UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE ELETRICIDADE

Ariel Soares Teles

Um Mecanismo Baseado em Lógica Nebulosa para a Identificação de Situações de Usuários Aplicado à Privacidade em Redes Sociais Móveis

São Luís
2017

Ariel Soares Teles

Um Mecanismo Baseado em Lógica Nebulosa para a Identificação de Situações de Usuários Aplicado à Privacidade em Redes Sociais Móveis

Tese apresentada ao Programa de Pós-Graduação em Engenharia de Eletricidade da Universidade Federal do Maranhão como requisito parcial para a obtenção do grau de DOUTOR em Engenharia de Eletricidade com área de concentração em Ciência da Computação.

Orientador: Francisco José da Silva e Silva

Doutor - UFMA

São Luís

2017

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Núcleo Integrado de Bibliotecas/UFMA

Soares Teles, Ariel.
Um Mecanismo Baseado em Lógica Nebulosa para a Identificação de Situações de Usuários Aplicado à Privacidade em Redes Sociais Móveis / Ariel Soares Teles. - 2017.
170 f.

Orientador(a): Francisco José da Silva e Silva.
Tese (Doutorado) - Programa de Pós-graduação em Engenharia de Eletricidade/ccet, Universidade Federal do Maranhão, São Luís, 2017.

1. Computação Situacional. 2. Lógica Nebulosa. 3. Privacidade. 4. Redes Sociais Móveis. I. José da Silva e Silva, Francisco. II. Título.

Ariel Soares Teles

Um Mecanismo Baseado em Lógica Nebulosa para a Identificação de Situações de Usuários Aplicado à Privacidade em Redes Sociais Móveis

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por Ariel Soares Teles e aprovada pela comissão examinadora.

Aprovada em 10 de fevereiro de 2017

BANCA EXAMINADORA

Francisco José da Silva e Silva (orientador)

Doutor - UFMA

María del Rosario Girardi Gutiérrez

Doutora - UFMA

Vicente Leonardo Paucar

Doutor - UFMA

Joaquim Celestino Júnior

Doutor - UECE

Markus Endler

Doutor - PUC-Rio

João António Correia Lopes

Doutor - FEUP

Dedico esta tese à minha família. Sem eles nada disso seria possível.

Agradecimentos

Agradeço a Deus em primeiro lugar, ele sempre sustenta todas minhas esperanças e me dar forças para continuar.

Agradeço a minha mãe Fátima, a meu pai Marcondes e a minha irmã Layla, que sempre me apoiaram incondicionalmente durante todo o tempo dedicado ao meu doutorado, inclusive em momentos que tudo parecia estar perdido.

Agradeço ao meu orientador, o professor Francisco, por me conduzir durante todos esses anos de doutorado na construção desse trabalho. Agradeço por ele ter confiado em mim no início e no trabalho que eu poderia realizar. Mas agradeço principalmente por ele não ter desacreditado de mim, foram muitas discussões, algumas fáceis e outras nem tanto, mas que me fizeram chegar até aqui.

Agradeço a toda equipe de professores e alunos que fazem e fizeram parte do Laboratório de Sistemas Distribuídos Inteligentes (LSDi) da Universidade Federal do Maranhão (UFMA), com os quais compartilhamos conhecimentos nas áreas de pesquisa. Em especial, agradeço a Jesseildo, Rômulo, Dejailson, Arikleyton, Marcelo, José Daniel, Eduardo, Robertim, professor Rafael e ao meu grande companheiro de doutorado Berto, que fizeram parte dessa história.

Agradeço ao professor Markus Endler, pelos muitos ensinamentos e por ter contribuído efetivamente com a construção desse trabalho durante todo o tempo de doutorado. Ele foi peça fundamental para a existência e concretização desse trabalho.

Agradeço ao professor João Correia Lopes e Artur Rocha, primeiramente por terem acreditado no trabalho desenvolvido e pelo suporte durante o doutorado sanduíche na Faculdade de Engenharia da Universidade do Porto (FEUP) e no Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência (INESC TEC), em Porto-Portugal.

Agradeço ao professor Ricardo de Andrade, pelos ensinamentos e discussões sobre sistemas nebulosos.

Ao Alcides, secretário administrativo do PPGEE, que sempre se faz presente e disposto a atender as nossas necessidades de aluno.

Aos membros da banca examinadora, por aceitarem a missão de avaliar este trabalho.

Agradeço a Fundação de Amparo à Pesquisa e ao Desenvolvimento Científico e Tecnológico do Maranhão (FAPEMA) e o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), pelo apoio financeiro concedido.

Agradeço a meus amigos, de Parnaíba e os que fiz durante esses sete anos de luta em São Luís desde o início do mestrado, que contribuíram, de forma direta ou indireta, para a concretização deste trabalho.

Por fim, gostaria de fazer um agradecimento especial ao professor Zair Abdelouahab (*in memoriam*), por ter feito parte da construção da minha vida acadêmica de pesquisa com muitos conhecimentos técnicos e, mais importante, ensinamentos de vida.

Pois ainda que o justo caia sete vezes, tornará a erguer-se...

Provérbios 24:16

Resumo

Esta pesquisa primeiramente investiga os requisitos de privacidade de usuários em Redes Sociais Móveis (RSMs) através de um estudo com 164 brasileiros, o qual indicou que seus requisitos são normalmente dinâmicos e contextuais. Em seguida, a pesquisa aplica o paradigma de Computação Situacional para o desenvolvimento de uma solução para atendê-los. Esta solução é chamada de *SelPri*, desenvolvida como prova de conceito em forma de uma aplicação social móvel para adaptar com autonomia as configurações de privacidade de postagens em RSMs de acordo com a situação do usuário. O *SelPri* utiliza um modelo conceitual que faz uso de lógica nebulosa como base para a construção de um motor de inferência para identificar as situações de usuários móveis a partir das seguintes informações de contexto: localização, período do dia, dias da semana, e co-localização. O *SelPri* é implementado integrado ao Facebook. Adicionalmente, para mostrar a flexibilidade do modelo conceitual, ele é também usado para a construção de um motor de inferência para ser utilizado em um domínio de aplicação diferente, o de saúde mental. Esse motor de inferência identifica situações de usuários a partir de informações contextuais diferentes: não utiliza a co-localização e passa a usar a atividade do usuário. A solução originada no domínio de saúde mental é chamada de *SituMan*. Dois experimentos foram realizados com ambas soluções, em que objetivaram verificar a acurácia do motor de inferência nebulosa para identificação de situações, e avaliar a satisfação do usuário. A avaliação da experiência de uso realizada com o *SelPri* destacou que a abordagem para atender os requisitos dinâmicos e dependentes de contexto de privacidade teve uma boa aceitação pelos participantes e provou ser de uso prático. As avaliações de experiência de uso também mostraram que ambas soluções foram bem avaliadas com relação a usabilidade. As avaliações de acurácia mostraram uma taxa de acerto elevada dos motores de inferência para identificar situações: ≈94,6% e ≈92,04%, para o *SelPri* e *SituMan*, respectivamente.

Palavras-chaves: Computação Situacional, Redes Sociais Móveis, Privacidade, Lógica Nebulosa.

Abstract

This research firstly investigates the privacy requirements of users in Mobile Social Networks (MSNs) through a study with 164 Brazilians, which indicated that their requirements are usually dynamic and contextual. Next, the research applies the Situational Computing paradigm to develop a solution to serve them. This solution is called *SelPri*, developed as proof of concept in the form of a mobile social application to autonomously adapt the privacy settings of posts in MSNs according to the user situation. *SelPri* uses a conceptual model with fuzzy logic as the basis for constructing an inference engine to identify mobile user situations from the following context information: location, time of the day, day of week, and co-location. *SelPri* is integrated with Facebook. Additionally, to show the flexibility of the conceptual model, it is also used to construct an inference engine to be used in a different application domain, the mental health. This second inference engine identifies user situations from different context information: it does not use co-location and uses the user activity. The solution originated in the mental health domain is called *SituMan*. Two experiments were carried out with both solutions, in order to verify the accuracy of the fuzzy inference engine to identify situations, and to evaluate the user satisfaction. The use experience evaluation with *SelPri* emphasized that the approach to meet the dynamic and context-dependent privacy requirements was well accepted by the participants and proved to be of practical use. The experiments also showed that both solutions were well evaluated with respect to usability. The accuracy evaluations showed a high hit rate of the inference engines to identify situations: $\approx$94.6% and $\approx$ 92.04%, for *SelPri* and *SituMan*, respectively.

Keywords: Situational Computing, Mobile Social Networks, Privacy, Fuzzy Logic.

Lista de Figuras

2.1 Grafo Social. 16

2.2 Definição de RSMs [132]. 17

2.3 Classificação dos tipos de contexto segundo Emmanouilidis et al. [47]. . 20

2.4 Arquiteturas de RSMs. 24

2.5 Ilustração do *Location Cheating Attack* [67]. 30

3.1 Arquitetura SDDL [40]. 42

3.2 Modelo de Identificação de Situação baseada em Especificação. 44

3.3 Conjuntos *crisp* e nebulosos da altura de uma pessoa. 47

4.1 Taxonomia dos Trabalhos Relacionados. 50

4.2 *Framework* PICOS [138]. 61

4.3 Configuração de Política de Privacidade no PeopleFinder [120]. 62

4.4 Privacidade com Restrição de Localização no PeopleFinder [120]. 63

4.5 Interfaces da Aplicação Móvel SPISM [23]. 66

4.6 Informações de Contexto Utilizadas para Tomada de Decisão no SPISM [23]. 68

4.7 Visão Geral do Guia de Privacidade [49]. 70

5.1 Frequência de Acesso dos Sujeitos. 80

5.2 Respostas dos Sujeitos para Quem Pode Acessar Conteúdos Postados. . 81

5.3 Resposta dos Sujeitos para os Fatores que Influenciaram Decisões para Controlar Acesso a Conteúdos. 82

5.4 Modelo Conceitual da Inferência de Situação. 91

5.5 Gráficos dos Conjuntos Nebulosos dos Dados de Contexto. 96

5.6 Diagrama dos Componentes do *SelPri*. 101

5.7 Interfaces Móveis do *SelPri* para Definição de PPSs. 106

5.8 Interfaces do *MoodBuster* para Requisitar Auto-avaliações dos Pacientes. 110

5.9 Interfaces do *SituMan* para Definição de Situações e Disponibilidade. . . 112

6.1 Resultados de Usabilidade. 124

6.2 Resultados sobre Consciência de Situação. 125

6.3 Resultados sobre Privacidade. 126

6.4 Resultados do Questionário. 132

Lista de Tabelas

4.1 Análise Comparativa dos Trabalhos Relacionados. 74

5.1 Funções dos Conjuntos Nebulosos de Localização. 93

5.2 Funções dos Conjuntos Nebulosos de Co-localização. 93

5.3 Funções dos Conjuntos Nebulosos de Tempo – Dias da Semana (1 semana = 7 dias). 94

5.4 Funções dos Conjuntos Nebulosos de Tempo – Períodos do Dia (1 dia = 24h). 95

5.5 Análise Comparativa dos Trabalhos Relacionados com a Solução Proposta. 113

6.1 Resultados da Avaliação de Acurácia. 120

6.2 Resultados da Avaliação de Acurácia do *SituMan*. 129

Lista de Siglas

AGPS	*Assisted Global Positioning System*.
API	*Application Programming Interface*.
CDAC	*Context-dependent Authentication and Access Control*.
DDS	*Data Distribution Service*.
EMA	*Ecological Momentary Assessment*.
EMI	*Ecological Momentary Intervention*.
FEUP	Faculdade de Engenharia da Universidade do Porto.
GPS	*Global Positioning System*.
HTTP	*Hypertext Transfer Protocol*.
IHC	Interação Humano-Computador.
INESC TEC	Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência.
IP	*Internet Protocol*.
ISMAI	Instituto Universitário da Maia.
LSDi	Laboratório de Sistemas Distribuídos Inteligentes.
MR-UDP	*Mobile Reliable - User Datagram Protocol*.
PoA	*Point of Attachment*.

PPS	Perfil de Privacidade Situacional.
QoC	*Quality of Context*.
QoD	*Quality of Device*.
QoS	*Quality of Service*.
RBAC	*Role-Based Access Control*.
RSMs	Redes Sociais Móveis.
RTPS	*Real-Time Publish-Subscribe*.
SDDL	*Scalable Data Distribution Layer*.
UFMA	Universidade Federal do Maranhão.
URL	*Uniform Resource Locator*.

Sumário

Lista de Figuras **x**

Lista de Tabelas **xii**

Lista de Siglas **xiii**

1 Introdução **1**

1.1 Contexto Geral 1

1.2 Caracterização do Problema 4

1.3 Hipótese de Pesquisa 7

1.4 Relevância do Trabalho 9

1.5 Objetivos 10

1.6 Metodologia de Pesquisa 11

1.7 Organização do Trabalho 13

2 Redes Sociais Móveis **15**

2.1 Conceitos 15

2.2 Informações de Contexto em RSMs 18

2.2.1 Inserção de Contexto em RSMs 21

2.3 Arquiteturas de RSMs 23

2.4 Segurança e Privacidade em Redes Sociais 25

2.4.1 Privacidade em Aplicações Sociais Móveis 29

2.4.2 Ataques contra a Rede Social 32

2.5 Conclusão 33

3 Computação Situacional **34**

3.1 Conceitos 34

3.2 Processamento de Contexto 36

3.3 Qualidade de Contexto 38

3.4 Distribuição de Dados de Contexto 40

3.4.1 SDDL 41

3.5 Identificação de Situações 43

3.6 Lógica Nebulosa 46

3.7 Conclusão 48

4 Trabalhos Relacionados **50**

4.1 Extensões do Modelo de Controle de Acesso Baseado em Papéis 51

4.2 Modelos de Controle de Acesso para Reses Sociais Online 52

4.3 Extensões dos Recursos de Controle de Privacidade 53

4.4 Privacidade Dependente de Contexto em Ambientes Ubíquos 54

4.4.1 *Context-Dependent Access Control for Contextual Information* 55

4.4.2 *A Comprehensive Approach for Context-dependent Privacy Management* 56

4.4.3 CPE 57

4.4.4 CPPL 59

4.5 Privacidade Dinâmica em Redes Sociais Móveis Baseadas em Localização . 60

4.5.1 PICOS 60

4.5.2 PeopleFinder e Locaccino 61

4.5.3 SPISM 65

4.6 Ajustes Automáticos de Privacidade em Redes Sociais Online 68

4.6.1 *Privacy Wizards for Social Networking Sites* 69

4.6.2 *Identifying Hidden Social Circles for Advanced Privacy Configuration* 70

4.6.3 *Privacy-driven Access Control in Social Networks by Means of Automatic Semantic Annotation* 71
4.7 Análise Comparativa dos Trabalhos Relacionados 72
4.8 Conclusão 76

5 Solução Proposta **77**
5.1 Elicitação de Requisitos: Estudo com Usuários 77
5.1.1 Objetivo, Metodologia e Características dos Participantes 77
5.1.2 Questões Pertinentes e Resultados 79
5.1.3 Conclusões e Limitações 82
5.2 Exemplos de Cenários 84
5.3 Visão Geral da Solução Proposta 86
5.3.1 Questões Relacionadas à Adoção do Paradigma de Computação Situacional 87
5.4 O Modelo de Identificação de Situação 88
5.4.1 O Uso da Lógica Nebulosa 89
5.4.2 O Modelo Conceitual 91
5.4.3 O Processo de Inferência Nebulosa Adaptado para Identificar Situações . 92
5.4.4 Limitações e Questões de Flexibilidade 96
5.5 Perfil de Privacidade Situacional 97
5.6 Gerenciamento Autônomo de Privacidade 99
5.7 Modelo Arquitetural e Aspectos de Implementação 100
5.7.1 O Gerenciamento da Informação de Co-localização 103
5.7.2 Economia de Recursos do Dispositivo Móvel 105
5.7.3 Definindo um Perfil de Privacidade Situacional 105
5.8 O Modelo de Identificação de Situação no Domínio de Saúde Mental 109
5.9 Análise Comparativa dos Trabalhos Relacionados com a Solução Proposta . 112
5.10 Limitações da Solução Proposta 116

5.11 Conclusão 117

6 Avaliações Experimentais **118**

6.1 Acurácia do Motor de Inferência de Situação Usada no *SelPri* 118

6.1.1 Metodologia e Participantes 119

6.1.2 Resultados 120

6.2 Experiência de Uso com o *SelPri* 122

6.2.1 Metodologia e Participantes 122

6.2.2 Resultados 124

6.3 Acurácia do Motor de Inferência de Situação Usado no *SituMan* 128

6.3.1 Metodologia e Participantes 129

6.3.2 Resultados 129

6.4 Experiência de Uso com o *SituMan* 130

6.4.1 Metodologia e Participantes 130

6.4.2 Resultados 131

6.5 Conclusão 133

7 Conclusões **135**

7.1 Contribuições 137

7.2 Trabalhos Futuros 138

7.3 Publicações 139

7.3.1 Publicações Relacionadas Diretamente com esta Pesquisa 139

7.3.2 Publicações Relacionadas Indiretamente com esta Pesquisa 141

Referências Bibliográficas **143**

A Questionário da Elicitação de Requisitos **160**

B Questionário da Avaliação de Acurácia do *SelPri* **166**

C Questionário da Experiência de Uso do *SelPri* **167**

D Questionário da Experiência de Uso do *SituMan* **169**

1 Introdução

1.1 Contexto Geral

O desenvolvimento e a popularização das tecnologias da informação e comunicação, em particular da Internet, tem causado um grande impacto na sociedade. Algumas das mais importantes mudanças estão relacionadas com a maneira como as pessoas estabelecem suas relações sociais e interagem umas com as outras. Diferentes formas de interação estão disponíveis para indivíduos e organizações, desde tecnologias mais difundidas como e-mail e mensagens instantâneas até soluções mais sofisticadas como conferências online ao vivo, ferramentas de trabalho colaborativo e Mídias Sociais. Através destas últimas, cada vez mais pessoas se comunicam e estabelecem novos relacionamentos sociais.

As Mídias Sociais são meios de comunicação usados para interações sociais entre seus usuários. As redes sociais[1] são o tipo de Mídia Social com maior popularidade. Conceitualmente, uma Rede Social é uma estrutura de entidades conectadas umas com as outras através de um ou mais tipos específicos de interdependências, tais como amizade, parentesco, interesse em comum, troca financeira, empatia, ou relações de crenças, conhecimento ou prestígio [142]. Estas entidades podem ser indivíduos, organizações ou sistemas que estão relacionados em grupos e cuja interação é possibilitada através de tecnologias da informação e comunicação.

As redes sociais tem recentemente despertado grande interesse tanto na academia quanto no mundo comercial. Diversos grupos de pesquisa focam seus esforços nesta área, resolvendo problemas em recursos providos pelas redes sociais ou criando novos recursos (por exemplo, serviços para socialização dos usuários ou mecanismos para garantir privacidade), como também extraindo conhecimento a ser utilizado em outras áreas, tais como ciências sociais, ciências da informação,

[1]O termo Redes Sociais é usado durante o texto para referir às redes sociais online, em que o acesso não é feito exclusivamente através de aplicações móveis.

psicologia, comunicação e economia, dentre outros. Organizações e empresas buscam utilizar recursos das redes sociais para se promover através de *marketing*, divulgação de seus produtos e também como meio de comunicação direta com seus clientes para relacionamento, atendimento e suporte.

Por outro lado, nos últimos anos é possível verificar um rápido crescimento na área da Computação Móvel [114], a qual tem se tornado cada vez mais parte da sociedade. Dispositivos móveis fornecem conectividade e podem permitir acesso, processamento e compartilhamento de informação a qualquer tempo e em qualquer lugar, provendo ubiquidade de acesso às infraestruturas de redes móveis. Eles também estão tendo uma melhor relação custo-benefício e provendo mais recursos como, por exemplo, maior poder de armazenamento e processamento, múltiplas interfaces de rede, *Global Positioning System* (GPS), e integrando uma variedade de sensores, como acelerômetro, magnetômetro e sensores de proximidade. Dessa forma, dispositivos móveis vêm permitindo a execução de aplicações cada vez mais sofisticadas e com capacidade de identificar[2] alguns aspectos do contexto do usuário ou até sua atividade/situação em um dado momento.

Anind K. Dey [41] define contexto como sendo qualquer informação que pode ser usada para caracterizar a situação de uma entidade. Uma entidade pode ser uma pessoa, lugar ou objeto que seja considerado relevante na interação do usuário com a aplicação. Os sistemas sensíveis ao contexto são habilitados para adaptar suas funcionalidades e comportamento de acordo com o contexto atual do usuário sem sua explícita intervenção. Considerando a situação de usuários, Anagnostopoulos et al. [4] afirmam que situação se refere a uma atividade do usuário (ou atividades concorrentes) realizada em uma localização específica por um certo período de tempo.

Como consequência da popularidade de redes sociais e do uso cada vez mais abrangente de dispositivos móveis, surgem as Redes Sociais Móveis (RSMs) [71, 77, 132, 140], também chamadas de Redes Sociais Pervasivas. Nelas os usuários utilizam dispositivos móveis com tecnologias de comunicação sem fio para acessar conteúdos das redes sociais, e informações de contexto são divulgadas (compartilhadas) explicitamente ou agregadas a conteúdos postados. Assim, usuários móveis podem acessar (ler), postar (publicar, escrever ou inserir), compartilhar

[2]Os vermos "identificar", "inferir" e "determinar" a situação – ou informação de contexto de alto nível – do usuário são usados durante o texto como sinônimos.

(retransmitir ou divulgar) ou deixar disponíveis (permitir requisições de acesso originadas por contatos) conteúdos criados por si mesmos, ou obtido através de sensores no dispositivo móvel. Essa forma de acesso e o compartilhamento de informações de contexto possibilita novas formas de interações para os usuários explorarem suas relações sociais.

Para exemplificar as aplicações de RSMs (também chamadas de aplicações sociais móveis) e sua popularidade, o Facebook possui aproximadamente 1,79 bilhões de usuários ativos mensais (em setembro de 2016)[3] e, dentre eles, 1,66 bilhões acessam através de dispositivos móveis. Tem-se também o Google+, Twitter, LinkedIn, YouTube, Instagram, Foursquare, Waze, Sina Weibo, dentre muitas outras, com milhões de usuários. Além desses, há alguns projetos desenvolvidos no sentido de diminuir a distância que existe entre o mundo físico e as Redes Sociais (mundos real e virtual), tais como o Google Glass[4] e o projeto *Touch Me Wear* [14]. Ambos projetos exploram a integração de serviços/tecnologias vestíveis a RSMs. O *Google Glass* é um dispositivo móvel utilizado pelo usuário, um óculos de apenas uma lente, em que por meio dele é possível, por exemplo, tirar fotos ou filmar algo que o usuário esteja vendo no momento e postar através do Google+ ou Facebook. No Projeto *Touch Me Wear* as informações de contexto são coletadas através de camisas com sensores embutidos e quando dois usuários tocam-se fisicamente, abraçam-se ou estão próximos, essa informação é postada no Facebook.

Aplicações sociais móveis podem auxiliar pessoas a manterem contato entre si em qualquer lugar, a qualquer momento, e também prover recomendações em tempo real sobre pessoas, lugares e eventos, ou até mesmo entregar conteúdo personalizado em função do contexto geo-social (localização, co-localização ou lugar de preferência do usuário). Um conteúdo personalizado pode ser, por exemplo, uma propaganda de uma loja próxima ao local em que o usuário se encontra em determinado momento e que não seria veiculada se o usuário estivesse em um local mais distante. Com isso, aplicações sociais móveis fornecem aos seus usuários acesso a serviços de rede social de forma ubíqua através de dispositivos móveis.

Neste cenário, aplicações sociais móveis são caracterizadas por adicionar informações de contexto às redes sociais, uma vez que dispositivos móveis sensoreiam

[3] `http://newsroom.fb.com/company-info/`

[4] `https://plus.google.com/+GoogleGlass`

dados físicos do ambiente e, assim, é possível combinar dados de contexto e inferir a situação dos usuários. Então, uma vez que dispositivos móveis proveem ubiquidade de acesso, RSMs possibilitam interações sociais entre entidades de forma a melhorar relações existentes ou criar novas a partir de interesses em comum, tais como lugares visitados e frequentados, esportes praticados, gostos musicais, conteúdos postados, ou até mesmo a situação de saúde em que os usuários se encontram (RSMs aplicadas à saúde) [133, 134].

1.2 Caracterização do Problema

Em 1975 Irwin Altman, um famoso psicólogo especialista em privacidade, analisou como as pessoas regulam sua privacidade, fazendo uma relação entre o indivíduo estando sozinho versus participando de interações sociais [2]. Como psicólogo, Altman observou mecanismos comportamentais que influenciavam na regulação de privacidade: interações verbais com outros indivíduos e interações espaciais. Estes mecanismos são as ferramentas pelas quais um indivíduo regula sua privacidade, por ouvir outros (entradas), falar para outros (saídas), posicionar-se em relação a outros (espaço pessoal) e a escolha da localização (territorial). Através dessa análise, Altman concluiu que ao invés de privacidade ser simplesmente um estado de solidão, ela é um processo dinâmico de negociação de limites que tem como entrada interações sociais.

Enquanto abordagens anteriores à de Altman entendem privacidade como um estado de retiro ou afastamento social, ele a vê como um processo dinâmico e dialético de regulação de limites. Para Altman, o nível ótimo de privacidade é alcançado quando o nível atingido é o desejado pelo indivíduo, ou seja, o nível de contato com outros. Isso implica que ter mais privacidade que o desejado pode levar o indivíduo a um sentimento de solidão e ter menos que o desejado pode levar ao incômodo e a um sentimento de estar sendo sobrecarregado. Para Altman, regulação de privacidade é então a *openness* e *closedness*[5] para outros em resposta a um desejo e ao ambiente.

[5]Controle da "abertura" ou "fechamento", imposição de limites, para acesso a algo que é considerado privado pelo indivíduo, por exemplo, informações pessoais.

Embora Altman tenha desenvolvido sua teoria para interações do mundo real, existe muito que pode ser aprendido a partir dela, no contexto de privacidade no mundo computacional. Palen e Dourish [109] associam esse conceito à presença da tecnologia da informação, estendendo a definição de privacidade de Altman. Para os autores, como um processo dialético, regulação de privacidade é condicionada pelas próprias expectativas e experiências do indivíduo, e por aquelas de outros com quem ele interage. Como um processo dinâmico, privacidade é entendida como sendo um gerenciamento e negociação contínua, com os limites que distinguem privacidade e publicidade refinados de acordo com a circunstância. Para Palen e Dourish, o gerenciamento de privacidade é o processo de dar e receber entre duas ou mais entidades técnicas ou sociais, desde indivíduos até grupos e instituições, na tensão sempre presente e natural com a necessidade simultânea de publicidade.

Com base no conceito de Altman, Marc Langheinrich [86] destaca que humanos não usam políticas e regras únicas para gerenciar sua privacidade interpessoal e diária, a invés disso, eles continuamente ajustam sua acessibilidade em relação a *openness* e *closedness* com uma variedade de mecanismos, a fim de alcançar o estado de privacidade desejado. Dourish e Anderson [46] defendem que privacidade não é simplesmente uma forma através da qual a informação é gerenciada, mas como os relacionamentos sociais são gerenciados. Dessa forma, para Marc Langheinrich [86], sistemas ubíquos que facilitam a comunicação e consciência (*awareness*) entre pares devem então prover ferramentas capazes de permitir o ajuste dinâmico de suas entradas e saídas, seus níveis de *openness* e *closedness* e seus espaços pessoal e territorial, para que eles possam alcançar o nível de privacidade desejado em relação a outros usuários. Então, para ele, mecanismos de regulação de privacidade precisam suportar controles implícitos e explícitos que permitem ajustes de acordo com a situação (*in situ adjustments*), ao invés de um simples painel de configuração que permite um conjunto de níveis de privacidade desejado para mais ou para menos.

Um aspecto levado em consideração no projeto, implementação e uso de redes sociais são as questões de privacidade. Preservar a privacidade dos usuários em redes sociais significa dar meios para eles decidirem o que pode e o que não pode ser feito com seus conteúdos. No projeto de redes sociais há um potencial conflito entre o oferecimento de recursos aos usuários para socialização e mecanismos de privacidade para conter o vazamento de dados pessoais dos usuários [158]. Dessa

forma, quanto maior a sociabilidade oferecida pela rede social, mais chances há de ocorrerem problemas com a privacidade de seus usuários. Isso ocorre devido à existência de uma demanda em se prover recursos para sociabilidade, tais como recomendação de amigos, lugares e páginas, acesso à lista de contatos de outros usuários, acesso a conteúdos públicos, entre outros. No entanto, quando esses recursos são fornecidos na rede social sem permitir o controle pelos usuários, mais problemas de privacidade surgem, os quais podem ser usados por entidades para obter acesso indevido às informações pessoais, o que é chamado de vazamento de privacidade. Dessa forma, o vazamento de privacidade ocorre quando os usuários não conseguem controlar quem pode acessar suas informações pessoais postadas nas RSMs.

Como descrito anteriormente, os requisitos de privacidade dos usuários são dinâmicos, então especificamente em RSMs as configurações de privacidade devem dar suporte a mudanças automáticas de controles de acesso a fim de atender às expectativas e desejos do usuário específicos de sua situação. Os requisitos de privacidade do usuário são inerentes ao ambiente no qual ele está localizado e suas ações para publicar ou tornar disponível conteúdo devem ser feitas por políticas adaptáveis a seu contexto [102]. Isso ocorre devido a conteúdos publicados ou disponíveis pelo usuário poderem estar relacionados com a atividade que ele está realizando no momento da publicação ou quando eles foram requisitados, como consequência da ubiquidade de acesso (em qualquer lugar e em qualquer momento) fornecida pela utilização de dispositivos móveis.

Devido ao fato dos requisitos de privacidade dos usuários serem normalmente dinâmicos e dependentes de contexto, alguns problemas surgem nas RSMs. Primeiramente, o usuário pode não ter um claro entendimento de quais situações/contextos são mais sensíveis para descobrir suas informações pessoais: algumas situações podem ser mais comprometedoras, então revelando aspectos particulares sobre a vida pessoal do usuário. Além disso, o usuário pode não estar desejando ou habilitado para manualmente definir as configurações de privacidade para cada situação/contexto antes de cada postagem, ou simplesmente não atentar para reconfigurar a privacidade em cada nova postagem. Portanto, é importante reduzir o esforço cognitivo para analisar sua situação atual e o tipo de conteúdo postado, e para escolher a configuração de privacidade apropriada. Por fim, existe uma inconsistência entre as atitudes de privacidade (ou seja, o que os usuários

desejam em relação a sua privacidade) e os comportamentos de privacidade (ou seja, como os usuários efetivamente se comportam em relação a sua privacidade), chamado de "Paradoxo de Privacidade" [80], onde eles revelam informações pessoais frequentemente apenas para chamar a atenção de seus contatos nas RSMs.

Vários trabalhos na literatura vêm mostrando que as políticas de privacidade gerais frequentemente aplicadas a redes sociais não são suficientes para RSMs [83, 88, 107] e que grande parte dos usuários tipicamente não estão satisfeitos com a maneira disponibilizada pelos provedores de serviços de redes sociais para configurar suas preferências de privacidade [92]. Essa insuficiência das políticas e insatisfação dos usuários ocorrem porque as ferramentas para gerenciar privacidade oferecidas por provedores de RSMs e aplicações sociais móveis como meio para atender os desejos de privacidade dos usuários em muitos casos esta restrito apenas a recursos em que o usuário escolhe manualmente e estaticamente configurações informando em quem ele confia ou não. Dessa forma, os mecanismos de gerenciamento de privacidade impõem ao usuário um alto custo de reconfiguração a cada nova situação, o que não é prático e, em muitos casos, inviabiliza atingir o nível de privacidade desejado pelo usuário.

Essa tese investiga os requisitos de privacidade dinâmicos e dependentes de contexto dos usuários em RSMs e como atendê-los. As questões de pesquisa fundamentais que norteiam a investigação são: (i) Os desejos de privacidade dos usuários em RSMs são dinâmicos?; (ii) Os desejos de privacidade dos usuários em RSMs são contextuais?; (iii) Quais fatores influenciam isso? E o problema principal abordado por esta tese de doutorado é: *os mecanismos de controle de privacidade adotados atualmente pelas RSMs são insuficientes para atender aos requisitos de privacidade dinâmicos e contextuais de seus usuários*.

