiência e eficácia da PIT-2 e PIT-3 é equivalente ou superior a de inspeções *ad hoc*, quando utilizadas para avaliar outros tipos de RSOs existentes.

As análises com o TAM e dos dados qualitativos mostraram que, de um modo geral, os participantes concordam que o conjunto de técnicas PIT-OSN é útil para encontrar problemas de privacidade. No entanto, muitos participantes ponderaram o custo e esforço mental que as técnicas podem exigir durante uma aplicação. Portanto, deve-se considerar que as técnicas são úteis para inspeções de privacidade, porém, pode haver um esforço mental inerente a uma atividade de detecção de defeitos com o uso das mesmas.

Nota-se também que, no geral, a PIT-OSN 2 e PIT-OSN 3 foram as técnicas consideradas mais fáceis de usar considerando que estas focam em características de privacidade, como controles (PIT-2) e políticas (PIT-3), que podem ser mais comuns para o inspetor durante uma avaliação. Em contrapartida, a PIT-OSN 1 foi considerada mais difícil de aplicar, no entanto, tal técnica foi a que obteve o maior indicador de eficiência e eficácia do conjunto, comparativamente a PIT-OSN 2 e 3. Isto pode ter ocorrido, pois a técnica PIT-OSN 1 focaliza em uma característica mais abstrata de privacidade (níveis), podendo ter aspectos que, em alguns pontos, são mais difíceis de analisar.

6.9 CONSIDERAÇÕES SOBRE O CAPÍTULO

Este capítulo teve como objetivo apresentar o percurso metodológico adotado para avaliação e evolução do conjunto de técnicas PIT-OSN. A metodologia seguida para a condução deste processo organiza suas atividades de modo que nos primeiros estudos executados sejam avaliadas as questões principais relacionadas ao custo-eficiência da técnica/tecnologia em desenvolvimento. Esta organização tem por objetivo evitar o desperdício de esforços e minimizar os problemas ao avaliar a nova tecnologia (SHULL *et al*. 2001).

Além disso, este capítulo também descreveu o planejamento, execução e análise de dois estudos de viabilidade. Os resultados obtidos a partir da execução destes estudos apoiaram a conclusão de que o conjunto de tecnologias PIT-OSN é viável. Os resultados quantitativos do segundo estudo viabilidade apontaram que a técnica PIT-OSN 1 foi significativamente mais eficaz e eficiente do que uma inspeção *ad hoc*. Enquanto as outras técnicas tiveram eficácia e eficiência similar, quando utilizadas para inspecionar redes sociais online. Os dados qualitativos dos questionários pós-inspeção demonstraram que, de um modo

geral, os participantes de ambos os estudos afirmam que o conjunto de técnicas ajuda a detectar problemas de privacidade. No próximo capítulo serão apresentadas as considerações finais e contribuições deste trabalho, bem como as perspectivas de trabalhos futuros para continuação desta pesquisa.

.

CAPÍTULO 7 – CONCLUSÕES E PRÓXIMOS PASSOS

Este capítulo apresenta as considerações finais desta pesquisa, resumindo sua proposta inicial e contribuições. Os próximos passos fornecem a direção para que seja dada a continuidade a este trabalho científico.

7.1 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo central propor um conjunto de técnicas de inspeção que apoia a avaliação de privacidade em RSOs, visando promover a qualidade de privacidade destas aplicações. Para atingir este propósito foi definida a PIT-OSN (*Privacy Inspection Technique for Online Social Network*). Estas técnicas foram desenvolvidas a partir de evidências coletadas na literatura científica e foram avaliadas empiricamente através de estudos de viabilidade.

Ao longo desta pesquisa, buscou-se aplicar conceitos recomendados pelo processo de desenvolvimento de tecnologias baseado em evidência, como a condução de um estudo secundário (mapeamento sistemático) e de um estudo primário (estudo de viabilidade) para validar o conjunto de tecnologias concebido.

Inicialmente, identificou-se a carência de tecnologias que apoiassem a avaliação de privacidade através de inspeção. A partir disso, buscou-se a proposição do conjunto de técnicas. Primeiramente, buscamos elaborar uma base de conhecimento prévia para a formulação das técnicas, identificando as principais características de privacidade que compõem a estrutura de uma RSO. Em seguida, optamos por construir uma técnica de leitura contendo itens de verificação agrupados em dimensões de privacidade.

Com base nos resultados dos estudos realizados, o conjunto de tecnologias proposto revelou-se aplicável mesmo por profissionais não especialistas em inspeção de interfaces. Por ser um conjunto de técnicas de inspeção baseado em leitura, o mesma orienta os inspetores a detectarem problemas/defeitos de privacidade, sem exigir que estes sejam especialistas em inspeção. No entanto, o estudo com as técnicas também denotou a necessidade de simplificar alguns pontos para facilitar sua execução e reduzir seu tempo de aplicação. Além disso, pode-se inferir que as tecnologias apresentam um bom nível de eficácia, eficiência, facilidade de uso e utilidade percebida.

Através da análise qualitativa foi possível obter indícios de como as técnicas podiam ser melhoradas para serem mais práticas ou mais fáceis de aprender e/ou aplicar. Ao longo do processo de desenvolvimento do conjunto de técnicas proposto, sempre após a execução de um estudo, novos reajustes nestas eram acrescentados com o propósito de aprimorá-las, até que fosse possível encontrar indicadores que apontassem que o conjunto de tecnologias PIT-OSN era positivamente viável para ser aplicado em RSOs.

Além da técnica, também foram definidos diretrizes e recursos para a realização das inspeções de privacidade, tais como: um processo de avaliação usando as técnicas, uma taxonomia de apoio para auxiliar na classificação dos defeitos de privacidade detectados e uma escala para definir o grau de severidade dos defeitos identificados. Espera-se que estes resultados possam incentivar designers e avaliadores de RSOs a aplicarem uma prática ainda não utilizada, que é a avaliação de privacidade através de inspeção. Desta forma, é possível detectar possíveis defeitos que possam comprometer a interação do usuário com os aspectos de privacidade da aplicação e melhorar a qualidade de uso da privacidade destes sistemas. A seguir são apresentados os requisitos que guiaram a proposta das técnicas e as respostas ao problema de pesquisa, obtidas através dos experimentos executados:

- *Ser fácil de aprender e de utilizar*: em termos de utilidade e facilidade de uso, a PIT-OSN apresenta vantagem sobre as demais tecnologias já existentes, na medida em que apresenta itens de verificação simples, objetivos e genéricos, desvinculados de conhecimentos teóricos do inspetor. Esta questão foi corroborada com base nos estudos realizados, onde todos os participantes foram capazes de desempenhar a atividade de detecção de defeitos. Além disso, as técnicas obtiveram grande aceitação pelos participantes dos estudos, sendo consideradas fáceis de aprender e usar.
- *Apresentar bom nível de eficácia*: a eficácia média do grupo de participantes que utilizou a PIT-OSN 1 foi de 14,00%, enquanto que a eficácia média utilizando inspeções ad hoc foi de 5,67%. Dessa forma, os resultados mostram que a eficácia média da PIT-OSN 1 foi duas vezes superior que a eficácia média de inspeções *ad hoc*. Em relação ao estudo de viabilidade com a PIT-OSN 2, a eficácia média do grupo que aplicou esta técnica foi de 9,05%, enquanto que a eficácia média utilizando inspeções *ad hoc* foi de 7,22%. Por fim, o estudo executado com a PIT-OSN 3 revelou que a eficácia média do grupo de inspetores que aplicaram esta técnica foi de 9,52%, enquanto que a eficácia média utilizando inspeções *ad hoc* foi de 6,35%.

- *Apresentar bom nível de eficiência*: a eficiência média do grupo de participantes que utilizou a PIT-OSN 1 foi de 6,24 defeitos/hora enquanto eficiência média utilizando as inspeções ad hoc foi de 2,94 defeitos/hora. No que tange à aplicação da PIT-OSN 2, a eficiência média do grupo de participantes que aplicou esta técnica foi de 3,97 defeitos/hora enquanto que a eficiência média utilizando inspeções ad hoc foi de 2,98 defeitos/hora. Por fim, no estudo realizado com a PIT-OSN 3, a eficiência média do grupo de inspetores que aplicou a esta técnica foi de 5,42 defeitos/hora enquanto que a eficiência média utilizando as inspeções ad hoc foi de 2,83 defeitos/hora.
- *Oferecer uma boa relação custo-benefício na sua aplicação*: os custos para aplicação do conjunto de técnicas são baixos, uma vez que necessitam de poucas pessoas durante a sua aplicação. Ou seja, duas pessoas conseguem produzir um bom diagnóstico de defeitos de privacidade em um curto período de tempo, tal como exposto nos estudos experimentais. Além disso, o conjunto de técnicas chama atenção para o fato de ser interessante não apenas por ser de baixo custo, mas por sere adequado à validação de aplicações. As técnicas destacam-se também por não serem limitadas a disponibilidade de um apoio ferramental, sendo independentes de um sistema de apoio para serem executadas. Podem ser aplicadas em várias fases do ciclo de design, tanto para uma avaliação formativa (desde que posterior a escolha das representações de interface) quanto em uma avaliação somativa. Ressalta-se também que estas são abrangentes, pois não se limitam a uma determinada rede social, podendo serem aplicadas em diversos contextos. Portanto, as tecnologias propostas oferecem uma boa relação custo-benefício em sua aplicação.

7.2 CONTRIBUIÇÕES

O estudo traz como principal contribuição uma nova abordagem para avaliação de privacidade através de inspeção, destacando o papel que o conjunto de tecnologias pode ter para melhorar a qualidade de privacidade de RSOs. Em outras palavras, fornecem subsídios relevantes para a identificação de problemas de privacidade e à articulação de causas e explicações para tais fenômenos.

Desse modo, além de servir como ferramenta para criar um diagnóstico de defeitos de privacidade, as técnicas também podem ser empregadas para apoiar a qualidade de um (re)projeto de interface no que diz respeito às categorias de privacidade que compõem a estrutura da PIT-OSN. Espera-se, com isso, contribuir para que designers e avaliadores de RSOs, ao utilizarem as técnicas, possam refletir sobre a situação do sistema referente à

privacidade, buscando elaborar uma solução mais adequada às necessidades e intenções de privacidade do usuário.

O uso deste tipo de técnica de inspeção chama atenção para o fato de contribuírem não apenas por serem de baixo custo, mas também por serem adequadas para julgar a qualidade de uso e buscar evidências que indiquem se as metas de design de privacidade foram alcançadas, ou seja, se a RSO possui os níveis de qualidade de uso desejados. Além disso, trata-se de enfatizar que o as PIT-OSN, justamente por serem técnicas de inspeção, colocam o avaliador na posição de produtor de conhecimento, em função do caráter exploratório e reflexivo das mesmas.

Destaca-se também, como contribuição, a realização de um mapeamento sistemático que possibilitou caracterizar tecnologias que apoiam o projeto e avaliação de privacidade no contexto de RSOs. Este instrumento pode servir de ferramenta para identificar e explorar um problema e buscar explicações teóricas para uma determinada questão de pesquisa.

Até o presente momento deste trabalho de mestrado, foram publicados dois artigos descrevendo os resultados de estudos realizados durante a execução desta pesquisa. O primeiro artigo apresenta um estudo empírico realizado com um modelo de design de privacidade (MDP) cujo resultado serviu como base para a construção do conjunto de técnicas proposto. Já o segundo artigo apresenta a proposta inicial do conjunto de tecnologias PIT-OSN seguido dos resultados de seu estudo preliminar.

Artigo 1 (publicado): Rodrigues, A. A., Valentim, N. M. C., & Conte, T. *Privacy Evaluation of Online Social Network Stories Feature: An Empirical Study with PDM*. In: Proceedings of the XVI Brazilian Symposium on Human Factors in Computing Systems. ACM, 2017. p. 43.

Artigo 2 (publicado): Rodrigues, A. A., Valentim, N. M. C., & Feitosa, F. *A Set of Privacy Inspection Techniques for Online Social Network*. In: Proceedings of the XVII Brazilian Symposium on Human Factors in Computing Systems. ACM, 2018.

7.3 DIFICULDADES ENCONTRADAS

As principais dificuldades encontradas neste trabalho estão relacionadas, principalmente, ao tamanho da amostra. Nos estudos realizados, a principal dificuldade era tentar selecionar um número ideal de participantes heterogêneos como amostra. No entanto, o pequeno número de participantes selecionados para os estudos pode não ser o ideal do ponto de vista estatístico. Ressalta-se que tamanho da amostra é um problema conhecido em estudos

IHC e ES (FERNANDEZ *et al*., 2009). Devido a estes fatos, há limitação dos resultados, sendo estes considerados indícios e não conclusivos.

7.4 PERSPECTIVAS FUTURAS

Como perspectivas futuras, destacamos a continuidade de estudos primários para avaliar a nova versão do conjunto de técnicas PIT-OSN com a finalidade de ampliar a confiabilidade dos resultados obtidos. Consequentemente, devem ser observados novos itens verificação que podem surgir nas situações de aplicação das técnicas para evoluí-las. Para este processo de evolução das tecnologias, almeja-se executar também estudos de natureza exploratória, como a entrevista ou grupos de foco, buscando principalmente explorar e explicar dados qualitativos que podem enriquecer o contexto das técnicas.

Nos estudos executados neste trabalho, não foi realizada uma análise específica sobre a taxonomia de defeitos e nem a gravidade dos mesmos. Estas limitações abrem novas perspectivas de pesquisa, como uma análise aprofundada dos tipos de defeitos e gravidade encontrados com o auxílio da taxonomia e da escala severidade propostas. Além disso, uma nova avaliação seguindo a visão de todo o processo de inspeção também pode ser explorada como trabalhos futuros, posto que somente a atividade de preparação e detecção de defeitos, do processo de avaliação, foram realizadas pelos participantes do estudo.

Almeja-se também propor novas tecnologias que possam ter como base o conjunto de técnicas proposto neste trabalho para construir técnicas que apoiem o projeto de modelos de análise, visando à privacidade da aplicação final. Identificou-se, através dos do mapeamento sistemático, uma carência de tecnologias com este propósito, por exemplo: há poucas tecnologias para apoiar a construção de modelos na fase de análise de um processo de desenvolvimento de RSOs. Este tipo de tecnologia permite uma forma proativa de considerar a privacidade desde as fases iniciais do processo de desenvolvimento.

REFERÊNCIAS

ACKERMAN, M., 2000. “The intellectual challenge of cscw: The gap between social requirements and technical feasibility”. Human-Computer Interaction, v. 15(2), pp. 179-203.

ALQARNI, A.; SAMPALLI, S., 2016. “Privacy-Enhancing of User's Behaviour Toward Privacy Settings in Social Networking Sites”. In Conference Extended Abstracts on Human Factors in Computing Systems, pp. 2758-2765.