1.3 Hipótese de Pesquisa

Diversos trabalhos na literatura (particularmente aqueles mostrados na seção anterior e os que serão discutidos na seção 4) apontam para a necessidade de se prover políticas de privacidade que permitam ao usuário expressar configurações de controle de acesso que sejam ajustadas dinamicamente. Esse é um processo que

na literatura também é chamado de gerenciamento de privacidade adaptativo [150], em que o sistema continuamente ajusta o comportamento das configurações de privacidade para descoberta de informações pessoais de acordo com os desejos de mudança do usuário em diferentes circunstâncias. Dessa forma, os controles de acesso não requerem intervenção constante do usuário para serem ajustados com o passar do tempo. Além dos diversos trabalhos encontrados na literatura, foi realizado um estudo com usuários ativos de RSMs para elicitação de requisitos ao longo do desenvolvimento desta pesquisa (descrito na seção 5.1), em que os resultados expressam a necessidade de se fornecer recursos para configurações de privacidade se tornarem dinâmicas e dependentes do contexto ou, mais especificamente, da situação atual do usuário.

Nesta tese de doutorado é proposta a utilização da situação atual do usuário para a escolha da configuração de privacidade mais adequada para uma postagem em RSMs. Entretanto, para esse trabalho a consciência de situação não é restrita apenas a dados de contexto isolados, mas sim a uma combinação de vários contextos pertinentes ao objetivo do sistema computacional, o que conduz a uma representação da situação do usuário que é de interesse do sistema. O objetivo do paradigma da computação situacional é fazer com que a interação entre o usuário e o dispositivo móvel seja feita de forma mais fácil e sem intervenção. Dessa forma, quando o sistema móvel reconhecer a situação do usuário, ele pode adaptar suas funções de acordo com ela. No caso da solução proposta nesta tese, a determinação da configuração de privacidade do conteúdo que está sendo postado. Portanto, a intervenção humana deve ser a menor possível, uma vez que sistemas que utilizam-se do paradigma de computação situacional são projetados para atender a esse objetivo.

Motivado por diversos trabalhos encontrados na literatura e pelo estudo realizado neste trabalho de tese para elicitação de requisitos, tem-se a seguinte hipótese de pesquisa para abordar o problema: *o paradigma de computação situacional possibilita o desenvolvimento de mecanismos mais eficazes para o atendimento dos requisitos dinâmicos e dependentes de contexto de privacidade dos usuários em aplicações sociais móveis*.

1.4 Relevância do Trabalho

A privacidade é um direito do ser humano. A Declaração Universal dos Direitos Humanos[6] em seu artigo XII e o Pacto Internacional sobre os Direitos Civis e Políticos[7] em seu artigo 17 diz: "Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques". Em 20 de novembro de 2013 a III Comissão da 68ª Assembleia Geral da Organização das Nações Unidas aprovou o projeto de resolução[8], o qual consta o seguinte texto:

> [...]
>
> 2. Reconhece a natureza global e aberta da Internet e do rápido avanço nas tecnologias de informação e comunicação como uma força motriz para acelerar o progresso rumo ao desenvolvimento em suas várias formas;
>
> 3. Afirma que os mesmos direitos que as pessoas possuem fora da Internet (offline) também devem ser protegidos na Internet (online), incluindo o direito à privacidade;
>
> 4. Convoca todos os Estados: (a) A respeitar e proteger o direito à privacidade, inclusive no contexto da comunicação digital;
>
> [...]

A Constituição da República Federativa do Brasil[9] diz em seu artigo 5º: "Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação [...]".

[6] http://www.dudh.org.br/

[7] http://www.gddc.pt/direitos-humanos/textos-internacionais-dh/tidhuniversais/cidh-dudh-direitos-civis.html

[8] http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1

[9] http://www.senado.gov.br/legislacao/const/con1988/con1988_05.10.1988/art_5_.shtm

Considerando a extrema atenção dada por essas diversas entidades e leis à privacidade das pessoas, então possibilitar que elas tenham privacidade em sistemas computacionais que fornecem recursos para sociabilidade, tais como as RSMs, é extremamente importante para garantir um direito que é intrínseco ao ser humano. Além disso, nos dias atuais as RSMs fazem parte da vida das pessoas. Dessa forma, as pessoas usuárias de RSMs usualmente geram uma grande quantidade de conteúdos, os quais normalmente estão relacionados com a sua vida pessoal, sejam eles informações pessoais ou de contexto. Por essa razão, os usuários de RSMs estão se tornando cada vez mais preocupados sobre os perigos de comprometer suas informações pessoais e, como consequência, uma grande quantidade de trabalhos na literatura [83, 88, 107, 132] vêm: (i) investigando as atitudes e comportamento dos usuários em relação a privacidade, (ii) identificando os problemas recorrentes nesse meio de comunicação, e (iii) propondo soluções para resolvê-los. Portanto, a provisão de privacidade em aplicações sociais móveis é uma tarefa desafiadora [107, 115, 132].

1.5 Objetivos

O objetivo geral dessa tese é investigar os requisitos dinâmicos e contextuais de privacidade de usuários em aplicações sociais móveis e contribuir com uma solução que atenda esses requisitos, explorando o paradigma de computação situacional para ajuste automático das permissões de acesso a conteúdos postados baseado na situação atual do usuário. Para tanto, consideram-se os seguintes objetivos específicos:

- Desenvolver um modelo conceitual para a identificação da situação atual do usuário a partir de informações de contexto obtidas a partir do dispositivo móvel;
- Implementar um motor de inferência baseado no modelo conceitual e aplicá-lo ao gerenciamento autônomo de privacidade em RSMs;
- Integrar a solução a uma rede social com grande popularidade, visando propiciar sua utilização por usuários em situações reais;
- Avaliar a usabilidade da solução proposta a fim de verificar o impacto de seu uso por usuários de RSMs e verificar se ele atende os requisitos dinâmicos e contextuais de privacidade dos usuários;

- Avaliar a acurácia do motor de inferência para identificar as situações dos usuários;

- Mostrar e avaliar a flexibilidade do modelo conceitual de forma a construir um motor de inferência para ser utilizado em outro domínio de aplicação.

1.6 Metodologia de Pesquisa

Essa tese de doutorado foi inicialmente contextualizada no projeto MobileHealthNet [133, 134], desenvolvido em parceria pelo LSDi da UFMA e o *Laboratory for Advanced Collaboration* da PUC-Rio. Em seguida, outros dois projetos de pesquisa fomentados pela Fundação de Amparo à Pesquisa e ao Desenvolvimento Científico e Tecnológico do Maranhão (FAPEMA) deram sequência a essa pesquisa, são eles: "Um Modelo de Segurança e Privacidade para Redes Sociais Móveis" (solicitação APP-UNIVERSAL-00542/13) e "Desenvolvimento de um Mecanismo para Identificação da Situação de Usuários Móveis" (solicitação UNIVERSAL-00538/15). Este segundo atualmente encontra-se em desenvolvimento, com seu cronograma de atividades encerrando-se em agosto de 2017. Todos os três projetos tiveram a participação de pesquisadores da UFMA, IFMA e PUC-Rio. Além disso, essa pesquisa de doutorado teve colaboração de pesquisadores da FEUP e do INESC TEC, ambos em Portugal, onde o autor dessa tese realizou seu estágio de doutorado sanduíche.

A metodologia de pesquisa adotada nessa tese de doutorado é baseada em [143] e possui as seguintes etapas:

1. Identificação dos problemas em aberto e a escolha do que seria abordado.

   A partir de um levantamento bibliográfico detalhado e exaustivo sobre RSMs e, mais especificamente, sobre privacidade em RSMs, se conheceu o estado da arte da linha de pesquisa. Portanto, foi possível identificar vários problemas em aberto. Procurou-se escolher um problema que estivesse alinhado com as temáticas de pesquisa do LSDi. Um critério adotado para a escolha foi ter afinidade e interesse em resolver o problema, além de poder idealizar algumas possíveis maneiras de como ele poderia ser abordado.

Após a escolha do problema a ser abordado, continuou-se fazendo um levantamento bibliográfico, mas focando em identificar todos os trabalhos que mantinham alguma relação com a problemática em questão. Além disso, identificou-se os principais grupos que realizavam esforços na linha de pesquisa, a fim de identificar seus trabalhos e no que eles estavam trabalhando especificamente. Essa etapa foi importante para verificarmos quais as contribuições científicas poderiam ser realizadas.

2. Processo de elicitação de requisitos.

   Foi realizado um estudo com usuários para reforçar a existência do problema, além de entendê-lo melhor e identificar os fatores que influenciavam a sua existência. Para isso, um levantamento de requisitos foi realizado com 164 usuários brasileiros de RSMs, a fim de melhor entender como eles compartilhavam suas informações através de postagens em RSMs e quais informações de contexto influenciam seus desejos dinâmicos em relação a privacidade. Nesse momento procurou-se ganhar conhecimento em profundidade e experiência sobre os requisitos de privacidade dos usuários de RSMs. Os detalhes do processo de elicitação de requisitos são descritos nessa tese, no capítulo 5.

3. Elaboração da hipótese de pesquisa.

   Com base nessa elicitação de requisitos e também em um conjunto variado de evidências encontrado em outros trabalhos relacionados, elaborou-se a hipótese de pesquisa.

4. Concepção e desenvolvimento de uma solução para abordar o problema.

   Para provar a hipótese, deu-se início a concepção e desenvolvimento da proposta de solução para abordar o problema identificado. Nesse ponto procurou-se conceber uma solução inovadora e diferenciada em relação aos trabalhos encontrados na literatura, e que abordavam o mesmo problema. Utilizou-se como metodologia de desenvolvimento de software os princípios dos métodos ágeis, tais como: (i) ciclos de interação curtos (semanais e/ou quinzenais) com os orientadores e pesquisadores envolvidos na pesquisa; (ii) realização do desenvolvimento efetuada de uma maneira colaborativa, em que os pesquisadores envolvidos contribuíram com sugestões para resolver problemas

de implementação específicos; e (iii) uso de refatoração de código para atender os requisitos da solução, bem como adaptações necessárias durante o processo de desenvolvimento.

5. Avaliação da solução proposta.

   Na sequência, avaliou-se a solução proposta. A solução proposta para privacidade em RSMs foi avaliada sob vários aspectos através de experimentos realizados diretamente com usuários. Procurou-se avaliar a satisfação dos usuários ao utilizarem a solução (avaliação qualitativa), bem como a acurácia do motor de inferência usado para identificar as situações dos usuários (avaliação quantitativa).

   Adicionalmente, o modelo conceitual para identificar situações de usuários móveis foi usado como base para a construção de um novo motor de inferência, o qual foi aplicado a um domínio bem diferente do tema principal dessa tese de doutorado, o de saúde mental, para o tratamento de pacientes depressivos. Essa especialização do modelo conceitual foi feita para mostrar sua característica de flexibilidade. A especialização do modelo foi muito importante também para ampliar a avaliação e verificar sua aplicabilidade em um domínio totalmente diferente.

1.7 Organização do Trabalho

O restante deste documento de tese está organizado da seguinte forma:

- O **capítulo 2** exibe uma revisão da literatura sobre RSMs, o papel das informações de contexto em RSMs, arquiteturas de RSMs, e segurança e privacidade em redes sociais;
- No **capítulo 3** é exibida uma fundamentação teórica abordando o tema Computação Situacional, o qual é conhecimento necessário para o entendimento desse trabalho;
- No **capítulo 4** são descritos os trabalhos relacionados ao problema abordado nesta pesquisa de doutorado, realizando-se um comparativo entre eles;

- O **capítulo 5** apresenta um estudo com usuários de RSMs e a solução proposta. Além disso, são destacadas as contribuições técnicas e científicas da solução proposta em relação aos trabalhos relacionados;

- O **capítulo 6** apresenta avaliações experimentais com a solução proposta nesta tese no domínio de privacidade em RSMs e saúde mental;

- No **capítulo 7** são descritas as conclusões deste documento de tese de doutorado.

2 Redes Sociais Móveis

Este capítulo faz uma apresentação às RSMs, inicialmente descrevendo conceitos de redes sociais e posteriormente mostrando o papel das informações de contexto em RSMs e também as arquiteturas de RSMs. Em seguida, as questões de segurança e privacidade em RSMs são detalhadas.

2.1 Conceitos

As redes sociais podem ser definidas como um conjunto de serviços baseados na *Web* que permitem a indivíduos: (1) construir um perfil público ou semi-público dentro do sistema; (2) manter uma lista de contatos[1] e se comunicar com os membros dessa lista e estabelecer elos para futuras interações; (3) consultar sua lista de contatos e de outros amigos e conhecidos dentro do sistema [26]. A semântica, a natureza e o tipo de relacionamento criado com esses elos pode variar entre sistemas, mas são genericamente representadas por um grafo, juntamente com os perfis dos usuários, chamado de Grafo Social. No grafo social, os vértices expressam os perfis dos usuários e as arestas os relacionamentos entre eles.

Como exemplo de um grafo social descrito em [135], quando um usuário (João) possui um elo com outro (Maria), existe uma aresta unindo o vértice A (João) ao vértice B (Maria), como ilustrado na Figura 2.1. Neste caso, o elo entre os usuários é mútuo, como ocorre, por exemplo, no Facebook. Porém, dependendo da rede social, essa aresta pode possuir uma orientação (direção), como é visto no grafo social B na mesma figura. Este é o caso de redes sociais como Twitter e Instagram, onde é utilizado o recurso "seguir". Como visto na aresta B, João segue Maria para ter acesso a conteúdos publicados por ela. No entanto, observa-se que Maria não segue João e, caso o perfil dele seja privado, ela não tem acesso a conteúdos publicados por ele. A aresta C também possui orientação, mas neste caso os dois usuários (Pedro e Ricardo) seguem um ao outro.

[1] Os termos elo e contato são utilizados como sinônimos durante o texto.

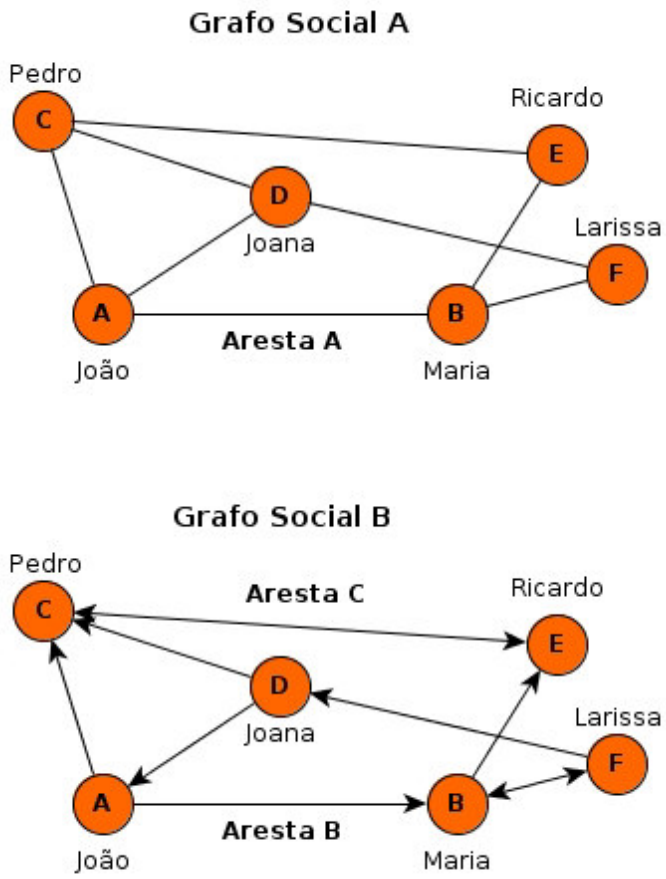

Figura 2.1: Grafo Social.

Os usuários de redes sociais tipicamente geram uma grande quantidade de conteúdos, tais como mensagens, fotos, áudio e vídeos. A representação de redes sociais através de um grafo facilita o entendimento da maneira pela qual esses conteúdos são disseminados na rede, percorrendo arestas e passando por vértices, sendo visualizados por outros usuários. Além disso, esse entendimento é necessário para conhecer os riscos de vazamento de privacidade, os quais serão detalhados ainda neste capítulo na seção 2.4.

A exibição pública dos contatos é um componente intrínseco das redes sociais. A lista de contatos contém *links* para o perfil de cada usuário, permitindo navegar pelas listas de contatos, e assim percorrer o grafo social. Na maioria das redes sociais, a lista de contatos permanece visível para quem está autorizado a visualizar o perfil do usuário, embora haja exceções. Por exemplo, no LinkedIn é possível aos usuários optar por não exibir seus contatos conhecidos.

A maioria das redes sociais também inclui mecanismos para deixar mensagens nos perfis de contatos, os chamados "comentários". Porém, cada rede social usa um nome diferente para este recurso. Além disso, redes sociais muitas vezes possuem o recurso de mensagens privadas. Embora seja comum a disponibilização de ambas as formas de comunicação (pública e privada), elas não estão presentes em todas as redes sociais.

Atualmente, muitas redes sociais podem ser consideradas RSMs [71, 140], em que os dispositivos móveis são o principal meio de acesso a rede e vários tipos de informações sobre o contexto do usuário têm ganho quase a mesma importância que o conteúdo gerado por ele. Nas RSMs, usuários móveis estão habilitados para compartilhar não somente conteúdo explicitamente gerado por eles, mas também dados e informações que são automaticamente obtidos ou inferidos a partir de sensores embarcados nos dispositivos móveis. As informações de contexto e os conteúdos dos usuários são então combinadas e usadas para a descoberta de novos contatos, como também para manter seus relacionamentos sociais existentes.

As RSMs podem ser vistas como uma combinação de três áreas do conhecimento: redes sociais, computação móvel e ciência de contexto [132], uma extensão do conceito formalizado em [77]. Esta visão de RSMs é ilustrada na Figura 2.2.

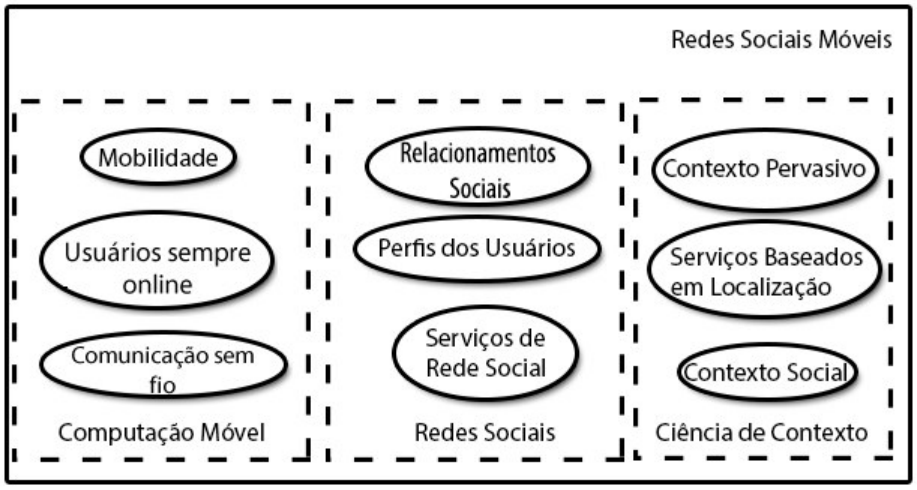

Figura 2.2: Definição de RSMs [132].

As redes sociais provêm funcionalidades para criar perfis que representam entidades, as quais relacionam-se socialmente trocando informações. Como visto anteriormente na seção 1.1, estas entidades podem ser indivíduos, organizações ou

mesmo sistemas. A computação móvel possibilita os usuários estarem sempre online, devido ao suporte de mobilidade provido pelos dispositivos portáteis e a ubiquidade da conectividade sem fio. A ciência de contexto adapta as funcionalidades das redes sociais e suas aplicações, oferecendo recursos de acordo com informações de contexto, o que será visto em detalhes a seguir.

2.2 Informações de Contexto em RSMs

Mark Weiser definiu o termo "Computação Ubíqua" (*Ubiquitous Computing*) em [144]. Para ele, as tecnologias mais profundas e duradouras são aquelas que desaparecem, elas dissipam-se nas coisas do dia a dia até tornarem-se indistinguíveis. Nesse cenário, o foco dos usuários seria a tarefa e não a ferramenta utilizada, e ele nem sequer perceberia ou necessitaria de conhecimentos técnicos relativos aos recursos computacionais utilizados. Então, para que esse nível de invisibilidade seja atingido, é fundamental que as aplicações sejam capazes de obter informações do ambiente no qual o usuário se encontra e prover a ele serviços e informações úteis.

O avanço contínuo no desenvolvimento do hardware de dispositivos móveis tem permitido a disponibilização de diversos recursos como, por exemplo, receptores GPS e a integração de uma rica variedade de sensores, como sensor de proximidade, magnetômetro e acelerômetro. Dessa forma, os dispositivos móveis vem permitindo a execução de aplicações cada vez mais sofisticadas e com capacidade de identificar alguns aspectos do contexto do usuário, informações do ambiente no qual o usuário se encontra ou até sua atividade/situação em um dado momento.

Bolchini et al. [25] descrevem as informações de contexto como sendo um conjunto de variáveis que podem ser de interesse para uma entidade e podem influenciar em suas ações. Por meio deste tipo de informação é possível o desenvolvimento de sistemas computacionais que podem se reconfigurar ou adaptar a uma determinada situação ou recomendar ações a partir de análises de informações coletadas do ambiente.

A utilização de informações de contexto permite que desenvolvedores de sistemas possam enriquecer a usabilidade de sua aplicação e, assim, o sistema sensível ao contexto pode reagir a determinadas situações sem a necessidade da interação com

o usuário. Por exemplo, caso o sistema detecte que o nível de bateria está abaixo de um limiar, ele pode realizar ações para economizá-la, seja reduzindo a luminosidade do visor do dispositivo ou desativando as interfaces de rede ou sensores que não estão em uso no momento.

Para Chen e Kotz [30] as informações de contexto podem ser classificadas em quatro tipos:

- **Contexto Físico**: informações sobre o mundo real, obtidas por meio de sensores. Por exemplo, sensor de luminosidade, sensor de ruído, temperatura, luminosidade e localização;
- **Contexto Computacional**: informações sobre um sistema computacional, como os seus recursos e características. Por exemplo, nível de bateria, consumo de memória ou processamento e conexões de rede disponíveis;
- **Contexto do Usuário**: informações que caracterizam o usuário, tais como: estado emocional, localização e atividade atual;
- **Contexto de Tempo**: informações relacionadas ao tempo de uma atividade real ou virtual. Está relacionada a dimensão do tempo, como por exemplo, hora do dia, dia da semana, mês, ano ou uma estação climática no ano.

Uma outra classificação mais atual é proposta por Emmanouilidis et al. [47], a qual possui cinco tipos de informações de contexto. A Figura 2.3 ilustra essa classificação. Essa classificação mantém uma relação com a proposta pelo autor anterior (Chen e Kotz [30]): usuário (*User*) é igual ao contexto do usuário, sistema (*System*) equivale ao contexto computacional e, por fim, ambiente (*Environment*) equivale a junção de contexto físico com contexto de tempo. Além desses, outros dois tipos de contexto são propostos por essa classificação, são eles: Social e Serviço (*Service*).

O termo contexto social é utilizado para caracterizar as possíveis formas de relacionamento e de interações entre pessoas, intermediadas ou não por alguma tecnologia de comunicação. O termo está relacionado ao ambiente social do usuário (por exemplo, uma festa ou uma reunião) e a relação que pode ser estabelecida com outros usuários. A noção de contexto social deve levar em consideração tanto as

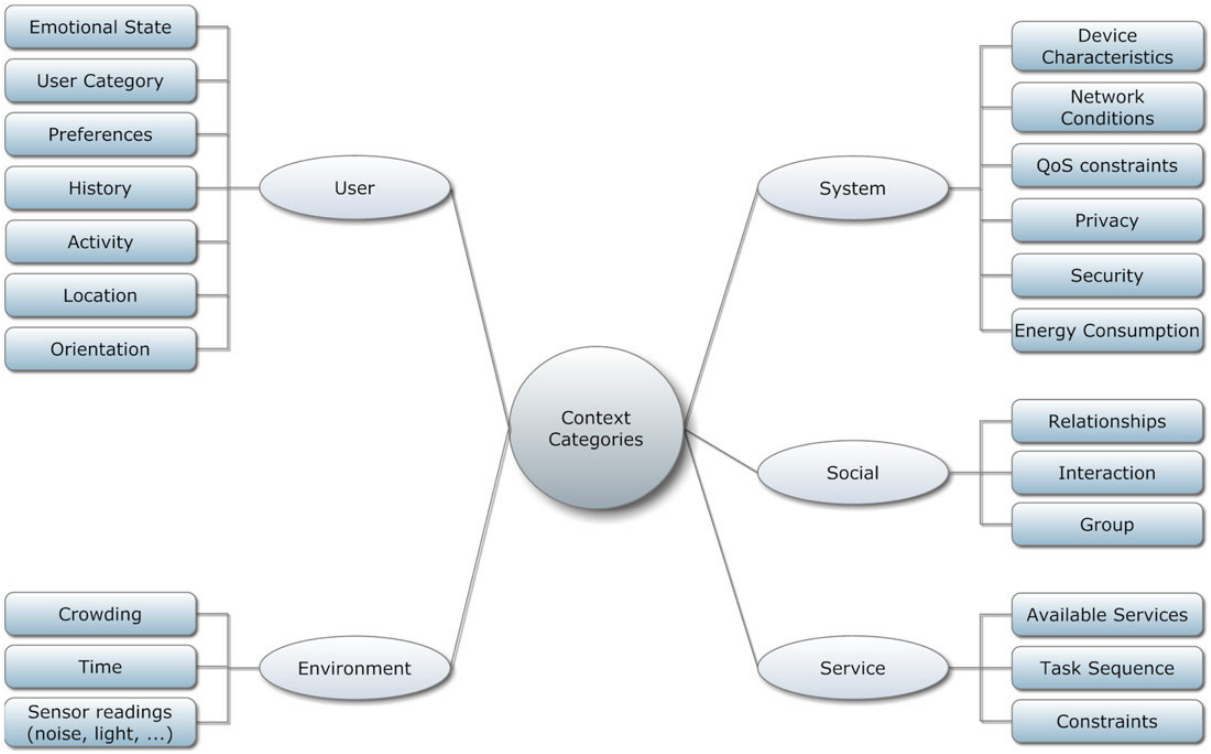

Figura 2.3: Classificação dos tipos de contexto segundo Emmanouilidis et al. [47].

experiências no mundo real quanto no virtual. Informações de contexto social podem ser extraídas por meio de redes sociais, sensores ou formulários. Essas informações são aspectos de contexto de alto nível relacionados com a dimensão social dos usuários, tais como o perfil do usuário, pessoas próximas, e sua atual situação social [1].

O contexto de serviço é qualquer informação usada para representar o estado de serviços disponíveis no ambiente em que o usuário se encontre e que queira utilizar. O estado de um serviço pode ser, por exemplo, o nível de congestionamento em uma determinada avenida (neste caso a avenida é o serviço) ou a quantidade de horas de espera para realizar uma compra em um supermercado (neste caso o supermercado é o serviço). O contexto de serviço pode ser utilizado também para guiar o usuário de maneira apropriada para a realização de uma sequência de tarefas de acordo com o estado dos serviços que ele deseja utilizar. Este contexto ainda leva em consideração restrições dos serviços (por exemplo, o horário de atendimento do serviço ou a interdependência entre serviços), as quais podem afetar a realização de uma dada tarefa.

Uma outra terminologia utilizada é o chamado contexto pervasivo, sendo aquele obtido a partir de sensores de hardware nos dispositivos móveis, os quais

podem ser de vários tipos, como por exemplo: luminosidade, visual (câmera), áudio, movimento ou acelerômetro, localização, toque, temperatura, físicos (bio-sensores), dentre outros [11].

Como visto, conceitos de redes sociais se unem à computação móvel e ciência de contexto e, a partir disso, Schuster et al. [126] desenvolveram o conceito de contexto social pervasivo. O contexto social pervasivo de um indivíduo é o conjunto de informações que surgem a partir de interações diretas e indiretas entre pessoas que carregam dispositivos móveis equipados com sensores e que estejam conectadas através de uma mesma rede social. Os autores ainda classificaram e diferenciaram várias formas em que o contexto social pervasivo pode ser utilizado baseados nas *W5H Questions*, como visto abaixo:

- Quem – ***W**ho*: expressa quem são os participantes envolvidos no consumo e produção das informações de contexto;
- O que – ***W**hat*: diz respeito a qual tipo de contexto é utilizado ou se é importante para a aplicação;
- Onde – ***W**here*: relaciona onde (localização física) os laços ou interações sociais são estabelecidos;
- Quando – ***W**hen*: caracteriza as interações entre usuários e as informações de contexto que eles produziram em uma perspectiva temporal;
- Porquê – ***W**hy*: expressa o porquê uma informação de contexto é usada, determinando a causa ou razão dela está sendo usada pela aplicação. Nesse caso, isso é bem relacionado ao objetivo da aplicação;
- Como – ***H**ow*: expressa como a informação de contexto (originada a partir do mundo real, mundo virtual ou de ambos) pode influenciar ou comprometer aplicações.

2.2.1 Inserção de Contexto em RSMs

A principal motivação para a inserção de contexto é formar RSMs nas quais a interação e a percepção mútua entre os usuários pode ser induzida ou aprimorada

através do compartilhamento de informações de contexto. Um usuário em uma festa, por exemplo, pode compartilhar a sua localização com seus contatos das redes sociais e, então, é possível que encontre algum conhecido que compartilhou a informação de também estar nessa mesma festa e, assim, eles podem se encontrar.

Dados gerados a partir de sensores pervasivos podem ser usados individualmente ou de forma combinada para inferir/identificar a situação do usuário. Essa situação pode ser, por exemplo, a (in)disponibilidade do usuário para realizar alguma atividade, seu estado de saúde ou o lugar em que se encontra (por exemplo, restaurante, residência ou local de trabalho). Portanto, informações de contexto pervasivo são bastante úteis para aplicações de RSMs.

A inferência da situação do usuário a partir de vários sensores pode prover uma variedade de informações a serem usadas por aplicações de RSMs para aumentar o nível de colaboração entre seus usuários. Por exemplo, informações do GPS podem revelar que o dispositivo, e o seu usuário, está em movimento e, a partir disso, a aplicação pode fornecer serviços de alerta para notificar amigos do usuário se ele está ocupado para receber notificações, conexões ou chamadas. Com isso, usuários de RSMs podem ficar mais cientes da situação de seus amigos na sua rede social, o que leva a uma maior integração entre os mundos real e virtual. O tema computação situacional será abordado em detalhes no capítulo 3.

Um exemplo dessa integração entre mundos real e virtual é o projeto *Touch Me Wear* [14], citado anteriormente na seção 1.1. Neste projeto, as informações de contexto são coletadas através de dispositivos vestíveis, onde o usuário utiliza uma camisa com sensores de toque e dispositivo *bluetooth* e, dessa forma são obtidos, respectivamente, os contatos físicos entre usuários (por exemplo, toque ou abraço) e informações de quem está na vizinhança (usuários próximos). A partir disso, quando dois usuários tocam-se fisicamente, abraçam-se ou estão próximos, essa informação é publicada em seus perfis, na rede social Facebook, com informações de quem o usuário tocou/abraçou ou esteve próximo e quando isso ocorreu. A rede de dispositivos vestíveis utilizada por esse projeto é chamada de *Body Sensor Network*, na qual sensores monitoram atividades fisiológicas e ações de humanos [31].

Nesse cenário surgem as Redes Geo-sociais, as quais proveem serviços cientes de contexto que agregam a localização de usuários a conteúdos [141]. Por

exemplo, a publicação de uma foto pode agregar informação sobre a localização na qual a foto foi tirada. Essa classe de RSMs combina as tecnologias de informação geográficas e serviços de redes sociais para ajudar pessoas a estabelecer relações sociais mais facilmente [72]. Essa facilidade surge devido ao interesse das pessoas em algo relacionado a uma localização específica, por exemplo, usuários que estudam na UFMA querem fazer amizades com outros que estudam nessa mesma universidade. Informações de localização são usadas por várias aplicações de RSMs, tais como o Foursquare e o Tinder.

A inserção de informações de contexto nas RSMs permite o estabelecimento dinâmico de elos e troca de conteúdos entre usuários. Este recurso é chamado de comunidades dinâmicas (ou grupos dinâmicos) [94]. Comunidades dinâmicas correspondem a grupos de usuários que são automaticamente criados baseados em: (i) interesses comuns derivados dos perfis de usuários, (ii) inferência de interesses comuns baseada no histórico de atividades do usuário, (iii) proximidade física de usuários ou localização. Como exemplo, estudantes do mesmo curso trocando informação sobre uma prova antes dela ser aplicada ou pessoas que estão assistindo a um mesmo espetáculo (por exemplo, a mania das pessoas de *Tweetar*[2] sobre um show ou um acontecimento usando *hashtags* que agrupam conteúdos) sendo presenciado conjuntamente. Neste caso, a rede social se torna mais dinâmica, uma vez que usuários podem entrar e sair das comunidades, pois eles podem se deslocar de uma lugar para outro ou mudar seus interesses.

2.3 Arquiteturas de RSMs

Na literatura, embora seja possível encontrar diversas arquiteturas para RSMs que permitem o estabelecimento de várias comunidades de usuários móveis e suas interações, sistemas de RSMs podem ser classificados em dois principais grupos: centralizado e distribuído, como ilustrados na Figura 2.4.

Em uma arquitetura centralizada, os dados estão centralizados em um ou mais servidores. Esses servidores são responsáveis pelo gerenciamento e entrega dos dados aos usuários móveis. Estes dados correspondem a informação dos perfis

[2] Ato de publicar uma mensagem, fazer um comentário ou postagem, na rede social Twitter.

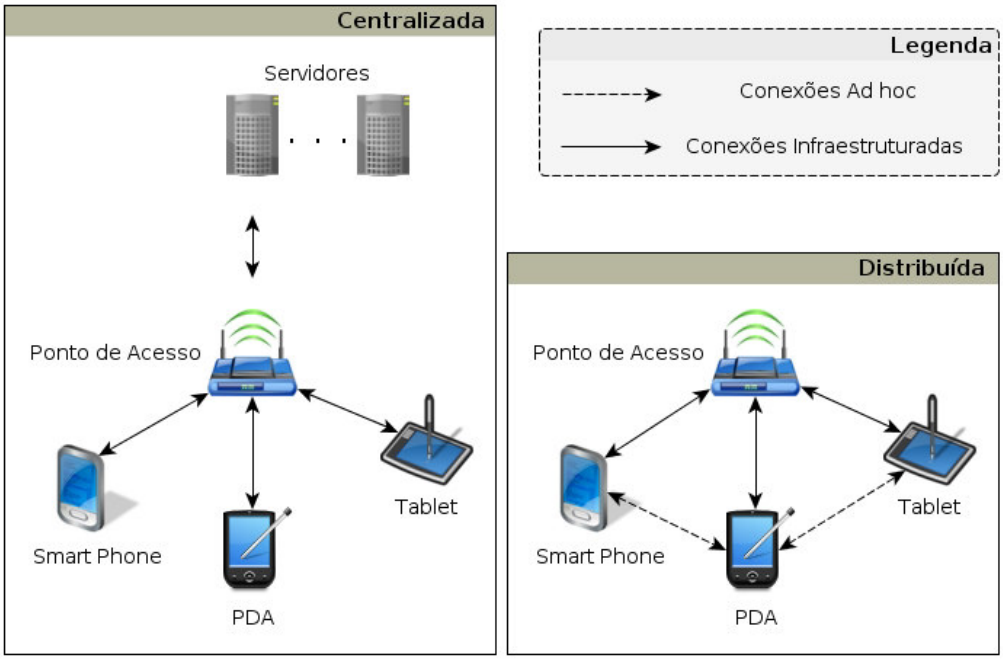

Figura 2.4: Arquiteturas de RSMs.

dos usuários, grupos, informações de contexto, murais, notificações, dentre outras. Usuários móveis são representados por aplicações móveis instaladas/armazenadas nos dispositivos móveis. Nessa arquitetura, toda comunicação é mediada pelos servidores. Dessa forma, os conteúdos são necessariamente acessados através dos servidores, e somente a partir deles, através de conexões estabelecidas pelas aplicações móveis.

Em uma arquitetura distribuída, os usuários móveis comunicam-se diretamente sem a necessidade do uso de servidores para mediar suas interações. Como visto na Figura 2.4, as conexões entre dispositivos de usuários podem ser estabelecidas através de uma infraestrutura de rede usando pontos de acesso ou também por meio de conexões *ad-hoc*. Nessa arquitetura, os usuários podem se comunicar e compartilhar conteúdo sem acesso à Internet, com o mínimo de infraestrutura de rede. Além disso, o conhecimento adquirido a partir das relações sociais entre usuários pode ser usado para criar melhores protocolos de roteamento e segurança. Por exemplo, a frequência na qual usuários encontram-se fisicamente pode ser levado em consideração como um critério influenciador para a escolha de uma rota, considerando-se que a probabilidade dos usuários se encontrarem fisicamente e poderem rotear um dado é maior [87].

Uma outra forma que componentes de uma RSMs podem ser organizados é através de uma arquitetura híbrida. Esta arquitetura combina as abordagens centralizadas e distribuídas por permitir que usuários móveis acessem e compartilhem dados através de servidores (centralizada), enquanto outros usuários (geralmente co-localizados ou próximos uns dos outros) estabeleçam conexões diretas uns com os outros sem a necessidade de um servidor (distribuída). Dessa forma, essa arquitetura pode aproveitar os benefícios oferecidos por ambas arquiteturas.

Essas arquiteturas implicam em diferentes formas de comunicação para obtenção de acesso a conteúdos da RSMs e entre os usuários, o que modifica a maneira deles interagirem, pois em alguns casos há necessidade por uma conexão com a Internet e, em outros, basta que os usuários estejam próximos fisicamente. Por exemplo, em uma arquitetura centralizada é apenas necessário que o usuário tenha uma conexão com a Internet para acessar qualquer conteúdo, diferentemente de uma arquitetura distribuída, onde em muitos casos os usuários necessitam estar próximos fisicamente de algum ponto de acesso, ou ainda estarem próximos de algum outro usuário que tenha conexão com a Internet. Neste último caso, um usuário teria conexão com a Internet e serviria de ponte para um segundo usuário obter acesso a conteúdos das RSMs.

A escolha da arquitetura para construção de RSMs tem grande impacto nos serviços que são disponíveis, pois a utilização de uma arquitetura pode não ser adequada para atender os requisitos de uma determinada aplicação. Além disso, a arquitetura é decisiva para a escolha dos algoritmos que serão adotados na construção do software.

2.4 Segurança e Privacidade em Redes Sociais

Todo o conteúdo gerado por usuários pode ser acessado ou compartilhado por muitas entidades, as quais podem representar as origens dos vazamentos de privacidade aos usuários de rede social. Para Gao et al. [60], estas entidades são consideradas brechas e podem ser: (i) outros usuários da rede social – os contatos, (ii) aplicações de terceiros, e (iii) o próprio provedor de serviços. Algumas questões importantes relacionadas a essas brechas são detalhadas a seguir. Além disso, algumas

questões de privacidade específicas a RSMs e ataques a redes sociais bem conhecidos na literatura são também apresentados.

Outros Usuários da Rede Social

Os outros usuários da rede social, os contatos, representam uma ameaça devido, sobretudo, à facilidade que usuários mal intencionados têm para ingressarem na rede social, ou seja, criarem uma conta através do provedor de serviços e tonarem-se membros autênticos. Quando isso ocorre, eles podem realizar tentativas de invasão de privacidade a fim de obter informações pessoais de outros usuários. A proteção oferecida pelo provedor de serviços é feita através de mecanismos de controle de acesso.

Em sistemas de controle de acesso, os objetos são as informações a serem protegidas, por exemplo, mensagens, fotos e vídeos. As ações podem ser executadas nesses objetos, por exemplo, curtir, comentar e compartilhar. Os sujeitos requisitam executar ações nos objetos, por exemplo, um amigo ou um seguidor. Por fim, as condições são usadas como restrições para executar ações, por exemplo, o sujeito precisa ser um membro da família para acessar uma foto [121].

Controles de acesso que representam as configurações de privacidade podem ser expressos de várias formas em redes sociais, e cada uma tem uma maneira específica de permitir os usuários a determinarem suas preferências. Por exemplo, a configuração de privacidade do Facebook usa listas de amigos para permitir usuários organizarem sujeitos (ou seja, um contato individual ou grupo de contatos) para quem é permitido ou negado ações em objetos. Similarmente com poucas diferenças, o Google+ usa a noção de círculos. O uso de listas de amigos no Facebook e círculos no Google+ torna possível selecionar especificamente a audiência desejada que terá permissão para executar ações em um conteúdo específico. Algumas RSMs permitem ao usuário expressar condições temporais, tais como o Snapchat, em que um conteúdo postado se mantém disponível por somente 24 horas. Entretanto, outras RSMs não têm controles de privacidade com granularidade fina, tais como o Instagram, que não permite o agrupamento de contatos e o usuário apenas determina se todas fotos publicadas podem ser ou não acessadas por contatos que não o seguem (recurso chamado de “Fotos privadas”). Para isso, previamente o usuário precisa aceitar uma

requisição de um outro que o deseja seguir, delimitando assim quem pode acessar seus conteúdos postados.

Como descrito anteriormente, as redes sociais podem ser representadas através de um Grafo Social, onde os usuários são representados por vértices e os elos por arestas. Neste cenário, os ataques de invasão de privacidade podem ocorrer via:

- **Acesso direto ou usuários conectados**: um vértice A tem uma aresta ligando-o a um vértice B. Por exemplo, os usuários João e Maria ligados diretamente pela aresta A na Figura 2.1, no Grafo Social A. Nesse caso, o vazamento de privacidade ocorre quando, por exemplo, Maria acessa um conteúdo de João sem que ele delegue uma permissão explícita;

- **Acesso indireto ou usuários conectados indiretamente**: um vértice D não tem uma aresta ligando-o a um vértice E, mas ambos vértices tem uma aresta ligando-os a um vértice C. Assim, existe um elo indireto entre eles, com um ou mais saltos. Nesse caso, o vértice D é amigo-de-amigo (do inglês, *friend-of-friend*) do vértice E. No exemplo da Figura 2.1, no Grafo Social A, Joana é amigo-de-amigo de Ricardo, pois ambos possuem um elo com Pedro. O vazamento de privacidade nesse caso ocorre, por exemplo, quando um vértice intermediário propaga (compartilha) um conteúdo sem permissão;

- **Acesso público**: não existe obrigatoriamente uma aresta, um ou mais vértices intermediários, ligando dois vértices. Alguns mecanismos de controle de acesso permitem a não restrição de acesso a conteúdos. Com esta política, o acesso a conteúdos é público a qualquer usuário.

Aplicações de Terceiros

Aplicações de terceiros são escritas utilizando uma *Application Programming Interface* (API) disponibilizada pelo provedor de serviços, a qual fornece uma interface aberta para a criação e adição de novos recursos à rede social. Essas aplicações são necessárias para prover novos serviços à rede social, demandados pelos próprios usuários. No entanto, essas aplicações são escritas por outras entidades, e naturalmente não são sempre confiáveis. Além disso, elas usualmente requerem ao usuário a permissão para acessar livremente suas informações pessoais. Aplicações de

terceiros podem ser categorizadas como no Facebook: jogos, diversão, estilo de vida, música, notícias, fotos, vídeos, esportes, lugares, entre outras.

O tipo de aplicação de terceiros que oferece mais risco é o das agências de publicidade. Estas companhias usualmente tem acesso às informações pessoais de usuários, autorizadas pelo provedor de serviços, a fim de realizar publicidade personalizada de acordo com os interesses dos usuários. Estas publicidades são consideradas cientes de contexto, uma vez que elas usualmente levam em consideração informações de contexto social extraídas dos perfis de usuários, tais como lugares frequentados, mensagens publicadas, comunidades as quais usuários estão inseridos, entre outras. Dessa forma, as agências de publicidade podem direcionar melhor seus anúncios.

As aplicações de terceiros, as quais têm permissões explícitas dos usuários para acessarem suas informações pessoais, podem disponibilizar essas informações a outras entidades não autorizadas. Por exemplo, um jogo social que requisita um subconjunto de informações do perfil do usuário (por exemplo, seu nome, e-mail, data do aniversário, local de trabalho, entre outras) pode disponibilizá-las a outra entidade.

Provedor de Serviços

O provedor de serviços é a entidade responsável por fornecer os serviços necessários aos usuários da rede social. Ele tem acesso a todos os dados pessoais inseridos/publicados pelos usuários. Exatamente por esse motivo, os usuários podem não confiar nesta provisão de serviços e ficarem cada vez mais preocupados, por não saberem realmente por quem seus dados pessoais são acessados [60].

Os provedores de serviços de redes sociais usualmente ganham vantagem dos dados de usuários, por oferecê-los a outras empresas, para que sejam utilizados, por exemplo, para publicidade ciente de contexto. Entretanto, uma vez que os conteúdos dos usuários são muito sensíveis, eles devem ser fornecidos de forma a não revelar a identidade do usuário. Dessa forma, caso alguma outra entidade externa ao provedor da rede social tenha acesso ao conteúdo, não será possível identificar seu dono a partir dele. Então diz-se que os dados estão anonimizados. As técnicas usadas para esconder a identificação dos donos dos dados armazenados no provedor de serviços das redes sociais é chamada de anonimização. A tentativa de vazamento

de privacidade para identificar o dono a partir de dados anonimizados é chamada de deanonimização [108].

2.4.1 Privacidade em Aplicações Sociais Móveis

As informações de contexto proveem uma riqueza de recursos e a possibilidade para construir muitos tipos de serviços para RSMs. Entretanto, elas também criam novos problemas de vazamento de privacidade. Informações de contexto publicadas na rede social podem comprometer a privacidade do usuário por conterem (ou a partir delas poder-se inferir) muitas informações pessoais sensíveis que um usuário não quer deixar disponível para outros vértices da rede social. Um fator agravante é a prática comum de agregação de informações de contexto a conteúdos (por exemplo, adicionar a uma foto a localização, data e horário a qual ela foi tirada), o que nem sempre é feito com o consentimento explícito do usuário. Dessa forma, informações de contexto podem ser expostas para usuários que somente têm permissão de acessar conteúdos publicados, e não informações de contexto agregadas. No entanto, em algumas aplicações sociais móveis, dependendo de seu domínio, muitas informações de contexto, e ainda sensíveis, devem ser continuamente transmitidas, como em RSMs aplicadas ao domínio da saúde, onde através de sensores (bio-sensores) profissionais de saúde podem continuamente monitorar o status de saúde dos pacientes. Schuster et al. [126] argumentam que o gerenciamento de privacidade deve ser feito em diferentes níveis, desde uma única informação de contexto pessoal (único sensor) até informações de contexto inferidas a partir de vários sensores.

Uma outra questão é que usuários maliciosos podem produzir falsas informações de contexto para aplicações sociais móveis. Estas informações podem ser usadas pelo atacante para ganhar acesso a algum recurso (*spoofing attack*) ou ganhar uma identidade temporária para agir como um usuário legítimo (*faking attack*) [44]. Portanto, o uso impróprio de informações de contexto pode seriamente influenciar a confiabilidade de aplicações sociais móveis. Isto traz sérios problemas quando as aplicações são usadas em ambientes críticos, como no domínio da saúde, onde decisões médicas podem ser tomadas baseadas em informações de contexto, tendo uma direta influência no tratamento dos pacientes.

Outro exemplo relacionado com a produção de informações de contexto falsas é o chamado *location cheating attack* [67], ilustrado na Figura 2.5. Neste ataque, quando o GPS do dispositivo móvel retorna as coordenadas de localização para a aplicação, o atacante bloqueia a informação original e cria uma informação de localização falsa, fazendo o provedor de serviços acreditar erroneamente que o dispositivo móvel está na falsa localização fornecida.

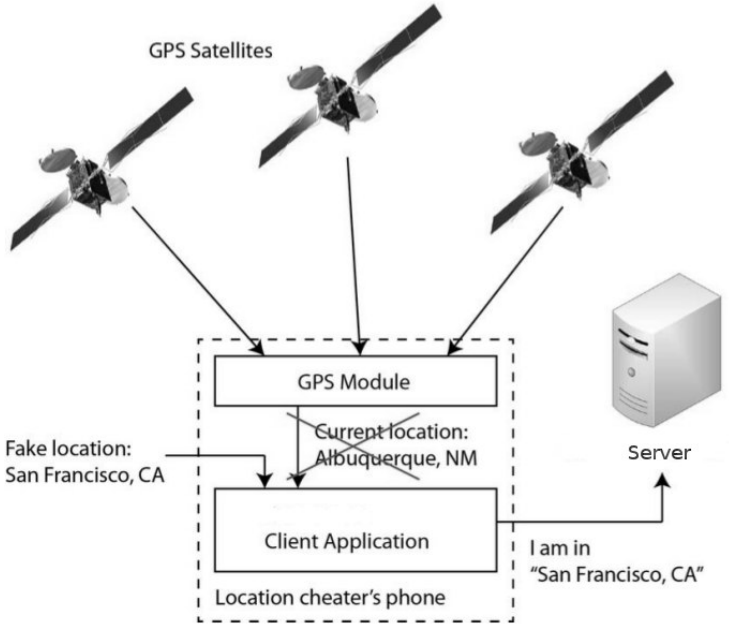

Figura 2.5: Ilustração do *Location Cheating Attack* [67].

Uma questão de privacidade que surge devido ao uso inadequado de informações de contexto está relacionado ao *tagging* (marcação) em conteúdos publicados. Várias aplicações sociais móveis permitem ao usuário associar um vértice, ao qual ele tem um elo estabelecido, a um conteúdo publicado, o que é chamado de *user tagging*. Por exemplo, é possível publicar uma foto no Facebook fazendo uma marcação de um amigo, dessa forma, caracterizando que o amigo está na foto ou tem alguma relação com ela. Se a associação é uma referência a uma localização, a marcação é chamada de *geotagging*, neste caso, isso caracteriza que o amigo está co-localizado ou tem alguma relação com o conteúdo postado. O *tagging* cria problemas de vazamento de privacidade, uma vez que o usuário marcado pode, eventualmente, não desejar que isso ocorra [58]. Por exemplo, um usuário não gostaria de ser marcado em uma foto ou em uma localização a qual pode lhe constranger.

Considerando as questões de privacidade descritas, é possível destacar alguns requisitos relacionados ao projeto das aplicações sociais móveis, os quais os desenvolvedores devem levar em consideração [132]:

- As aplicações devem prover mecanismos que permitam ao usuário não somente definir regras de controle de acesso a conteúdos publicados, mas também para informações de contexto associadas, em vários níveis de granularidade;
- Em muitos casos, a publicação de informações de contexto é feita implicitamente e escondida do usuário. As aplicações devem expor ao usuário de alguma maneira quais informações de contexto estão sendo publicadas e permiti-lo desabilitar esta publicação quando desejar;
- As aplicações devem prover usabilidade para permitir ao usuário configurar políticas de privacidade com facilidade.

A proteção da informação de contexto de localização é particularmente importante em aplicações sociais móveis, devido à grande quantidade de aplicações que proveem serviços baseado em localização (*location-based services*). A informação de localização pode ser publicada nas RSMs de forma explícita, mas também implícita, sem permitir ao usuário determinar a sua não publicação, o que é agravante para alcançar privacidade. Além disso, a localização do usuário pode estar disponível em tempo real para que seus contatos a acessem [9].

As seguintes categorias de privacidade de localização podem, então, ser identificadas [8]:

- **Privacidade da Identidade**: onde o objetivo é proteger a identificação do usuário associada ou inferida a partir das informações de localização. Informações de localização podem ser providas a alguma entidade, mas a identidade do usuário deve ser preservada;
- **Privacidade de Posição**: onde o objetivo é adulterar a localização exata do usuário a fim de proteger sua real localização;
- **Privacidade de Caminho**: onde o objetivo é não revelar localizações anteriores ao qual o usuário passou, ou seja, o caminho percorrido pelo usuário.

2.4.2 Ataques contra a Rede Social

Vários ataques são discutidos na literatura, os quais objetivam perturbar a correta operação da rede social, onde o provedor de serviços, aplicações de terceiros e os usuários podem ser prejudicados. Alguns ataques têm a intenção de enfraquecer a confiança dos usuários em relação ao provedor de serviços e, caso isto ocorra, o provedor poderá perder rendimentos financeiros. Estes ataques também geram um impacto negativo aos desenvolvedores de aplicações de terceiros, por diminuir as negociações de seus produtos. Em um caso mais grave e impactante, os usuários podem ser prejudicados, sofrendo com o vazamento de privacidade ou sendo infectados com códigos maliciosos.

Um problema comum em redes sociais é o *Spam*. O termo *spam* é utilizado para referenciar o recebimento de uma mensagem não solicitada, que geralmente tem o caráter de fazer propaganda de algum produto ou assunto não desejado. Spam torna-se um problema mais sério quando combinado com a disseminação de códigos maliciosos (*malware*). O usuário, ao clicar em uma *Uniform Resource Locator* (URL) com código malicioso, infecta seu computador e permite ao dono do *malware* acessar sua conta da rede social. Grier et al. [63] analisaram 25 milhões de URL compartilhadas no Twitter e identificaram que 8% delas apontam para páginas *Web* catalogadas em listas negras, por possuir códigos maliciosos. Ao analisar as contas usadas para envio de *spams*, os autores encontraram evidências de que as mensagens de *spam* foram originadas por contas de usuários legítimos, mas infectadas por *malware*. A disseminação de código malicioso gera um grande impacto negativo à rede social, como ocorrido em agosto de 2008, quando o Koobface, um *malware*, causou grandes problemas a várias redes sociais [151]. Os provedores de serviço podem agir na detecção, redução ou mesmo parar a disseminação de códigos maliciosos.

Um outro tipo de ataque é o chamado *Sybil* [45], que ocorre quando um atacante adultera o sistema de reputação da rede social através da criação de várias contas (alguns ataques requerem apenas 7, enquanto outros milhões de contas). O atacante influencia diversos resultados da rede social usando contas controladas que agem coletivamente como usuários legítimos. Por exemplo, um ataque *sybil* poderia influenciar os resultados de uma enquete realizada na rede social.

Em [22], os autores apresentam dois ataques chamados *Same-site profile cloning* e *Cross-site profile cloning*. No primeiro, o atacante cria uma conta a qual tem informações de perfil idênticas a de outro usuário. Em seguida, ele envia requisições para o estabelecimento de arestas para uma lista de contatos do usuário legítimo do qual ele clonou a conta. Estes contatos, acreditando na familiaridade do usuário (por exemplo, colega de estudo, colega de trabalho ou um membro da família) aceita a requisição e, assim, inicia a exposição de suas informações pessoais ao atacante. Essa exposição ocorre devido ao fato de muitas políticas de privacidade permitirem acesso a conteúdos pessoais a contatos. O segundo ataque é similar ao primeiro, diferenciado pelo fato de que a criação de um perfil falso não é feita na mesma rede social onde o usuário legítimo tem um perfil válido, mas em uma rede social diferente. Em [22], os autores propõem um método para a detecção destes ataques através de *Captcha*[3], uma vez que a definição de perfis falsos é usualmente feita de forma automática através de códigos maliciosos, os quais têm dificuldades de passar por desafios de *captcha*.

2.5 Conclusão

Esse capítulo apresentou uma fundamentação sobre o cenário em que este trabalho está inserido, as RSMs. Nele foram vistos os conceitos fundamentais de redes sociais e mais especificamente de RSMs, mostrando como as informações de contexto são utilizadas nesses sistemas sociais. Dessa forma, foi apresentado o cenário principal em que essa tese é desenvolvida. Os vários tipos de arquiteturas que RSMs podem ser implementadas também foram mostrados. Esse conhecimento é necessário para distinguir as diversas maneiras em que as RSMs podem ser organizadas, sendo importante para o entendimento de como a solução proposta nessa tese foi concebida e implementada. Em seguida, foram descritos os problemas de vazamentos de privacidade e de segurança em redes sociais. A visão geral sobre esses prolemas é indispensável para conhecer amplamente a existência das muitas dificuldades enfrentadas nessa área de pesquisa e compreender a delimitação do escopo do problema abordado e da solução proposta por essa tese.

[3] *Captcha* é um tipo de teste desafio-resposta usado em computação como uma tentativa de garantir que a resposta é gerada por uma pessoa humana e não por uma máquina.

3 Computação Situacional

Este capítulo apresenta uma introdução a computação situacional, conhecimento essencial para o entendimento da solução proposta nessa tese. Portanto, apresenta-se uma fundamentação ao tema de computação situacional devido a tomada de decisão feita pela solução proposta nesta tese ter como base a situação atual do usuário. Inicialmente o capítulo mostra os conceitos introdutórios de situação, ciência de situação e computação situacional. Em seguida, a fase de processamento do ciclo de vida de informações contextuais é detalhada. Na sequência, uma fundamentação sobre *Quality of Context* (QoC) é feita, juntamente com a fase de distribuição, em que é destacado o uso do *middleware Scalable Data Distribution Layer* (SDDL) para realizá-la. Por fim, uma fundamentação às técnicas usadas para identificação de situação, com ênfase na lógica nebulosa, é apresentada.

3.1 Conceitos

O conceito de **situação** não é fácil para definir e pode ter muitos significados [152]. Estes significados delimitam o escopo das informações que caracterizam uma situação. No dicionário Aurélio, situação é a maneira como um objeto está colocado, estado e condição de um ser ou coisa. Segundo o filósofo e matemático Jon Barwise [13] situação é o estado de algo em um contexto particular. Para o filósofo John Perry [113] uma situação corresponde a partes limitadas de uma realidade que seres humanos percebem, raciocinam e vivem.

Em uma visão mais atual, para Anagnostopoulos et al. [7] situação é uma abstração que existe dentro de nossas mentes, descrevendo fenômenos que observamos em seres humanos realizando alguma atividade. Para eles, em computação ubíqua uma situação é uma sequência finita de ações que podem descrever comportamentos humanos e estados ambientais e de aplicação. Para Lin et al. [91], situação é a combinação de forma lógica de dados de contexto. Fleishmann [53] diz: “uma situação consiste da interpretação de um conjunto de elementos de contexto

instanciados, relacionando cada um de forma a prover alguma informação válida em um intervalo de tempo específico. Uma situação identifica o contexto válido em determinado intervalo de tempo, o qual representa um estado específico do usuário, sua situação". Por exemplo, estudando na universidade pela tarde, jantando em um dado restaurante, trabalhando pela manhã.

Na literatura existem muitos trabalhos propostos relacionados a teoria e aplicações de **ciência de situação** (*situation awareness*) [145]. Endsley [48] em 1995 apresentou, de forma concreta, a teoria e o modelo conceitual de ciência de situação. Para ele, a ciência de situação é a percepção dos elementos no ambiente dentro de um volume de tempo e espaço, a compreensão de seus significados, e a projeção de seus estados no futuro próximo. O autor divide esta definição em três etapas:

1. **Percepção dos elementos no ambiente**. Responsável por perceber o estado, atributos e características dinâmicas dos elementos relevantes no ambiente;

2. **Compreensão da situação atual**. Fase com a função de conhecer os elementos do ambiente e utilizá-los para formular um entendimento da situação, levando em consideração as necessidades de quem está interessado nela. Esta fase é responsável por processar os elementos coletados individualmente a fim de produzir um conhecimento sobre a situação;

3. **Projeção de estados futuros**. Esta fase é responsável por identificar a melhor ação a ser feita de acordo com a situação compreendida na fase anterior. Além disso, ela é responsável pela capacidade de antecipação de ocorrências futuras, a partir da compreensão dos elementos no ambiente atual.

Em uma visão moderna, a ciência de situação é considerada um particular tipo de ciência de contexto [41]. Ciência de situação não é restrita ao uso de dados de contexto isolados, mas ela está relacionada a combinação de dados de contexto relevantes para identificar corretamente a situação do usuário [3]. A ciência de situação em computação ubíqua/pervasiva objetiva formalizar e inferir situações do mundo real a partir de dados de contexto [27]. Portanto, o paradigma de **computação situacional** refere-se a aplicação da ciência de situação em um ambiente de computação ubíqua/pervasiva, em que uma aplicação ciente de situação tem a habilidade para interagir com o usuário, aprender com ele, e autonomamente

se adaptar ao contexto situacional do usuário [7]. Os dispositivos computacionais que conhecem mais sobre o contexto do usuário estão habilitados para adaptar efetivamente e transparentemente suas funções a situação atual do usuário, levando à ideia de Weiser [144] da computação invisível.

Aplicações cientes de situação (*situation-aware applications*) é uma classe de aplicações capazes de reconhecer a situação do usuário por meio de dados de contexto [6] e de usar as situações para executar ações [91]. Portanto, as aplicações cientes de situação possuem mecanismos para detecção de situações do usuário em dispositivos móveis de forma automática. Consequentemente, aplicações móveis podem reconhecer a situação do usuário em condições de mobilidade e realizar ações com base nelas.

3.2 Processamento de Contexto

O gerenciamento de contexto refere-se ao acompanhamento do ciclo de vida das informações de contexto, desde o provedor até o consumidor das informações. Existem diversas propostas de modelos de gerenciadores de contexto, não há um padrão único que estabeleça as fases pelas quais podem passar as informações de contexto. Bellavista et al. [17] apresentam quatro fases principais no ciclo de gerenciamento de contexto: produção, processamento, armazenamento e distribuição. Perera et al. [112] promovem uma análise dos ciclos de vida de informação de contexto mais recorrentes na literatura, e com base nessa análise propõem um ciclo de vida semelhante ao anterior, contendo as seguintes fases: aquisição, modelagem, raciocínio e disseminação. Nessa proposta, em que o processamento ocorre em duas fases (modelagem e raciocínio), o armazenamento não é considerado uma fase essencial. Já as fases de aquisição e disseminação correspondem respectivamente as fases de produção e distribuição da proposta anterior.

Na fase de produção (ou aquisição), as informações de contexto são coletas do ambiente através de diversos processos e fontes. A fase de armazenamento da informação de contexto é importante em casos em que o histórico da informação possa afetar o comportamento do sistema. A fase de distribuição (ou disseminação)

de informações de contexto está presente em sistemas que enviam informações de contexto para outros sistemas interessados nas mesmas.

A fase de processamento engloba a realização de operações de transformação, tais como raciocínio e filtragem, para atender às necessidades adaptativas do sistema. O raciocínio de contexto refere-se ao emprego de um conjunto de métodos e processos que viabilizam a identificação, aprendizagem, a derivação, a predição de tendências, padrões ou preferências sobre as informações contextuais. O raciocínio de informações contextuais deriva novos fatos de contexto a partir de fatos já existentes, e consequentemente gera abstrações de informações de contexto de alto nível que modelam situações do mundo real [21]. Por exemplo, as informações de localização e tempo, além da presença de outros usuários co-localizados, podem ser combinadas para inferir que o usuário está no trabalho, o que constitui uma informação de contexto de alto nível. Portanto, para realizar a inferência de um fato novo é necessário encontrar um conjunto de informações de contexto que possam caracterizar uma outra informação de contexto. O objetivo de raciocinar sobre informação de contexto é obter informações de alto nível que permitem melhorar a compreensão de um determinado contexto pela aplicação de modo a modificar o seu comportamento ou auxiliá-la na tomada de decisões [38].

As filtragens são operações que visam reduzir o volume de dados que são recebidos do ambiente de modo a viabilizar o processamento eficiente do que realmente é necessário. Por exemplo, se para um determinado sistema a localização do usuário só é importante em determinado período do dia, então o sistema não precisa receber esta informação o dia todo, pois isto apenas acarretaria em processamento desnecessário.

Diante desses conceitos, o processamento de informações contextuais consiste no uso de um conjunto de técnicas que permitem a partir de uma base de conhecimento (por exemplo, uma base de informações contextuais coletadas, um histórico de contexto, ou especificações feitas por pessoas), a inferência ou geração de novas informações mais refinadas e relevantes que serão posteriormente empregadas para prover serviços, tais como personalização e adaptação de sistemas computacionais e recomendação de conteúdo [38].

Existem dois principais desafios durante o processo de inferência. O primeiro refere-se a QoC, em que é necessário tratar informações sensoreadas que apresentam baixa qualidade, lidando com a incerteza que existe nas informações obtidas por sensores. A próxima seção é dedicada a discutir questões específicas relacionadas a QoC. O segundo desafio está relacionado ao fato de que os mecanismos de inferência em alguns casos devem ser executados exclusivamente no dispositivo móvel (por exemplo, no caso em que não é possível compartilhar o processamento com um lado servidor) e, portanto, requerem algoritmos rápidos e com baixo custo computacional, preocupando-se principalmente com o consumo da bateria do dispositivo [85]. Dessa forma, soluções propostas para inferir contexto e identificar situações de interesse devem dar atenção a esses dois desafios.