ALTMAN, I., 1975. “The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding”. Inc., Monterry, CA: Brooks/Cole Pub. Co.

ANTHONYSAMY, P.; GREENWOOD, P.; RASHID, A., 2014. “A method for analysing traceability between privacy policies and privacy controls of online social networks”. In Annual Privacy Forum, Springer, pp. 187-202.

ANTHONYSAMY, P.; RASHID, A.; WALKERDINE, J.; GREENWOOD, P.; LARKOU, G., 2012. “Collaborative privacy management for third-party applications in online social networks”. In Workshop on Privacy and Security in Online Social Media, p. 5.

BARANAUSKAS, M.; DE SOUZA, C.; PEREIRA, R. 2012. I GranDIHC-BR - Grand Research Challenges for Human-Computer Interaction in Brazil. ISBN: 9788576692966. Human-Computer Interaction Special Committee (CEIHC) of the Brazilian Computer Society (SBC).

BARBOSA, S. D. J., SILVA, B. S., 2010. “Interação Humano-Computador”. Rio de Janeiro, RJ: Elsevier.

BASILI, V., 1997. Evolving and Packaging Reading Technologies. The Journal of Systems and Software, v. 38, pp. 3-12

BASILI, V., ROMBACH, H., 1988. "The TAME project: Towards improvement-oriented software environments". In IEEE Transactions on Software Engineering, v. 14 (6), pp. 758-773.

BESMER, A. e LIPFORD, H. R., 2010. “Moving beyond untagging: photo privacy in a tagged world”. In Proceedings of the Conference on Human Factors in Computing Systems, pp. 1563-1572.

BESMER, A.; LIPFORD, H. R.; SHEHAB, M.; CHEEK, G., 2009. “Social applications: exploring a more secure framework”. In Symposium on Usable Privacy and Security, ACM, p. 2.

BIAS, R. e MAYHEW, D. 2005. “Cost-Justifying Usability”. San Francisco, CA: Morgan Kaufmann Publishers.

BLOMKVIST, S., 2005. “Towards a Model for Bridging Agile Development and User-Centered Design”. In: A. Seffah, J. Gulliksen & M.C. Desmarais (eds.), Human-Centered Software Engineering: Integrating Usability in the Software Development Lifecycle. Springer, pp. 219–244.

BOLCHINI, D., GARZOTTO, F., 2007. "Quality of Web usability evaluation methods: an empirical study on MiLE+". In International Workshop on Web Usability and Accessibility, pp. 481-492.

BOYD, D. M., ELLISON, N. B. 2008. “Social network sites: Definition, history, and Scholarship”. Journal of Computer-Mediated Communication, v. 13(1), pp. 210-230.

CALEFATO, F., LANUBILE, F., MINERVINI, P., 2010. "Can Real-Time Machine Translation Overcome Language Barriers in Distributed Requirements Engineering?". In IEEE International Conference on Global Software Engineering, pp. 257-264.

CARVALHO, J.; LAMMEL, F.; DA SILVA, J.; CHIPEAUX, L.; SILVEIRA, M., 2012. “Inspeção Semiótica e Avaliação de Comunicabilidade: identificando falhas de comunicabilidade sobre as configurações de privacidade do Facebook”. In Brazilian Symposium on Human Factors in Computing Systems, pp. 73-74.

CHEN, G.; RAHMAN, F., 2008. “Analyzing privacy designs of mobile social networking applications”. In International Conference on Embedded and Ubiquitous Computing, IEEE, pp. 83-88.

CHEN, T. Y.; POON, P. L.; TANG, S. F., 2002. “Towards a Problem-Driven Approach to Perspective-Based Reading”. In International Symposium on High Assurance Systems Engineering, pp. 221-229.

CHRISTIN, D.; LÓPEZ, P. S.; REINHARDT, A.; HOLLICK, M.; KAUER, M., 2013. “Share with strangers: Privacy bubbles as user-centered privacy control for mobile content sharing applications”. Information Security Technical Report, v. 17(3), pp. 105-116.

COELHO, J., DUARTE, C. 2016. A literature survey on older adults' use of social network services and social applications. Computers in Human Behavior, 58, 187-205.

CONTE, T. U.; VALENTIM, N.; CABREJOS, L. J. E. R.; LOPES, ADRIANA; OLIVEIRA, E.; STEINMACHER, I. F. 2018. Modelo de Aceitação de Tecnologia. Automatização de teste de software com ferramentas de software livre. 1ed.: Elsevier Editora Ltda., v. 1, pp. 229-238.

CONTE, T.; MASSOLAR, J.; MENDES, E.; TRAVASSOS, G.H., 2009. “Web Usability Inspection Technique Based on Design Perspectives”. IET Software Journal, v.3, pp. 106-123.

CORBIN, J., STRAUSS, A., 2008. "Basics of Qualitative Research. Techniques and Procedures for Developing Grounded Theory". Sage, 3ª edição, 400 páginas.

COURAGE, C.; BAXTER, K., 2005. “Understanding your users: a practical guide to user requirements, methods, tools, and techniques”. San Francisco, CA: Morgan Kaufmann Publishers.

DAVIS, F., 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology". In MIS Quarterly, v. 13 (3), pp. 319-340.

DE MELLO, R. M., 2011. “Técnica para Inspeção de Diagramas de Atividades”. Tese (Doutorado). Universidade Federal do Rio de Janeiro. 166 páginas.

DE SOUZA, C. S., 2005. “The semiotic engineering of human computer interaction”. MIT Press, Cambridge, MA.

DE SOUZA, C.S.; LEITÃO, C.F.; PRATES, R.O.; DA SILVA, E.J., 2006. “The Semiotic Inspection Method”. In Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais, pp. 148-157.

DECEW, J. W., 1997. “In Pursuit of Privacy: Law, Ethics, and the Rise of Technology“. Cornell University Press.

DIX, A.; FINLAY, J. E.; ABOWD, G. D.; BEALE, R., 2003. “Human-Computer Interaction (3rd Edition)”. Upper Saddle River, NJ: Prentice-Hal.

EMANUEL, L.; BEVAN, C.; HODGES, D., 2013. “What does your profile really say about you?: privacy warning systems and self-disclosure in online social network spaces”. In CHI'13 Extended Abstracts on Human Factors in Computing Systems, pp. 799-804.

EPSTEIN, D. A.; JACOBSON, B. H.; BALES, E.; MCDONALD, D. W., MUNSON, S. A. 2015. “From nobody cares to way to go!: A design framework for social sharing in personal informatics”. In Proceedings of the 18th Conference on Computer Supported Cooperative Work & Social Computing, pp. 1622-1636.

FAGAN, M. E. 1986. “Advances in software inspections”. In Pioneers and Their Contributions to Software Engineering. Springer. pp. 335-360.

FANG, L.; LEFEVRE, K., 2010. “Privacy wizards for social networking sites”. In international conference on World wide web (pp. 351-360). ACM.

FERNANDEZ, A., 2009. "WUEP: Un Proceso de Evaluación de Usabilidad Web Integrado en el Desarrollo de Software Dirigido por Modelos". Dissertação (Mestrado) - Universitat Politècnica de València, 173 páginas

FONG, P. W.; ANWAR, M.; Zhao, Z., 2009. “A privacy preservation model for facebook-style social network systems”. In European Symposium on Research in Computer Security, pp. 303-320.

GAO, B. e BERENDT, B., 2013. “Circles, posts and privacy in egocentric social networks: An exploratory visualization approach”. In Proceedings International Conference on Advances in Social Networks Analysis and Mining, pp. 792-796.

GARLAND, R., 1991. "The Mid-Point on a Rating Scale: Is it Desirable?" In Marketing Bulletin 2, 1991, pp. 66-70.

GURSES, S.; RIZK, R.; GUNTHER, O., 2008. “Privacy design in online social networks: Learning from privacy breaches and community feedback”. In International Conference on Information Systems, pp. 90.

HE, L. e CARVER, J., 2006. “PBR vs. checklist: a replication in the n-fold inspection context”. In International Symposium on Empirical Software Engineering, pp. 95-104.

HEWETT, T. T.; BAECKER, R.; CARD, S.; CAREY, T.; GASEN, J.; MANTEI, M.; VERPLANK, W., 1992. ACM SIGCHI curricula for human-computer interaction.

IACHELLO, G. e HONG J., 2007. “End-user privacy in human-computer interaction”. Foundations and Trends in Human-Computer Interaction, v. 1(1), pp. 1-137.

JAMIL, H. M., 2017. “Using stratified privacy for personal reputation defense in online social networks”. In Symposium on Applied Computing, pp. 1037-1044.

JOHNS, R., 2005. "One Size Doesn't Fit All: Selecting Response Scales For Attitude Items". In Journal of Elections, Public Opinion, and Parties, v. 15 (2), pp. 237-264.

JOINSON, A. N. e PAINE, C. B., 2007. “Self-disclosure, privacy and the internet”. The Oxford handbook of Internet psychology, pp. 235-250

KALINOWSKI, M.; SPINOLA, R.; TRAVASSOS, G. H., 2004. “Infra-Estrutura Computacional para Apoio ao Processo de Inspeção de Software”. In Simpósio Brasileiro de Qualidade de Software, pp. 62-77.

KIMURA, M. H.; MANTAU, M. J.; KEMCZINSKI, A.; GASPARINI, I., 2012. “Avaliação de usabilidade das funcionalidades assíncronas de privacidade do Facebook”. In Workshop sobre Aspectos da Interação Humano-Computador para a Web Social, pp. 11-20.

KIRNER, T. G.; ABIB, J. C., 1998. “Inspection of Software Requirements Documents: A Pilot Study”. In International Conference on System Documentation. pp.161-171.

KITCHENHAM, B.; CHARTERS, S., 2007. "Guidelines for performing systematic literature reviews in software engineering". In EBSE Technical Report EBSE-2007-01, Software Engineering Group Department of Computer Science Keele University.

LAITENBERGER, O.; EL EMAM, K.; HARBICH, T. G., 2001. “An internally replicated quasi-experimental comparison of checklist and perspective based reading of code documents”. IEEE Transactions on Software Engineering, v. 27(5), pp. 387-421.

LANUBILE, F.; MALLARDO, T.; CALEFATO, F., 2003. “Tool support for Geographically Dispersed Inspection Teams". In Software Process Improvement and Practice, v. 8, pp, 217-231.

LANUBILE, F.; SHULL, F.; BASILI, V. R., 1998. “Experimenting with error abstraction in requirements documents”. In Software Metrics Symposium, 1998. Metrics 1998. pp. 114-121.

LAZAR, J.; FENG, J. H.; HOCHHEISER, H. 2010. “Research methods in human-computer interaction”. Wiley.

LEDERER, S.; HONG, J. I.; DEY, A. K.; LANDAY, J. A., 2004. “Personal privacy through understanding and action: five pitfalls for designers”. Personal and Ubiquitous Computing, v. 8(6), pp. 440-454.

LICHTENSTEIN, S., 2003. “Adding value to online privacy for consumers: Remedying deficiencies in online privacy policies with an holistic approach”. In Hawaii International Conference on System Sciences, pp. 10.

LIU, Y.; GUMMADI, K. P.; MISLOVE, A., 2011. “Analyzing facebook privacy settings: User expectations vs. reality”. In Proceedings of the ACM SIGCOMM Internet Measurement Conference, pp. 61-70.

LOPES, B. G. C.; DOS SANTOS, G. E.; VILLELA, M. L.; PRATES, R. O., 2016. “Privacy Design Model Application on Sharing Pictures Apps”. In Brazilian Symposium on Human Factors in Computer Systems, p. 46.

MACIEL, C., PEREIRA, V. C. 2013. “Social network users’ religiosity and the design of post mortem aspects”. In IFIP Conference on Human-Computer Interaction. Springer, Berlin, Heidelberg, pp. 640-657.

MAFRA, S.N.; TRAVASSOS, G.H., 2005. “Técnicas de Leitura de Software: Uma Revisão Sistemática”. In Simpósio Brasileiro de Engenharia de Software, pp. 16-31.

MALANDRINO, D.; PETTA, A.; SCARANO, V.; SERRA, L.; SPINELLI, R. & KRISHNAMURTHY, B., 2013. “Privacy awareness about information leakage: Who knows what about me?” In Proceedings of Workshop on Workshop on Privacy in the Electronic Society, WPES ’13, pp. 279-284.

MAZZIA, A.; LEFEVRE, K.; ADAR, E., 2012. “The pviz comprehension tool for social network privacy settings”. In Proceedings of the Eighth Symposium on Usable Privacy and Security, pp. 13:1-13:12.

MENDES, E., 2005. “A systematic review of Web engineering research”. In Proceedings of International Symposium on Empirical Software Engineering, pp. 498 – 507.

MINAYO, C. S., 2003. “Pesquisa social: teoria, método e criatividade”. Rio de Janeiro, RJ: Vozes, 2003.

NAGARAJ, S. K., BRYANT, A. 2016. “Factors in Building Transparent, Usable and Comprehensive User Privacy Policy System”. In 11th International Conference on Cyber Warfare and Security: ICCWS2016. Academic Conferences and publishing limited, pp. 253.

NETTER, M.; RIESNER, M.; WEBER, M.; PERNUL, G., 2013. “Privacy settings in online social networks–preferences, perception, and reality”. In Hawaii International Conference on System Sciences, pp. 3219-3228.

NIELSEN, J., 1994. “Heuristic Evaluation”. In: R. Mack & J. Nielsen (eds.), Usability Inspection Methods. New York, NY: John Wiley e Sons, pp. 25-62.

NORMAN, D.A., 1988. “Psychology of Everyday Things”. Basic Books.

PANG, J. e ZHANG, Y., 2015. “A new access control scheme for facebook-style social networks”. Computers & Security, v. 54(1), pp. 44–59.

PARNAS, D. L. e WEISS, D. M., 1985. “Active design reviews: principles and practices”. In International Conference on Software Engineering, pp. 132-136.

PEREIRA, F. H. S.; PRATES, R. O. 2017. “A Conceptual Framework to design Users Digital Legacy Management Systems”. In Proceedings of the XVI Brazilian Symposium on Human Factors in Computing Systems (pp. 1). ACM.

PETERSEN, K.; VAKKALANKA, S.; KUZNIARZ, L., 2015. "Guidelines for conducting systematic mapping studies in software engineering: An update". In Information and Software Technology, v. 64, pp. 1-18.

PETERSSON, H., 2002. “Supporting Software Inspections through Fault Content Estimation and Effectiveness Analysis”. Department of Communication Systems, Lund Institute of Technology. Technical report 147.

PETRONIO, S., 2002. “Boundaries of privacy: Dialectics of disclosure”. Suny Press.

PONTES, D. R. G. D., 2016. “Geração de rótulo de privacidade por palavras-chaves e casamento de padrões”. Dissertação (Mestrado). Universidade Federal de São Carlos, 103 páginas.