3.3 Qualidade de Contexto

A realização do processamento de contexto é uma tarefa desafiadora devido a natureza imperfeita dos dados de contexto [21, 68]. Para Ye et al. [154], existem pelo menos três fatores responsáveis pela imperfeição dos dados de contexto sensoreados:

- **Limitação técnica dos sensores**: os sensores físicos, devido às suas próprias naturezas, podem estar sujeitos a erros de leitura provocados pela má calibração ou falha de fabricação. Os sensores também podem estar mal posicionados e gerar informações incorretas;
- **Ruído do ambiente**: a acurácia de alguns sensores pode estar sujeita a interferências de rádio, temperatura, umidade, ruído de som ou materiais refletores que causam problemas em sinais sem fio;
- **Os usuários**: a configuração de sensores por usuários pode afetar a acurácia dos sensores. Em informações de contexto baseadas em perfis do usuário, a omissão do usuário em fornecer entradas ou ofuscação de dados por conta de questões de privacidade pode fazer com que algumas informações sejam desconhecidas.

Henricksen e Indulska [68] identificaram quatro tipos de imperfeição nas informações de contexto, as quais são motivadas por algum dos fatores descritos acima.

1. **Incógnita**: quando a informação de contexto ou um de seus atributos não é conhecido ela é considerada incógnita. Por exemplo, quando a localização do usuário ou um de seus atributos (latitude, longitude ou altitude) não são conhecidos;

2. **Ambiguidade**: a informação de contexto é ambígua quando diferentes fontes de contexto fornecem valores diferentes ou contraditórios para o mesmo tipo de informação. Por exemplo, dispositivos distintos com GPS fornecem dados de localização diferentes ou contraditórios de um determinado usuário em um mesmo momento;

3. **Incorreção**: considerando a dinamicidade e heterogeneidade das fontes de informação, os dados de contexto estão incorretos quando não refletem o contexto real. Por exemplo, a localização errada do usuário;

4. **Imprecisão**: a informação pode estar imprecisa, ainda que esteja correta, caso não seja provida com precisão ou granularidade (nível de detalhes) suficiente para que seja útil. Por exemplo, a localização do usuário fornecida ao nível de bairro, enquanto é esperado que seja fornecida com granularidade ao nível de rua.

Há diversas definições de QoC, mas não existe um consenso na literatura acerca de qual é a mais correta. Buchholz et al. [28] definem QoC como sendo qualquer informação que descreve a qualidade da informação que é usada como informação de contexto. Assim, QoC refere-se a qualidade da própria informação, e não ao processo ou componente de hardware que a fornece. Esses autores identificaram cinco parâmetros de QoC, a partir da experiência deles, como sendo os mais importantes, são eles: precisão, probabilidade de acerto, resolução, confiabilidade e idade.

Na visão de Buchholz et al. [28], a QoC é uma qualidade intrínseca à informação e que difere de *Quality of Service* (QoS) e de *Quality of Device* (QoD). Nesse mesmo trabalho, QoS é definida como qualquer informação que descreve o quão bem um serviço executa. A QoD é definida como qualquer informação sobre as características técnicas e as capacidades de um dispositivo. Mesmo distintas, QoC, QoS e QoD possuem uma relação de interdependência, sendo que qualquer uma delas pode influenciar no comportamento ou ser influenciada pelas demais.

Manzoor et al. [97–99] propuseram dividir a noção de QoC em duas visões: a objetiva e a subjetiva. A visão objetiva é independente do cenário em que as informações de contexto são utilizadas e das exigências dos consumidores. Essa visão objetiva de QoC é determinada pelas características dos sensores utilizados para coletar os dados de contexto, bem como as condições em que a medição do valor de contexto foi feita (contexto de medição). A visão subjetiva de QoC expressa o quanto uma informação de contexto está em conformidade com as exigências de uma aplicação consumidora em particular. Os autores argumentam que o contexto adequado para a utilização da informação por uma aplicação pode não ser a recomendada para a utilização dessa mesma informação por outra aplicação. Eles ainda propuseram um conjunto de parâmetros de QoC agrupados em três categorias: (i) características dos sensores (acurácia, precisão, granularidade, intervalo de medição, estado físico do sensor, distância do sensor); (ii) contexto de medição (instante da medição, localização do sensor, localização da entidade, atributos disponíveis); (iii) especificações e requisitos do consumidor (tempo de validade, atributos requeridos, valor crítico e nível acesso ao dado).

3.4 Distribuição de Dados de Contexto

Em algumas casos, para identificar a situação do usuário com maior acurácia é necessário processar dados de contexto que são oriundos de fontes que não estão unicamente no dispositivo móvel. Dessa forma, é necessário realizar a fase de distribuição de contexto, como explicado na seção 3.2. Em relação a essa fase, existem vários modelos de comunicação que permitem a entrega das informações produzidas aos consumidores interessados. Geralmente os modelos de comunicação se diferenciam em relação ao acoplamento entre produtores e consumidores e a sincronia na comunicação entre eles. Os principais modelos empregados são passagem de mensagem, (*publish/subscribe* – pub/sub) e espaço de tuplas. Esta seção dá ênfase ao modelo pub/sub e sua implementação através do SDDL [40], um *middleware* que foi usado na solução proposta nesta tese.

O paradigma pub/sub é uma alternativa possível para o tratamento de aplicações móveis em larga escala [59]. Eventos contêm dados que descrevem uma requisição ou mensagem e são propagados dos componentes emissores, chamado

de publicadores, para os componentes receptores, denominados subscritores. Os publicadores são os agentes que enviam informação a um componente central ou a tópicos de interesse, enquanto os subscritores expressam seu interesse no recebimento de eventos particulares. O *broker*, quando existir, é o componente central responsável por registrar todas as subscrições, comparar as publicações com todas as subscrições e notificar os subscritores interessados. Arquiteturas baseadas em eventos ou pub/sub oferecem um modelo de coordenação com fraco acoplamento entre os publicadores e subscritores e onde a notificação assíncrona de eventos é naturalmente suportada.

3.4.1 SDDL

O SDDL é um *middleware* de comunicação escalável de alto desempenho desenvolvido pelo *Laboratory of Advanced Collaboration* (LAC) da PUC-Rio com a colaboração do Laboratório de Sistemas Distribuídos Inteligentes (LSDi) da UFMA. O SDDL conecta nodos estacionários em uma rede cabeada (a nuvem SDDL ou *SDDL Core*) a nodos móveis através de uma conexão baseada em redes *Internet Protocol* (IP) sem fio [39, 40]. Na arquitetura do SDDL, mostrada na Figura 3.1, parte dos nodos estacionários localizados na nuvem SDDL são destinados ao processamento de dados de contexto. Alguns nodos são *Gateways*, que servem de ponte para a comunicação entre a nuvem e os nodos móveis. Há também nodos de monitoramento e controle do sistema. Esses nodos exibem a posição atual dos nodos móveis (ou qualquer outra informação) e também são capazes de gerenciar grupos de nodos e enviar mensagens para os nodos móveis individualmente ou em grupo.

O SDDL emprega dois protocolos de comunicação: o *Mobile Reliable - User Datagram Protocol* (MR-UDP), para comunicação entre os nodos móveis e a nuvem SDDL, e o *Data Distribution Service* (DDS) / *Real-Time Publish-Subscribe* (RTPS) [65, 110] para comunicação escalável entre os nodos do *SDDL Core*: *Gateway*, *PoA-Manager*, *Processing Nodes*, e *Load Balancer*.

O ***Gateway*** define um único ponto de ligação (*Point of Attachment* (PoA)) para a conexão dos nodos móveis com a nuvem SDDL. Ele é responsável por gerenciar uma conexão separada com cada nodo, bem como encaminhar qualquer mensagem dos nodos móveis para o *SDDL Core* e, na direção oposta. Sendo o manipulador de conexões com os nodos móveis, o *Gateway* também é responsável por notificar outros

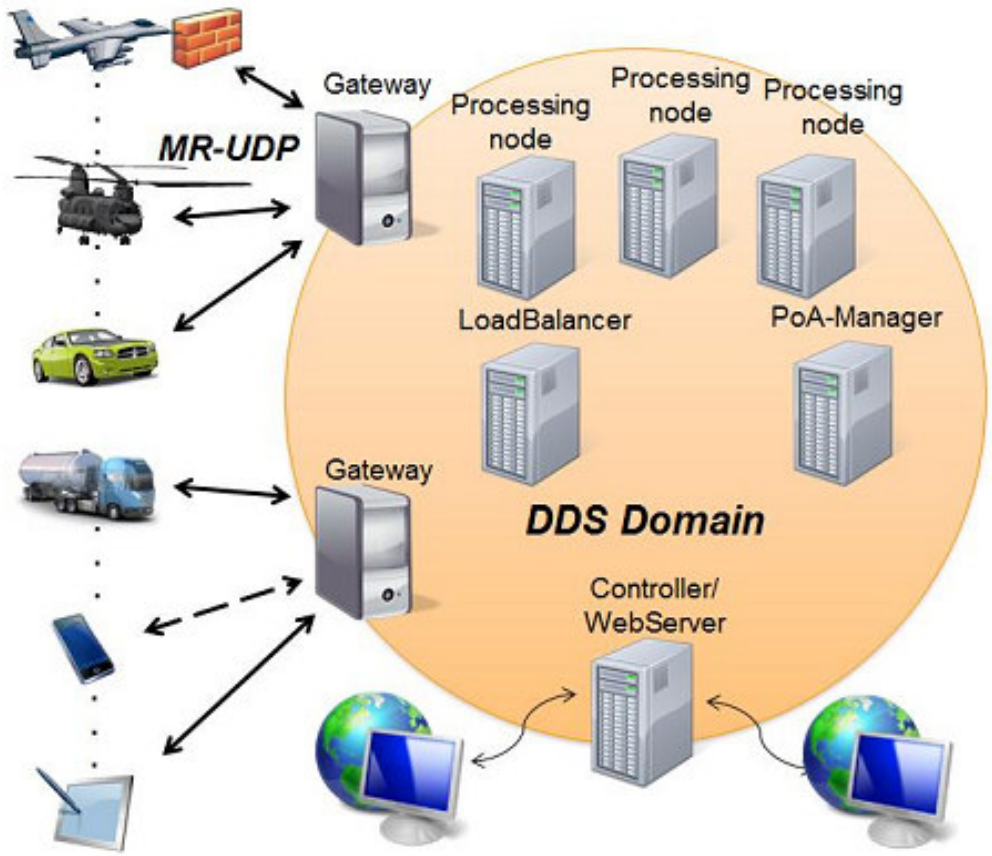

Figura 3.1: Arquitetura SDDL [40].

nodos da nuvem SDDL quando um novo nodo móvel se torna disponível ou quando eles são desconectados. Esta informação é necessária para algumas funcionalidades do *SDDL Core*, tais como o armazenamento de mensagens endereçadas a nodos móveis temporariamente *offline*, possibilitando a entrega posterior dessas mensagens.

O **PoA-Manager** é responsável por duas tarefas: distribuir periodicamente uma lista de PoA (*PoA-List*) para os nodos móveis e, eventualmente, solicitar que alguns nodos móveis mudem para um novo *Gateway*/PoA (*handover*). A *PoA-List* é sempre um subconjunto de todos os *Gateways* disponíveis na nuvem *SDDL*, e a ordem na lista é relevante, ou seja, o primeiro elemento aponta para o *Gateway*/PoA preferencial e assim por diante. Por ter uma *PoA-List* atualizada, um nodo móvel pode mudar para um outro *Gateway* da lista se, por exemplo, detectar uma conexão fraca ou uma desconexão com o *Gateway* atual. Além disso, através da distribuição de diferentes *POA-List* para diferentes grupos de nodos móveis, o *PoA-Manager* é capaz de equilibrar a carga entre os *Gateways*, bem como anunciar para os nodos móveis quando *Gateways* são adicionados ou removidos.

Os **Processing Nodes** são servidores que estendem o poder de processamento e armazenamento dos nodos móveis, sendo capazes de, por exemplo, realizar tarefas de computação intensiva e armazenar dados de interesse para todo o sistema. Quando um nodo de processamento recebe um dado de contexto, ele verifica se é responsável pelo tratamento desse dado. Os dados para o qual um nodo não é responsável por processar são simplesmente ignorados, uma vez que são processados pelo nodo(s) de processamento que são realmente responsável(is) por eles. Por fim, o **Load Balancer** é responsável por monitorar a carga dos nodos de processamento, a fim de redistribuir a carga de trabalho do sistema quando situações de desbalanceamento são detectadas.

3.5 Identificação de Situações

O ser humano é capaz de identificar situações e a suas relações com base no conhecimento empírico adquirido ao longo de sua vida. Como situações são abstrações semânticas a partir de valores de contexto de baixo nível, o conhecimento e interpretação humano do mundo pode ser integrado dentro de um modelo ou representação de situação. Dessa forma, sistemas computacionais podem também ter a habilidade para reconhecer situações [21].

As técnicas de identificação de situação abstraem dados de contexto de baixo nível para informações de contexto de alto nível com maior significado para seres humanos. Por meio delas o sistema pode analisar um conjunto de informações visando reconhecer um padrão que caracteriza uma informação de alto nível. Muitos trabalhos para realizar identificação de situações a partir de dados de contexto em ambientes pervasivos tem sido desenvolvidos na literatura [153], cada qual propondo soluções para casos particulares e resolvendo problemas específicos.

A descrição de uma situação pode ser feita durante o processo de especificação, ou seja, um humano define as situações e seus relacionamentos baseado em seu próprio conhecimento. Entretanto, o sistema computacional pode também inferir novos fatos utilizando técnicas de aprendizagem de máquina. Nesse segundo caso, situações são reconhecidas e aprendidas automaticamente: as percepções de sensores são agregadas e associadas através de técnicas de aprendizagem de máquina

para uma situação rotulada por um ser humano. Com isso, Ye et al. [153] propuseram uma classificação para as técnicas de inteligência artificial [119] que podem ser usadas na concepção de soluções para identificação de situação, descritas a seguir.

Baseadas em especificação. Estas técnicas consistem em definir especificações que representam conhecimento através de regras lógicas e aplicam motores de inferência para identificar situações a partir de dados de contexto de entrada. Exemplos de técnicas baseadas em especificação são: Programação Lógica, Lógica Temporal e Espacial, Ontologias, Lógica Nebulosa e Teoria da Evidência.

A Figura 3.2 mostra o modelo base utilizado pelas técnicas de identificação de situação baseadas em especificação. Nesse modelo, os fatos são processados por um motor de inferência, o qual necessita de uma base de regras que são utilizadas para determinar um novo fato.

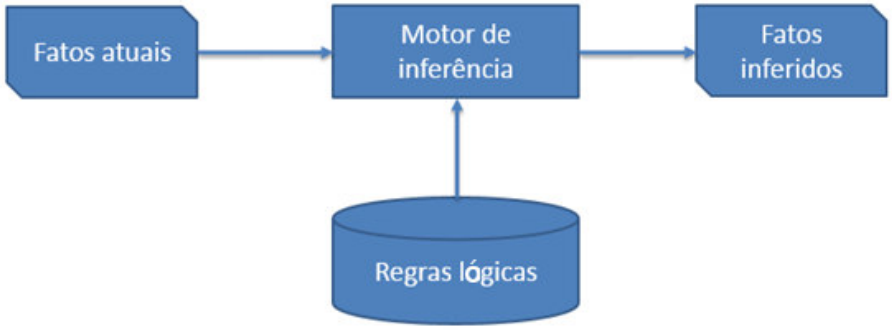

Figura 3.2: Modelo de Identificação de Situação baseada em Especificação.

Baseadas em aprendizagem. Estas técnicas usam aprendizagem de máquina e mineração de dados para explorar relacionamentos de associação entre os dados de contexto e situações de interesse. Aprendizagem de máquina é um campo da inteligência artificial dedicado a criar algoritmos e técnicas capazes de ensinar um computador a reconhecer padrões de informação a partir de exemplos [104]. Este campo do conhecimento visa criar técnicas de aprendizagem similares ao raciocínio humano, para que computadores possam raciocinar sobre um conjunto de dados.

Técnicas para identificar situações baseadas em aprendizagem são melhores usadas em cenários onde é difícil definir especificações de situações a partir de uma grande quantidade de dados de contexto que podem sofrer de algum tipo de imperfeição [153]. Exemplos de técnicas baseadas em aprendizagem são: aprendizado Bayesiano (*Naive Bayes* e redes Bayesianas), modelos escondidos de Markov, árvores de

decisão, redes neurais artificiais, máquinas de vetor de suporte, mineração de dados *Web*, dentre outras [104].

Existem vários características que podem ser consideradas na escolha de uma técnica para identificação de situações em um sistema. Pode-se adotar ainda mais de uma técnica simultaneamente, e nesse caso há uma abordagem híbrida, a qual se aproveita das qualidades de mais de uma técnica. Primeiramente, algumas técnicas dão suporte ao estabelecimento (especificação e modelagem) de relacionamentos entre situações, e não apenas realizam a definição/rotulação e identificação de situações [21]. Alguns desses relacionamentos são descritos a seguir [153].

- **Generalização**: uma situação pode ser considerada mais geral do que uma outra e, dessa forma, a ocorrência de uma situação mais específica (a situação implica na ocorrência da situação mais geral (a situação formadora). Por exemplo, a situação "assistindo televisão" é considerada mais específica do que a situação "entretenimento";

- **Composição**: uma situação pode ser decomposta dentro de um conjunto de situações menores. Por exemplo, uma situação "cozinhando" é composta de uma situação "usando o fogão" e uma outra "organizando ingredientes de comida";

- **Dependência**: uma situação depende de uma outra situação se sua ocorrência for determinada pela ocorrência desta segunda;

- **Contradição**: duas situações podem ser consideradas mutualmente exclusivas se elas não podem ocorrerem em um mesmo instante de tempo, no mesmo lugar com o mesmo sujeito. Por exemplo, um usuário não pode estar nas situações "cozinhando" e "dormindo" ao mesmo tempo;

- **Sequencia temporal**: uma situação pode ocorrer antes, depois ou mesmo intervalada com uma outra situação. Por exemplo, a situação "tomar remédio" deve ser realizada antes da situação "jantando".

Além desses relacionamentos, algumas técnicas dão suporte para a identificação de situações nos seguintes casos:

- **Múltiplos usuários**: identificação de situações em que estão sendo analisados dados de contexto de vários usuários simultaneamente e as situações de interesse

estão relacionadas as atividades que eles estão fazendo colaborativamente ou concorrentemente em conjunto e seus significados semântico. Por exemplo, pessoas em uma sala realizando uma reunião;

- **Imperfeição**: identificação de situações com o uso de dados de contexto que podem sofrer com falta de qualidade (ver seção 3.3), tal como incompletude, ausência, imprecisão, problemas de acurácia, e serem desatualizados.

3.6 Lógica Nebulosa

A Lógica Nebulosa (do inglês, *Fuzzy Logic*) é uma das técnicas usadas na concepção de soluções para identificação de situações mais adequadas para tratar informações de contexto incertas [5], a qual foi escolhida para ser usada na solução proposta nesta tese. A Lógica Nebulosa [157] tem como principal objetivo a modelagem computacional do raciocínio humano, impreciso, ambíguo, vago e qualitativo. Através da lógica nebulosa é possível representar, por exemplo, a seguinte expressão: *Embora o transformador esteja* ***um pouco*** *carregado, pode-se utilizá-lo por* ***um tempo***. Nesse exemplo, os termos *um pouco* e *um tempo* são conhecimentos humanos imprecisos e, dessa forma, podem ser representados em um sistema computacional que utilize lógica nebulosa. Como os sistemas de inferência nebulosa são potencialmente capazes de expressar e manipular informações qualitativas, especialistas de um domínio podem mapear a sua experiência e o seu processo de tomada de decisão de forma linguística (qualitativa).

Conjuntos nebulosos são caracterizados por funções de pertinência (*membership functions*) que tentam descrever a vagueza e ambiguidade. Essas funções atribuem para cada elemento em um universo de discurso (ou um domínio) um grau de pertinência (*degree of membership*) ou valor de verdade que vai de 0 (exclusão completa) a 1 (pertencer completo – *full belongingness*) [155]. Um conjunto nebuloso contém elementos que tem vários graus de pertinência e, porque valores de pertinência não precisam ser completos (não serem 1), podem também serem membros de outros conjuntos nebulosos no mesmo domínio com graus de pertinência diferentes ou mesmo iguais.

As variáveis linguísticas têm valores que não são números, mas são palavras (por exemplo, “distante”, “lerdo”, “médio”) ou sentenças (por exemplo, “razoavelmente alto”, “não pequeno”, e “muito vermelho”) expressados em uma linguagem natural ou artificial [156]. As variáveis linguísticas podem representar o conhecimento humano qualitativo e impreciso e são usadas para rotular conjuntos nebulosos [118]. A lógica nebulosa permite o raciocínio aproximado para conclusões que vão de falso a verdadeiro, ou seja, parcialmente verdadeiro (ou parcialmente falso).

A seguir é apresentada a Figura 3.3, a qual mostra uma representação na forma de conjuntos da altura de uma pessoa comparando a lógica convencional (à esquerda – conjuntos *crisp*) e lógica nebulosa (à direita – conjuntos nebulosos).

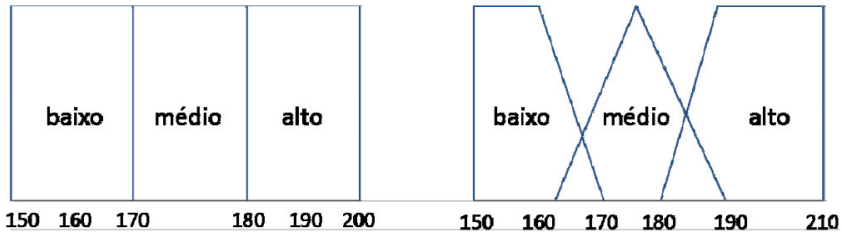

Figura 3.3: Conjuntos *crisp* e nebulosos da altura de uma pessoa.

Considerando a Figura 3.3, dado dois valores x_1 = 1,69 e x_2 = 1,71, na lógica clássica os dois elementos pertencem a classes (conjuntos *crisp*) diferentes: x_1 pertence à classe baixo e x_2 à classe médio. Isso pode não expressar a realidade, pois é difícil afirmar que uma pessoa com 1,69m e outra com 1,71m pertencem a classes de alturas diferentes. Na lógica nebulosa o x_1 e o x_2 tem graus de pertinências aos conjuntos nebulosos definidos, que podem variar de 0 a 1 (parcialmente falso a parcialmente verdadeiro). Ou seja, é possível expressar utilizando lógica nebulosa a altura de uma pessoa considerado-a parcialmente da classe médio e parcialmente da classe alto.

Considerando um conjunto hipotético A e um elemento x, a lógica clássica é representada pela seguinte função:

$$f(x) = \begin{cases} 1 & \text{se, e somente se, } x \in A \\ 0 & \text{se, e somente se, } x \notin A \end{cases}$$

Da mesma forma, considerando um conjunto nebuloso hipotético B e um elemento y, a lógica nebulosa é representada pela seguinte função:

$$\mu(y) = \begin{cases} 1 & \text{se, e somente se, } y \in B \\ 0 & \text{se, e somente se, } y \notin B \\ 0 < \mu(y) < 1 & \text{se } y \text{ pertence parcialmente a } B \end{cases}$$

Um sistema de inferência nebuloso é fundamentado em regras de produção linguísticas do tipo se/então, uma forma dedutiva para expressar inferência [111]. Ou seja, uma inferência nebulosa é a aplicação de estruturas de decisão, chamadas de regras nebulosas, utilizando valores lógicos nebulosos e conectivos lógicos. Regras nebulosas podem ser criadas utilizando os seguintes operadores: Negação ($\neg$), E ($\wedge$), OU ($\vee$), Implica ($\Rightarrow$) e Se e somente se ($\Leftrightarrow$).

Sistemas de inferência nebulosos habilitam especialistas humanos em um domínio para mapear sua experiência e seu processo de tomada de decisão para sistemas computacionais usando regras nebulosas. Os sistemas de inferência nebulosos têm seu funcionamento baseado em três etapas: *fuzzificação*, procedimentos de inferência e *defuzzificação*. A *fuzzificação* é um mapeamento das entradas numéricas a conjuntos nebulosos. Então a fase de *fuzzificação* é responsável pelo mapeamento de informação quantitativa para informação qualitativa. O procedimento de inferência nebuloso é responsável por, a partir dos valores de entrada *fuzzificados*, inferir o valor de saída *fuzzificado* correspondente. A *defuzzificação* é usada para associar um valor numérico ao conjunto nebuloso de saída, o qual é obtido do procedimento de inferência nebulosa. Portanto, a fase de *defuzzificação* mapeia informação qualitativa inferida para informação quantitativa.

3.7 Conclusão

Nesse capítulo foram vistos primeiramente os conceitos de situação, ciência de situação e computação situacional. Em seguida foi apresentada a fase de processamento do ciclo de gerenciamento de informações contextuais, onde ficou evidente a necessidade por dados de contexto com qualidade, conteúdo que foi abordado na sequência. Também apresentou-se a fase de distribuição de dados de contexto, em que foi dado ênfase ao *middleware* SDDL. Além disso, foram listadas e classificadas as principais técnicas usadas para identificação de situação, sendo que ao final foi detalhada a técnica baseada em especificação Lógica Nebulosa. Todo o

conteúdo abordado nesse capítulo é fundamental para o entendimento da solução proposta por essa tese de doutorado.

4 Trabalhos Relacionados

Muitos trabalhos têm proposto soluções para problemas de segurança e privacidade em RSMs [107, 132], mas poucos têm investigado as características dinâmicas e contextuais das configurações de privacidade. Nesse capítulo são descritos os trabalhos relacionados a solução proposta nessa tese de doutorado, os quais são classificados em seis categorias, vistas a seguir na taxonomia apresentada na Figura 4.1.

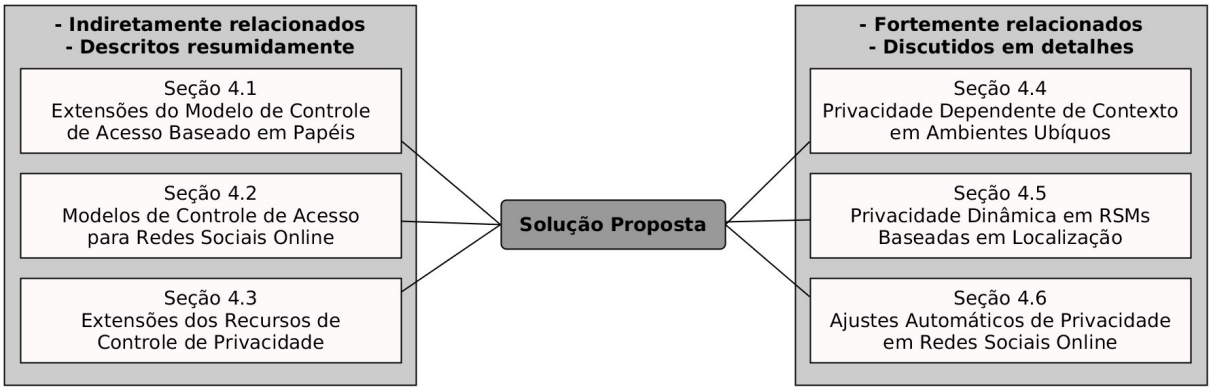

Figura 4.1: Taxonomia dos Trabalhos Relacionados.

Nas três primeiras categorias (lado esquerdo da Figura 4.1) os trabalhos são resumidamente descritos, devido terem alguma relação com a proposta dessa tese, mas não poderem ser comparados diretamente com ela. Inicialmente, na primeira categoria, são apresentadas extensões do modelo de controle de acesso baseado em papéis, os quais propõem um uso diversificado de restrições de contexto. As restrições de contexto são permissões que consideram alguma informação contextual para dar (ou negar) permissão para realizar alguma ação em algum dado. Na sequência são descritos modelos de controle de acesso especificamente propostos para redes sociais online. Em seguida, na terceira categoria, são apresentadas soluções que propõem extensões dos recursos de controle de privacidade disponibilizados pelos provedores de serviços de RSMs.

Nas outras três categorias (lado direito da Figura 4.1) os trabalhos são fortemente relacionados e apresentados em detalhes. Na quarta categoria são mostrados trabalhos que propõem mecanismos de privacidade dependente de

contexto para ambientes ubíquos/pervasivos. Na quinta categoria são descritas propostas que visam tornar dinâmica a configuração de privacidade em RSMs baseadas em localização. A última categoria apresenta as soluções que objetivam automatizar as configurações de privacidade de redes sociais online. Ao final desse capítulo é feita uma análise comparativa entre os trabalhos mais fortemente relacionados, ou seja, os trabalhos destas três últimas categorias.

4.1 Extensões do Modelo de Controle de Acesso Baseado em Papéis

O modelo de Controle de Acesso Baseado em Papéis (*Role-Based Access Control* (RBAC)) [50, 122] tem seu funcionamento baseado na definição de papéis, ou perfis. Estes papéis representam níveis funcionais hierárquicos dentro de uma organização (por exemplo, empresa, hospital, universidade). Cada usuário é associado a um ou mais papéis e esses, por sua vez, estão relacionados a permissões, que definem o tipo de acesso (por exemplo, leitura, execução, escrita) permitido aos recursos do sistema. Dessa forma, o modelo RBAC possui quatro tipos de entidades: usuários, papéis, permissões e sessões. Um usuário neste modelo é uma pessoa, ou processo agindo em nome dela. Um papel é uma função ou cargo dentro da organização que possui uma semântica que representa a autoridade e a responsabilidade conferidas aos membros desse papel. Uma permissão é um direito específico de acesso a um ou mais objetos no sistema. Uma sessão corresponde a um usuário acessando o sistema com um determinado conjunto de papéis ativos.

Alguns trabalhos encontrados na literatura propõem extensões para o modelo RBAC e que, ao mesmo tempo, utilizam dados de contexto como base para tomada de decisão para modificar dinamicamente as permissões de acesso. Essas propostas são conhecidas como Controle de Acesso e Autenticação Dependente de Contexto – *Context-dependent Authentication and Access Control* (CDAC) [78]. A partir de 2001 estes trabalhos vêm sendo desenvolvidos, possibilitando a criação de restrições de acesso com base em informações do objeto requisitado [106], tais como a data de criação, o tamanho e o tipo do objeto (por exemplo, MP3, JPEG, programa executável), bem como baseado no tempo [19] (por exemplo, dia da semana, hora do dia) e também

possibilitando determinar o tempo de ativação (validade) de um papel [76]. No trabalho desenvolvido em [20] os autores propõem o GEO-RBAC, uma extensão em que os papéis são ativados de acordo com a posição geográfica dos usuários.

O trabalho desenvolvido em [84] propõe o modelo CA-RBAC (*Context-Aware RBAC*), o qual utiliza dados de contexto de tempo e localização para restringir acesso a dados pessoais no sistema. Ele ainda ativa determinados papéis apenas quando um usuário específico já estiver inserido em um outro papel, criando a noção de extensão de papeis. Ou seja, além das restrições de localização e tempo, um usuário precisa estar previamente inserido em um papel A para poder obter permissões de um papel B. A vantagem disto é poder criar dependências entre papeis, os quais podem ser administrados por usuários diferentes. Uma outra extensão do modelo RBAC é o trabalho desenvolvido em [51, 52], em que sua principal contribuição é levar em consideração ao mesmo tempo informações de contexto do dono do recurso, do usuário requisitante e também do próprio recurso que está sendo requisitado. O contexto do recurso é qualquer informação que pode ser usada para caracterizar a situação na qual o objeto requisitado foi criado ou seu estado atual (por exemplo, o local em que uma foto foi tirada).

4.2 Modelos de Controle de Acesso para Reses Sociais Online

Uma grande quantidade de modelos de controle de acesso para sistemas sociais são propostos na literatura [123]. Isso ocorre porque redes sociais populares incorporam mecanismos limitados para controlar acesso a informações pessoais. Considerando estas limitações, os modelos de controle de acesso propostos são desenvolvidos com novos recursos ou tipos de restrições que objetivam garantir o controle de informações pessoais nestes sistemas.

Alguns modelos propõem o uso de ontologias como mecanismo para possibilitar que os usuários tenham mais expressividade com políticas de controle de acesso de granularidade fina [29, 100, 101]. Outros modelos propostos consideram informações contextuais de relacionamentos entre usuários como base para expressar as chamadas políticas relacionais [54, 55]. Essas políticas são expressadas em uma

linguagem específica para permitir o uso de restrições de contexto específicas da rede social, tais como: o tipo de relacionamento entre contatos (por exemplo, se eles são membros família, amigos, ou têm uma relação profissional), a distância lógica entre os contatos no grafo da rede social, a direção (por exemplo, o relacionamento de pai para filho é diferente do oposto, de filho para pai), e os relacionamentos que contatos têm em comum.

À medida que novos recursos de sociabilidade são providos para os usuários, tais como o *tagging* e as aplicações de terceiros, mais capacidades são requeridas dos modelos de controle de acesso. Hu et al. [70] propõem um modelo para controlar acesso a conteúdos que são associados a múltiplos usuários (por exemplo, uma foto na qual aparecem várias pessoas). Esse modelo possibilita um gerenciamento colaborativo (chamado em inglês de *multiparty*) de controle de acesso, em que permissões são gerenciadas pelos usuários que estão relacionados ao conteúdo postado. Dessa forma, os usuários podem também definir permissões de acesso ao conteúdo que eles são marcados (*tagged*) por contatos. No sentido de controlar acesso a partir de aplicações de terceiros, Shehab et al. [127] propõem um modelo que permite aos usuários especificar quais informações pessoais podem ser acessadas a partir desse tipo de aplicação e, ao mesmo tempo, permite determinar o nível de especificidade na qual as informações podem ser acessadas.

4.3 Extensões dos Recursos de Controle de Privacidade

Idealmente, RSMs devem ser projetadas desde o seu início levando-se em consideração recursos de suporte à privacidade, tal como o Safebook [37], o qual consiste de um sistema social descentralizado que explora relacionamentos de confiança que são parte das redes sociais da vida real para prover mecanismos de privacidade. Entretanto, como provedores de RSMs não implementam mecanismos de privacidade suficientes para atender os requisitos de seus usuários, muitas soluções estão sendo propostas na literatura que proveem extensões dos recursos de controle de privacidade já existentes. Elas propõem recursos de privacidade desenvolvidos em uma camada sobre a infraestrutura do provedor de serviço como reforço adicional para garantir privacidade aos usuários, o que é uma abordagem similar a proposta dessa tese.

Algumas das extensões dos recursos de controle de privacidade são implementadas como aplicações de terceiros, tais como o FlyByNight [95] e o Persona [10]. Outras soluções são disponibilizadas como extensões ou *plug-ins* para navegadores *Web*, tais como o NOYB [66], o FaceCloak [96] e o Scramble [15]. Essas abordagens protegem a privacidade do usuário publicando informações encriptadas ou falsas, não provendo as reais informações do usuário para o provedor de serviços, aplicações de terceiros, e contatos não desejados.

Existem também algumas propostas que objetivam prover canais de comunicação privados entre contatos fora do sistema social, mas requerendo relacionamentos sociais estabelecidos dentro do sistema para criar tais canais. Sorniotti e Molva [130] seguem essa ideia e propõem o uso de Grupos de Interesse Secretos (*Secret Interest Groups* - SIGs), que são grupos criados para troca de informações privadas entre contatos através de um servidor externo. Uma outra contribuição proposta nessa mesma linha é o conceito de Rede Social Privada Virtual (*Virtual Private Social Network* - VPSN) [34], que é análogo às bem conhecidas redes privadas virtuais (VPNs) usadas em redes de computadores. Como uma extensão de privacidade, uma VPSN tem de ser integrada com a arquitetura e a infraestrutura de um já existente sistema social [35]. Além disso, uma VPSN é escondida do provedor de serviço e para outros usuários fora da VPSN. O FaceVPSN [34,35] é uma implementação de VPSN em forma de uma extensão de navegador proposta para proteger informações de usuários do Facebook.

4.4 Privacidade Dependente de Contexto em Ambientes Ubíquos

Privacidade dependente de contexto é o termo utilizado para qualquer mecanismo de configuração de privacidade em ambientes ubíquos/pervasivos que possibilita utilizar restrições de contexto. Como se trata desses ambientes, a obtenção dos dados de contexto não é sempre feita utilizando sensores embutidos no dispositivo móvel, mas também sensores pervasivos espalhados no ambiente. Todos os trabalhos descritos em detalhes nessa categoria têm como propósito, e também critério de

categorização, a adaptação dinâmica com a utilização de dados de contexto do processo de controle de acesso em ambientes ubíquos/pervasivos.

Muitos trabalhos encontrados na literatura propuseram na década passada soluções para privacidade dependente de contexto [36,43,73,105,150] e também outros mais recentes que ainda estão em fase de desenvolvimento [81, 124, 125]. Adotou-se como critérios de escolha dos trabalhos descritos a seguir a data de publicação, optando-se pelos mais recentes, e também a maturidade do trabalho, optando-se pela não inclusão de trabalhos que ainda estão em desenvolvimento.

4.4.1 *Context-Dependent Access Control for Contextual Information*

Groba et al. [64] propõem um mecanismo para controlar acesso aos próprios dados de contexto em um ambiente de computação ubíqua. Este mecanismo possui dois principais recursos. O primeiro é o uso de uma abordagem centrada no dono da informação, a qual possibilita cada usuário determinar para quem seu dado de contexto é propagado. Dessa forma, o próprio usuário (e não o administrador do sistema) define os membros que fazem parte de papéis que têm permissão de acesso aos dados de contexto, substituindo o modelo em que os papéis são definidos de forma centralizada e aplicados a todo o sistema. No segundo, o mecanismo utiliza as informações de contexto para ajustar dinamicamente as permissões de acesso a elas mesmas.

Nesse mecanismo o dono das informações pessoais, incluindo os dados de contexto, é considerado o administrador da segurança, sendo responsável por criar individualmente suas próprias políticas. Essa criação de políticas inclui: a definição de papéis, a atribuição das permissões para cada papel em forma de regras de acesso dependentes de contexto (*context-dependent access rules* – CDAR), e a atribuição de papéis para cada potencial usuário requisitante. As regras de acesso dependentes de contexto definem a condição para uma permissão ser considerada válida em um certo papel.

Estas CDARs são organizadas como segue. A regra é composta por uma quadrupla contendo o nome do papel, o modo de acesso, o objeto requisitado e a restrição de contexto *access rule:=(role, mode, object, context constraint)*. O modo de acesso determina as permissões de um requisitante. O objeto requisitado pode ser um dado

pessoal ou um dado de contexto. A restrição de contexto é uma conjunção de uma ou mais condições *context constraint* := $condition_1 \cup$ ... $\cup condition_n$. Uma condição é composta por uma disjunção de um ou mais *statements condition* := $statement_1 \cap$ ... $\cap statement_n$. Um *statement* consiste de um atributo de contexto, um operador e um valor de referência. O operador pode ser uma comparação matemática ($\leq$, $\geq$, $\neq$, $=$) ou um conjunto de valores definidos pelo usuário para ser considerado verdadeiro (ou seja, *within*) *statement := (context attribute operation reference value)*. Segue um exemplo de uma CDAR em que um requisitante que faz parte do papel "professor" tem permissão de leitura da informação de localização quando a hora do dia estiver entre 8:00 e 18:00:

access rule := (professor, read, location, context constraint)
context constraint := $condition_1$
$condition_1$:= $statement_1 \cap statement_2$
$statement_1$:= *(time* $\geq$ *8:00)*
$statement_2$:= *(time* $\leq$ *18:00)*

As regras funcionam utilizando uma abordagem de lista branca, em que por padrão todos os acessos são negados, dando permissão apenas quando uma requisição é liberada por alguma regra. Dessa forma, uma regra é uma permissão explícita que é válida somente se o papel, o objeto requisitado e o modo de acesso combinam com os parâmetros passados pelo usuário requisitante e se as restrições de contexto avaliadas são verdadeiras.

4.4.2 *A Comprehensive Approach for Context-dependent Privacy Management*

A abordagem proposta por Franz et al. [57] adota o conceito de *Privacy-Enhancing Identity Management* (PIM), usando as chamadas identidades parciais. Estas identidades permitem delimitar as informações pessoais que podem ser acessadas por determinados requisitantes. Dessa forma, é possível criar identidades diferentes de um usuário para determinados requisitantes ou grupo de requisitantes. Cada identidade é nomeada pelo usuário através de um pseudônimo, ao invés de nomes reais. Como um usuário possui diferentes identidades parciais, o acesso a suas informações pessoais é restringido de maneira diferente a cada um delas.

A abordagem proposta nesse trabalho combina o uso de PIM com o modelo RBAC e funciona da seguinte maneira: um papel do modelo RBAC é utilizado pelos requisitantes de uma informação pessoal disponível por uma determinada identidade parcial de um usuário, ou seja, uma identidade parcial é atrelada a um papel. Portanto, membros de um determinado papel podem acessar um conteúdo pessoal de um usuário apenas se este dado estiver disponível pela identidade parcial atrelada a este papel.

Nessa solução as informações de contexto são utilizadas para sugerir ao usuário qual a melhor identidade parcial a ser usada em uma ação. Esta ação pode ser, por exemplo, a requisição de acesso do usuário a um serviço ubíquo disponível no ambiente, como um tocador de música. A sugestão é feita através de regras as quais são configuradas previamente pelo usuário e que possui restrições de contexto.

Uma característica desse trabalho é o desenvolvimento de quatro tipos de provedores de contexto, criados para diferentes tipos de informação. Eles aumentam a diversidade de dados de contexto que podem ser utilizados para a criação de restrições de contexto. São eles:

- **Contexto interno à aplicação**. Informações relacionadas a eventos monitorados dentro da aplicação, ou seja, uma ação que o usuário tem realizado (por exemplo, a execução de um determinado componente da aplicação);
- **Contexto relacionado ao histórico**. Informações adquiridas a partir do histórico de ações realizadas pelo usuário, por exemplo, a quantidade e o tipo de ações;
- **Contexto independente da aplicação**. Informações que não possuem relação com a aplicação, por exemplo, dados obtidos de sensores, tais como contexto de tempo e localização;
- **Contexto relacionado ao requisitante**. Informações relacionadas ao requisitante, por exemplo, a identidade parcial utilizada pelo requisitante.

4.4.3 CPE

Blount et al., em [24], apresentam o projeto e implementação do *Context Privacy Engine* (CPE), uma extensão das listas de controle de acesso (*Access Control List*

– ACL) a qual utiliza políticas dependentes de contexto. O CPE é projetado como um mecanismo de avaliação de políticas, em que um cliente requisita uma informação pessoal de um usuário e regras com restrições de contexto são verificadas. Uma política dependente de contexto no CPE possui os seguintes campos:

- Sujeito: um usuário ou grupo de usuários cujas informações pessoais são protegidas pela política;
- Informações: os dados do sujeito para o qual a política controla o acesso;
- Requisitante: um usuário individual ou grupo de usuários para quem a política é aplicada quando a informação é requisitada;
- Aplicação: as aplicações pelas quais as informações podem ser acessadas;
- Contexto: um conjunto de restrições de contexto que devem ser satisfeitas para que a política permita acesso;
- Nível de Política: nível hierárquico de políticas, utilizado para permitir a criação de prioridades entre políticas;
- *Release*: a decisão da política, permitindo (*grant*) ou negando (*deny*) o acesso.

Segue um exemplo de política de privacidade no CPE: o Presidente (sujeito) permite (*release*) a equipe de profissionais da casa branca (requisitantes) saberem sua localização (informação) quando ambos estiverem localizados na casa branca (contexto).

Uma política utiliza dois campos que podem ser confundidos: a aplicação e o requisitante. Isso é utilizado para prover flexibilidade às políticas, de forma que informações podem ser usadas por uma aplicação para executar um serviço sem necessariamente exibi-las ao usuário requisitante. Essa é uma das contribuições desse trabalho. Uma outra contribuição é o critério adotado para resolução de conflitos entre políticas, o nível de política. Quando políticas entram em conflito, o CPE verifica qual é o nível de prioridade das políticas conflitantes e escolhe a que possui maior nível. Caso o nível seja o mesmo, se alguma das políticas conflitantes nega acesso, essa política é adotada.

Um outro diferencial deste trabalho é a preocupação com a ausência do dado de contexto utilizado para a criação de uma política. Quando isso ocorre em políticas que possuem o *release* "deny", elas são aplicadas da mesma forma, pois garantem que não haja acesso indevido. No entanto, quando ocorre em políticas que possuem o *release* "grant", a política é considerada inaplicável. Essa abordagem garante que negações de permissões se sobreponham a concessões na ausência de dados de contexto.

4.4.4 CPPL

Behrooz e Devlic, em [16], desenvolvem uma Linguagem de Política de Privacidade Ciente de Contexto (*Context-aware Privacy Policy Language* - CPPL) que habilita usuários móveis a controlar quem pode acessar suas informações de contexto utilizando regras dependentes de contexto. A linguagem proposta neste trabalho estende o padrão OASIS *eXtensible Access Control Markup Language* (XACML)[1] para a definição de restrições de contexto.

A linguagem desenvolvida por este trabalho adota o conceito de situação, a qual é caracterizada por condições de contexto. Assim, para uma situação ser considerada válida, todas as condições de contexto devem ser verdadeiras. Quando uma situação é identificada, apenas as regras de privacidade para ela são selecionadas, limitando a quantidade de regras de controle de acesso a serem avaliadas quando um dado é requisitado. Ou seja, quando a situação do usuário muda, as regras de controle de acesso são atualizadas para aquela nova situação. Então quando ocorre uma requisição a uma informação, apenas as regras da situação mais atual são verificadas.

Uma outra contribuição deste trabalho é a utilização de uma restrição de contexto chamada de Relacionamento Social. Esta restrição permite que usuários possam definir condições baseadas na relação social que eles têm com os requisitantes. Por exemplo, Bob é marido de Alice e isso é representado por um campo configurado na aplicação. Bob ao criar uma restrição de contexto pode informar que, quando o requisitante é sua esposa, determinadas regras de controle de acesso são aplicáveis.

[1] `https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml`

4.5 Privacidade Dinâmica em Redes Sociais Móveis Baseadas em Localização

Alguns trabalhos vêm propondo mecanismos que tornam dinâmica a configuração de privacidade em aplicações sociais móveis baseadas em localização (RSMs de rastreamento de localização - *tracking location*). Neste tipo de aplicação, um contato realiza a requisição da informação de localização do usuário. Embora estes trabalhos estejam mais focados em RSMs baseadas em localização, as configurações de privacidade propostas por eles permitem que os usuários expressem seus desejos dinâmicos de privacidade. Eles realizaram testes e avaliações com usuários utilizando suas propostas, tanto em laboratório quanto em campo, e suas conclusões reforçam que usuários de RSMs necessitam de recursos que os possibilitem expressar seus desejos dinâmicos de privacidade.

4.5.1 PICOS

O trabalho apresentado em [138] foi desenvolvido junto ao projeto PICOS[2]. Os autores realizaram um levantamento de requisitos com três grupos de usuários: pescadores recreativos, motoristas de táxi independentes e jogadores de games online. Para isso eles utilizaram entrevistas, questionários e técnicas de observação. Através desse levantamento eles identificaram 48 requisitos de privacidade para RSMs. Além disso, eles chegaram a uma conclusão, e por isso defendem, que existe uma dificuldade em identificar requisitos de privacidade genéricos aplicáveis a qualquer rede social. Isso ocorre devido ao fato de que cada tipo de grupo de usuários possui características e necessidades próprias.

Em seguida os autores desenvolveram um *framework* também chamado de PICOS, ilustrado na Figura 4.2, com recursos para atender uma parte dos requisitos identificados: gerenciamento de identidades parciais, escolha de lugares privados, um suporte de ajuda aos usuários para configurações de suas políticas de privacidade, e ofuscação da informação de localização. O gerenciamento de identidades parciais funciona igualmente ao recurso provido no trabalho desenvolvido em [57], explicado anteriormente na seção 4.4.2. A funcionalidade de lugares privados permite que

[2] `http://www.picos-project.eu/`

usuários definam coordenadas e o raio a partir delas (definidas em metros) com controles de acesso mais restritos. Em lugares privados o usuário define quem pode ter acesso a sua localização, possibilitando, inclusive, que nenhum contato tenha acesso a ela.

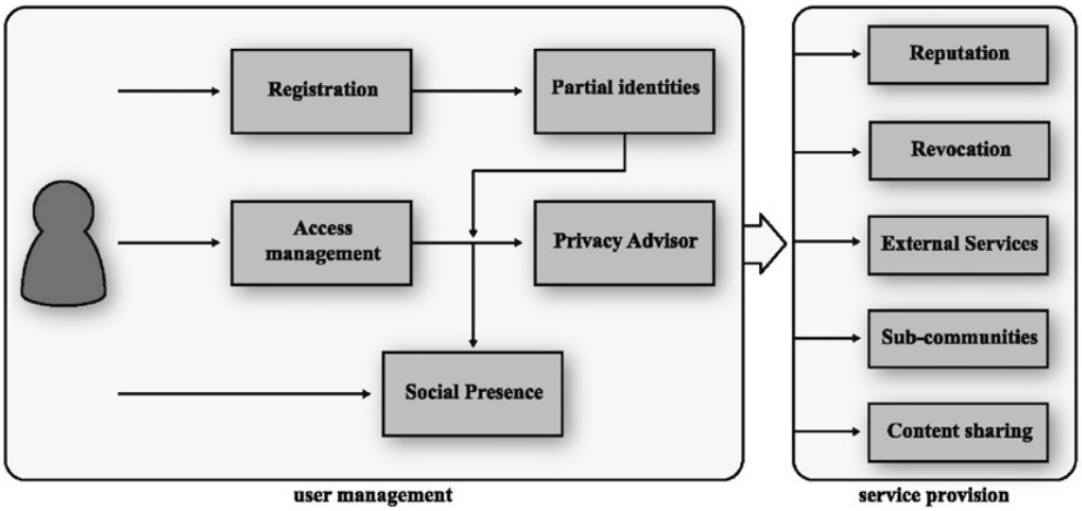

Figura 4.2: *Framework* PICOS [138].

O suporte de ajuda serve como um guia que provê dicas e informações adicionais ao usuário em relação às suas configurações de privacidade. A ofuscação da informação de localização ocorre no processo de compartilhamento, quando as reais coordenadas são modificadas de maneira que o requisitante não saiba o local exato em que o usuário está, pois as coordenadas divulgadas são apenas de sua proximidade.

4.5.2 PeopleFinder e Locaccino

O trabalho apresentado em [120] por um grupo de pesquisa da *Carnegie Mellon University* descreve uma aplicação chamada PeopleFinder, a qual permite a usuários de dispositivos móveis (*smartphones* e notebooks) tornarem disponível suas localizações para seus contatos. Basicamente, os usuários da aplicação a utilizam para consultar as localizações de seus contatos, as quais são exibidas em um mapa. Uma versão mais recente desta aplicação é o Locaccino[3] [136].

Para obtenção das coordenadas geográficas o PeopleFinder utiliza várias tecnologias, tais como GPS, AGPS, triangulação GSM e Wi-Fi para ambientes *indoor*. Um outro ponto importante da implementação desta aplicação é que as informações

[3] `http://locaccino.org/`

de localização não são consultadas diretamente na aplicação cliente do usuário, ao invés disso, elas ficam armazenadas em um lado servidor. Quando a localização de um usuário muda, sua aplicação cliente a atualiza junto ao servidor. Um outro recurso desta aplicação é a criação de notificações ao usuário, a fim de avisá-lo quando e por quem sua localização é requisitada.

Para que uma localização seja vista é necessário que a política de privacidade configurada pelo usuário dono da localização conceda acesso. Portanto, esta aplicação de acesso a localização de contatos funciona utilizando políticas expressadas pelos usuários, representadas por um conjunto de regras de controle de acesso. Como mostrado na Figura 4.3, um usuário pode definir regras em que ele permite acesso à sua localização para contatos individuais ou grupo de contatos. Dessa forma, a aplicação possibilita o gerenciamento desses grupos.

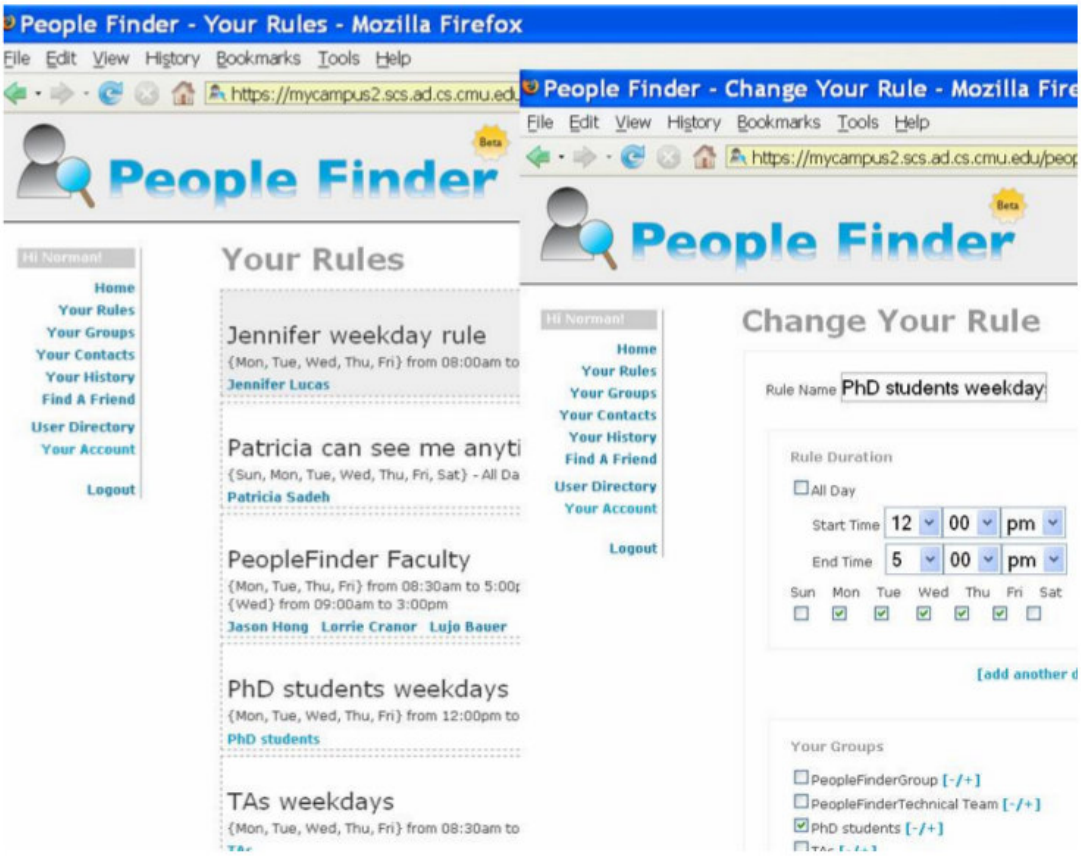

Figura 4.3: Configuração de Política de Privacidade no PeopleFinder [120].

Cada regra pode incluir restrições de tempo, incluindo dias da semana e hora do dia. Além disso, as regras são criadas com restrições de localização, possibilitando ao usuário definir lugares em que ele se encontra e não gostaria que sua localização fosse acessada. Esses lugares são especificados em retângulos no mapa,

como pode ser visto na Figura 4.4. Para evitar conflitos entre as regras, somente é possível criar regras para concessão de acesso. Por exemplo, um usuário pode criar a regra "Maria pode ver minha localização entre 9 e 17 horas", mas não pode especificar "Colegas de trabalho não podem ver minha localização aos finais de semana".

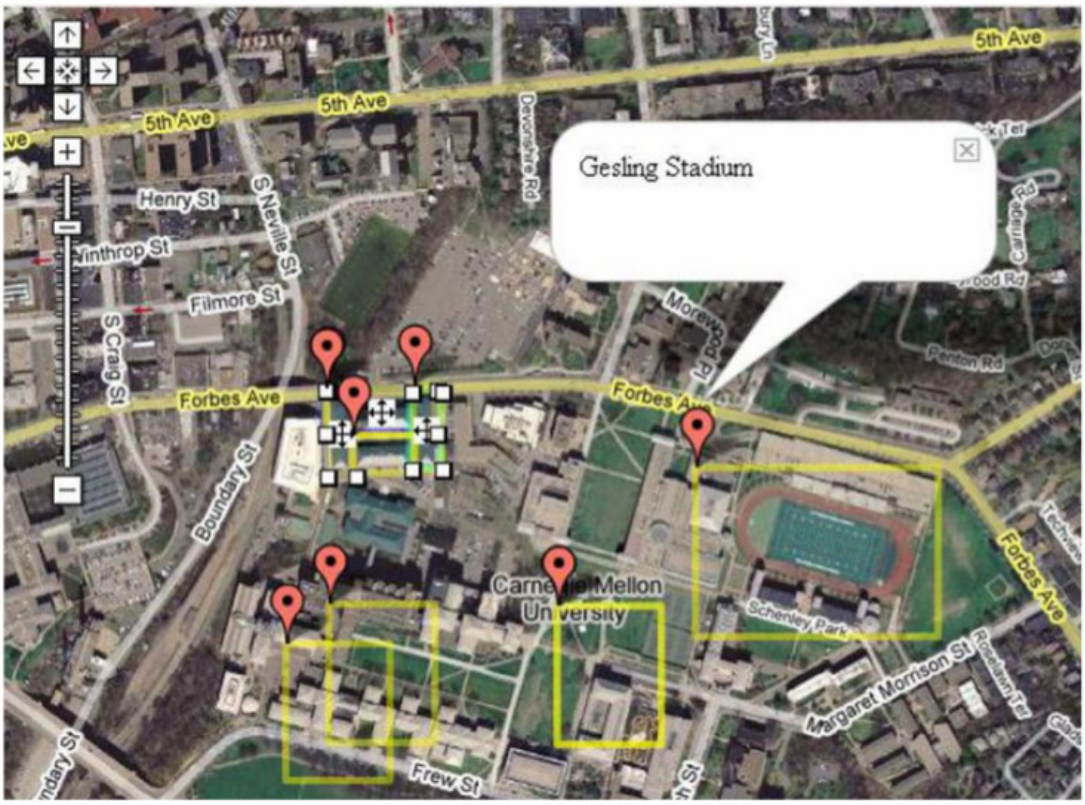

Figura 4.4: Privacidade com Restrição de Localização no PeopleFinder [120].

Ao propor a aplicação PeopleFinder, os autores deste trabalho objetivam melhorar o entendimento das atitudes e comportamentos das pessoas em relação à sua privacidade e como elas interagem com a aplicação. Dessa forma, eles buscam explorar tecnologias que permitem aos usuários definir mais eficientemente e efetivamente suas preferências de privacidade. Para isso, eles analisaram o impacto dessa aplicação realizando testes em laboratório com 19 participantes e em campo com 60 participantes. Os resultados confirmaram que as pessoas estão preocupadas com problemas de vazamento de privacidade associadas com suas localizações. Eles mostraram também que preferências de privacidade tendem a ser complexas e dependem de uma variedade de atributos contextuais.

Um outro resultado interessante comprovado através desta pesquisa é que mesmo os usuários estando preocupados com sua privacidade, eles não conseguem expressar suas reais preferências (o chamado paradoxo de privacidade). A acurácia das

políticas expressadas por eles não condiz com seus desejos reais e apenas com o passar do tempo de uso da aplicação é que elas melhoram e conseguem atender seus desejos de privacidade. Dessa forma, eles implementaram também técnicas de aprendizagem de máquina para ajudar usuários a melhor especificar as regras de controle de acesso de suas políticas de privacidade. Os resultados obtidos através dos testes com essas técnicas mostraram que elas podem ser efetivas em ajudar a melhorar a acurácia das regras em relação aos desejos dos usuários e, portanto, os resultados iniciais sugeriram que elas são bastante promissoras.

Um trabalho publicado pelo mesmo grupo de pesquisa em [18] utilizando o PeopleFinder avalia vários tipos de configurações de privacidade em vários níveis de complexidade, desde simples listas brancas (lista de usuários que podem acessar determinado conteúdo) até regras mais complexas com restrições de contexto. Os resultados mostram que tipos de configurações de privacidade mais complexas são necessárias para atender os reais desejos de privacidade de localização dos usuários. No entanto, eles mostram que estas configurações não vêm sem um custo e, portanto, configurações mais complexas implicam em esforço adicional ao usuário.

O mesmo grupo de pesquisa propõe abordagens interessantes para configurações de privacidade em RSMs, tais como o uso de *feedback* [137] e o reuso de perfis de privacidade [116, 146]. O recurso de *feedback* possibilita fornecer um retorno ao usuário de quem está acessando seus dados pessoais e, dessa forma, permite a ele o refinamento de suas configurações a fim de atender seus reais desejos de privacidade. Um perfil de privacidade é um conjunto de configurações de privacidade que são utilizados por usuários. O reuso de perfis de privacidade possibilita usuários escolherem qual perfil já definido se ajusta mais à sua necessidade, não se preocupando em configurar manualmente e individualmente suas políticas.

Um trabalho mais recente deste grupo de pesquisa publicado em [90] estuda e compara os desejos de privacidade de usuários dos Estados Unidos e China. Os resultados mostram que o desejo de compartilhar a localização dos usuários de ambas nacionalidades depende significativamente de por quem ela é acessada. Ou seja, uma principal preocupação dos usuários é saber qual contato da rede social deseja acessar sua localização e poder limitar acesso de acordo com o requisitante. No entanto, muitos resultados apontaram grandes diferenças entre as duas nacionalidades, dentre elas o fato de usuários americanos se preocuparem mais em compartilhar sua localização

quando estão em casa do que quando estão no trabalho, diferentemente dos chineses, que se preocupam em ambos casos. A conclusão do trabalho sugere que aplicações sociais móveis baseadas em localização devem prover mecanismos flexíveis para usuários configurarem suas políticas, pois inclusive aspectos culturais relacionados à nacionalidade dos usuários influencia nos desejos de privacidade.

4.5.3 SPISM

Bilogrevic et al., em [23], descrevem o SPISM, um sistema que permite usuários compartilharem com contatos a sua localização, sua atividade e também a informação de quais dispositivos estão co-localizados. A localização é obtida através de GPS e sistema *indoor* com uso de conexões de redes locais sem fio (trilateração WiFi) e a atividade do usuário é obtida através de sua agenda de tarefas. Já os usuários do sistema co-localizados são reconhecidos através de varreduras periódicas utilizando as interfaces de rede sem fio do dispositivo (WiFi e Bluetooth), à procura dos endereços MAC dos dispositivos próximos. Neste último caso, cada usuário ao utilizar o sistema deve se registrar, informando junto a este registro seus endereços MAC das interfaces de rede.

O SPISM possui ainda um recurso que possibilita ao usuário especificar em qual nível de detalhe (granularidade) a informação requisitada deve ser compartilhada: baixo, médio ou alto. O usuário requisitante também deve informar em qual nível de detalhe ele deseja receber a informação, porém, o que prevalece é a política configurada pelo usuário requisitado. Para atender esses níveis de detalhes, as coordenadas (localização) são exibidas nestes três níveis. Já a presença de contatos (co-localização) é exibida de três formas: (i) exibe apenas “alguns dispositivos próximos” ou “sem dispositivos próximos”, (ii) exibe o número exato de dispositivos próximos ou, (iii) exibe os identificadores dos dispositivos próximos, os endereços MAC. Para possibilitar a especificação dos três níveis de granularidade da atividade realizada pelo usuário, no nível baixo é exibido apenas se ele está ocupado ou disponível, no nível médio é exibido o título da atividade registrado na agenda e no nível alto são exibidos, além do título, os detalhes da atividade, que também é registrado na agenda.

A Figura 4.5 mostra as principais interfaces da aplicação móvel do SPISM. A primeira tela é onde os usuários podem se registrar e fazer login. A segunda mostra

a tela principal, onde é possível requisitar as informações dos contatos, ver lista de contatos e verificar as atividades passadas, tais como requisições de contatos, decisões de acesso tomadas e em qual nível de granularidade, bem como as configurações da aplicação. A terceira mostra a resposta da requisição de uma localização de um contato. A última mostra o registro (*log*) de requisições recebidas e as decisões feitas para cada uma delas.