PORTER, A. A. e VOTTA, L. G., 1994. “An experiment to assess different defect detection methods for software requirements inspections”. In International Conference on Software Engineering, pp. 103-112.

PORTER, A. A.; VOTTA, L. G.; BASILI, V. R., 1995. “Comparing detection methods for software requirements inspections: A replicated experiment”. IEEE Transactions on software Engineering, v. 21(6), pp. 563-575.

PRATES, R. O., BARBOSA, S. D. J., 2007. “Introdução à teoria e prática da interação humano computador fundamentada na engenharia semiótica”. Atualizações em informática, 263-326.

RECUERO, R. 2009. “Redes sociais na internet”. 1. ed. Porto Alegre: Sulina, 191 páginas.

ROCHA, H., BARANAUSKAS, M., 2003. "Design e Avaliação de Interfaces Humano-Computador". NIED, UNICAMP, Campinas, 244 páginas.

RODRIGUES, A. A., CLEMENTE, F. A. S., & DOS SANTOS, A. A. S., 2016. “An information window about online privacy aspects perceived by social networks users”. In Brazilian Symposium on Human Factors in Computer Systems, pp. 18.

RODRIGUES, A. A., VALENTIM, N. M. C., CONTE, T., 2017. “Privacy Evaluation of Online Social Network Stories Feature: An Empirical Study with PDM”. In Brazilian Symposium on Human Factors in Computing Systems pp. 43.

RODRIGUES, K. R.; CANAL, M. C.; XAVIER, R. A.; ALENCAR, T. S.; NERIS, V., 2012. “Avaliando aspectos de privacidade no Facebook pelas lentes de usabilidade, acessibilidade e fatores emocionais”. In Brazilian Symposium on Human Factors in Computing Systems pp. 75-76.

ROMERO, N. A.; MARKOPOULOS, P.; Greenberg, S., 2012. “Grounding privacy in mediated communication”. Computer Supported Cooperative Work. v. 22(1), pp. 1-32.

RUBIN, J., 1994. “Handbook of Usability Testing”. New York, NY: John Wiley & Sons.

SABALIAUSKAITE, G.; MATSUKAWA, F.; KUSUMOTO, S.; INOUE, K., 2003. “Further investigations of reading techniques for object-oriented design inspection”. Information and Software Technology, v. 45(9), pp. 571-585.

SANTOS, G.; ROCHA, A. R.; CONTE, T.; BARCELLOS, M. P.; PRIKLADNICKI, R., 2012. Strategic Alignment between Academy and Industry: A Virtuous Cycle to Promote Innovation in Technology. In Simpósio Brasileiro de Engenharia de Software, pp. 196-200.

SAUER, C., JEFFERY, D., LAND, L., YETTON, P., 2000. "The Effectiveness of Software Development Technical Review: A Behaviorally Motivated Program of Research". In IEEE Transactions on Software Engineering, v. 26 (1), pp. 1-14.

SHARP, H.; ROGERS, Y.; PREECE, J., 2007. “Interaction design: beyond human-computer interaction”, 2ª edição. New York, NY: John Wiley & Sons.

SHEHAB, M.; CHEEK, G.; TOUATI, H.; SQUICCIARINI, A. C.; CHENG, P. C., 2010. Learning based access control in online social networks. In International Conference on World Wide Web, pp. 1179-1180.

SHI, P.; XU, H.; ERICKSON, L.; ZHANG, C., 2012. “See Friendship: Interpersonal Privacy Management in a Collective World”. In America Conference on Information Systems Washington, Seattle, USA.

SHULL, F., 1998. “Developing Techniques for Using Software Documents: A Series of Empirical Studies”. Tese (Doutorado), Department of Computer Science, University of Maryland.

SHULL, F.; CARVER, J.; TRAVASSOS, G. H., 2001. “An empirical methodology for introducing software processes". ACM SIGSOFT Software Engineering Notes, v. 26(5), pp. 288-296.

SHULL, F.; CARVER, J.; TRAVASSOS, G. H.; MALDONADO, J. C.; CONRADI, R.; BASILI, V. R., 2003. “Replicated studies: building a body of knowledge about software reading techniques”. In Lecture notes on empirical software engineering, pp. 39-84.

SHULL, F.; MENDONCA, M. G.; BASILI, V.; CARVER, J.; MALDONADO, J. C.; FABBRI, S.; TRAVASSOS, G. H.; FERREIRA, M. C., 2004. "Knowledge-Sharing Issues in Experimental Software Engineering." Empirical Software Engineering, v. 9, n. 1-2, pp. 111-137.

TELES, A. S.; SILVA, F. J. D.; ENDLER, M., 2017. “Situation-based privacy autonomous management for mobile social networks. Computer Communications”. v. 07, pp. 75-92.

TIERNEY, M.; SPIRO, I.; BREGLER, C.; SUBRAMANIAN, L., 2013. “Cryptagram: Photo privacy for online social media”. In Conference on Online social networks, pp. 75-88.

TRAVASSOS, G. H.; SHULL, F.; CARVER, J.; BASILI, V., 2002. “Reading Techniques for OO Design Inspections”. Technical Report CS-TR-4353, University of Maryland Computer Science Department.

UR, B.; WANG, Y., 2013. “A cross-cultural framework for protecting user privacy in online social media”. In International Conference on World Wide Web, ACM, pp. 755-762.

VALENTIM, N. M. C. 2017. Antecipando a usabilidade nas fases iniciais do processo de desenvolvimento de software. Tese (Doutorado) – Universidade Federal do Amazonas, 249 páginas.

VAN DER VALK. R. V. R.; HELMS, R. W.; VAN DE WETERING, R.; BEX, F. J.; CORTEN, R., 2016. “Feeling Safe? Privacy controls and Online DIS-Closure Behavior”. In European Conference on Information Systems, pp. 51.

VENKATESH, V., BALA, H., 2008. "Technology Acceptance Model 3 and a Research Agenda on Interventions". In Decision Sciences, v. 39 (2), pp. 273-315.

VILLELA, M. L. B., 2016. “Um modelo de design de privacidade para o compartilhamento de informações pessoais em redes sociais online”. Tese (Doutorado). Universidade Federal de Minas Gerais, 157 páginas.

VILLELA, M. L. B.; PRATES, R. O., 2015. “Supporting designer in modeling privacy for social network sites”. Em Proceedings of Brazilian Symposium on Human Factors in Computer Systems (IHC 2015), pp. 113-122.

WANG, Y. e ZHOU, M. X., 2015. “Veilme: An interactive visualization tool for privacy configuration of using personality traits”. In Proceedings of Conference on Human Factors in Computing Systems, pp. 817-826.

WESTIN, A. F., 2003. “Social and political dimensions of privacy”. Journal of Social Issues, v. 59(2), pp. 431-453

WISNIEWSKI, P. J.; KNIJNENBURG, B. P.; LIPFORD, H. R., 2017. “Making privacy personal: Profiling social network users to inform privacy education and nudging”. International Journal of Human-Computer Studies, v. 98, pp. 95-108.

WIXON, D. e WILSON, C., 1997. “The usability engineering framework for product design and evaluation”. In: M.G. Helander, T.K. Landauer, P.V. Prabju (eds.), Handbook of Human-Computer Interaction. Elsevier, Amsterdam, pp. 653–688.

WONG, Y. K. (Ed.)., 2006. “Modern Software Review: Techniques and Technologies” Techniques and Technologies. IGI Global.

YAMAUCHI, E. A.; DE SOUZA, P. C.; JUNIOR, D. P., 2016. “Prominent issues for privacy establishment in privacy policies of mobile apps”. In Symposium on Human Factors in Computer Systems, pp. 26.

YU, W. D.; DODDAPANENI, S.; MURTHY, S., 2006. “A privacy assessment approach for serviced oriented architecture application”. In International Symposium on Service-Oriented System Engineering, pp. 67-75.

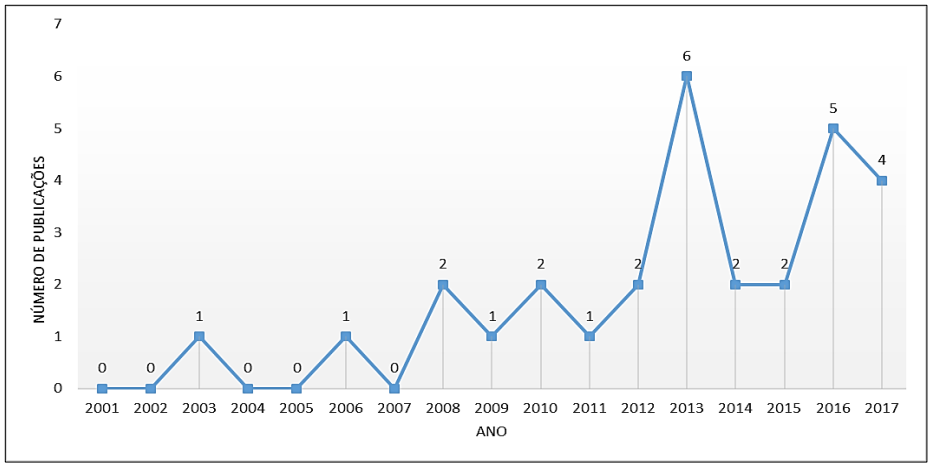
APÊNDICE A – RESULTADOS DO MAPEAMENTO SISTEMÁTICO

A.1 VISÃO GERAL DOS RESULTADOS

A.1.1 Ano de Publicação dos Artigos

Os artigos selecionados foram publicados entre março de 2003 e outubro de 2017. Com base na visão temporal fornecida pela Figura 31, nota-se uma variabilidade na quantidade de publicações. Nos anos de 2003 a 2007 poucas publicações foram retornadas, considerando que nesta época estavam emergindo as pesquisas sobre privacidade no contexto de RSOs. Percebe-se também, de acordo com o cenário cronológico deste MSL, que nos anos de 2009, 2011, 2014 e 2015, houve um número limitado de publicações sobre o tema em questão (01 ou 02 artigos). O ano de 2013 é o que reuni a maior quantidade de publicações (06 artigos), seguido de 2016 (05 artigos).

Figura 31. Visão temporal das publicações identificadas no MSL



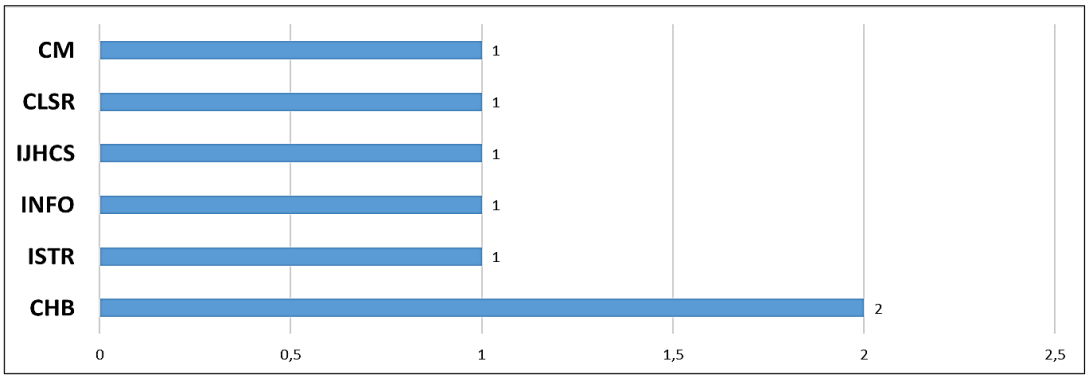
Fonte: Próprio autor.

A.1.2 Locais de publicação

Neste MSL, foram considerados apenas documentos publicados na forma de artigos em periódicos (*journals*) ou conferências (*proceedings*). A Figura 32 concede uma visão geral da distribuição de artigos por periódico. O principal veículo que mais publicou sobre o tema foi o *Computers in Human Behavior* (CHB), com dois artigos publicados. Em seguida, tem-se o *Information Security Technical Report* (ISTR), *Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media* (INFO), *International Journal of Human-*

Computer Studies (IJHCS), *Computer Law and Security Review* (CLSR) e o *Computer Communications* (CM), com um artigo cada.

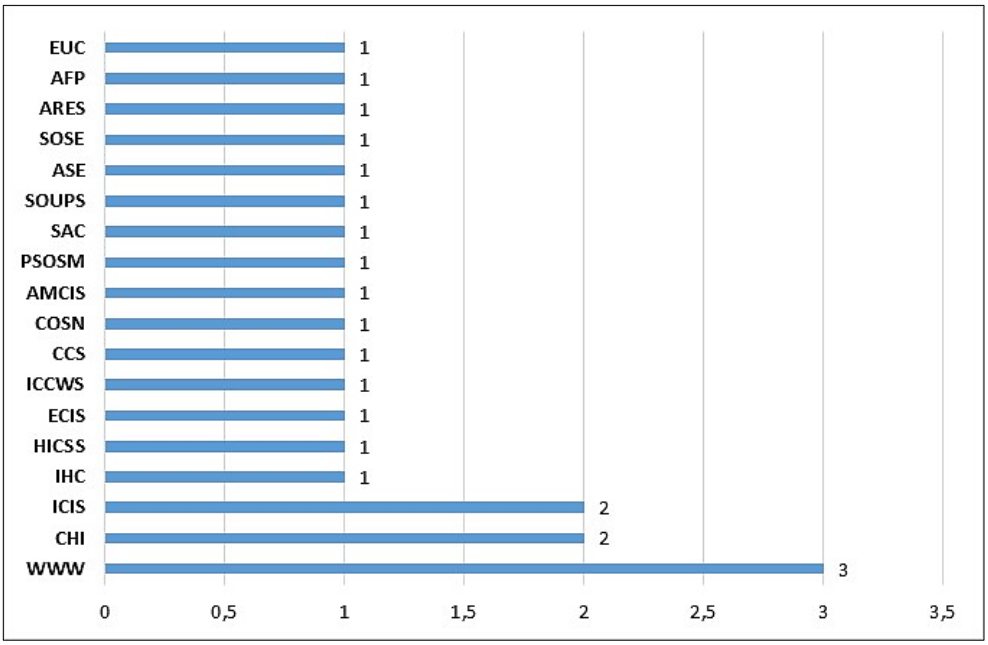
Figura 32. Distribuição de artigos por periódico



Fonte: Próprio autor.

Em relação a distribuição de artigos por conferências (Figura 33), o principal evento de publicação foi o *International Conference on World Wide Web* (WWW), com três artigos publicados. *Conference on Human Factors in Computing Systems* (CHI) e *International Conference on Information Systems* (ICIS), possuem dois artigos cada. Outras conferências como *Symposium on Usable Privacy and Security* (SOUPS) e *Brazilian Symposium on Human Factors in Computer Systems* (IHC), possuem apenas um artigo publicado sobre a temática foco deste mapeamento.

Figura 33. Distribuição de artigos por conferências



Fonte: Próprio autor.

A.1.3 Tipo de tecnologia (SQ1)

Os resultados desta subquestão denotam que a maioria (57,14%) das tecnologias identificadas destinam a sua proposta para apoiar o projeto de soluções de interfaces que podem ser integradas ao design de RSOs, com foco em privacidade. As redes sociais permitem ao usuário um determinado controle sobre a privacidade de suas informações. Com o propósito de melhorar esse controle de acesso, algumas tecnologias apresentam soluções alternativas que podem ser incorporadas para aprimorar o design de privacidade em RSOs. Um exemplo disso, é o trabalho de Teles *et al.* (2017) que desenvolveram um mecanismo para ajustar de forma automatizada as configurações de privacidade do usuário em uma RSO específica. Desta forma, os autores conceberam o *SelPri* que permite aos usuários definir as configurações de privacidade dependentes do contexto, permitindo uma publicação seletiva de conteúdo com base na situação atual do usuário. Ao mesmo tempo, permite que os próprios usuários controlem as permissões atribuídas a todos os conteúdos publicados em cada situação na RSO.

Outros autores focaram na concepção de tecnologias de projeto enfatizando diferentes aspectos de privacidade inerentes ao controle de acesso. Christin *et al.* (2013) concentraram sua pesquisa em torno da privacidade relacionada aos serviços de localização. Desta forma, os autores criaram as “Bolhas de Privacidade” como sendo uma abordagem inovadora que foca na questão sobre como compartilhar conteúdo com uma determinada audiência controlando o rastreamento de localização. Para compartilhar conteúdo com pessoas na localidade física, os usuários criam uma bolha de privacidade determinando seu raio e duração. A bolha de privacidade criada é centrada em torno do usuário e representa metaforicamente sua esfera privada. Esse tipo de tecnologia pode ser facilmente usada por designers de RSOs que buscam mitigar a distância entre os serviços de localização e a privacidade do usuário.

Outros autores destacaram a importância de preservar o conteúdo das fotos publicadas em RSOs e construíram uma tecnologia que observa esse aspecto especialmente importante relacionado a privacidade. Trata-se do *Cryptagram* (TIERNEY *et al.,* 2013), um modelo que pode ser adaptado, como uma solução de projeto, para aumentar a privacidade do compartilhamento de fotos em uma determinada RSO. O *Cryptagram* converte as fotos em imagens criptografadas, quando carregadas nas RSOs. Os usuários gerenciam diretamente o controle de acesso a essas fotos através de chaves compartilhadas que são independentes da rede social utilizada ou da aplicação de terceiros.

Alguns trabalhos salientaram também o impasse entre privacidade e aplicações de terceiros presentes nas RSOs. Um exemplo disso, é o artigo de Besmer *et al.* (2009) que propuseram um modelo de controle de acesso para restringir as ações de aplicações de terceiros presentes em sites de redes sociais. Este modelo adiciona uma nova política de aplicação que restringe em uma larga escala as informações que os aplicativos podem acessar, enquanto ainda permitem o compartilhamento de informações. A proposta também adiciona algumas mudanças às plataformas dos aplicativos existentes, possibilitando que tal abordagem seja facilmente adotada em vários contextos. O sucesso do modelo, no entanto, depende do papel do usuário em configurar adequadamente a nova política sobre a aplicação que está instalada no perfil do indivíduo.

Outros autores como Gürse *et al.* (2008) e Shi *et al.* (2012) ponderaram a questão de usar heurísticas para auxiliar no processo de design e que podem ser usadas para melhorar a interação do usuário com os aspectos de privacidade concebidos pelo sistema. O trabalho de Shi *et al* (2009), por exemplo, apresenta heurísticas que foram originadas com base em comentários da comunidade online e que apontam recomendações que podem ser refletidas pelo designer do sistema a como melhorar a ideia de privacidade. Essa proposta nos aproxima dos modelos conceituais que não representam apenas funcionalidade, comportamento ou persistência, mas também diretrizes relacionados a privacidade. Já o trabalho de Gürse *et al.* (2008) é melhor explanado na seção **Erro! Fonte de referência não encontrada.** de trabalhos relacionados.

Além disso, outros resultados desta subquestão indicam que apenas uma única tecnologia apoia tanto o projeto como a avaliação de privacidade em RSOs. Trata-se do MDP proposto por Villela e Prates (2015), sendo retornado no mapeamento um estudo sobre o mesmo realizado por Lopes *et al.* (2016). O Modelo de Design de Privacidade (MDP) consiste em uma ferramenta proposta para apoiar o design e a avaliação de redes sociais online, com foco na privacidade relacionada ao compartilhamento de informações pessoais. Com o MDP é possível analisar as redes sociais online visando identificar os níveis de privacidade que elas oferecem a seus usuários e não as opções de privacidade fornecidas aos usuários. Esse tipo de tecnologia serve como base e direcionamento para auxiliar designers a refletirem em como comunicar a ideia de privacidade sobre os fluxos de informações de uma RSOs.

Em relação às tecnologias de avaliação, nota-se que foi retornado neste MSL um número inferior (39,29%), se comparado ao número de tecnologias de projeto. Com base em seus benefícios, as tecnologias de avaliação possuem uma grande importância dentro do

contexto da Interação Humano-Computador. Barbosa e Silva (2010) ressaltam que a avaliação de IHC, principalmente as de perspectiva formativa, julgam a qualidade de uso de um sistema buscando evidências que indiquem se as metas de design foram alcançadas, ou seja, se o produto possui os níveis de qualidade de uso desejados.

No que diz respeito às tecnologias de avaliação, alguns autores buscaram construir propostas que avaliam diversos aspectos de privacidade, entre eles, destaca-se o controle de acesso disponibilizado pelas RSOs. Como exemplo, tem-se o trabalho de Alqarni e Sampalli (2016) que desenvolveram o PSM (*Privacy Setting Model*), um modelo conceitual que avalia as configurações de privacidade e permite que o usuário alcance seu estado desejado de privacidade através da combinação de três níveis conceituais: o nível cognitivo, o nível de controle e o nível de atualização do usuário. Essa proposta contribui de forma significativa para avaliar o que o sistema oferece em relação ao controle de acesso e o que o usuário precisa para atingir seu estado desejado de privacidade.

Outros autores enfatizaram a importância das políticas de privacidade como um aspecto significativo para conquistar a confiança e demonstrar credibilidade e transparência aos usuários de RSOs. Para elencar esta questão, pode-se destacar o trabalho de Yu *et al.* (2006) que criaram uma abordagem de verificação de política de privacidade. A proposta verifica e certifica se as políticas examinadas estão em conformidade com os princípios e declarações de privacidade apresentados no artigo. Esse tipo de tecnologia contribui para apoiar profissionais envolvidos no projeto de desenvolvimento de políticas de RSOs a refletirem sobre diversos fatores que devem ser considerados para construir uma política de privacidade com qualidade de uso.

Dentro da SQ1, há uma subquestão chamada SQ1.1 (Tipo de avaliação da tecnologia). As tecnologias de avaliação foram classificadas com base nos tipos de avaliação de IHC descritos por (DIX *et al.,* 2003 e BARBOSA e SILVA, 2010). Os resultados da SQ1.1 apontam que o tipo de avaliação mais usado pelas tecnologias propostas é a avaliação através de investigação, cerca de 91,67%. As tecnologias de avaliação através da investigação são frequentemente utilizadas para identificar necessidades e oportunidades de intervenção, bem como explorar formas alternativas de intervenção (avaliação formativa), assim como também são usadas para avaliar uma solução parcial ou completa (avaliação somativa) ou até mesmo um sistema interativo implementado (SHARP *et al.,* 2007). Um exemplo disso, é o trabalho de Anthonysamy *et al.* (2014) e Ur e Wang (2013) que apresentam tecnologias de avaliação que utilizam a investigação para examinar a conformidade das políticas de privacidade de uma RSO.

As tecnologias de avaliação que utilizam a observação representam apenas 8,33% das tecnologias identificadas neste MSL. Um exemplo disso, é o trabalho de Alqarni e Sampalli (2016) que propuseram uma abordagem para avaliar as configurações de privacidade de uma RSO a partir de experiências de uso dos próprios usuários da aplicação, utilizando-se a observação como instrumento de avaliação. Tal tecnologia permite entender melhor como os usuários se apropriam das configurações de privacidade disponibilizadas pelas RSOs e quais barreiras podem comprometer a interação de tais usuários em contextos de uso reais.

Em relação às tecnologias de avaliação através de inspeção, percebe-se que não foram retornados estudos que focassem nesse tipo de avaliação. A avaliação por inspeção permite identificar problemas que os usuários podem vir a ter quando interagirem com o sistema, ou seja, permite o avaliador examinar (ou inspecionar) a qualidade de uso do sistema. Barbosa e Silva (2010) ressaltam que a avaliação por inspeção costuma ser mais rápida e de custo de execução mais baixo do que os métodos de investigação e de observação, pois eles não gastam tempo com recrutamento e sessões de coleta de opiniões ou de observação de usuários. Nesse sentido, nota-se que há uma necessidade de propor novas tecnologias nesse contexto, pois a inspeção, pode ser uma forma dinâmica de apoiar a avaliação de RSOs focando na qualidade de uso inerente a privacidade do usuário.

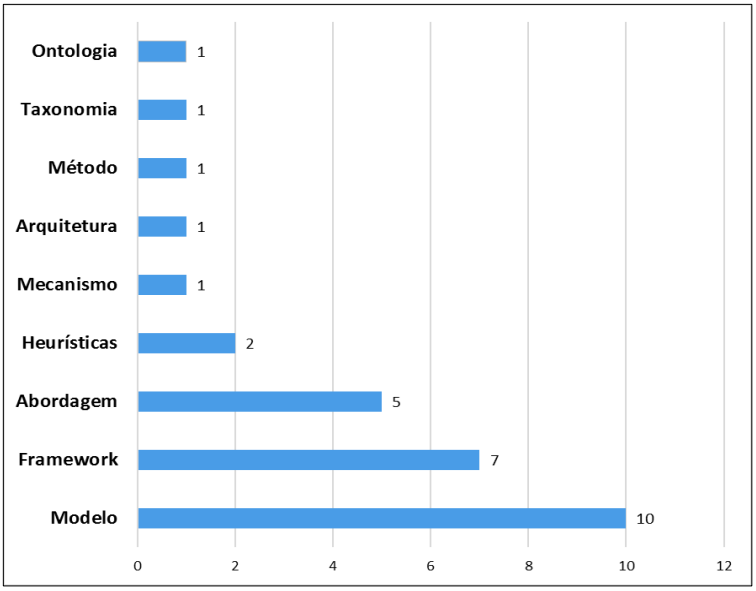
A.1.4 Tipo de contribuição (SQ2)

Essa subquestão buscou identificar qual a principal contribuição dos artigos analisados, ou seja, a determinação do tipo de intervenção sendo estudada, que pode ser uma ferramenta, métodos, métricas, modelos, diretrizes, entre outros (PETERSEN *et al*., 2015). Ressalta-se que todas as contribuições identificadas nos artigos foram classificadas com base nas nomenclaturas dadas pelos próprios autores das tecnologias. A Figura 34 demonstra os resultados desta subquestão. Observa-se que dez (10) das tecnologias propostas são modelos. Um exemplo de um modelo é apresentado por Jamil (2017). O modelo é denominado de *GreenShip*, uma proposta construída para controlar a reputação pessoal do usuário em redes sociais online, onde a mesma utiliza como base estratégias de privacidade cuja função é limitar os danos causados por amigos mal-intencionados referentes à reputação pessoal do usuário dentro das RSOs.

Sete tecnologias empregam o uso de frameworks em sua proposta. Por exemplo, Anthonysamy *et al.* (2012) propuseram o *Collaborative Privacy Management* (CPM), um framework que torna explícito para o usuário todas as informações e quais dados podem ser acessados por aplicativos de terceiros (*Third Party Applications* - *TPAs*) dentro das RSOs.

Desta forma, os resultados desta subquestão apontam que os maiores tipos de contribuição identificados nos artigos deste MSL são modelos e frameworks.

Figura 34. Tipo de contribuição das tecnologias



Fonte: Próprio autor.

A.1.5 Apoio ferramental (SQ3)

Esta subquestão buscou coletar se as tecnologias identificadas requerem ou sugerem o uso de um sistema de apoio ou se são dependentes de uma ferramenta específica de apoio para executar seus passos. A partir desta análise, os resultados desta subquestão indicam que 67,86% das tecnologias não necessitam de suporte ferramental para auxiliar os profissionais na execução de suas propostas (ver **Erro! Fonte de referência não encontrada.**). Para elucidar esta questão, tem-se os trabalhos de Masoumzadeh e Joshi (2013) e Shi *et al.* (2012) que apresentam tecnologias que não demandam do uso de ferramentas para proceder suas funções. Entretanto, cerca de 32,14% das tecnologias identificadas exigem o uso de apoio de ferramentas para desempenhar a sua proposta. Como exemplo disso, tem-se o trabalho de Emanuel *et al.* (2013) que propuseram um modelo que gera comentários automatizados sobre a exposição da identidade online do usuário em uma RSO. A proposta denominada de "*feedback de privacidade*" conta com um suporte ferramental para realizar sua função de prover um retorno para o usuário sobre sua exposição online.

Um ponto importante a ser observado é que a avaliação de privacidade automatizada tem algumas deficiências e limitações. Apesar das tecnologias focarem no aspecto privacidade almejando a qualidade de uso de uma determinada RSO, algumas delas que

contam com apoio ferramental não são orientadas a coleta de dados subjetivos e acabam não considerando percepções e preferências do usuário no processo de avaliação. No entanto, vale a pena ressaltar que o uso de tecnologias automatizadas pode reduzir o tempo e o esforço dos profissionais que irão aplicá-las em uma atividade de avaliação.

A.1.6 Estudos empíricos (SQ4)

Os resultados desta subquestão indicam que 57,14% das tecnologias foram avaliadas empiricamente. As demais tecnologias (42,86%) não contaram com avaliação empírica. Com base neste resultado, nota-se que é necessário realizar mais estudos empíricos sobre a temática foco deste mapeamento, pois quase metade das tecnologias identificadas neste MSL não foram avaliadas empiricamente.

Dentro da SQ4, também foram definidas algumas subquestões: SQ4.1 (Tipo de instrumentos de coleta de dados), SQ4.2 (Tipo de dados coletados), SQ4.3 (Tipo de análise) e SQ4.4 (Ambiente de avaliação).

Sobre a SQ4.1, o tipo de instrumentação utilizado nos estudos foi classificado com base na descrição de Dix *et al.* (2003). Os resultados da SQ4.1 demonstraram que o tipo de instrumento de coleta de dados mais empregado na execução dos estudos empíricos foi o questionário, cerca de 68,75%, conforme mostrado no trabalho de Wisniewski *et al.* (2017) e Shehab *et al.* (2010), onde os autores aplicaram um questionário online para obter dados quantitativos sobre suas pesquisas e justificaram o uso do instrumento como sendo uma boa opção para obter uma amostra diversificada e agilizar a coleta e análise dos dados.