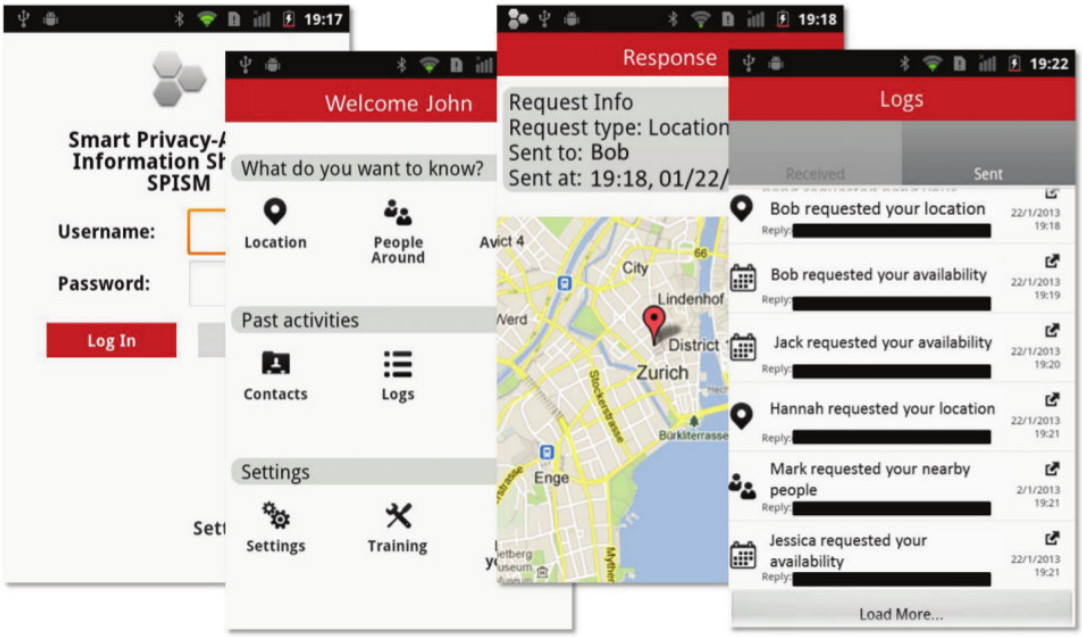

Figura 4.5: Interfaces da Aplicação Móvel SPISM [23].

O SPISM utiliza uma arquitetura cliente-servidor, em que o lado servidor é um componente chamado de *Information Sharing Directory* (ISD). O ISD é usado para permitir que o usuário descubra os endereços IP de seus contatos quando eles quiserem enviar as requisições por informações. O ISD armazena as informações de registro de todos os usuários cadastrados no SPISM, suas credenciais, suas listas de contatos e os endereços MAC das interfaces de rede de seus dispositivos, a ser utilizado no sistema de co-localização. Um usuário do SPISM interage com o ISD nas seguintes situações: (i) na fase de registro, (ii) durante o login, (iii) quando faz o download da lista de contatos, (iv) quando requisita alguma informação de um contato e (v) quando periodicamente atualiza seu endereço IP e seu estado mantendo-o online. Neste último caso, a atualização do endereço IP é necessária para que o ISD encaminhe as requisições ao endereço correto do requisitado. Além disso, o dispositivo precisa manter seu estado online para que outros dispositivos saibam que ele está ativo e

disponível para receber requisições. Toda comunicação entre as aplicações móveis e o ISD é criptografada utilizando chaves assimétricas.

Um diferencial do SPISM é ter um mecanismo que tem a capacidade de decidir dinamicamente dar permissão de acesso para as requisições feitas sem necessitar consultar o usuário, utilizando para isto aprendizagem de máquina. O mecanismo de aprendizagem de máquina do SPISM utiliza 18 dados brutos de contexto para realizar a tomada de decisão, das quais 17 são exibidas na Figura 4.6. Estes 18 dados brutos de contexto representam 9 informações de contexto: informações de perfil, informações de serviços de terceiros utilizados (por exemplo, Google Maps), tipo de dado requisitado, localização, tempo, atividade realizada pelo usuário, informações sobre usuários co-localizados, informações da última interação e ainda o tipo de dado que é processado, podendo ser categorias (conjunto de valores pré-definidos, por exemplo, o laço social tal como Pai, Amigo, Colega de Trabalho), inteiro ou float. Por exemplo, a informação de localização é representada por 3 dados brutos de contexto: latitude, longitude ou representação semântica. Na Figura elas são agrupadas (*person*, *service*, *What?*, *Location*, *When?*, *With whom?*, *Last Interaction*), chamadas de *feature*. Todas estas informações de contexto são agregadas e passadas para um classificador que irá fazer a tomada decisão, a qual pode ser: Não (nega acesso), Sim (baixa granularidade), Sim, (média) e Sim (alta). A técnica de aprendizagem de máquina utilizada pelo SPISM é um classificador implementado pela biblioteca Android WEKA. A sua utilização permite ao sistema, após uma certa quantidade de decisões de compartilhamento feitas pelo usuário, automaticamente decidir se deve ou não dar permissão de acesso às informações requisitadas. Este classificador utiliza aprendizagem ativa, ou seja, em tempo de execução exemplos podem ser modificados ou adicionados aos dados de treinamento.

Neste trabalho os autores ainda fizeram uma pesquisa através de questionário com 70 usuários, com objetivo de identificar qual a razão pela qual os usuários compartilham conteúdos em redes sociais e em qual grau de privacidade eles desejam fazer isto. Esta pesquisa foi utilizada como base para se realizar um levantamento de requisitos para a proposta do SPISM.

	Feature	Type
Person	Familiarity	Float
	Social tie	Cat.
	User ID	Cat.
Service	Service category	Cat.
What?	Request type	Cat.
	Details	Float
Location	Latitude	Float
	Longitude	Float
	Semantic location	Cat.

	Feature	Type
When?	Time	Int.
	Weekday	Cat.
	Daytime	Cat.
	Activity	Cat.
With whom?	Neighbors	Int.
	Neighbors Type	Cat.
Last interact.	Time last request	Float
	Details last request	Float

Figura 4.6: Informações de Contexto Utilizadas para Tomada de Decisão no SPISM [23].

4.6 Ajustes Automáticos de Privacidade em Redes Sociais Online

A classificação de contatos em grupos é útil para reduzir o esforço administrativo dos usuários. O sistema social pode gerenciar facilmente o acesso para novos contatos, bastando classificá-los em grupos que já possuem as permissões delegadas pelo usuário. Além disso, os contatos podem fazer parte de mais de um grupo ou mudarem de grupo.

Existem trabalhos na literatura que visam automatizar as configurações de privacidade em redes sociais tentando reduzir o esforço do usuário no processo de especificação de seus requisitos de privacidade. Estes trabalhos objetivam adaptar dinamicamente as configurações de privacidade de conteúdos postados para serem acessados por apenas determinados grupos de contatos ou contatos individuais. Eles visam organizar automaticamente os contatos nos grupos e também adaptar o nível de granularidade no qual as postagens de conteúdo podem ser acessadas de acordo com o grupo do qual o contato faz parte. Essa categoria de trabalhos descreve três recentes propostas que têm esse objetivo.

4.6.1 *Privacy Wizards for Social Networking Sites*

Fang e LeFevre, em [49], propõem um guia para auxiliar o usuário na definição de suas configurações de privacidade, o qual é focado em determinar controles de acesso a informações que podem ficar disponíveis no perfil do usuário. A solução proposta por esse trabalho usa técnicas de aprendizagem de máquina para configurar automaticamente preferências de privacidade.

O guia de privacidade proposto inicialmente requisita ao usuário para delegar permissões de acesso a informações pessoais de seu perfil para alguns contatos. Essas permissões dadas a alguns contatos fazem parte da fase de treinamento da técnica de aprendizagem supervisionada adotada. A partir das permissões iniciais dadas pelo usuário, juntamente com as informações de perfis dos contatos e informações do grafo social, a solução treina um classificador que irá delegar automaticamente permissões de acesso às informações de perfil do usuário para o restante de seus contatos. Mais especificamente, são usadas e avaliadas duas técnicas de aprendizagem nos classificadores: *Naive Bayes* e árvores de decisão. Além disso, contatos adicionados são automaticamente classificados em um grupo e herdam as configurações de privacidade dele.

As informações de perfil dos contatos usadas no classificador são: gênero, idade, histórico de educação e trabalho, status de relacionamento, afinidades políticas e religiosas. As informações do grafo social usadas no classificador estão relacionadas com a criação de comunidades que representam vértices densamente conectados entre si. Portanto, essas comunidades representam que o usuário e o grupo de contatos que compõem a comunidade possuem muitos relacionamentos em comum na rede social e, por essa razão, o guia pode delegar configurações de privacidade similares para esses contatos da comunidade.

A Figura 4.7 ilustra uma visão geral de como funciona o guia proposto por esse trabalho, o qual é composto de três principais partes. ***User Input***: o guia solicita entradas a partir do usuário em relação as suas preferências de privacidade para um grupo inicial de contatos, através de questões e respostas. ***Feature Extractor***: usando informações visíveis (ou seja, informações de perfil dos contatos e obtidas a partir do grafo social), o classificador cria os grupos de contatos. ***Privacy-Preference Model***: usando as entradas iniciais do usuário e os grupos que são resultado do classificador, o

guia constrói um modelo de preferência de privacidade, o qual é usado para especificar automaticamente as configurações de privacidade do usuário. Dessa forma, à medida que o usuário provê mais entradas ou adiciona novos amigos, o modelo adapta as configurações de privacidade automaticamente.

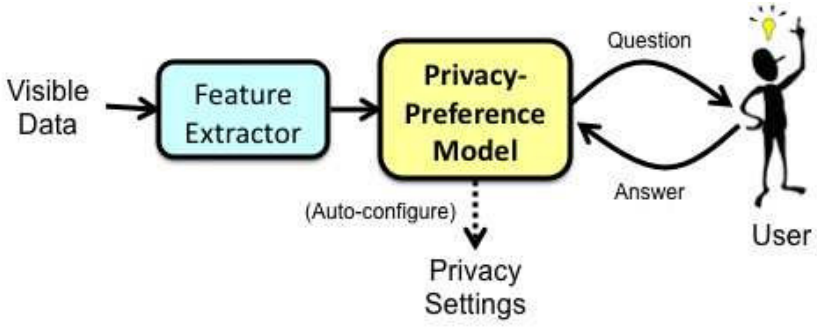

Figura 4.7: Visão Geral do Guia de Privacidade [49].

4.6.2 *Identifying Hidden Social Circles for Advanced Privacy Configuration*

Squicciarini et al., em [131], propõem um sistema de recomendação de configurações de privacidade para usuários classificados em grupos. Os grupos no Google+ são chamados de círculos e a solução desse trabalho foi implementada e integrada a essa rede social. O sistema objetiva ajudar os usuários a gerenciar automaticamente seus contatos associando-os a grupos relevantes nos quais os contatos tenham características em comum. Similarmente ao trabalho anterior, no sistema de recomendação quando um usuário estabelece um novo relacionamento, ele identifica o grupo (ou o círculo) que é mais adequado a esse novo contato.

O sistema é considerado de recomendação por indicar ao usuário configurações de privacidade para postagens, em que ele identifica o grupo (ou mais de um grupo) que é mais adequado a ter permissões de acesso ao conteúdo que está sendo postado. A ideia básica usada pelo sistema é: (1) identificar as configurações de privacidade usadas em conteúdos postados anteriormente que são mais similares ao que está sendo postado e recomendar que seja adotada a mesma configuração; (2) identificar os contatos que já fazem parte dos grupos (ou círculos) do usuário que são mais similares ao que está sendo adicionado e recomendar que ele seja adicionado a um ou mais destes grupos. A intuição dessa solução é de que um usuário tipicamente

tem requisitos de privacidade em relação a conteúdos similares e também a contatos com características similares. Por exemplo, fotos da família podem ser normalmente compartilhadas com o grupo de contados dos membros da família.

Uma outra contribuição da solução proposta por esse trabalho é prover a habilidade de identificar círculos considerados escondidos, os quais são subgrupos em que os contatos possuem determinadas características mais particulares. Por exemplo, dentro de um grupo de contatos do usuário em que estejam seus amigos pode existir um subgrupo que inclui os amigos mais próximos com quem o usuário interage com mais frequência ou compartilha uma maior quantidade maior de conteúdos. Para os autores esse recurso é importante para o gerenciamento de privacidade e pode não ser considerado pelos usuários quando criam os círculos manualmente sem a ajuda da solução proposta. Isso ocorre porque configurações de privacidade podem ser diferentes para grupos escondidos distintos.

4.6.3 *Privacy-driven Access Control in Social Networks by Means of Automatic Semantic Annotation*

Imran-Daud et al., em [74], propõem um controle de acesso para postagens de mensagens textuais. Esse controle de acesso analisa a semântica de cada mensagem postada e avalia o grau de sensibilidade de seu conteúdo, detectando-o automaticamente usando processamento de linguagem natural. Essa sensibilidade é identificada de acordo com os requisitos de privacidade especificados pelo usuário, em que ele informa quais tipos de informação podem prejudicar de alguma forma a sua privacidade. A solução proposta permite ao usuário determinar a sensibilidade de conteúdos para os seguintes tipos de informação: relacionados a saúde ou dados médicos, religião, raça (cor, origem, nacionalidade, etc), política e sexualidade.

Uma vez que a sensibilidade do conteúdo é identificada, a solução cria versões diferentes do texto postado com níveis de detalhes modificados, chamadas de versões "higienizadas". As versões são acessadas por diferentes grupos de contatos, de acordo com os requisitos de privacidade do usuário. Dessa forma, esse controle de acesso tem autonomia para decidir quais configurações devem ser usadas para atender os requisitos de privacidade especificados pelo usuário, com base em preferências definidas inicialmente. Os requisitos de privacidade são especificados pelos usuário

considerando os grupos de contatos. Por exemplo, somente contatos que estejam no grupo da família podem ter acesso a conteúdos postados relacionados a orientação sexual. Portanto, os contatos podem ter acesso a versões diferentes do conteúdo original postado. As versões diferentes são semanticamente coerentes em relação a mensagem original postada.

4.7 Análise Comparativa dos Trabalhos Relacionados

Esta seção faz uma análise comparativa através da Tabela 4.1 entre os trabalhos relacionados apresentados anteriormente. Para isso, são adotados os seguintes critérios de comparação:

1. O critério *Tipo* determina em qual das três últimas categorias descritas anteriormente o trabalho proposto se encontra: A – Privacidade Dependente de Contexto em Ambientes Ubíquos; B – Privacidade Dinâmica em Redes Sociais Móveis Baseadas em Localização; e C – Ajustes Automáticos de Privacidade em Redes Sociais Online;

2. *Proposta* especifica o tipo de solução com a qual o trabalho contribui;

3. O *Tipo de Contexto* informa quais informações a solução proposta possibilita utilizar como restrição. Quando informada genérica, considera-se que a solução pode ser utilizada independente do tipo de informação de contexto;

4. *Requisitos* informa se o trabalho realizou um processo preliminar de elicitação de requisitos diretamente com usuários para identificar suas necessidades e tê-las como base e motivação para o desenvolvimento da proposta;

5. O critério *Avaliação* determina se o trabalho foi avaliado com usuários reais utilizando a solução, ou uma aplicação que o utiliza em sua implementação, ou mesmo em um estudo de caso;

6. O critério *Autonomia* informa se a solução proposta possui alguma autonomia para a realização de tomada de decisão sobre as configurações de privacidade a informações pessoais;

7. O critério *Ciência de Situação* informa se o trabalho adota, mesmo que preliminarmente, o paradigma de computação situacional, realizando algum tipo de processamento de dados de contexto ou identificação da situação do usuário para adaptar as configurações de privacidade;

8. *Granularidade* determina em qual nível de granularidade as permissões de acesso são dadas, podendo ser: papéis, usuário individual (UI) ou grupo de usuários (GU) e possibilita acesso a informação ofuscada. Nesta última, a solução permite que a informação seja acessada por um usuário individual ou grupo com diferentes níveis de ofuscação;

9. O *Conteúdo* é um critério usado apenas para comparar os trabalhos desenvolvidos para sistemas sociais e informa qual tipo de conteúdo é disponibilizado na aplicação social móvel;

10. Por fim, o *Ano* informa a data de publicação do trabalho.

Os critérios *Levantamento com Usuários* e *Avaliação* são importantes para identificar se os trabalhos verificaram de alguma maneira a viabilidade de utilização de suas soluções propostas.

Trabalho	Tipo	Proposta	Tipo de Contexto	Requisitos	Avaliação	Autonomia	Ciência de Situação	Granularidade	Conteúdo	Ano
Groba et al. [64]	A	Mecanismo	Genérico	Não	Não	Não	Não	Papéis	-	2007
Franz et al. [57]	A	Arquitetura	Genérico	Não	Não	Não	Não	Papéis	-	2008
CPE [24]	A	Mecanismo (*Engine)*	Genérico	Não	Não	Não	Não	UI/GU	-	2008
CPPL [16]	A	Linguagem	Genérico	Não	Não	Não	Sim	UI/GU	-	2012
PICOS [138]	B	*Framework* e Aplicação	Localização	Sim	Sim	Não	Não	UI/GU	Informações em geral	2011
PeopleFinder e Locaccino [120, 136]	B	Aplicação	Tempo e Localização	Sim	Sim	Não	Não	UI/GU	Localização	2009-2013
SPISM [23]	B	Aplicação	9 tipos	Sim	Não	Sim	Não	UI/GU e informação ofuscada	Localização, atividade e contatos co-localizados	2013
Fang e LeFevre [49]	C	Guia	Contexto social	Não	Sim	Sim	Não	UI/GU	Informações de perfil	2010
Squicciarini et al. [131]	C	Mecanismo	Contexto social	Não	Sim	Não	Não	UI/GU	Postagens	2014
Imran-Daud et al. [74]	C	Controle de acesso	Contexto semântico	Não	Não	Sim	Não	UI/GU e informação ofuscada	Postagens de mensagens	2016

Tabela 4.1: Análise Comparativa dos Trabalhos Relacionados.

Como visto na Tabela 4.1, quatro dos trabalhos são classificados como privacidade dependente de contexto em ambientes ubíquos (A), três estão na classe de privacidade dinâmica em RSMs baseadas em localização (B), e três são propostas para ajustes automáticos de privacidade em redes sociais online (C). Em relação ao segundo critério, são propostas diversos tipos de soluções. Sobre o tipo de dado de contexto, várias soluções propõem recursos em que podem ser usados qualquer dado de contexto (Genérico), sem haver uma limitação do tipo de dado. O trabalho proposto por Franz et al. [57] é considerado genérico, adotando o conceito de contexto interno a aplicação, relacionado ao histórico, requisitante e independente da aplicação. O CPE [24] é também considerado genérico, mas exemplos de uso da solução são dados apenas com a informação de localização. O CPPL [16] é considerado genérico, o qual inclui também informações de relações sociais dos usuários. Os trabalhos de Fang e LeFevre [49] e Squicciarini et al. [131] consideram o contexto social obtido a partir de perfis de contatos. Os trabalhos de Squicciarini et al. [131] e Imran-Daud et al. [74] levam em consideração o contexto semântico dos conteúdos postados na rede social. Em relação a elicitação de requisitos com usuários, apenas os trabalhos da quinta categoria (B) a realizaram. Os trabalhos Franz et al. [57] e CPPL [16] apenas ilustraram em cenários de uso a necessidade pelas soluções que propuseram. Dentre todos os trabalhos, apenas quatro trabalhos realizaram avaliações práticas com as soluções que propuseram. O trabalho de Franz et al. [57] ilustrou somente um estudo de caso, mas a solução não foi avaliada com usuários finais. Três soluções têm autonomia para a realização de tomada de decisão sobre as configurações de privacidade de informações pessoais. O SPISM [23] inicia em uma fase de treinamento que o usuário escolhe quais requisições às informações pessoais são aceitas, posteriormente o sistema decide com autonomia com base nas escolhas do usuário quem pode acessá-las. O trabalho de Fang e LeFevre [49] possui autonomia para classificar contatos em grupos. O trabalho de Imran-Daud et al. [74] tem autonomia para criar versões diferentes de uma postagem de mensagem e permitir acesso a elas de acordo com o contato ou grupo de contatos. Apenas o CPPL [16] adota preliminarmente o paradigma de computação situacional, com uso de regras. Em relação a granularidade, a maioria dos trabalhos delegam permissões de acesso a informações pessoais para usuários individuais ou grupo de usuários. O SPISM [23] e o trabalho de Imran-Daud et al. [74] ainda possibilitam a ofuscação da informação. Dentre os trabalhos desenvolvidos para

sistemas sociais, vários tipos de conteúdos podem ser compartilhados pelos usuários. Por exemplo, o PICOS [138] permite que o usuário compartilhe informações em geral com comunidades de interesse em comum. Já o PeopleFinder e o Locaccino [120, 136] permitem que contatos acessem somente a localização do usuário. Os trabalhos comparados na Tabela 4.1 foram publicados em um intervalo de 10 anos, de 2007 a 2016.

4.8 Conclusão

Este capítulo descreveu os trabalhos relacionados à pesquisa descrita nessa tese de doutorado, os quais foram categorizados em seis grupos, para facilitar o entendimento e também o contexto em que a contribuição desse trabalho se insere. Inicialmente, nas três primeiras categorias, foram apresentadas as extensões do modelo RBAC, os modelos de controle de acesso para redes sociais, e as extensões dos recursos disponibilizados pelos provedores de RSMs para controles de privacidade. Posteriormente foram mostrados propostas de mecanismos de privacidade dependente de contexto para computação ubíqua e, em seguida, as propostas que visam tornar dinâmica com base em dados de contexto as configurações de privacidade em RSMs baseadas em localização. Na última categoria ficaram os trabalhos que visam tornar automático os ajustes de configurações de privacidade. As categorias de trabalhos relacionados foram comparadas ao final desse capítulo. Os trabalhos apresentados a partir da quarta categoria, os quais foram explicados mais detalhadamente, tiveram ênfase na comparação e foram colocados em uma tabela comparativa com diversos critérios.

5 Solução Proposta

Este capítulo apresenta a proposta de solução para abordar o problema foco desta pesquisa. A seção inicial narra o processo de levantamento de requisitos de privacidade com usuários brasileiros de RSMs. Posteriormente, são descritos exemplos de cenários reais que motivam alcançar um gerenciamento autônomo das configurações de privacidade baseado na situação atual do usuário. Na sequência, uma visão geral da solução completa proposta nessa tese é mostrada, para facilitar o entendimento, juntamente com problemas mais específicos que surgem com a utilização do paradigma de computação situacional. Na seção seguinte, o modelo conceitual proposto para se alcançar consciência de situação na solução é detalhado. As Seções seguintes descrevem os conceitos propostos pela solução desenvolvida nessa tese: o Perfil de Privacidade Situacional e o Gerenciamento Autônomo de Privacidade com o uso dos níveis de autonomia. Em seguida detalha-se a arquitetura da solução proposta, descrevendo-se também os principais aspectos relacionados a sua implementação. Adicionalmente, uma especialização do modelo conceitual de identificação de situação é descrita, em que ele foi aplicado ao domínio de saúde mental. Ao final desse capítulo é feita uma análise comparativa entre a solução proposta nessa tese e os trabalhos mais fortemente relacionados descritos no capítulo anterior (capítulo 4) e também são descritas suas limitações.

5.1 Elicitação de Requisitos: Estudo com Usuários

5.1.1 Objetivo, Metodologia e Características dos Participantes

Para melhor entender como os usuários compartilham suas informações através de postagem de conteúdo em RSMs e quais informações de contexto influenciam seus desejos dinâmicos em relação à privacidade, realizou-se um estudo com usuários[1] durante sete dias em setembro de 2014. O estudo consistiu de uma

[1]Os termos "participantes" e "sujeitos" também são utilizados neste texto para denotar os indivíduos que participam de estudos e avaliações realizados.

aplicação de questionário online, feita através do Google Forms[2], usado para coletar informações dos usuários em relação a seu uso de RSMs e, principalmente, suas preocupações em relação à privacidade quando postam conteúdo.

Particularmente, o foco deste levantamento foi verificar se os usuários tinham realmente desejos dinâmicos e contextuais em relação a privacidade, tentando também entender quais fatores influenciavam para que isso acontecesse. Para tanto, questões constantes do questionário visavam colocar os sujeitos em cenários de uso realísticos de RSMs, mais especificamente em situações de postagem de conteúdo no Facebook. Ao se depararem com as situações sugeridas nas questões, os participantes eram questionados sobre quem poderia ver seus conteúdos postados.

Divulgou-se o questionário através de perfis de redes sociais de integrantes do LSDi e listas de e-mail (por exemplo, as listas da Sociedade Brasileira de Computação) durante os sete dias de aplicação. Os participantes eram informados sobre o objetivo do *survey* antes de responderem as questões e, além disso, eles eram assistidos por textos descritivos durante todo o preenchimento. Durante o período de aplicação um total de 164 participantes brasileiros completaram o questionário.

Os trabalhos relacionados descritos no capítulo 4 adotaram a prática de encorajar a participação dos sujeitos oferecendo um pagamento para que eles participassem respondendo completamente seus questionários. Nesta elicitação de requisitos não foi adotada essa estratégia, pois apenas foram feitos convites para as pessoas participarem. Por essa razão, acredita-se que a quantidade de sujeitos que participaram espontaneamente desse estudo já é um indício de que usuários brasileiros estão preocupados com sua privacidade em RSMs.

O questionário continha 20 questões organizadas em quatro etapas, o qual pode ser visto no Apêndice A deste documento. Para respondê-lo completamente, o participante precisaria ter uma conta no Facebook com pelo menos 50 contatos e acessá-la utilizando dispositivo móvel, além de ser maior de idade, ou seja, idade igual ou superior a 18 anos. Essas duas condições eram levantadas nas duas primeiras questões referentes à primeira etapa: "Qual sua idade?" e "Você possui uma conta no Facebook com no mínimo 50 amigos e utiliza algum dispositivo móvel como um dos

[2] `http://www.google.com/forms/about/`

meios de acesso a ela?". Neste ponto as idades dos participantes foram de 18 a 55 anos (Média = ≈29,51, DP[3] = ≈7,74).

Em seguida, os sujeitos informaram seus gêneros, nível educacional e o lugar onde residiam atualmente, correspondentes às 3 questões referentes à segunda etapa. Os resultados mostraram que, dos 164 participantes, 103 deles eram do gênero masculino e 61 feminino. Em relação ao nível educacional, 12 tinham o ensino médio ou médio-técnico completo, 37 estavam cursando o nível superior, 35 tinham o curso superior completo e 80 tinham finalizado algum nível de pós-graduação: 25 especialização, 34 mestrado e 21 doutorado. Acredita-se que o número elevado de participantes com algum nível de pós-graduação se deu pela divulgação do *survey* através da lista de e-mail da Sociedade Brasileira de Computação, a qual possui muitos pesquisadores registrados. Entretanto, mesmo com esse número alto de pós-graduados, os participantes representam um conjunto de pessoas com níveis educacionais bastante diferenciados. Em relação ao local onde os sujeitos residiam, houve representatividade de todas as cinco regiões brasileiras, e 3 participantes moravam fora do Brasil. O questionário abrangeu representantes de vários níveis educacionais e de todas as regiões geográficas do Brasil, e consideramos, portanto, que ele possui uma boa representatividade do contexto brasileiro.

5.1.2 Questões Pertinentes e Resultados

Posteriormente, os sujeitos foram questionados na terceira etapa sobre seu uso de RSMs e suas preocupações em relação a privacidade, a qual possuía três questões. Primeiramente os sujeitos respondiam qual a frequência que eles usavam o Facebook através de dispositivos móveis, seja para acessar, postar ou compartilhar conteúdo. A Figura 5.1 mostra as respostas obtidas. Observa-se que muitos dos usuários usam RSMs várias vezes por dia. Mais especificamente, 116 sujeitos (78 + 38, ≈71%) usam duas ou mais vezes ao dia.

Em seguida, ainda na terceira etapa, foi questionado se eles se julgavam preocupados sobre sua privacidade quando usavam redes sociais, e 146 responderam que sim (≈89%). Adicionalmente, eles responderam a seguinte questão: "Você acha que o fato de acessar mídias sociais através de dispositivos móveis faz com que você

[3]Desvio Padrão.

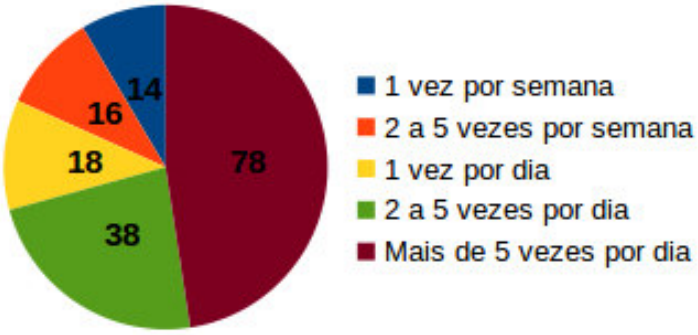

Figura 5.1: Frequência de Acesso dos Sujeitos.

esteja sujeito a uma quantidade maior de problemas relacionados a sua privacidade?" e 112 responderam que sim (≈68%). Este número mostra que uma grande porção de usuários estão preocupados com sua privacidade quando o acesso a redes sociais é realizado através de dispositivos móveis.

Na parte inicial da quarta etapa, composta de 10 questões, optou-se por analisar apenas as respostas dos 146 sujeitos que se julgavam preocupados com sua privacidade. Esta etapa colocou os sujeitos em dez possíveis cenários reais onde eles estavam em situações realísticas de postagem de conteúdo em RSMs, por exemplo: "Você está em uma festa pela madrugada com um grupo de amigos e publica uma foto sua com eles.", "Você está trabalhando em seu expediente e publica um vídeo curto que representa um pouco de sua rotina de trabalho.", "Você está em uma comemoração com seus amigos em uma choperia (bar ou *pub*) e publica sua localização (*check-in*) fazendo marcação de seus amigos mostrando que eles estão co-localizados.". Os participantes eram então questionados sobre quem poderia acessar suas postagens de conteúdo, podendo ser: 1. Contato ou grupo, 2. Todos contatos, 3. Público, 4. Exceção de contato ou grupo. Essa última opção é utilizada para permitir o usuário esconder (ou seja, negar acesso) a sua postagem para um contato ou grupo de contatos. Esse esquema de controle de acesso já é provido pelo Facebook. As respostas eram colocadas aleatoriamente para prevenir que os participantes respondessem sem lê-las, forçando-os a analisar qual a resposta mais adequada.

A partir da segunda situação realística adicionou-se uma quinta possibilidade de resposta: 5. Igual à questão anterior. Decidiu-se adicionar esta resposta por duas razões: (i) para forçar os participantes a refletirem sobre suas respostas para as questões anteriores (a cada questão ele precisaria verificar o que

respondeu anteriormente), e (ii) seria possível verificar se os usuários tinham a mesma resposta para todas as questões. Caso um participante respondesse a opção 5 em todas as situações, com exceção da primeira, isso indicaria que seu desejo em relação a privacidade era estático. Dos 146 participantes, apenas 6 se enquadraram neste caso, e todos os outros usuários mudaram suas respostas. Este número indica que os requisitos de privacidade dos usuários em RSMs são dinâmicos.

A Figura 5.2 mostra as resposta dos 140 sujeitos que tinham desejos dinâmicos de privacidade (≈85% do total). Os participantes tinham a opção de não responder as questões, elas eram opcionais por considerar-se que algum usuário poderia nunca ter postado conteúdo na situação ilustrada na questão, ou não conseguir ou poder se imaginar naquela situação. Neste caso as respostas foram computadas como "Não respondida". Um resultado é particularmente interessante e pode ser visto na figura: considerando 9 situações, com exceção da primeira, existem 1260 respostas e, dentre elas, 1039 **não** são: "Igual à questão anterior" ou "Não respondida". Este resultado mostra que os sujeitos mudaram suas respostas a cada questão e, por isso, indica novamente que requisitos de privacidade dos usuários em RSMs são dinâmicos.

Figura 5.2: Respostas dos Sujeitos para Quem Pode Acessar Conteúdos Postados.

Por fim, nas duas últimas questões da etapa quatro e do questionário, os sujeitos foram questionados para indicar quais fatores influenciaram suas respostas. Na questão 19, a qual foi formulada levando em consideração os resultados obtidos de outros estudos [137] [18] [23] e também de nossa experiência, os sujeitos tinham a opção de determinar se os seguintes quatro fatores tinham influenciado suas respostas: localização (por exemplo, em casa, no trabalho, em um bar, em uma outra cidade), tempo (ou seja, período do dia ou dia da semana), pessoas co-localizadas (ou seja, contatos próximos), e o tipo de conteúdo a ser publicado (ou seja, mensagem, foto,

vídeo ou *check-in*). Essa questão é aparentemente tendenciosa, entretanto, deixou-se explícito para os sujeitos que outros fatores poderiam provavelmente influenciar suas respostas e que eles deveriam listá-los na questão seguinte. O resultado é mostrado na Figura 5.3 e, novamente, ele considera os 140 sujeitos que tem desejos de privacidade dinâmicos dentre os 146 que se julgavam preocupados com sua privacidade. Como pode ser visto, os quatro fatores significantemente influenciaram a tomada de decisão dos sujeitos para controlar acesso a conteúdos postados em RSMs.