Um total de 31,25% das tecnologias usou o estudo de campo como instrumento de coleta de dados. Um exemplo disso, é o trabalho de Besmer *et al.* (2009) e Chen e Rahman (2008), onde os pesquisadores buscaram coletar dados qualitativos sobre como as tecnologias apresentada por eles é aplicada em um contexto de uso real, procurando uma compreensão refinada sobre a tecnologia proposta ao presenciarem eventuais dificuldades que os participantes possam ter. Por fim, os demais instrumentos como entrevista, grupos de foco, classificação de cartões e registros de usos não foram utilizados nas avaliações empíricas.

Com base nos resultados da SQ4.1, observou-se que a instrumentação mais usada para coletar dados foi o questionário e o estudo de campo. De acordo com Courage e Baxter (2005) o questionário é uma excelente técnica de levantamento, pois permite coletar rapidamente dados (principalmente quantitativos) de muitos usuários, no entanto, o avaliador deve ser experiente para evitar perguntas que induzam certas respostas. Já o estudo de campo permite

compreender melhor o usuário, seu ambiente e suas tarefas em contexto, todavia, exige um nível de esforço maior para conduzir e analisar os dados (COURAGE e BAXTER, 2005).

Quanto à SQ4.2 (Tipo de dados coletados), 18,75% das tecnologias avaliaram seus dados de forma qualitativa, como o estudo apresentado por Lopes *et al.* (2016) e Masoumzadeh e Joshi (2013). Cerca de 31,25% das tecnologias avaliaram seus dados coletados de forma quantitativa, como o de Fang e LeFevre (2010) e Emanuel *et al.* (2013). Cerca de 50,00% das tecnologias avaliaram seus dados de forma quantitativa e qualitativa, como Van Der Valk *et al.* (2016) e Christin *et al.* (2013). Com base nos resultados da SQ4.2, percebe-se que a maioria dos estudos empíricos encontrados neste MSL foram analisados tanto de forma qualitativa como de forma quantitativa. Os dados quantitativos representam numericamente uma quantidade. Desta forma, os pesquisadores podem verificar hipóteses através de dados estatísticos, o que significa traduzir em números opiniões e informações para classificá-las e analisá-las. Por outro lado, os dados qualitativos buscam compreender em profundidade os fenômenos segundo a perspectiva dos sujeitos, ou seja, dos participantes da situação em estudo. Considera-se ambas abordagens relevantes para a concepção e evolução de uma tecnologia.

Em relação à SQ4.3 (Tipo de análise), 56,25% das tecnologias apresentam análise interpretativa sobre o estudo, como a de Alqarni s Sampalli (2016) e Christin *et al.* (2013), na qual os autores buscaram coletar dados a partir da interação do usuário com tecnologia concebida. Cerca de 31,25% das tecnologias apresentam análise experimental, como exemplo tem-se o trabalho de Anthonysamy *et al.* (2012) e Shehab *et al.* (2010), onde os pesquisadores realizaram as coletas de dados em ambientes controlados. Apenas 12,50% das tecnologias realizaram análise preditiva nos estudos empíricos. Como a maioria dos estudos foram executados diretamente com usuários, os tipos de análises mais utilizadas pelos pesquisadores em função dos dados coletados foram as análises interpretativas e experimental, em que os avaliadores buscaram explicar os fenômenos em função das variáveis sendo observadas. Por fim, notou-se que poucas análises preditivas foram desempenhadas. Isso demonstra que um pequeno número de estudos com especialistas foi executado sobre o tema deste MSL.

Quanto à SQ4.4 (Ambiente de avaliação), cerca de 50% das tecnologias foram avaliadas em ambiente de laboratório com usuários reais. Os ambientes de laboratório com profissionais e ambiente acadêmico com alunos tiveram o mesmo resultado (25,00% cada). Nenhuma tecnologia foi aplicada em ambiente misto. Os resultados da SQ4.4 indicam que mais da metade das tecnologias foram avaliadas sob o ponto de vista de usuários reais, o que

torna relevante a execução de estudos nesse tipo de ambiente. Ou seja, tal ambiente pode demonstrar a efetividade de uma tecnologia proposta.

A.1.7 Contexto da aplicação (SQ5)

Os resultados desta subquestão apontam que 82,14% das tecnologias são genéricas, isto é, não limitadas a um tipo de específico de rede social. Por exemplo, o trabalho de Ur e Wang (2013) apresenta um framework conceitual para avaliar se as opções de privacidade disponibilizadas pelos sites de redes sociais são oferecidas e comunicadas de forma clara para apoiar a interação social do usuário. Com base no framework, torna-se possível que os provedores de serviços de RSOs identifiquem possíveis lacunas no suporte à privacidade do usuário. Por ser abrangente, tal tecnologia pode ser aplicada em um amplo contexto de redes sociais online.

Cerca de 17,86% das tecnologias identificadas foram desenvolvidas para um contexto específico, ou seja, limitada a um tipo específico de RSO (como rede social móvel, rede social acadêmica, rede social de compartilhamento de fotos, entre outras). Isto não é tão positivo, pois o uso desse tipo de tecnologia só pode ser desempenhado dentro do contexto para o qual se destina. Como exemplo de tecnologia específica, tem-se o trabalho de Teles *et al.* (2017) que propuseram um mecanismo para reduzir os níveis de preocupação de privacidade do usuário, configurando de forma automatizada seu controle de acesso com base na situação atual do indivíduo. Entretanto, a tecnologia só pode ser utilizada por redes sociais em dispositivos móveis. Ou seja, caso o usuário acesse a RSO através do seu computador pessoal, o mecanismo não será executado.

Com base nos resultados desta subquestão, observou-se a importância em propor tecnologias que possam ser empregadas em contextos gerais, ou seja, genéricos. As tecnologias limitadas a um tipo específico de rede social ou a um domínio específico de aplicação, tornam-se restritas para serem utilizadas.

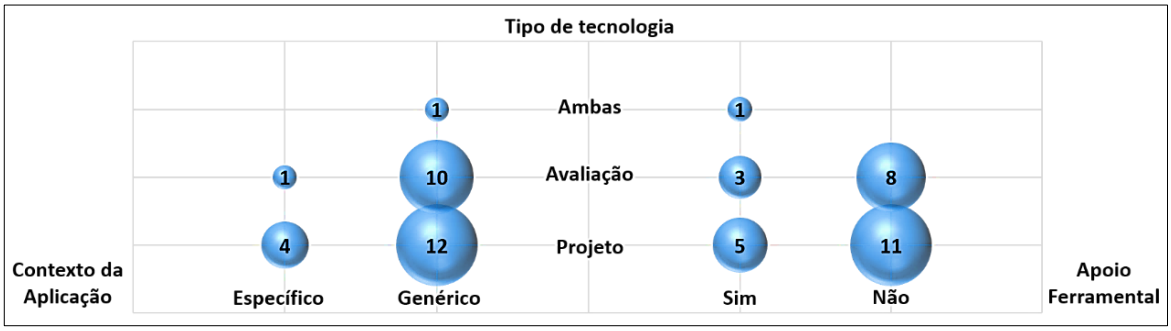
A.1.8 Combinação dos resultados das subquestões

As subquestões de pesquisa investigadas neste MSL foram combinadas com o propósito de fornecer uma visão mais ampla sobre o tema Projeto e Avaliação de Privacidade em Redes Sociais Online. A subquestão SQ2 (Tipo de Contribuição da Tecnologia) não foi utilizada nesta combinação, uma vez que a mesma possui diversas respostas. Esse tipo de análise possibilitou obter uma visão mais detalhada e um conhecimento mais aprofundado

sobre como os resultados de cada subquestão estão relacionados com os resultados de outras subquestões e quais as possíveis lacunas identificadas sobre o tema em evidência.

A Figura 35 demonstra a combinação das subquestões SQ1 (Tipo de tecnologia) em comparação com as demais subquestões de pesquisa SQ5 (Contexto da aplicação) e SQ3 (Apoio ferramental). Com base em tais combinações, os resultados apontam que a maioria das tecnologias de projeto e/ou avaliação foram desenvolvidas para desempenhar suas funções em contextos genéricos, isto é, não limitadas a um tipo específico de rede social online e não necessitam de apoio de ferramentas.

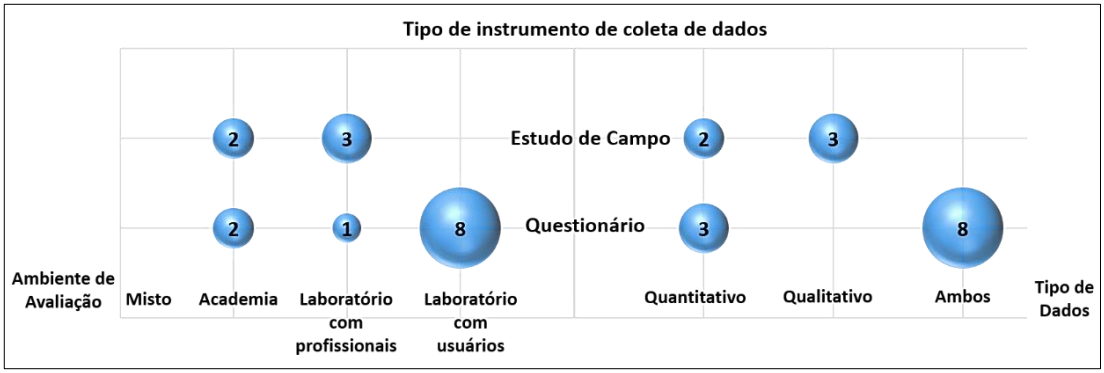
Figura 35. Combinação 1 das subquestões de pesquisa



Fonte: Próprio autor.

A Figura 36 apresenta a combinação dos resultados da subquestão SQ4.1 (Tipo de instrumento de coleta de dados) em comparação com as subquestões SQ4.4 (Ambiente de avaliação) e SQ4.2 (Tipo de dados coletados). Como apenas dois tipos de instrumentos de coleta de dados foram identificados, questionário e estudo de campo, somente estes foram representados na ilustração. Nesta direção, os resultados indicam que: (a) a maioria dos questionários foram aplicados em ambiente de laboratório com usuários reais e buscaram coletar dados tanto de natureza quantitativa como qualitativa, destacando a importância de incluir em questionários perguntas abertas e de natureza exploratória; (b) nenhum estudo foi realizado em ambiente misto, e (c) poucos estudos apresentam somente dados qualitativos e desses estudos todos utilizaram com instrumento de coleta de dados o estudo de campo.

Figura 36. Combinação 2 das subquestões de pesquisa

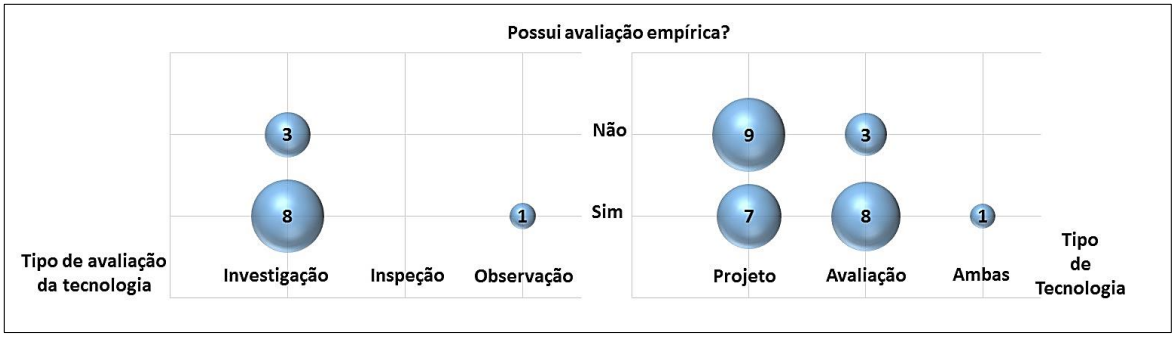


Fonte: Próprio autor.

A partir destas análises, observou-se que a maioria das tecnologias foram utilizadas ou desenvolvidas a partir de projetos acadêmicos, não sendo testadas ou empregadas em projetos reais na indústria ou outras organizações. Além disso, dado que o ambiente de avaliação mais utilizado foi o laboratório com usuários reais, outros tipos de instrumentos de coleta de dados poderiam ter sido utilizados, como a entrevista ou os grupos de foco por exemplo, pois ambos permitiriam gerar dados de natureza mais qualitativa que foram pouco explorados pelas tecnologias identificadas neste MSL.

Por fim, a Figura 37 apresenta os resultados referentes aos tipos de tecnologias de um modo geral. Desta forma, realizou-se uma combinação entre as subquestões SQ1.1 (Tipo de avaliação da tecnologia) e SQ1 (Tipo de tecnologia) comparando com a SQ4 (Avaliação empírica). Nesse sentido, os resultados indicam que: (a) a maioria das tecnologias que foram avaliadas empiricamente são tecnologias de avaliação e usam a investigação como forma de avaliar um determinado artefato de privacidade; (b) apenas uma tecnologia utilizou a observação como tipo avaliação; (c) nenhuma tecnologia usou a inspeção como forma de avaliação; e (d) a maioria das tecnologias de projeto de privacidade não foram avaliadas empiricamente.

Figura 37. Combinação 3 das subquestões de pesquisa



Fonte: Próprio autor.

Com base nestes resultados, observou-se que uma das maiores lacunas de pesquisa identificadas neste mapeamento sistemático foi a inexistência de tecnologias de avaliação de privacidade em RSOs do tipo inspeção. Como “usabilidade” e a “segurança”, a privacidade é uma propriedade holística dos sistemas interativos que incluem as pessoas que os utilizam, podendo influenciar também na qualidade de uso, ou seja, um sistema inteiro pode ser comprometido se tiver único componente mal implementado que compartilha informações sigilosas do usuário (IACHELLO e HONG, 2007), ou uma interface discrepante na qual os usuários não conseguem compreender os elementos de privacidade. Em vista disso, nota-se a importância de construir novas tecnologias de inspeção de privacidade, principalmente porque este tipo de tecnologia contribui para garantir a qualidade de uso de sistemas interativos e a segurança de seus usuários.