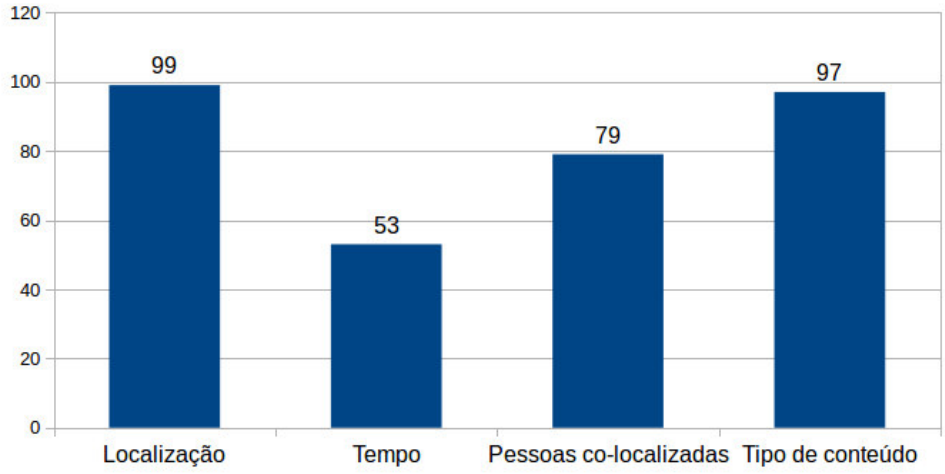

Figura 5.3: Resposta dos Sujeitos para os Fatores que Influenciaram Decisões para Controlar Acesso a Conteúdos.

Para se obter um resultado qualitativo, na questão 20 os sujeitos poderiam descrever livremente quais seriam outros possíveis fatores que influenciaram suas decisões em relação à escolha da configuração de privacidade aos conteúdos postados, além dos quatro listados na questão anterior. Como resultado, os sujeitos confirmaram os quatro fatores previamente listados na questão 19 usando diferentes palavras, além de tentarem justificar a motivação para suas respostas. Em relação ao fator tempo, três sujeitos reportaram espontaneamente na questão 20 que este fator não influenciou suas decisões devido eles realizarem suas postagens depois de obter o conteúdo a ser publicada, ou seja, em um tempo futuro.

5.1.3 Conclusões e Limitações

Os resultados desse estudo indicaram que os requisitos de privacidade dos usuários em RSMs são normalmente dinâmicos porque suas preferências dependem fortemente de detalhes da situação/contexto no tempo de postagem do conteúdo.

Em resumo, os resultados deste estudo sugeriram algumas conclusões em relação a postagem de conteúdo em RSMs, são elas:

- Os desejos de privacidade dos usuários são usualmente dinâmicos. Usuários querem modificar as configurações de privacidade de conteúdos postados ao longo do tempo;
- Os desejos de privacidade dos usuários são usualmente contextuais. O desejo para modificar as configurações de privacidade de postagens é feito de acordo com a situação atual do usuário;
- Existem quatro fatores que certamente influenciam os desejos de privacidade do usuário: localização, tempo, pessoas co-localizadas e o tipo de conteúdo postado.

Levando em consideração os resultados obtidos a partir desse estudo, os mecanismos usados para especificar preferências de privacidade em RSMs devem dar suporte a ajustes automáticos nos controles de privacidade a fim de atender os requisitos do usuário. Dessa forma, permissões de acesso a conteúdos postados devem ser regradas por políticas que consideram a situação atual do usuário no momento da postagem.

Considera-se que a principal limitação desse estudo é a nacionalidade dos sujeitos envolvidos, devido ao fato de que somente cidadãos brasileiros terem participado. Uma outra questão que poderia ser encarada como limitação é a heterogeneidade dos usuários. Os usuários de RSMs podem ser agrupados em vários perfis considerando as estratégias de gerenciamento de privacidade adotadas [148]. Por exemplo, há alguns usuários que não se preocupam com sua privacidade na rede social, mas há outros extremamente preocupados com o acesso às suas informações pessoais que estão inseridas nas redes sociais. Portanto, os usuários não têm os mesmos comportamentos quando regulam suas preferências de privacidade em RSMs. Entretanto, é importante ressaltar que os resultados do estudo apresentado não contradizem isso, eles indicam que uma grande quantidade dos usuários tem atitudes de privacidade com requisitos dinâmicos e contextuais. Portanto, esses requisitos são comuns em diferentes perfis de usuários.

5.2 Exemplos de Cenários

A seguir são descritos dois cenários em que um gerenciamento adaptativo dos controles de privacidade em RSMs é necessário para atender os requisitos dinâmicos e dependentes de contexto dos usuários. Como é mostrado, o gerenciamento deve ocorrer de acordo com o contexto do usuário. Os cenários mostram que, se as configurações de privacidade não são adaptativas à situação do usuário, então não atendem seus desejos e expectativas. Estes cenários proveem uma motivação para alcançar um gerenciamento autônomo das configurações de privacidade e são descritos aqui para ilustrar melhor a aplicabilidade da solução proposta.

Cenário 1 – Socialização. Dispositivos móveis equipados com diversas tecnologias embutidas (por exemplo, câmera, acelerômetro, GPS, sensor de batimento cardíaco, e muitos outros) são utilizados para obter e inserir nas RSMs uma grande quantidade de conteúdos. Indivíduos e organizações tipicamente geram uma quantidade significativa desses conteúdos, usados por eles para socialização, objetivando relacionarem-se uns com os outros. Usuários normalmente publicam conteúdos relacionados a sua vida pessoal e a situação a qual eles estão ou a atividade que eles estão realizando. Isso ocorre principalmente devido a facilidade que os usuários têm para obter esses conteúdos. Portanto, os conteúdos obtidos por meio dos dispositivos móveis são pessoais e totalmente relacionados ao usuário e ao ambiente (contexto ou situação) em que ele se encontra. Por esta razão, em muitos casos, os usuários querem que o conteúdo esteja disponível somente para contatos ou grupos de contatos específicos, ao invés de torná-lo acessível para sua lista completa de contatos.

Para ilustrar, considere o seguinte exemplo. Maria está em seu trabalho e posta uma foto. Maria tem como requisito de privacidade que, quando estiver no trabalho, somente os amigos próximos (um grupo de contatos chamado “amigos próximos”) vejam os conteúdos que ela postar. Então, para a aplicação suportar esse requisito de privacidade, é necessário que tenha a capacidade de reconhecer quando Maria estiver na situação “trabalho” e ajustar automaticamente as configurações de privacidade da foto postada. Portanto, a aplicação deve ter habilidade para **identificar a situação do usuário** (no caso de Maria, trabalhando) e, com base nisso, **ajustar automaticamente as configurações de privacidade dos conteúdos postados**.

Cenário 2 – Aplicações de *check-in*. Muitas RSMs, tais como Google+ e Facebook, permitem ao usuário fazer *check-in* em um lugar físico e disponibilizar o compartilhamento de suas localizações com seus contatos. Indivíduos com dispositivos móveis fazem *check-in* em uma localização através das coordenadas geográficas obtidas pela aplicação via GPS, *Assisted Global Positioning System* (AGPS), e redes móveis. As aplicações de *check-in* tem o botão "Lugares" onde o usuário vê uma lista de lugares próximos à coordenada obtida que podem ser escolhidos para identificar o *check-in*. Se um local não está na lista de lugares próximos, o usuário pode adicioná-lo manualmente, e esta informação será compartilhada com outros usuários que desejam fazer *check-in* no mesmo local.

Como exemplo, considere uma pessoa chamada Alice, uma usuária que gosta de divulgar os lugares que ela visita para seus contatos através de postagens de *check-in*. Entretanto, ao mesmo tempo ela está preocupada com sua privacidade. Então ela pode desejar que em situações específicas a sua localização seja vista somente por um grupo seleto de contatos, por exemplo, os membros de sua família. Uma situação bem específica é que a Alice deseja que somente a sua família tenha acesso a suas postagens de *check-in* quando ela estiver em casa nos finais de semana pela manhã acompanhada de sua mãe.

Em uma aplicação social móvel na qual a localização do usuário deve ser preservada, as configurações de privacidade devem garantir que: (i) recursos oferecidos pela aplicação continuem sendo providos, não sendo bloqueados devido a omissão da localização, (ii) a localização deve ser descoberta somente em lugares em que o usuário deseja, sendo possível criar uma lista de lugares nos quais ele deseja que a aplicação não revele sua localização ou a revele apenas para contatos específicos, por exemplo, no local de trabalho ou em uma festa noturna[4], e (iii) a localização é descoberta somente com a presença de um contato (co-localização).

[4]Os lugares em que não é permitida a publicação da localização são muito particulares a cada usuário e pode variar bastante.

5.3 Visão Geral da Solução Proposta

A solução proposta nessa tese de doutorado objetiva atender aos requisitos dinâmicos e contextuais de privacidade dos usuários em RSMs. Ela é chamada de ***SelPri***, a qual foi concebida a partir do paradigma de computação situacional e implementada como prova de conceito em forma de uma aplicação social móvel. A implementação atual do *SelPri* é integrada ao Facebook. Como visto anteriormente no capítulo 1, o Facebook é a rede social que possui mais usuários no mundo e no Brasil com acesso através de dispositivos móveis e, portanto, essa foi a razão principal dele ter sido escolhido nesta pesquisa. O nome *SelPri* é uma alusão ao termo *self-privacy* (auto-privacidade).

Em uma visão geral do funcionamento do *SelPri*, ele visa tornar dinâmica as configurações de privacidade dos usuários de RSMs, permitindo o ajuste automático da escolha da audiência que terá acesso a conteúdos postados de acordo com a situação em que o usuário se encontre no momento da postagem. Essa audiência depende de como as configurações de privacidade podem ser determinadas, mas na maioria dos casos ela é configurada através da escolha dos grupos de contatos ou contatos individuais que podem ter acesso a um conteúdo. Dessa forma, o *SelPri* especifica dinamicamente os grupos de contatos ou contatos individuais que podem acessar um conteúdo postado, de acordo com a situação atual do usuário que ele identificar. O *SelPri* foi integrado ao Facebook, que é uma das redes sociais que adota essa maneira de especificar configurações de privacidade.

Como o *SelPri* utiliza a situação do usuário para tomada de decisão de mudança dos controles de acesso a conteúdos postados na rede social, a capacidade de interação do sistema com o usuário para a definição das situações e o processo de inferência destas são muito importantes. Primeiramente o usuário irá configurar no *SelPri* as possíveis situações em que ele poderá se encontrar, que utilizará uma técnica de identificação de situações baseada em especificação. Para isso, o usuário define informações de contexto que caracterizam cada situação, as quais são: localização do usuário, contatos co-localizados e que também estejam utilizando o *SelPri*, dia da semana, período do dia e o tipo de conteúdo que o usuário deseja postar (mensagem, foto, vídeo ou *check-in*).

Juntamente com a especificação da situação, o usuário determina as configurações de privacidade aplicadas às situações quando forem identificadas, ou seja, ele define a audiência da postagem. Pelo fato do *SelPri* ser integrado ao Facebook, as opções de audiência que o usuário tem para escolher são: amigos, amigos de amigos, somente eu, público e personalizado, em que ele pode escolher contatos individuais para conceder (ou negar) permissão de acesso.

Para realizar o processo de inferência, os dados de contexto são obtidos por um serviço de contexto e analisados para identificar a situação atual do usuário, utilizando lógica nebulosa. No momento em que o usuário realiza uma postagem de conteúdo é verificada em que situação ele se encontra e são aplicadas as configurações de privacidade previamente definidas para a situação. Dessa forma, o sistema usa automaticamente a configuração de privacidade configurada para a situação identificada. A descrição detalhada do funcionamento do *SelPri* é mostrada nas próximas Seções.

5.3.1 Questões Relacionadas à Adoção do Paradigma de Computação Situacional

Ao se adotar o paradigma de computação situacional para a concepção da solução proposta, as seguintes questões devem ser resolvidas:

1. **Como o usuário define uma situação na aplicação?** A solução deve ter interfaces para permitir que o usuário defina facilmente situações em que ele possa se encontrar;

2. **Como identificar em tempo real uma situação do usuário?** A solução deve conseguir identificar em tempo real e corretamente mudanças de situação do usuário;

3. **Ao ser identificada uma mudança de situação, como adaptar as configurações de privacidade de conteúdos postados na rede social de acordo com a nova situação?** Após ser reconhecida uma mudança de situação do usuário, a solução deve ser capaz de adaptar as configurações de privacidade para conteúdos postados na rede social de acordo com a situação identificada;

4. **Como possibilitar ao usuário conceder autonomia ao sistema e verificar se ele está agindo corretamente?** O usuário precisa estar ciente do funcionamento do sistema e, mais precisamente, que uma mudança de situação pode refletir em uma tomada de decisão feita com autonomia pelo sistema. Adicionalmente, o sistema deve permitir que o usuário delegue, com ou sem sua intervenção, autonomia ao sistema para realizar as definições das configurações de privacidade.

A solução desenvolvida ao longo dessa pesquisa de doutorado foi concebida objetivando resolver essas questões.

5.4 O Modelo de Identificação de Situação

A tomada de decisão feita pelo gerenciamento autônomo de privacidade do *SelPri* tem como base a situação do usuário. Isto é, a decisão de quais permissões de acesso devem ser aplicadas a um dado conteúdo postado é realizada baseada na situação atual do usuário. A definição de situação do usuário é baseada nos resultados da elicitação de requisitos que mostrou os quatro fatores que certamente influam nos requisitos dinâmicos e contextuais de privacidade dos usuário. Portanto, uma situação é definida como uma tupla $S : < L, T, CL, TC >$, em que L representa a localização atual do usuário (Onde), T é o tempo representado por dia da semana e tempo/período do dia (Quando), CL representa um ou mais contatos co-localizados ao usuário (Com Quem), e TC é o tipo de conteúdo a ser postado (O que). O tipo de conteúdo postado pode ser, por exemplo, uma foto ou um vídeo. As situações representam semanticamente a rotina diária do usuário, por exemplo, se ele está estudando, trabalhando, em alguma atividade de lazer, ou realizando alguma atividade física. Em suma, uma situação é identificada a partir da correlação de dados de contexto por meio de um motor de inferência que faz uso de lógica nebulosa.

5.4.1 O Uso da Lógica Nebulosa

Como visto na seção 3.5, existem muitas abordagens usadas para inferir situações a partir de dados de contexto, mas decidiu-se usar uma técnica baseada em especificação pelas seguintes razões [153]:

1. O usuário precisa conhecer as circunstâncias que caracterizam uma dada situação e conhecer quando o sistema identifica que ele está vivenciando aquela situação. Isso é necessário principalmente porque o usuário determina as ações que o sistema deve realizar quando a situação é identificada. As decisões de raciocínio de como são realizadas as inferências podem ser conhecidas pelo usuário em técnicas baseadas em especificação, porque as circunstâncias que caracterizam uma situação e ações para serem realizadas a partir dela são especificadas pelos próprios usuários. Dessa forma, técnicas baseadas em especificação permitem aos usuários desenvolverem um modelo mental do sistema e entenderem as decisões do sistema;

2. Não existe a necessidade de uma fase de treinamento como seria requerido se alguma técnica de aprendizagem de máquina supervisionada fosse utilizada. Isso ocorre porque os usuários definem suas situações usando especificações, tais como regras nebulosas, ou seja, usuários realizam o papel de especialistas no sistema. O uso de aprendizagem de máquina supervisionada para identificar situações iria requerer que cada usuário passasse por uma fase de treinamento individual, o que poderia consumir muito tempo e depender de um constante retorno do usuário. Essa fase é utilizada para criar a base de conhecimento do sistema e ela é requerida porque os dados de contexto usados para definir uma dada situação vivenciada por usuários distintos são normalmente diferentes. Por exemplo, a situação "trabalhando" vivenciada por João é diferente da que é vivenciada por Maria. Além disso, mudanças na rotina diária do usuário iriam requerer a realização de uma nova fase de treinamento a fim de aprender as novas situações vivenciadas naquela nova rotina. Usando uma técnica baseada em especificação, o usuário deve simplesmente definir as novas situações que ele pode vivenciar. Nesse sentido, a necessidade pela realização de uma fase de treinamento individual poderia dificultar a adoção da solução proposta;

3. Mesmo se alguma técnica baseada em aprendizagem supervisionada fosse usada, ela requereria esforços manuais do usuário para rotular as situações a partir dos dados de contexto observados. Portanto, técnicas de aprendizagem supervisionada requiriam um processo de rotulação manual dos dados de treinamento.

Entre as diversas técnicas baseadas em especificação descritas na seção 3.5, optou-se por utilizar especificamente a lógica nebulosa pelas seguintes razões [5, 111, 118]:

1. Como descrito na literatura de QoC (ver seção 3.3), as informações de contexto obtidas a partir de sensores podem não ter qualidade. A lógica nebulosa é amplamente usada para lidar com incerteza (ver seção 3.6);

2. Situações correspondem a uma realidade que pessoas percebem, vivem e raciocinam [113]. O raciocínio humano é naturalmente ambíguo, impreciso, vago e qualitativo e a lógica nebulosa tem sido usada para modelá-lo computacionalmente;

3. A lógica nebulosa provê uma notação para representar o processo de inferência usando regras que podem ser facilmente entendidas. As regras nebulosas proveem uma linguagem que usa variáveis linguísticas, as quais permitem ao usuário expressar informações contextuais que representam valores como termos ao invés de conjuntos *crisp*. Além disso, esses termos podem ser representados em interfaces amigáveis;

4. A lógica nebulosa impõe um baixo custo computacional para realizar o processo de inferência e, portanto, pode ser executado no próprio dispositivo móvel, o que evita uma distribuição do processamento com um lado servidor, eventualmente disponível através de uma infraestrutura de computação em nuvem. Dessa forma, o processo de identificação da situação atual do usuário não depende de condições do canal de comunicação ou disponibilidade de uma infraestrutura de serviços em um lado servidor. Isso é importante porque a situação atual do usuário é requerida em tempo real no momento da postagem.

5.4.2 O Modelo Conceitual

Para realizar o processo de identificação de situações em que o usuário está, propõe-se um modelo conceitual em camadas ilustrado na Figura 5.4. Inicialmente os dados brutos são obtidos de fontes de contexto, tais como sensores de localização, relógio do dispositivo, dentre outras fontes, as quais são detalhadas na seção 5.4.3. Após isso eles são modelados, primeiramente realizando-se um pré-processamento para formatar os dados de maneira a serem utilizados, por exemplo, retirando informações redundantes ou não usadas. Em seguida, eles passam pelo processo de *fuzzificação*. Ao final, na fase de inferência nebulosa (*fuzzy*) os diferentes tipos de informações de contexto são combinados e correlacionados para identificar uma situação do usuário, o que corresponde ao raciocínio de contexto.

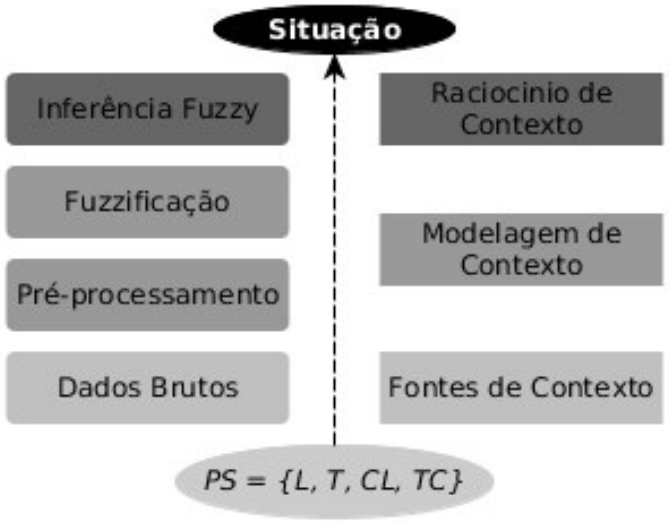

Figura 5.4: Modelo Conceitual da Inferência de Situação.

Na fase de *fuzzificação*, dados de contexto são representados por variáveis linguísticas, ou seja, é feito um mapeamento de informações quantitativas para qualitativas. Portanto, dados de localização e tempo são representados através das seguintes variáveis linguísticas:

- L = {**mesmo lugar** da localização escolhida no mapa, **próximo** à localização escolhida, lugar diferente (ou **distante**) da localização escolhida};
- $T_{periodo}$ = {madrugada, manhã, tarde, noite};
- T_{semana} = {dias da semana, final de semana};

- *CL* = {o usuário está **co-localizado** com um grupo de contatos ou contatos individuais, ele **não está co-localizado** com contatos}

A informação de contexto sobre o tipo de conteúdo não é usada pelo modelo, ao invés disso ela é usada para restringir quais situações definidas devem ser levadas em consideração no processo de inferência. Por exemplo, uma situação pode ser identificada somente em postagens de fotos ou de vídeos. Os tipos de conteúdos usados são: *TC = {mensagem, foto, vídeo e check-in}*. Portanto, o tipo de conteúdo é usado como um verificador com o objetivo de validar se a situação inferida é aplicada ao tipo de conteúdo a ser postado. Caso não seja, a situação referente à regra seguinte que tem maior valor de ativação é escolhida. Neste ponto, observa-se que é possível haver algum caso em que nenhuma regra seja ativada, logo, o usuário deve configurar uma política de privacidade padrão para ser aplicada, caso não seja inferida nenhuma situação registrada.

Ressalta-se ainda que o tipo de conteúdo não está relacionado com a semântica da informação que está sendo postada. Isso requereria uma análise mais aprofundada da informação contida na postagem de maneira a entender seu significado, o que foge do escopo desta tese. Além disso, a consideração da semântica do conteúdo para identificar uma situação demandaria esforços para conceber uma solução que entendesse a semântica de cada tipo de mídia (mensagem, foto, vídeo e *check-in*).

É importante frisar também que as regras nebulosas (a base de conhecimento do sistema) que representam situações são criadas em tempo de execução, ou seja, o *SelPri* habilita o gerenciamento (adição e remoção) das regras através de interfaces gráficas. Uma base de conhecimento em um sistema nebuloso é normalmente estática e criada por um especialista no domínio da aplicação, mas no *SelPri* ela é mantida pelos próprios usuários.

5.4.3 O Processo de Inferência Nebulosa Adaptado para Identificar Situações

Os conjuntos nebulosos dos dados de contexto de localização, co-localização e tempo (dias da semana e períodos do dia) são representados por funções trapezoidais

e triangulares vistas nas tabelas a seguir (Tabelas 5.1, 5.2, 5.3 e 5.5), com seus respectivos graus de pertinência (μ) e variáveis linguísticas. Posteriormente, as funções são ilustradas graficamente na Figura 5.5. Após isto é dada uma explicação do funcionamento de uso dos conjuntos nebulosos.

Conjunto (variável linguística)	**Grau de Pertinência**
Mesmo Local	$\mu(x) = \begin{cases} 1, & \text{se } 0 \leq x \leq 300; \\ \frac{300-x}{200}, & \text{se } x \in (100, 300); \\ 0, & \text{se } x \geq 300. \end{cases}$
Próximo	$\mu(x) = \begin{cases} 0, & \text{se } x \leq 0; \\ \frac{x}{300}, & \text{se } x \in (0, 300); \\ 1, & \text{se } 300 \leq x \leq 800; \\ \frac{1200-x}{400}, & \text{se } x \in (800, 1200); \\ 0, & \text{se } x \geq 1200. \end{cases}$
Locais Distantes	$\mu(x) = \begin{cases} 0, & \text{se } x \leq 800; \\ \frac{x-800}{400}, & \text{se } x \in (800, 1200); \\ 1, & \text{se } x \geq 1200. \end{cases}$

Tabela 5.1: Funções dos Conjuntos Nebulosos de Localização.

Conjunto (variável linguística)	**Grau de Pertinência**
Não co-localizado	$\mu(x) = \begin{cases} 1, & \text{se } x = 0; \\ \frac{1-x}{1}, & \text{se } x \in (0, 1); \\ 0, & \text{se } x = 1. \end{cases}$
Co-localizado	$\mu(x) = \begin{cases} 0, & \text{se } x = 0; \\ \frac{x}{1}, & \text{se } x \in (0, 1); \\ 1, & \text{se } x = 1. \end{cases}$

Tabela 5.2: Funções dos Conjuntos Nebulosos de Co-localização.

Para o dado de localização (*L*) é utilizada a distância euclidiana em metros entre o ponto (coordenada geográfica – latitude e longitude) que o usuário está e o ponto referente ao lugar registrado na situação. Logo, x = loc_{atual} - loc_{perfil}, em que loc_{atual} é a localização atual do usuário, e loc_{perfil} é a localização de um lugar. Para o dado de co-localização (*CL*) também é utilizada a distância euclidiana, porém entre o usuário e os contatos que ele deseja considerar para a situação. Portanto, é

Conjunto (variável linguística)	Grau de Pertinência
Final de Semana	$\mu(x) = \begin{cases} 1, & \text{se } 0 \leq x \leq 0.7; \\ \frac{1.3-x}{0.6}, & \text{se } x \in (0.7, 1.3); \\ 0, & \text{se } x \geq 1.3. \end{cases}$
Final de Semana - 2	$\mu(x) = \begin{cases} 0, & \text{se } x \leq 5.7; \\ \frac{x-5.7}{0.6}, & \text{se } x \in (5.7, 6.3); \\ 1, & \text{se } x \geq 6.3. \end{cases}$
Dias da Semana	$\mu(x) = \begin{cases} 0, & \text{se } x \leq 0.7; \\ \frac{x-0.7}{0.6}, & \text{se } x \in (0.7, 1.3); \\ 1, & \text{se } 1.3 \leq x \leq 5.7; \\ \frac{6.3-x}{0.6}, & \text{se } x \in (5.7, 6.3); \\ 0, & \text{se } x \geq 6.3. \end{cases}$

Tabela 5.3: Funções dos Conjuntos Nebulosos de Tempo – Dias da Semana (1 semana = 7 dias).

possível adicionar mais de um contato à co-localização. Isso é feito como explicado na seção 5.7.1.

Os conjuntos nebulosos de *T* para "dias da semana" e "períodos do dia" são cíclicos, ou seja, eles reiniciam ao final da escala de conjuntos. Dessa forma, para modelar estes dados de contexto em conjuntos nebulosos houve a necessidade de criar dois conjuntos para representar a mesma variável linguística. No caso de dias da semana criou-se os conjuntos "Final de Semana" e "Final de Semana - 2", e períodos do dia criou-se os conjuntos "Noite" e "Noite - 2". Na implementação isso é facilmente ajustado de maneira que o usuário conheça apenas uma única variável linguística. Por exemplo, caso o usuário crie uma situação com um período do dia "Noite", o mecanismo de inferência registra uma regra da seguinte forma: **Se** *(Período do dia é "Noite" ou "Noite2")* **Então** *Situação A*. Dessa forma, ambos os conjuntos são verificados a fim de validar a regra.

Como exemplo de situação, considere um cenário a seguir com sua respectiva regra nebulosa:

- Localização (*L*): o usuário registrou um ponto nas proximidades da UFMA e optou pela variável linguística "Mesmo Local";

Conjunto (variável linguística)	Grau de Pertinência
Madrugada	$\mu(x) = \begin{cases} 0, & \text{se } x \leq 0; \\ \frac{x}{2}, & \text{se } x \in (0,2); \\ 1, & \text{se } 2 \leq x \leq 4; \\ \frac{6-x}{2}, & \text{se } x \in (4,6); \\ 0, & \text{se } x \geq 6. \end{cases}$
Manhã	$\mu(x) = \begin{cases} 0, & \text{se } x \leq 4; \\ \frac{x-4}{2}, & \text{se } x \in (4,6); \\ 1, & \text{se } 6 \leq x \leq 12; \\ \frac{14-x}{2}, & \text{se } x \in (12,14); \\ 0, & \text{se } x \geq 14. \end{cases}$
Tarde	$\mu(x) = \begin{cases} 0, & \text{se } x \leq 12; \\ \frac{x-12}{2}, & \text{se } x \in (12,14); \\ 1, & \text{se } 14 \leq x \leq 17; \\ \frac{17-x}{2}, & \text{se } x \in (17,19); \\ 0, & \text{se } x \geq 19. \end{cases}$
Noite	$\mu(x) = \begin{cases} 0, & \text{se } x \leq 17; \\ \frac{x-17}{2}, & \text{se } x \in (17,19); \\ 1, & \text{se } 19 \leq x \leq 23.99. \end{cases}$
Noite - 2	$\mu(x) = \begin{cases} \frac{2-x}{2}, & \text{se } x \in (0,2); \\ 0, & \text{se } x \geq 2. \end{cases}$

Tabela 5.4: Funções dos Conjuntos Nebulosos de Tempo – Períodos do Dia (1 dia = 24h).

- Tempo (*T*): para os dias da semana o usuário optou pela variável linguística "Dias da Semana", e para períodos do dia ele escolheu as variáveis "Manhã" e "Tarde";
- Co-localização (*CL*): o usuário determinou que estaria co-localizado (com variável linguística de mesmo nome) a João e Maria (por consequência, estes contatos devem também estar utilizando o *SelPri*);
- Tipo de conteúdo (*TC*): por escolha do usuário, fotos e vídeos postados serão considerados para esta situação.

A regra nebulosa originada a partir destas características é: **Se** *(Localização é "Mesmo Local")* **E** *(Dia da Semana é "Dias da Semana")* **E** *(Período do dia é "Manhã"*

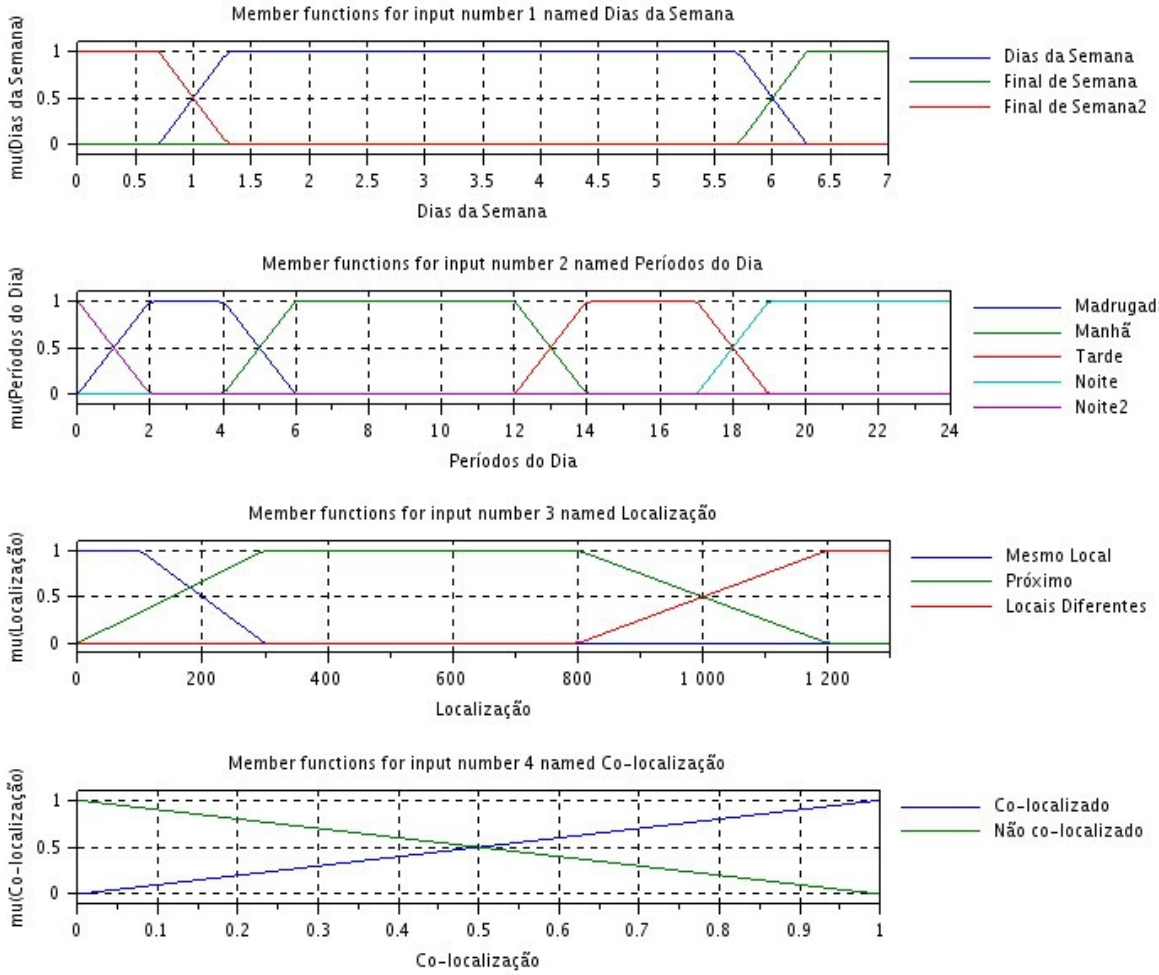

Figura 5.5: Gráficos dos Conjuntos Nebulosos dos Dados de Contexto.