APÊNDICE B – GUIA PRÁTICO PARA APLICAÇÃO DO CONJUNTO DE TÉCNICAS PIT-OSN (V4)

PROCESSO DE AVALIAÇÃO USANDO O CONJUNTO DE TÉCNICAS	
Objetivo:	Promover uma melhor organização durante as inspeções
Instruções:	Para aplicar o conjunto de técnicas PIT-OSN, recomenda-se seguir um processo de avaliação. Para a execução deste processo sugerimos a participação de no mínimo duas pessoas. O processo de avaliação é composto por cinco etapas, as quais serão descritas a seguir.
PREPARAÇÃO	
Atividade 1	Nesta etapa, o processo de inspeção é preparado e organizado. Uma pessoa, desempenhando o papel de moderador, deve selecionar os inspetores, definir o contexto da inspeção, onde é feita uma breve apresentação sobre o conjunto de técnicas PIT-OSN, e distribuir os recursos das mesmas a serem aplicados (documento de inspeção, taxonomia para classificação de defeitos e grau de severidade para medir a gravidade dos defeitos detectados).
DETECÇÃO DE DEFEITOS	
Atividade 2	Nesta etapa, cada inspetor realiza sua inspeção individualmente reportando os itens de verificação que foram violados, descrevendo e classificando os possíveis defeitos de privacidade identificados em um relatório de discrepâncias. Uma discrepância representa um possível defeito detectado durante a inspeção, mas este só será julgado como um defeito real de privacidade na etapa de discriminação.
COLEÇÃO	
Atividade 3	Nesta etapa, as listas individuais de discrepâncias (possíveis defeitos) produzidas pelos inspetores são integradas em uma única lista referente ao foco de cada técnica. Um dos inspetores pode ser o responsável por realizar esta integração. Após a geração das listas únicas, uma reunião é feita para a eliminação de discrepâncias repetidas, encontradas por mais de um inspetor, mantendo apenas um registro para cada discrepância.
DISCRIMINAÇÃO	
Atividade 4	Nesta etapa, os inspetores devem discutir sobre as discrepâncias detectadas. Durante esta discussão, algumas discrepâncias serão classificadas como falso-positivos e outras como um defeito real de privacidade. Os falsos positivos devem ser descartados, pois representam os pontos que o inspetor pode ter reportado como um defeito, mas não é, seja porque ele não checou a rede social corretamente ou porque não entendeu completamente o que o item de verificação solicitava. Posteriormente, os problemas reais são registrados em uma única lista de defeitos gerando um relatório consolidado.
PROPOSTA DE SOLUÇÃO	
Atividade 5	Por fim, nesta etapa, os inspetores podem julgar a justificativa dos defeitos detectados e apontar recomendações de solução.

PIT 1 - Inspeção dos Níveis de Privacidade	
Objetivo:	Inspecionar os níveis de privacidade da rede social. **Níveis de privacidade** representam o comportamento da rede social em relação a adequação e distribuição das informações e publicações do usuário em relação a privacidade
Instruções:	Antes de começar a inspeção observe as seguintes diretrizes: *a.* Observe e anote (no documento disponibilizado) em qual parte da rede social você identifica um problema de privacidade com base nos itens de verificação descritos abaixo *b.* Escreva o ID do item de verificação na planilha de discrepância *c.* Reporte o tipo de defeito identificado na planilha de discrepância *d.* Defina o grau de severidade para o defeito identificado *e.* Descreva sobre o problema de privacidade identificado
1A. Fonte de Informação	
1A1	Verifique se outro usuário (um amigo ou seguidor) tem autonomia para compartilhar conteúdos publicados sobre um determinado indivíduo dentro do sistema sem permissão
1A2	Verifique se outras fontes, como aplicativos ou sites de terceiros, tem autonomia para compartilhar informações sobre um determinado usuário sem o seu consentimento ou conhecimento
1B. Espaço de Comunicação	
1B1	Verifique se um conteúdo publicado sobre um determinado usuário pode ser compartilhado em um outro espaço de publicação que não seja seu, provavelmente sem a sua permissão
1B2	Verifique se um conteúdo publicado sobre um determinado indivíduo pode ser acessado através de um espaço público fora do sistema (como em mecanismos de busca) sem a sua permissão
1C. Conteúdo dos dados	
1C1	Verifique se a rede social coleta dados pessoais (como data de nascimento, número de telefone, endereço de e-mail) e expõe essas informações na própria rede social sem a permissão do usuário
1D. Persistência temporal	
1D1	Verifique se a rede social permite restringir a duração de um conteúdo publicado no sistema, possibilitando criar postagens curtas que desapareçam depois de um determinado período de tempo
1D2	Verifique se a rede social permite ao usuário que, ao aceitar a solicitação de um determinado indivíduo, este tenha acesso apenas as informações que forem compartilhadas a partir do momento em que tal usuário começou a fazer parte da audiência (tempo presente) e não tenha acesso as publicações antigas (tempo passado)
1E. Audiência	
1E1	Verifique se a rede social permite que uma audiência desconhecida (como amigos em comum por exemplo) possa visualizar determinadas ações do indivíduo no sistema, sem fazer parte da lista de amigos
1F. Notificação	
1F1	Verifique se rede social não notifica o indivíduo sobre as interações de outros usuários com o seu conteúdo que é compartilhado no sistema

1G. Discurso do sistema sobre o indivíduo	
1G1	Verifique se a rede social toma a iniciativa de gerar novos conteúdos sobre o usuário sem a sua permissão, com base no processamento de uma ou mais informações pessoais já compartilhadas anteriormente (como retrospectivas e *scores* por exemplo)
1G2	Verifique se a rede social toma a iniciativa de recomendar o perfil do indivíduo para outros usuários sem a sua permissão (como as sugestões de pessoas por exemplo)
1H. Disseminação da Informação	
1H1	Verifique se a rede social permite à audiência repostar com outras pessoas uma publicação de um determinado usuário sem a sua permissão, ou seja, de maneira irrestrita

PIT 2 - Inspeção dos Controles de Privacidade	
Objetivo:	Inspecionar os controles de privacidade da rede social. **Controles de privacidade** representam o que a rede social disponibiliza de opções, recursos e ferramentas que auxiliam o usuário a controlar sua privacidade
Instruções:	Antes de começar a inspeção observe as seguintes diretrizes: *a.* Observe e anote (no documento disponibilizado) em qual parte da rede social você identifica um problema de privacidade com base nos itens de verificação descritos abaixo *b.* Escreva o ID do item de verificação na planilha de discrepância c. Reporte o tipo de defeito identificado na planilha de discrepância *d.* Defina o grau de severidade para o defeito identificado *e.* Descreva sobre o problema de privacidade identificado
2A. Direito de Privacidade	
2A1	Verifique se rede social permite ao usuário denunciar uma informação, imagem ou vídeo que viola os seus direitos de privacidade
2A2	Verifique se há uma opção que permite denunciar uma conta que está se passando por um usuário (conta *fake*)
2B. Usabilidade e Privacidade	
2B1	Verifique se há atalhos de privacidade que forneçam acesso rápido a algumas das configurações e ferramentas de privacidade mais relevantes da rede social
2B2	Verifique se o usuário tem a opção de um mecanismo de ajuda que facilite a localização de um determinado controle de privacidade
2B3	Verifique se em algum controle de privacidade aparecem informações escritas em um idioma diferente do utilizado eventualmente pelo usuário
2C. Transparência de dados	
2C1	Verifique se há uma opção que permite ao usuário solicitar acesso aos dados pessoais armazenados na rede social
2C2	Verifique se o usuário tem a opção de acessar um registro ou histórico de atividades realizados na rede social
2D. Aplicativos de terceiros	
2D1	Verifique se a rede social permite ao usuário visualizar os aplicativos ou sites de terceiros ativos em sua conta
2D2	Verifique se o usuário tem a opção de editar as informações que os aplicativos ou sites de terceiros podem ter acesso na sua conta
2D3	Verifique se a rede social permite ao usuário remover os aplicativos ou sites de terceiros que não desejam mais ter acesso ou utilizar
2D4	Verifique se a rede social permite ao usuário denunciar um aplicativo ou site de terceiros que estejam comprometendo a sua privacidade
2E. Solicitações de relacionamento	
2E1	Verifique se a rede social permite editar quem pode seguir ou enviar solicitação de relacionamento para um determinado usuário
2E2	Verifique se há uma opção para o usuário remover alguém da sua lista de relacionamento da rede social

2F. Bloqueio	
2F1	Verifique se o usuário tem a opção de bloquear uma pessoa que esteja comprometendo a sua privacidade
2G. Privacidade na busca	
2G1	Verifique se há uma opção que restringe a indexação pública do perfil do usuário por outros mecanismos de busca fora da rede social
2G2	Verifique se a rede social disponibiliza um controle que possa restringir quem pode procurar pelo usuário usando informações pessoais do contato, como o endereço de e-mail ou o número de telefone
2H. Controle de reputação	
2H1	Verifique se a rede social permite ocultar do perfil do usuário uma publicação a qual o mesmo foi marcado ou mencionado sem a sua permissão
2H2	Verifique se o usuário tem a opção de analisar publicações que as pessoas o marcaram ou mencionaram antes de serem exibidas em seu perfil na rede social
2I. Publicação seletiva	
2I2	Verifique se a rede social permite o usuário criar listas personalizadas para que seja possível compartilhar as postagens com grupos específicos de amigos
2J. Gerenciamento de informações sobre o usuário	
2J1	Verifique se o usuário tem a opção de alterar informações de seu login na rede social
2J2	Verifique se o usuário tem a opção de desativar a sua conta temporariamente ou permanentemente na rede social
2J3	Verifique se o usuário tem a opção de criar um filtro avançado para desativar as notificações de determinados usuários que deseja evitar
2J4	Verifique se o usuário tem a opção de selecionar quem pode visualizar a sua lista de amigos ou seguidores na rede social
2L. Confidencialidade	
2L1	Verifique se há uma opção que permita o usuário limpar o seu histórico de busca ou ações na rede social
2L2	Verifique se o usuário tem a opção de ocultar uma publicação compartilhada por ele em seu perfil
2M. Comentários	
2M1	Verifique se o usuário tem a opção de controlar quem pode comentar sua publicação no sistema
2M2	Verifique se o usuário tem a opção de denunciar um comentário, tanto em sua publicação pessoal quanto na publicação de outro indivíduo, que contenha conteúdo impróprio
2M3	Verifique se o usuário tem a opção de ativar um filtro de palavras-chave para ocultar para que ninguém veja comentários que contenham palavras, frases, números ou emojis considerados inapropriados ou ofensivos
2N. Controle de localização	
2N1	Verifique se o usuário tem a opção de desativar os serviços de localização na rede social
2N2	Verifique se o usuário tem a opção de editar ou remover a sua localização em uma determinada publicação na rede social

2O. Legado Digital Pós-Morte	
2O1	Verifique se o usuário tem a opção de escolher indicar um contato herdeiro para gerenciar a sua conta caso o mesmo venha a falecer
2O2	Verifique se a rede social permite transformar a conta de um usuário falecido em memorial digital
2O3	Verifique se a rede social permite solicitar que a conta de um usuário falecido seja permanentemente removida do sistema

PIT 3 - Inspeção das Políticas de Privacidade	
Objetivo:	Inspecionar as políticas de privacidade da rede social. **Políticas de privacidade** representam os documentos que especificam os termos para garantir a privacidade das informações do usuário.
Instruções:	Antes de começar a inspeção observe as seguintes diretrizes: *a.* Observe e anote (no documento disponibilizado) em qual parte da rede social você identifica um problema de privacidade com base nos itens de verificação descritos abaixo *b.* Escreva o ID do item de verificação na planilha de discrepância *c.* Reporte o tipo de defeito identificado na planilha de discrepância *d.* Defina o grau de severidade para o defeito identificado *e.* Descreva sobre o problema de privacidade identificado
3A. Coleta de dados	
3A1	Verifique se há alguma informação detalhada sobre os tipos de dados que estão sendo coletados do usuário
3A2	Verifique se a política de privacidade especifica qual o meio que a rede social utiliza para coletar dados do usuário (se é através do cadastro de conta, se através de informações de compras ou comentários por exemplo)
3B. Uso e divulgação dos dados	
3B1	Verifique se a política de privacidade especifica como a rede social pode utilizar e manipular as informações fornecidas pelo usuário
3B2	Verifique se a política de privacidade especifica com quem (parceiros, provedores ou outros usuários) a rede social pode divulgar as informações fornecidas pelo usuário
3B3	Verifique se há declarações informando em que circunstâncias que a rede social pode divulgar informações do usuário a terceiros, como em casos de razões legais por exemplo
3B4	Verifique se há alguma declaração informando sobre o que acontece com as informações do usuário no caso de uma alteração de controle (como venda ou transferência da rede social para outra empresa)
3C. Armazenamento de dados	
3C1	Verifique se há declarações sobre como a rede social armazena e processa (se em bancos de dados de outros países) os dados coletados do usuário
3C2	Verifique se a política de privacidade especifica por quanto tempo a rede social pode manter armazenado os dados do usuário, caso o indivíduo escolha desativar sua conta
3C3	Verifique se as políticas de privacidade especificam como utilizam os cookies e outras tecnologias de armazenamento
3D. Clareza	
3D1	Verifique se a política apresenta alguma descrição visual (como vídeos breves ou ilustrações) que tornam o documento mais fácil de entender
3D2	Verifique se há alguma informação sobre possíveis modificações ou atualizações nas políticas de privacidade da rede social e se há formas adicionais de notificação de mudanças para o usuário (como lembretes regulares)
3D3	Verifique se as políticas de privacidade possuem alguma informação escrita em outro idioma diferente do idioma do usuário

3E. Ajuda online	
3E1	Verifique se as políticas de privacidade especificam algum meio para o usuário entrar em contato com a rede social
3F. Anonimato em transações	
3F1	Verifique se é especificada alguma medida para preservar informações financeiras do usuário disponibilizadas em transações na rede social (como conexão criptografada e proteção de hardware e software por exemplo)
3G. Dados confidenciais	
3G1	Verifique se as políticas de privacidade especificam as opções para obter o consentimento do usuário quando algumas informações confidenciais precisarem ser usadas ou divulgadas
3G2	Verifique se as políticas de privacidade apresentam um relatório de transparência sobre as informações mais solicitadas em processos jurídicos ou sobre as ações do usuário na rede social
3I. Restrição de idade	
3H1	Verifique se as políticas de privacidade fornecem informações sobre o acesso e envolvimento de crianças na rede social
3H2	Verifique se as políticas de privacidade especificam algum mecanismo de restrição de idade para preservar a participação de menores na rede social
3J. Legislação vigente	
3I1	Verifique se as políticas de privacidade especificam se estão cumprindo ou seguindo a legislação vigente do país em que a rede social está em uso
3L. Serviços de publicidade	
3J1	Verifique se há informações sobre os serviços de publicidade e como eles atuam na rede social
3J2	Verifique se as políticas de privacidade especificam informações sobre preferências publicitárias e como o usuário pode deixar de receber anúncios indesejados

TAXONOMIA PARA CLASSIFICAÇÃO DE DEFEITOS		
Classe	**Tipo**	**Descrição**
OMISSÃO	*Funcionalidade Omitida*	Ocorre quando uma informação ou descrição sobre alguma funcionalidade de privacidade deixou de ser informada ou não existe no sistema
	Feedback Omitido	Ocorre quando não é percebida ou compreendida a resposta dada pelo sistema para uma determinada ação em relação a privacidade (a ação foi realizada, mas está faltando a resposta)
	Interface Omitida	Ocorre quando se deseja achar alguma informação ou funcionalidade de privacidade que existe no sistema e não a consegue encontrar na interface em um primeiro instante
INADEQUAÇÃO	*Informação Ambígua*	Um elemento importante, uma frase ou uma sentença de não foram bem definidos (nos níveis, nos controles ou nas políticas da rede social) causando assim múltiplas interpretações
	Informação Inconsistente	Uma informação ou um elemento de privacidade é representado de maneira diferente em duas visões, ou seja, possuem o mesmo sentido, mas nomes distintos (sinônimos)
	Funcionalidade Incorreta	Alguma funcionalidade de privacidade foi descrita ou representada de maneira incorreta
	Seção Incorreta	Alguma informação ou elemento de privacidade está em um local errado dentro do sistema
DISSEMINAÇÃO	*Exposição Passiva*	Ocorre quando o sistema permite a exposição de um determinado indivíduo por meio das ações de outros usuários ou de terceiros
	Difusão Indevida	Ocorre quando a própria rede social toma a iniciativa de divulgar informações do usuário no sistema ou em outros meios de comunicação

Grau	**Grau de severidade para julgar os problemas detectados**
0	Não considero um problema de privacidade nesta rede social
1	Somente um problema de privacidade cosmético – consertar apenas se houver tempo disponível;
2	Problema leve de privacidade – baixa prioridade para consertá-lo;
3	Problema grave de privacidade – alta prioridade para consertá-lo;
4	Problema catastrófico de privacidade – é imperativo consertá-lo.

APÊNDICE C – MATERIAIS USADOS NOS ESTUDOS COM A PIT-OSN

C.1 TERMO DE CONSENTIMENTO USADO PARA A PIT-OSN

Prezado (a)

Eu, Andrey Antonio de Oliveira Rodrigues, orientado pelo Prof. Dr. Eduardo Luzeiro Feitosa e coorientado pela Profa. Dra. Natasha Malveira Costa Valentim, estou desenvolvendo como parte da minha pesquisa de mestrado uma Técnica de Inspeção de Privacidade orientada a Redes Sociais Online (RSOs). Trata-se da PIT-OSN, uma proposta que tem como objetivo examinar categorias de privacidade de uma aplicação (níveis, controles e políticas) para detectar violações de itens de privacidade estabelecidos, evidenciando um defeito de privacidade. Neste contexto, um defeito de privacidade é qualquer condição ou situação que poderia levar o sistema a se comportar de maneira indesejada e representar um risco para a privacidade do usuário.

Diante disso, você está sendo convidado para participar de uma avaliação, que tem como finalidade avaliar o uso da técnica proposta no processo de inspeção de uma determinada rede social online, com foco na avaliação de categorias de privacidade. Além disso, este estudo também tem como objetivo avaliar a facilidade de uso, utilidade percebida e intenções de uso futuro da técnica em questão. Neste contexto, gostaria de solicitar que você manifeste o seu consentimento para participar deste estudo, realizando as seguintes atividades:

- Ouvir uma explicação sobre a proposta geral técnica, sua estrutura e exemplos;
- Realizar as atividades de inspeção solicitadas;
- Responder um questionário pós-teste para que você possa relatar suas experiências na aplicação da técnica.

O estudo completo terá duração aproximada de quatro horas, incluindo todas as atividades descritas acima, e será dividido em dois dias. É importante você saber que:

1. Os dados coletados durante o estudo serão utilizados **estritamente** no contexto acadêmico e de pesquisa.
2. A equipe envolvida neste estudo tem o compromisso de publicar os resultados de suas pesquisas em fóruns acadêmicos. Entretanto, a publicação é baseada em respeito à **privacidade** e **anonimato** dos participantes. Assim, a sua identidade e a sua participação nesta pesquisa serão mantidas em sigilo e os dados divulgados pela pesquisa não conterão nomes ou quaisquer outras informações que permitam identificá-lo(a).
3. O consentimento para participar deste estudo é uma **escolha livre** de sua parte, realizada a partir do esclarecimento de todas as suas dúvidas e questões sobre a pesquisa.
4. Você não terá **nenhum gasto ou ônus** com a sua participação no estudo e também não receberá qualquer espécie de reembolso ou gratificação devido à participação na pesquisa.
5. Você **pode interromper a sua participação** neste estudo a qualquer momento, sem sofrer nenhuma penalidade. Neste caso, todos os seus dados e resultados parciais serão descartados.
6. Eu, Andrey Rodrigues, responsável pela condução do presente estudo, estou **disponível** para contato pelo e-mail andrey@icomp.ufam.edu.br

De posse das informações acima apresentadas, gostaria que você se pronunciasse sobre a sua decisão:

( ) Dou o meu consentimento para participar do presente estudo. ( ) Não dou o meu consentimento para participar do presente estudo.

Manaus, ____ de _____ de 2018.

Nome do participante: _____

Assinatura do participante: _____

Nome do pesquisador: Andrey Antonio de Oliveira Rodrigues

Assinatura do pesquisador: _____

C.2 TERMO DE CONSENTIMENTO USADO PARA AS INSPEÇÕES *AD HOC*

Prezado (a)

Eu, Andrey Antonio de Oliveira Rodrigues, orientado pelo Prof. Dr. Eduardo Luzeiro Feitosa e coorientado pela Profa. Dra. Natasha Malveira Costa Valentim, estamos realizando uma pesquisa sobre técnicas de inspeção de privacidade orientada a redes sociais online. Um dos fatores decisivos no planejamento e nos resultados da inspeção de um artefato de software é a definição da técnica de inspeção que será utilizada. Nesse sentido, estamos investigando a aplicação de uma técnica de inspeção *ad hoc*. Esse tipo de inspeção, como o nome indica, baseia-se exclusivamente na experiência dos avaliadores, não havendo direcionamento sobre como proceder ou o que deve ser verificado especificamente durante a atividade inspeção.

Diante disso, você está sendo convidado para participar de uma avaliação, que tem como finalidade examinar o uso desse tipo de técnica no processo de inspeção de privacidade de uma determinada rede social online. Além disso, esta avaliação também tem como objetivo avaliar a facilidade de uso, utilidade percebida e intenções de uso futuro da técnica em questão. Neste contexto, gostaria de solicitar que você manifeste o seu consentimento para participar desta avaliação, realizando as seguintes atividades:

- Ouvir uma explicação sobre a proposta geral da técnica, sua estrutura e exemplos;
- Realizar as atividades de inspeção solicitadas;
- Responder um questionário pós-teste para que você possa relatar suas experiências na aplicação da técnica.

A avaliação completa terá duração aproximada de quatro horas, incluindo todas as atividades descritas acima, e será dividida em dois dias. É importante você saber que:

1. Os dados coletados durante o estudo serão utilizados **estritamente** no contexto acadêmico e de pesquisa.

2. A equipe envolvida neste estudo tem o compromisso de publicar os resultados de suas pesquisas em fóruns acadêmicos. Entretanto, a publicação é baseada em respeito à **privacidade** e **anonimato** dos participantes. Assim, a sua identidade e a sua participação nesta pesquisa serão mantidas em sigilo e os dados divulgados pela pesquisa não conterão nomes ou quaisquer outras informações que permitam identificá-lo(a).

3. O consentimento para participar deste estudo é uma **escolha livre** de sua parte, realizada a partir do esclarecimento de todas as suas dúvidas e questões sobre a pesquisa.

4. Você não terá **nenhum gasto ou ônus** com a sua participação no estudo e também não receberá qualquer espécie de reembolso ou gratificação devido à participação na pesquisa.

5. Você **pode interromper a sua participação** neste estudo a qualquer momento, sem sofrer nenhuma penalidade. Neste caso, todos os seus dados e resultados parciais serão descartados.

6. Eu, Andrey Rodrigues, responsável pela condução do presente estudo, estou **disponível** para contato pelo e-mail andrey@icomp.ufam.edu.br

De posse das informações acima apresentadas, gostaria que você se pronunciasse sobre a sua decisão:

( ) Dou o meu consentimento para participar do presente estudo. ( ) Não dou o meu consentimento para participar do presente estudo.

Manaus, ____ de novembro de 2018

Nome do participante: _____

Assinatura do participante: _____

Nome do pesquisador: Andrey Antonio de Oliveira Rodrigues

Assinatura do pesquisador: _____

C.3 QUESTIONÁRIO DE CARACTERIZAÇÃO

QUESTIONÁRIO DE CARACTERIZAÇÃO
(1) Por favor, preencha o questionário abaixo. Suas repostas irão nos ajudar a analisar as informações que serão coletadas durante a avaliação.

1. DADOS PESSOAIS:

Nome: _____Sexo (M ou F): ___ Idade: _____ Formação: _____ Profissão: _____

2. EXPERIÊNCIA DE USO DE REDES SOCIAIS ONLINE:

Por favor, preencha os campos com a opção que melhor representa a sua resposta a cada pergunta

2.1. Você utiliza alguma das redes sociais online (RSO) abaixo? Se sim, assinale quais delas?

☐ Facebook

☐ Google +

☐ Instagram

☐ Myspace

☐ Snapchat

☐ Twitter

☐ LinkedIn

☐ ResearchGate

☐ Outra(s). Quais? _____

2.2. Caso sua resposta à questão 2.1 tenha sido sim, com qual frequência você utiliza RSOs?

☐ Mais de uma vez por dia

☐ Uma vez por dia

☐ 2 a 3 vezes por semana

☐ 1 vez por semana

☐ Menos de 1 vez por semana

2. CONHECIMENTO SOBRE AVALIAÇÃO DE PRIVACIDADE

2.1. Você já avaliou interfaces de usuário?

☐ Nunca avaliei

☐ Sim, já avaliei em disciplina de graduação ou pós-graduação

☐ Sim, já avaliei em pesquisa

☐ Sim, já avaliei no mercado de trabalho

3.2. Em relação ao grau do seu conhecimento prévio sobre privacidade digital, marque os itens abaixo que melhor se aplicam a sua resposta

☐ Não possuo nenhum conhecimento prévio sobre privacidade

☐ Tenho algumas noções de privacidade adquiridas através de leitura/palestra

☐ Participei de ____ projeto(s) ou avaliação(ões) de privacidade em sala de aula

☐ Participei de ____ projeto(s) ou avaliação(ões) de privacidade na indústria

C.4 PLANILHA PARA O RELATO DE DISCREPÂNCIAS DA PIT-OSN

Inspetor	

Horário Inicial	
Horário Final	

ID DO ITEM DE VERICAÇÃO	TIPO DE DEFEITO	GRAU DE SEVERIDADE	DESCRIÇÃO DO PROBLEMA ENCONTRADO

C.5 PLANILHA PARA O RELATO DE DISCREPÂNCIAS DA ADHOC

Inspetor	

Horário Inicial	
Horário Final	

LOCAL DO DEFEITO NA APLICAÇÃO	DESCRIÇÃO DO PROBLEMA ENCONTRADO

C.6 DIRETRIZES PARA A EXECUÇÃO DAS INSPEÇÕES *AD HOC*

C.6.1 Diretrizes para Inspeção *Ad hoc* de Níveis de Privacidade

Inspeção dos Níveis de Privacidade	
Objetivo:	Inspecionar os níveis de privacidade da rede social
Instruções:	Antes de começar a inspeção observe as seguintes diretrizes: *a.* Anote o **horário inicial** da sua avaliação na planilha de discrepâncias b. Observe e anote (no documento disponibilizado) em **qual local** da rede social você identifica um problema de privacidade com base na sua percepção sobre os **Níveis de Privacidade.** c. Descreva sobre o **problema de privacidade** identificado na planilha de discrepâncias d. Anote o **horário final** da sua avaliação na planilha de discrepância
Categoria	**Nível de privacidade:** O nível de privacidade refere-se à possibilidade de um determinado indivíduo aumentar ou diminuir os seus limites de acesso para alcançar o seu nível desejado de privacidade. Isto indica que pode haver um ponto contínuo de níveis de privacidade que podem ser alcançados pelo indivíduo, variando desde um nível de privacidade baixo (mínimo), onde todas as informações ficam acessíveis para uma ampla audiência ou até o nível de privacidade alto, onde nenhuma informação é compartilhada pelo indivíduo. O MDP considera que as RSOs podem permitir que seus usuários atinjam diferentes níveis de privacidade, dependendo de diferentes elementos envolvidos no compartilhamento de suas informações. Estes elementos estão relacionados a quem compartilha, o que é compartilhado e para quem, em que local e por quanto tempo a informação fica disponível, além dos efeitos gerados por tal compartilhamento.

C.6.2 Diretrizes para Inspeção *Ad hoc* de Controles de Privacidade

Inspeção dos Controles de Privacidade	
Objetivo:	Inspecionar os controles de privacidade da rede social
Instruções:	Antes de começar a inspeção observe as seguintes diretrizes: *a.* Anote o **horário inicial** da sua avaliação na planilha de discrepâncias b. Observe e anote (no documento disponibilizado) em **qual local** da rede social você identifica um problema de privacidade com base na sua percepção sobre o **Controle de Privacidade.** c. Descreva sobre o **problema de privacidade** identificado na planilha de discrepâncias d. Anote o **horário final** da sua avaliação na planilha de discrepância
Categoria	**Controle de privacidade:** Os controles de privacidade representam o que a rede social disponibiliza de opções, recursos e ferramentas que auxiliam o usuário a regular sua privacidade. Um ponto importante a ser ressaltado é que os controles fornecidos por estas aplicações, geralmente estão elencados através de informações ou representados através de elementos que indicam como funcionam estes determinados recursos.

C.6.2 Diretrizes para Inspeção *Ad hoc* de Políticas de Privacidade

Inspeção das Políticas de Privacidade	
Objetivo:	Inspecionar as políticas de privacidade da rede social
Instruções:	Antes de começar a inspeção observe as seguintes diretrizes: *a.* Anote o **horário inicial** da sua avaliação na planilha de discrepâncias b. Observe e anote (no documento disponibilizado) em **qual local** da rede social você identifica um problema de privacidade com base na sua percepção sobre as **Políticas de Privacidade.** c. Descreva sobre o **problema de privacidade** identificado na planilha de discrepâncias d. Anote o **horário final** da sua avaliação na planilha de discrepância
Categoria	**Políticas de privacidade:** Políticas de privacidade são documentos (contratos) que descrevem termos para garantir a privacidade das informações dos usuários. A política de privacidade informa ao usuário questões relacionadas à privacidade de seus dados, por exemplo, informações a respeito da coleta e tratamento dos dados e localização dos servidores. A partir dessas definições, quais seriam os problemas de privacidade que você identifica neste documento de políticas?

C.7 QUESTIONÁRIO PÓS-INSPEÇÃO PARA O CONJUNTO DE TÉCNICAS PIT-OSN

QUESTIONÁRIO PÓS-INSPEÇÃO PIT-OSN 1
Por favor, preencha o questionário abaixo. Suas repostas irão nos ajudar a analisar as informações que serão coletadas durante a avaliação.
Nome:

1) Responda as questões a seguir considerando sua experiência com a técnica PIT-OSN 1, utilizando a seguinte escala (1) Discordo Totalmente, (2) Discordo Fortemente, (3) Discordo Parcialmente, (4) Concordo Parcialmente, (5) Concordo Fortemente, (6) Concordo Totalmente

Facilidade de Uso Percebida

	1	2	3	4	5	6
F1. Minha **interação** com a PIT-OSN 1 foi **clara e compreensível**						
F2. Utilizar a PIT-OSN 1 **não exige** muito do meu **esforço mental**						
F3. Considero a PIT-OSN 1 **fácil de usar**						
F4. Considero fácil utilizar a PIT-OSN 1 **para fazer o que eu quero que ela faça**, apoiar a avaliação dos níveis de privacidade em RSOs através de inspeção						

Utilidade Percebida

	1	2	3	4	5	6
U1. Usar a PIT-OSN 1 melhorou o meu **desempenho** na inspeção de níveis de privacidade em RSOs.						
U2. Usar os itens de verificação da PIT-OSN 1 melhorou a minha **produtividade** na inspeção de níveis de privacidade em RSOs						
U3. Usar a PIT-OSN 1 aumentou a minha **eficácia** na inspeção de níveis de privacidade em RSOs						
U4. Eu considero a PIT-OSN 1 **útil** para apoiar o processo de inspeção de níveis de privacidade de RSOs						

Intenção de Uso

	1	2	3	4	5	6
I1. Supondo que eu tenho acesso a PIT-OSN 1, **eu pretendo usá-la**						
I2. Levando em conta que eu tenho acesso a PIT-OSN 1 **eu prevejo que eu irei usá-la** em outros momentos						

2) Você discordou parcialmente, fortemente ou totalmente de algum indicador acima (facilidade de uso, utilidade e intenção de uso futuro)? Em caso afirmativo, por que você discordou?

3) Por favor, descreva os pontos positivos e negativos de fazer uma inspeção de privacidade usando a técnica PIT-OSN 1.

4) Você poderia descrever sugestões de melhorias para a técnica PIT-OSN 1 ou sugestões de novos itens de verificação ou novos tipos de defeitos que a técnica ainda não contempla?

QUESTIONÁRIO PÓS-INSPEÇÃO PIT-OSN 2
Por favor, preencha o questionário abaixo. Suas repostas irão nos ajudar a analisar as informações que serão coletadas durante a avaliação.
Nome:

1) Responda as questões a seguir considerando sua experiência com a técnica PIT-OSN 2, utilizando a seguinte escala (1) Discordo Totalmente, (2) Discordo Fortemente, (3) Discordo Parcialmente, (4) Concordo Parcialmente, (5) Concordo Fortemente, (6) Concordo Totalmente

Facilidade de Uso Percebida

	1	2	3	4	5	6
F1. Minha **interação** com a PIT-OSN 2 foi **clara e compreensível**						
F2. Utilizar a PIT-OSN 2 **não exige** muito do meu **esforço mental**						
F3. Considero a PIT-OSN 2 **fácil de usar**						
F4. Considero fácil utilizar a PIT-OSN 2 **para fazer o que eu quero que ela faça**, apoiar a avaliação de controles de privacidade em RSOs através de inspeção						

Utilidade Percebida

	1	2	3	4	5	6
U1. Usar a PIT-OSN 2 melhorou o meu **desempenho** na inspeção de controles de privacidade em RSOs						
U2. Usar os itens de verificação da PIT-OSN 2 melhorou a minha **produtividade** na inspeção de controles de privacidade em RSOs						
U3. Usar a PIT-OSN 2 aumentou a minha **eficácia** na inspeção de controles de privacidade em RSOs						
U4. Eu considero a PIT-OSN 2 **útil** para apoiar o processo de inspeção de controles de privacidade de RSOs						

Intenção de Uso

	1	2	3	4	5	6
I1. Supondo que eu tenho acesso a PIT-OSN 2, **eu pretendo usá-la**						
I2. Levando em conta que eu tenho acesso a PIT-OSN 2 **eu prevejo que eu irei usá-la** em outros momentos						

2) Você discordou parcialmente, fortemente ou totalmente de algum indicador acima (facilidade de uso, utilidade e intenção de uso futuro)? Em caso afirmativo, por que você discordou?

3) Por favor, descreva os pontos positivos e negativos de fazer uma inspeção de privacidade usando a técnica PIT-OSN 2.

4) Você poderia descrever sugestões de melhorias para a técnica PIT-OSN 2 ou sugestões de novos itens de verificação ou novos tipos de defeitos que a técnica ainda não contempla?

QUESTIONÁRIO PÓS-INSPEÇÃO PIT-OSN 3
Por favor, preencha o questionário abaixo. Suas repostas irão nos ajudar a analisar as informações que serão coletadas durante a avaliação.
Nome:

1) Responda as questões a seguir considerando sua experiência com a técnica PIT-OSN 3, utilizando a seguinte escala (1) Discordo Totalmente, (2) Discordo Fortemente, (3) Discordo Parcialmente, (4) Concordo Parcialmente, (5) Concordo Fortemente, (6) Concordo Totalmente.

Facilidade de Uso Percebida

	1	2	3	4	5	6
F1. Minha **interação** com a PIT-OSN 3 foi **clara e compreensível**						
F2. Utilizar a PIT-OSN 3 **não exige** muito do meu **esforço mental**						
F3. Considero a PIT-OSN 3 **fácil de usar**						
F4. Considero fácil utilizar a PIT-OSN 3 **para fazer o que eu quero que ela faça**, apoiar a avaliação de políticas de privacidade em RSOs através de inspeção						

Utilidade Percebida

	1	2	3	4	5	6
U1. Usar a PIT-OSN 3 melhorou o meu **desempenho** na inspeção de políticas de privacidade em RSOs						
U2. Usar os itens de verificação da PIT-OSN 3 melhorou a minha **produtividade** na inspeção de políticas de privacidade em RSOs						
U3. Usar a PIT-OSN 3 aumentou a minha **eficácia** na inspeção de políticas de privacidade em RSOs						
U4. Eu considero a PIT-OSN 3 **útil** para apoiar o processo de inspeção de políticas de privacidade de RSOs						

Intenção de Uso

	1	2	3	4	5	6
I1. Supondo que eu tenho acesso a PIT-OSN 3, **eu pretendo usá-la**						
I2. Levando em conta que eu tenho acesso a PIT-OSN 3, **eu prevejo que eu irei usá-la** em outros momentos						

2) Você discordou parcialmente, fortemente ou totalmente de algum indicador acima (facilidade de uso, utilidade e intenção de uso futuro)? Em caso afirmativo, por que você discordou?

3) Por favor, descreva os pontos positivos e negativos de fazer uma inspeção de privacidade usando a técnica PIT-OSN 3 .

4) Você poderia descrever sugestões de melhorias para a técnica PIT-OSN 3 ou sugestões de novos itens de verificação que a técnica ainda não contempla?

C.8 QUESTIONÁRIO PÓS-INSPEÇÃO PARA AS INSPEÇÕES *AD HOC*

QUESTIONÁRIO PÓS-INSPEÇÃO DE CONTROLES *AD HOC*
Por favor, preencha o questionário abaixo. Suas repostas irão nos ajudar a analisar as informações que serão coletadas durante a avaliação.
Nome:

1) Responda as questões a seguir considerando sua experiência com uma inspeção *ad hoc* utilizando a seguinte escala (1) Discordo Totalmente, (2) Discordo Fortemente, (3) Discordo Parcialmente, (4) Concordo Parcialmente, (5) Concordo Fortemente, (6) Concordo Totalmente

Facilidade de Uso Percebida

	1	2	3	4	5	6
F1. Minha **interação** com a técnica de inspeção *ad hoc* foi **clara e compreensível** para inspecionar controles de privacidade em RSOs						
F2. Utilizar a técnica *ad hoc* para inspecionar os controles de privacidade em redes sociais **não exige** muito do meu **esforço mental**						
F3. Considero a técnica *ad hoc* **fácil de usar**						
F4. Considero fácil utilizar a técnica *ad hoc* **para fazer o que eu quero que ela faça**, apoiar a avaliação de controles privacidade em RSOs através de inspeção						

Utilidade Percebida

	1	2	3	4	5	6
U1. Usar a técnica *ad hoc* melhorou o meu **desempenho** na inspeção de controles de privacidade em redes sociais online						
U2. Usar a técnica *ad hoc* melhorou a minha **produtividade** na inspeção de controles de privacidade em redes sociais online						
U3. Usar a técnica *ad hoc* aumentou a minha **eficácia** na inspeção de controles de privacidade em redes sociais online						
U4. Eu considero a técnica *ad hoc* **útil** para apoiar o processo de inspeção de controles de privacidade de redes sociais online						

Intenção de Uso

	1	2	3	4	5	6
I1. Supondo que eu tenho acesso a técnica *ad hoc* para inspecionar controles de privacidade em RSOs, **eu pretendo usá-la**						
I2. Levando em conta que eu tenho acesso a técnica *ad hoc* para inspecionar controles de privacidade em RSOs**, eu prevejo que eu irei usá-la** em outros momentos						

2) Você discordou parcialmente, fortemente ou totalmente de algum indicador acima (facilidade de uso, utilidade e intenção de uso futuro)? Em caso afirmativo, por que você discordou?

3) Por favor, descreva os pontos positivos e negativos de fazer uma inspeção de controles de privacidade usando uma técnica *ad hoc* .

4) Você poderia sugerir alguma melhoria para o processo de inspeção de controles de privacidade *ad hoc*?

QUESTIONÁRIO PÓS-INSPEÇÃO DE POLÍTICAS *AD HOC*
Por favor, preencha o questionário abaixo. Suas repostas irão nos ajudar a analisar as informações que serão coletadas durante a avaliação.
Nome:

1) Responda as questões a seguir considerando sua experiência com uma inspeção *ad hoc* utilizando a seguinte escala (1) Discordo Totalmente, (2) Discordo Fortemente, (3) Discordo Parcialmente, (4) Concordo Parcialmente, (5) Concordo Fortemente, (6) Concordo Totalmente

Facilidade de Uso Percebida

	1	2	3	4	5	6
F1. Minha **interação** com a técnica de inspeção *ad hoc* foi **clara e compreensível** para inspecionar políticas de privacidade em RSOs						
F2. Utilizar a técnica *ad hoc* para inspecionar as políticas de privacidade em redes sociais **não exige** muito do meu **esforço mental**						
F3. Considero a técnica *ad hoc* **fácil de usar**						
F4. Considero fácil utilizar a técnica *ad hoc* **para fazer o que eu quero que ela faça**, apoiar a avaliação de políticas privacidade em RSOs através de inspeção						

Utilidade Percebida

	1	2	3	4	5	6
U1. Usar a técnica *ad hoc* melhorou o meu **desempenho** na inspeção de políticas de privacidade em redes sociais online						
U2. Usar a técnica *ad hoc* melhorou a minha **produtividade** na inspeção de políticas de privacidade em redes sociais online						
U3. Usar a técnica *ad hoc* aumentou a minha **eficácia** na inspeção de políticas de privacidade em redes sociais online						
U4. Eu considero a técnica *ad hoc* **útil** para apoiar o processo de inspeção de políticas de privacidade de redes sociais online						

Intenção de Uso

	1	2	3	4	5	6
I1. Supondo que eu tenho acesso a técnica *ad hoc* para inspecionar políticas de privacidade em RSOs, **eu pretendo usá-la**						
I2. Levando em conta que eu tenho acesso a técnica *ad hoc* para inspecionar políticas de privacidade em RSOs**, eu prevejo que eu irei usá-la** em outros momentos						

2) Você discordou parcialmente, fortemente ou totalmente de algum indicador acima (facilidade de uso, utilidade e intenção de uso futuro)? Em caso afirmativo, por que você discordou?

3) Por favor, descreva os pontos positivos e negativos de fazer uma inspeção de políticas de privacidade usando uma técnica *ad hoc*

4) Você poderia sugerir alguma melhoria para o processo de inspeção de políticas de privacidade *ad hoc*?

QUESTIONÁRIO PÓS-INSPEÇÃO DE NÍVEIS *AD HOC*
Por favor, preencha o questionário abaixo. Suas repostas irão nos ajudar a analisar as informações que serão coletadas durante a avaliação.
Nome:

1) Responda as questões a seguir considerando sua experiência com uma inspeção *ad hoc* utilizando a seguinte escala (1) Discordo Totalmente, (2) Discordo Fortemente, (3) Discordo Parcialmente, (4) Concordo Parcialmente, (5) Concordo Fortemente, (6) Concordo Totalmente

Facilidade de Uso Percebida

	1	2	3	4	5	6
F1. Minha **interação** com a técnica de inspeção *ad hoc* foi **clara e compreensível** para inspecionar níveis de privacidade em RSOs						
F2. Utilizar a técnica *ad hoc* para inspecionar os níveis de privacidade em redes sociais **não exige** muito do meu **esforço mental**						
F3. Considero a técnica *ad hoc* **fácil de usar**						
F4. Considero fácil utilizar a técnica *ad hoc* **para fazer o que eu quero que ela faça**, apoiar a avaliação de níveis privacidade em RSOs através de inspeção						

Utilidade Percebida

	1	2	3	4	5	6
U1. Usar a técnica *ad hoc* melhorou o meu **desempenho** na inspeção de níveis de privacidade em redes sociais online						
U2. Usar a técnica *ad hoc* melhorou a minha **produtividade** na inspeção de níveis de privacidade em redes sociais online						
U3. Usar a técnica *ad hoc* aumentou a minha **eficácia** na inspeção de níveis de privacidade em redes sociais online						
U4. Eu considero a técnica *ad hoc* **útil** para apoiar o processo de inspeção de níveis de privacidade de redes sociais online						

Intenção de Uso

	1	2	3	4	5	6
I1. Supondo que eu tenho acesso a técnica *ad hoc* para inspecionar níveis de privacidade em RSOs, **eu pretendo usá-la**						
I2. Levando em conta que eu tenho acesso a técnica *ad hoc* para inspecionar níveis de privacidade em RSOs**, eu prevejo que eu irei usá-la** em outros momentos						

2) Você discordou parcialmente, fortemente ou totalmente de algum indicador acima (facilidade de uso, utilidade e intenção de uso futuro)? Em caso afirmativo, por que você discordou?

3) Por favor, descreva os pontos positivos e negativos de fazer uma inspeção de níveis de privacidade usando uma técnica *ad hoc.*

4) Você poderia sugerir alguma melhoria para o processo de inspeção de níveis de privacidade *ad hoc*?