OU *"Tarde")* **E** *(Co-localização é "Co-localizado")* **Então** *Situação B*. Entretanto, essa regra apenas se aplica a postagens de conteúdos de fotos e vídeos, como foi especificado no tipo de conteúdo (*TC*). Para a informação de localização, no momento da postagem é verificada a localização mais atual do usuário e o ponto registrado referente a UFMA, em seguida sendo calculada a distância euclidiana entre eles. Para a informação de co-localização, é calculada a distância euclidiana entre o usuário e os contatos João e Maria, tendo como valor de entrada correspondente a esse dado de contexto na regra nebulosa uma função de decaimento temporal que será explicada detalhadamente na seção 5.7.1.

5.4.4 Limitações e Questões de Flexibilidade

A versão atual do motor de inferência nebulosa de situação implementado baseado no modelo conceitual para ser usado no *SelPri* considera um conjunto limitado

de dados de contexto. Entretanto, o motor já permite a definição de muitas situações que representam a vida diária de uma pessoa. A escolha deste conjunto específico de dados de contexto para compor a definição de uma situação foi motivada pela elicitação de requisitos realizada (seção 5.1). Adicionalmente, o modelo conceitual proposto é flexível, permitindo a adição e remoção de outras informações contextuais para compor e definir uma situação. Para fazer isso, os novos dados de contexto devem ser modelados em conjuntos nebulosos úteis e um novo motor de inferência de situação deve ser implementado. Portanto, embora a implementação atual do motor de inferência limite quais dados de contexto são usados para definir uma situação, o modelo conceitual é flexível, permitindo a incorporação de novos dados de contexto.

Considerando essa possibilidade de ser implementado com dados de contexto diferentes destes descritos nesta seção, o modelo conceitual proposto pode ser adaptado para permitir a identificação de outros tipos de situação, aplicáveis a outros domínio além da privacidade em RSMs. Para demonstrar a flexibilidade do modelo conceitual proposto nesta tese, um outro motor de inferência foi implementado baseado no modelo para ser usado em um domínio totalmente diferente (o de saúde mental) com outros dados de contexto, o qual é detalhado na seção 5.8.

Uma limitação do motor de inferência nebulosa é a necessidade por todos os dados de contexto utilizados para a identificação de situações. Dessa forma, quando algum dos dados de contexto não está presente, não é possível identificar a situação atual do usuário. Por exemplo, caso o usuário desative a obtenção da localização através das configurações do sistema operacional Android, então o motor de inferência não identifica a situação atual. Apesar disso, o *SelPri* solicita ao usuário para que seja ativada a obtenção da localização a cada vez que ele tenta realizar uma inferência e essa informação não é disponibilizada pelo sistema operacional. Portanto, o motor de inferência nebulosa funciona corretamente somente quando obtêm todos dados de contexto utilizados para identificar a situação do usuário.

5.5 Perfil de Privacidade Situacional

O *SelPri* propõe um recurso para ser usado em modelos de controle de acesso de RSMs existentes, chamado de Perfil de Privacidade Situacional (PPS). As

especificações das situações e das configurações de privacidade aplicadas a elas são definidas no PPS, o qual possui a seguinte definição:

Perfil de Privacidade Situacional. *Um conjunto de dados de contexto agregados, configurados pelo usuário, usados para identificar sua situação que é mapeado para uma configuração de privacidade da rede social móvel, utilizado para expressar o desejo de privacidade dinâmico do usuário considerando a situação em que ele se encontre em um dado momento.*

Em sistemas de controle de acesso, os objetos (por exemplo, mensagens, fotos, vídeos) são as informações a serem protegidas, ações (por exemplo, curtir, comentar, compartilhar) podem ser executadas nos objetos, sujeitos (por exemplo, um amigo ou um seguidor) requisitam a execução de ações sobre os objetos, e condições (por exemplo, o sujeito precisa ser um membro da família para acessar um conteúdo) são restrições usadas para controlar ações [121]. Os controles de acesso que representam as configurações de privacidade podem ser expressados de várias formas em RSMs, e cada um deles tem uma forma específica de permitir aos usuários determinarem suas preferências. Por exemplo, as configurações de privacidade do Facebook usam lista de amigos para permitir usuários organizarem sujeitos (ou seja, um contato individual ou grupo de contatos) para quem é concedida ou negada ações a objetos. Similarmente (com poucas diferenças), o Google+ usa a noção de círculos. O uso de lista de amigos no Facebook e círculos no Google+ permite o usuário selecionar a audiência permitida para acessar um conteúdo específico. Algumas RSMs permitem aos usuários expressarem condições temporais, como o Snapchat, em que um conteúdo postado é mantido disponível para visualização por somente 24 horas para os contatos do usuário. Entretanto, outras RSMs não têm controles de privacidade de granularidade fina, tal como o Instagram, que não permite o agrupamento de contatos.

O PPS permite ao usuário configurar quais sujeitos terão permissões de executar ações no conteúdo postado para cada situação definida. Dessa forma, a situação do usuário é a condição usada para a escolha da audiência de uma postagem. O PPS é criado pelo usuário, o qual deve informar as informações de contexto que caracterizam a situação e a configuração de privacidade, a ser aplicada a seus conteúdos postados se ele estiver naquela dada situação. O usuário também deve

nomear o perfil com uma palavra ou uma oração/frase curta, chamando-o por algum nome que caracteriza a situação, por exemplo. O *SelPri* é então proposto para ser usado em RSMs que têm configurações de privacidade de granularidade fina com controles que permitem especificar a audiência permitida para executar ações em conteúdos postados.

Para ilustrar o uso do PPS, considere um exemplo chamado "estudando", para o qual foi configurado o acesso ao conteúdo publicado em uma dada situação somente a contatos do grupo família. Dessa forma, a situação é inferida e em seguida a configuração de privacidade estabelecida durante a criação do PPS é aplicada ao conteúdo postado. Ressalta-se que o usuário tem um papel fundamental neste processo de especificação do PPS, pois ele o cria, determinando os dados de contexto que caracterizam a situação e também a quem são dadas permissões de acesso ao conteúdo. Exatamente por esse motivo considera-se que a interação do usuário com o sistema é um ponto de avaliação nesta proposta, além de verificar se a proposta em si atende seus desejos dinâmicos e contextuais de privacidade. As avaliações do *SelPri* são apresentadas no capítulo 6.

5.6 Gerenciamento Autônomo de Privacidade

A privacidade é um desejo centrado no usuário (*user-centric*), ou seja, o usuário deve poder decidir o que é feito com suas informações pessoais. Para atender este requisito e ao mesmo tempo possibilitar que o sistema possua autonomia para escolher qual configuração de privacidade deve ser usada em postagens, de acordo com a situação do usuário, esta proposta adota o que chama-se de **Gerenciamento Autônomo de Privacidade**, através da definição de níveis de autonomia. São dois níveis que foram concebidos para o usuário poder entender como o *SelPri* funciona e de forma gradual confiar sua privacidade ao sistema. Esse gerenciamento é uma configuração que permite o usuário definir qual dos níveis deseja utilizar.

No **nível de autonomia 1 (sem autonomia)**, o *SelPri* gera uma notificação ao usuário quando um conteúdo é postado, questionando-o se deve ser usada a configuração de privacidade associada com a situação identificada, de acordo com as definições dos PPSs. Caso o usuário decida por não utilizar, a configuração

de privacidade padrão é aplicada. Consequentemente, esse nível requer entradas do usuário a cada postagem para confirmar se a configuração de privacidade recomendada deve ser usada. Usando esse nível, o usuário deve gradualmente se tornar mais confiante em relação à habilidade que o *SelPri* tem para identificar corretamente suas situações e aplicar configurações de privacidade adequadas, como definidas nos perfis.

No **nível de autonomia 2 (com autonomia)**, o usuário delega completamente para o *SelPri* a tarefa de aplicar a configuração de privacidade sem requerer qualquer ação por parte do usuário no ato da postagem. Nesse caso o usuário somente é notificado do perfil que foi selecionado pelo *SelPri* cada vez que uma postagem é feita. A configuração de privacidade padrão somente é usada quando nenhuma situação é identificada. Portanto, a definição da configuração de privacidade das postagens nesse nível é completamente transparente ao usuário.

Destaca-se que os usuários podem modificar o nível de autonomia a qualquer momento, mas, por padrão, utiliza-se o nível 1. Além disso, para o correto funcionamento da solução, os usuários devem configurar previamente seus perfis e definir uma configuração de privacidade padrão.

5.7 Modelo Arquitetural e Aspectos de Implementação

O modelo conceitual descrito anteriormente é genérico o suficiente para ser utilizado em diversos cenários de RSMs, integrado a diferentes redes sociais existentes. O modelo conceitual e os conceitos propostos de PPS e gerenciamento autônomo de privacidade desta pesquisa é que considera-se como contribuição. Porém, para mostrar sua viabilidade, desenvolveu-se um protótipo.

O protótipo do *SelPri* foi desenvolvido para o sistema operacional Android[5], o qual tem uma plataforma de desenvolvimento bastante robusta e com muitos recursos[6]. Além disso, uma grande quantidade de dispositivos móveis e vestíveis o utilizam, tais como: *smartphones*, *tablets*, relógios, televisões e automóveis. Ressalta-se que o *SelPri* é integrado ao Facebook devido este ser a rede social mais utilizada

[5] `http://www.android.com/`

[6] `http://developer.android.com/index.html`

atualmente no mundo e no Brasil. A arquitetura do *SelPri* é exibida na Figura 5.6 e explicada logo em seguida. Para a implementação foi utilizada a linguagem de programação Java, a qual é utilizada por todos os componentes do modelo arquitetural.

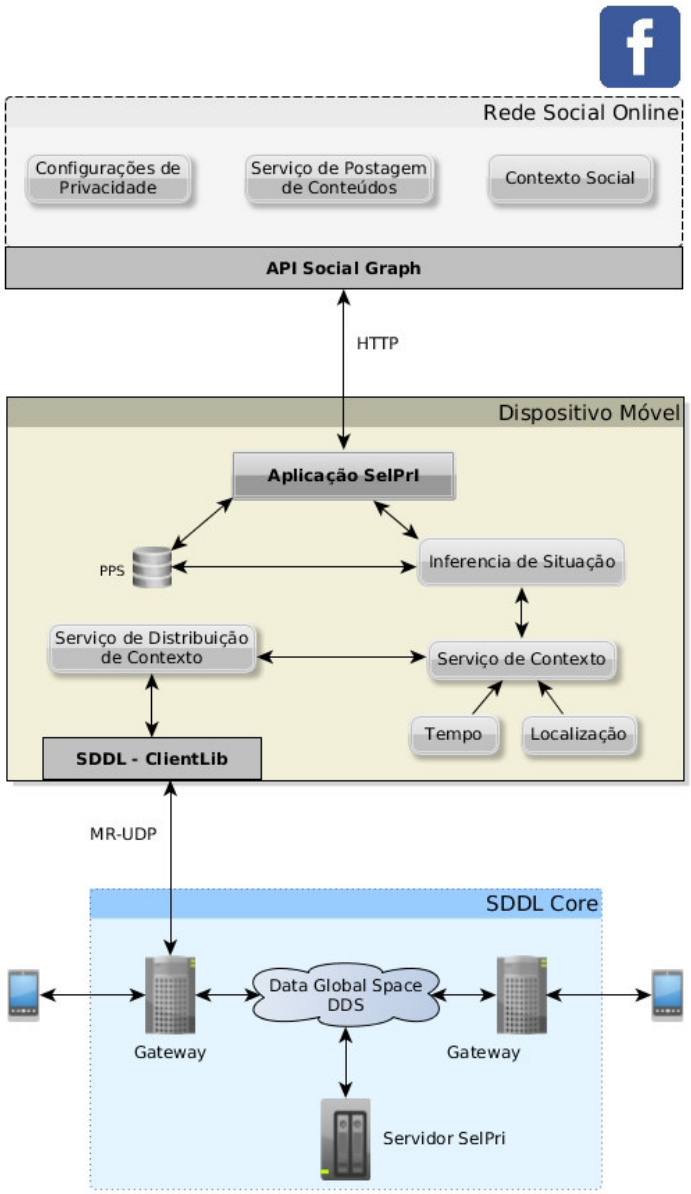

Figura 5.6: Diagrama dos Componentes do *SelPri*.

Como o protótipo do *SelPri* é integrado ao Facebook, as postagens de conteúdos são realizadas nesta rede social. O *SelPri* utiliza a API do Facebook, chamada de *Social Graph* (ou somente *Graph API*)[7], para: realizar postagem de conteúdo, modificar as configurações de privacidade das postagens, e também realizar consultas a dados de contexto social. Os métodos usados para consultas a dados de

[7] `https://developers.facebook.com/`

contexto social retornam: o identificador do usuário no Facebook, o nome do usuário, a lista de contatos, e também a representação semântica de coordenadas para realizar postagens de *check-in*. A API *Social Graph* usa o protocolo de comunicação *Hypertext Transfer Protocol* (HTTP).

A aplicação *SelPri* possui as interfaces visuais com o usuário para: (i) configuração de PPSs (criação e exclusão), (ii) postagem de conteúdos na rede social (Facebook), (iii) configuração dos níveis de autonomia, (iv) interação com o usuário nos cenários explicados nos dois níveis de autonomia, seja requisitando o usuário para confirmar se deve usar a configuração de privacidade de acordo com a situação identificada e definida do PPS, ou apenas notificando o usuário da configuração de privacidade aplicada, (v) ajuda ao usuário, (vi) uma opção "Sobre" para que o usuário conheça do que se trata a aplicação, e (vii) interfaces para funcionalidades básicas, tais como *login* e *logout*. Uma dessas interfaces é responsável pela definição de PPSs (como explicado a seguir na seção 5.7.3) armazenando-os em memória permanente na base base de dados PPS, a fim de serem utilizados pelo componente de inferência de situação.

O componente de inferência de situação utiliza a biblioteca *jFuzzyLogic*[8] [32, 33], a qual possui a versão *core* que é específica para aplicações móveis. Para realizar o processo de inferência de situação esse componente obtém os dados de contexto do serviço de contexto.

O serviço de contexto é um serviço Android responsável por obter, formatar e prover dados de contexto. As coordenadas de localização são obtidas por ele através do GPS e da rede móvel. O tempo é adquirido através do relógio local do dispositivo. A co-localização é uma informação de localização que utiliza o serviço de distribuição de contexto. Como será explicado detalhadamente na seção 5.7.1, a co-localização é obtida através do cálculo da distância euclidiana entre as localizações do usuário e de seus contatos.

O serviço de distribuição de contexto é o componente responsável por usar a comunicação do *middleware* SDDL (ver seção 3.4.1) para transmitir atualizações da informação de localização (longitude e latitude) para o servidor *SelPri* e também registrar interesse em obter a localização de outros contatos. A biblioteca do SDDL

[8] `http://jfuzzylogic.sourceforge.net/`

utilizada no dispositivo móvel é chamada de *ClientLib* que, por sua vez, se comunica com o *gateway* utilizando o protocolo MR-UDP. O *gateway* funciona como uma ponte, transmitindo dados originados dos dispositivos móveis que usam o protocolo MR-UDP para o núcleo da rede (o *SDDL Core*) e vice-versa. Os dispositivos que compõem o núcleo SDDL se comunicam através de uma implementação da especificação DDS. A quantidade de *gateways* é escalável, podendo aumentar de acordo com a necessidade de suportar mais dispositivos móveis conectados simultaneamente. O SDDL permite o uso de três implementações do DDS e optou-se por usar o *OpenSplice* por ser aberto e ter uma versão *Community* com licença LGPLv3[9], além de ser estável.

A informação de localização é enviada para contatos através do servidor *SelPri* localizado no *SDDL Core*. Esse servidor foi desenvolvido como uma extensão de um *processing nodes* dentro da arquitetura do *middleware* SDDL (ver seção 3.4.1). Os demais componentes do *middleware* não foram alterados. O servidor *SelPri* mantém a informação de co-localização de todos os usuários associada a seus identificados do Facebook e é responsável pela distribuição dessa informação para os contatos interessados. Um nó móvel consulta periodicamente o servidor buscando as localizações dos contatos do usuário que são de interesse (ou seja, que constam nos PPSs definidos pelo usuário), a fim de manter os dados necessários para processar as regras nebulosas que usam a informação de co-localização. Consequentemente, a informação de co-localização pode ser inferida somente entre usuários do *SelPri* e, ao mesmo tempo, que sejam amigos no Facebook. Outra questão importante é que esse servidor *SelPri* também é utilizado para receber e armazenar o log das avaliações, as quais são explicadas no próximo capítulo, como também manter a base de dados dos usuários que possuem a aplicação.

5.7.1 O Gerenciamento da Informação de Co-localização

O gerenciamento da informação de co-localização é particularmente crítico, por conta de questões de mobilidade, segurança e privacidade. Com relação à mobilidade, um dispositivo móvel pode ficar temporariamente desconectado da Internet ou passar por períodos de conectividade fraca ou intermitente, sem poder atualizar adequadamente sua localização junto ao servidor *SelPri*. Dessa forma,

[9] `https://www.gnu.org/licenses/lgpl.html`

a informação de localização necessária para identificar os contatos co-localizados pode ficar desatualizada no servidor. Um processo de inferência da situação usando informações de co-localização desatualizadas ou nulas (por questões de não disponibilidade) resulta na não ativação de regras nebulosas. Portanto, o uso da informação de co-localização pode diminuir a acurácia do motor de inferência para identificar situações. Por esse motivo o motor de inferência utiliza uma função de decaimento temporal. Além disso, ressalta-se que o uso da informação de co-localização para compor uma situação é opcional na atual implementação do motor de inferência usado no *SelPri*.

O valor de entrada utilizado no motor de inferência de situação para o conjunto nebuloso de co-localização é obtido a partir dos seguintes passos: (i) verifica-se qual a distância euclidiana do usuário para o(s) contato(s) constantes nos PPSs especificados, e considera-se co-localizado o contato que está até 300 metros do usuário; (ii) com base da idade da informação de localização de todos os contatos considerados co-localizados, calcula-se um valor de confiança através de uma função de decaimento temporal (quanto mais velha, menor é o valor de confiança) com idade máxima de 3 horas (quando a idade chega em 180 minutos seu valor de confiança equivale a zero). Segue um exemplo: se a última atualização da localização de um contato tem 1 hora então seu valor de confiança é aproximadamente 0,66, mas se ela tem 2 horas e 30 minutos então o valor obtido é próximo a 0,16; (iii) soma-se todos os valores de confiança e calcula-se qual a porcentagem que eles representam em relação a quantidade de contatos escolhidos na situação (ou seja, no PPS) – por exemplo, se o usuário definiu 5 contatos, mas apenas 2 estão co-localizados, e a soma dos valores de confiança deles é 1,5, o resultado obtido com o cálculo será 0,3 (ou seja, 1,5/5); (iv) o resultado final dessa computação é utilizado como valor de entrada no conjunto nebuloso de co-localização.

A confidencialidade, integridade e autenticação na comunicação entre os dispositivos móveis e o lado servidor é garantida pelo SDDL [61]. O protótipo do *SelPri* provê meios para garantir a privacidade no gerenciamento da informação de co-localização. Um usuário pode obter a localização de um outro somente nas seguintes condições: (1) se eles são amigos no Facebook; (2) se o dono da localização autoriza o *SelPri* a transmiti-la ao contato que definiu uma situação (ou seja, um perfil) adicionando-o dentre os contatos co-localizados; (3) se o usuário tiver habilitado

as atualizações de localização no servidor *SelPri* (isso porque ele pode suspender as atualizações em qualquer tempo). Esses mecanismos permitem aos usuários controlar o acesso a suas informações de localização. Dessa forma, observa-se que a implementação preocupa-se com questões de privacidade, evitando que um usuário do *SelPri* tenha acesso a localização de outro livremente.

5.7.2 Economia de Recursos do Dispositivo Móvel

Os usuários podem se sentir incomodados com um possível uso de bateria em excesso pela aplicação ou com o uso de tráfego na rede, devido ao envio das localizações ao servidor *SelPri*, o qual pode consumir seu plano de dados junto a operadora de telefonia móvel. A implementação do *SelPri* possui mecanismos que garantem uma gestão eficiente dos recursos utilizados para sua execução, em especial a bateria e o tráfego na rede.

Os serviços de contexto e distribuição inicializam junto ao sistema operacional, mas são ativados apenas quando existir algum usuário logado na aplicação. Essa é uma primeira medida para economia de energia, visto que os serviços só são realmente ativados quando forem necessários. Uma outra solução adotada é fazer com que o processo de obtenção e distribuição dos dados de contexto se adapte ao nível de bateria (*energy awareness*). Neste sentido, há três intervalos de tempo para a obtenção dos dados de contexto e atualização de localização do servidor *SelPri*: um para quando o nível de bateria for maior que 80% (a cada 5 minutos), outro quando ela estiver entre 30% e 79% (a cada 10 minutos) e quando o nível for menor que 30% (a cada 15 minutos).

5.7.3 Definindo um Perfil de Privacidade Situacional

Um requisito essencial para a adoção do *SelPri* é a provisão de interfaces fáceis para serem usadas para definir PPSs. A lógica nebulosa provê variáveis linguísticas que facilitam essa tarefa. A Figura 5.7 mostra as interfaces gráfica do *SelPri* usadas para definir PPSs. A criação dos perfis pode ser realizada por usuários a qualquer momento e eles podem refinar seus perfis ao longo do tempo de uso da aplicação.

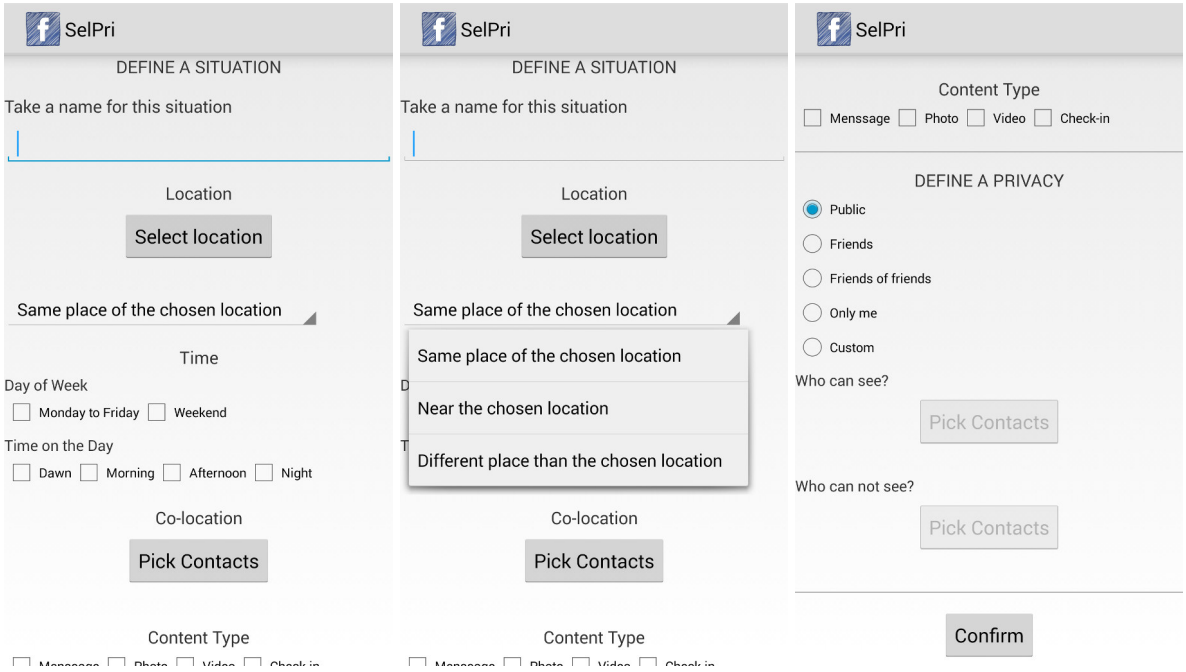

Figura 5.7: Interfaces Móveis do *SelPri* para Definição de PPSs.

Inicialmente o usuário define as informações de contexto que caracterizam uma situação, como descrito anteriormente na seção 5.4, provendo as informações de localização, dia da semana, período do dia, co-localização, e o tipo de conteúdo que ele deseja postar (mensagem, foto, vídeo e *check-in*). Dessa forma, o usuário provê os dados necessários para a definição das regras que representam suas situações. O usuário também define as configurações de privacidade que serão usadas em cada perfil, as quais são as mesmas do Facebook. Por fim, os PPSs definidos são salvos em uma base de dados local no dispositivo móvel do usuário.

Os usuários podem definir 24 regras de situação diferentes usando os conjuntos nebulosos de informações de contexto do protótipo do *SelPri*: 3 (três tipos de localização) * 4 (quatro períodos do dia diferentes) * 2 (dias da semana e final de semana) * 1 (existem dois conjuntos nebulosos para a informação de co-localização, mas quando ela é usada apenas o conjunto "co-localizado" é inserido em uma regra – decidiu-se não permitir a criação de uma situação informando que o usuário não está co-localizado a um determinado contato, ou seja, usar o conjunto "não co-localizado") = 24. Entretanto, a avaliação das regras de situação não é atômica, ou seja, regras de situação são avaliadas individualmente para determinação de seus graus de ativação. Isso permite que os valores de entrada no precedente sejam diferentes em cada regra e, portanto, regras idênticas podem ter graus de ativação diferentes.

Mais especificamente, valores de entrada em relação a localização e co-localização são determinados a cada nova avaliação das regras, uma vez que: (i) o valor de entrada para a condição relacionada a localização pode mudar frequentemente, porque a distância Euclidiana entre o usuário e o ponto provido no mapa na criação do perfil pode alterar; (2) similarmente, o valor de entrada para a condição relacionada a co-localização muda, porque uma regra pode ser criada com diferentes contatos co-localizados, e a distância entre o usuário e os contatos pode mudar também frequentemente. Dessa forma, o *SelPri* permite a criação de regras iguais para se referir a situações diferentes e, para fazer isso, basta que os usuários escolham localizações ou contatos co-localizados diferentes.

Um Exemplo de PPS e Inferência de Situação

Considere um exemplo PPS chamado de "trabalhando" pelo usuário, o qual é definido com as seguintes informações:

- Localização: item "mesmo lugar" escolhido pelo usuário, ou seja, mesmo lugar que um ponto definido no mapa pelo usuário, o qual equivale a seu local de trabalho;
- Dia da semana: opção "dias da semana" marcada pelo usuário;
- Período do dia: opções "manhã" e "tarde" marcadas pelo usuário;
- Co-localização: o usuário escolhe um colega de trabalho chamado João para caracterizar a situação;
- Tipo de conteúdo: todas opções são marcadas pelo usuário;
- Privacidade: o usuário seleciona a opção "Personalizado" e informa o grupo de contatos chamado de "Colegas de trabalho" para os contatos que não podem ver o conteúdo.

A regra nebulosa originada a partir desse PPS é a seguinte: **Se** Localização = "Mesmo lugar" **E** Dia da semana = "dias da semana" **E** Período do dia = "Manhã" **OU** "Tarde" **E** Co-localização = "Co-localizado" **ENTÃO** a situação é *Trabalhando*. Ressalta-se que essa situação é aplicada a todos os quatro tipos de conteúdo que podem ser

postados pelo usuário através do *SelPri*: mensagem, foto, vídeo, e *check-in*. Quando essa situação é inferida pelo *SelPri*, todos contatos, com exceção do grupo de contatos chamado "Colegas de Trabalho" poderão acessar o conteúdo que está sendo postado pelo usuário. A regra nebulosa é avaliada pelo motor de inferência da seguinte forma:

- Localização: no momento da inferência, o motor: (1) verifica a localização atual do usuário, (2) verifica as coordenadas armazenadas no PPS (ou seja, o local de trabalho do usuário), e (3) então calcula a distância euclidiana entre os esses dois pontos para determinar o valor de entrada;
- Tempo: no momento da inferência, o motor: (1) verifica o tempo atual a partir do relógio do dispositivo móvel, (2) formata os dados para informações numéricas usadas nas escalas dos conjuntos nebulosos relacionados ao tempo, e (3) determina os valores de entrada para as duas informações de contexto relacionadas ao tempo;
- Co-localização: o contato João é adicionado ao grupo de contatos do usuário que o *SelPri* periodicamente verifica a localização atual consultando o servidor *SelPri*. A distância euclidiana entre o usuário e o João, e a idade da informação de localização do João, são usadas como entrada na função de decaimento temporal para computar e determinar o valor de entrada.

A regra nebulosa terá um grau de ativação máximo quando determinado os seguintes valores de entrada para as condições:

- Localização: de 0 a 100;
- Dia da semana: de 1.3 a 5.7;
- Período do dia: de 6 a 12, ou de 14 a 17;
- Co-localização: 1.

5.8 O Modelo de Identificação de Situação no Domínio de Saúde Mental

A fim de comprovar que o modelo conceitual de inferência de situação proposto nesta tese é flexível, o mesmo foi utilizado como base para a construção de um motor de inferência de situações voltado para o domínio da saúde mental. Esta seção descreve de maneira sucinta este trabalho.

Os dispositivos móveis têm sido aplicados à área de saúde mental como parte dos serviços médicos, psicológicos e de saúde em geral, objetivando ajudar no tratamento de transtornos mentais [62]. Exemplos de transtornos mentais incluem, por exemplo, transtornos ligados ao uso de drogas e álcool, transtornos de humor (por exemplo, depressão), e transtornos delirantes. O *Ecological Momentary Assessment* (EMA) é um mecanismo normalmente usado na psicologia/psiquiatria para solicitar repetidamente a um indivíduo (ou paciente) que responda questões sobre o que ele está fazendo (ou têm feito), ou como ele se sente relativamente a questões de interesse para um tratamento específico que esteja fazendo, durante sua rotina diária. O EMA objetiva avaliar o fluxo de experiências e comportamentos ao longo do tempo, capturando a vida como ela é vivida, momento a momento, hora a hora, dia a dia, como uma forma de caracterizar fielmente indivíduos e de capturar a dinâmica de vivenciar e se comportar ao logo do tempo e em diversos contextos [128]. Já o *Ecological Momentary Intervention* (EMI) provê um mecanismo para tratamentos em que há a necessidade de realizar intervenções psicológicas[10] na vida diária do paciente [69]. Ambos os mecanismos são "ecológicos" por ocorrem em um ambiente natural, e eles são momentâneos devido ao fato de requisitarem auto-avaliações e proverem suporte de tempo real no dia-a-dia do paciente. O EMA e o EMI têm sido implementados como aplicações que executam em dispositivos móveis, por estes fazerem parte da vida cotidiana das pessoas.

A aplicação móvel *MoodBuster* [139] foi desenvolvida no escopo dos projetos ICT4Depression[11] [117] e *European Comparative Effectiveness Research on Internet-based*

[10] Intervenção psicológica é toda forma de tentativa de influenciar de maneira transitória ou definitiva o comportamento humano através do uso de meios psicológicos, ou seja, a influência se dá através de novas formas de comportamento e de experimentar o mundo [69].

[11] `http://www.ict4depression.eu/`

Depression Treatment (E-Compared)[12] [79]. O *MoodBuster* é uma aplicação móvel de EMA e EMI para uso em tratamentos de depressão, questionando ao paciente sobre seus estados relacionados a esse transtorno mental. Por exemplo, ele questiona o paciente sobre suas experiências e estados mentais, tais como humor, motivação, ansiedade e qualidade do sono. A Figura 5.8 mostra três exemplos de interfaces gráfica do *MoodBuster* usadas para requisitar auto-avaliações dos pacientes. A aplicação também apresenta as respostas acumuladas ao longo do tempo em um gráfico, que pode ser consultado também por profissionais envolvidos no tratamento (por exemplo, psicólogos ou psiquiatras). Isso ajuda um paciente a identificar e se preparar para momentos difíceis em que seu humor estiver baixo ou alto.

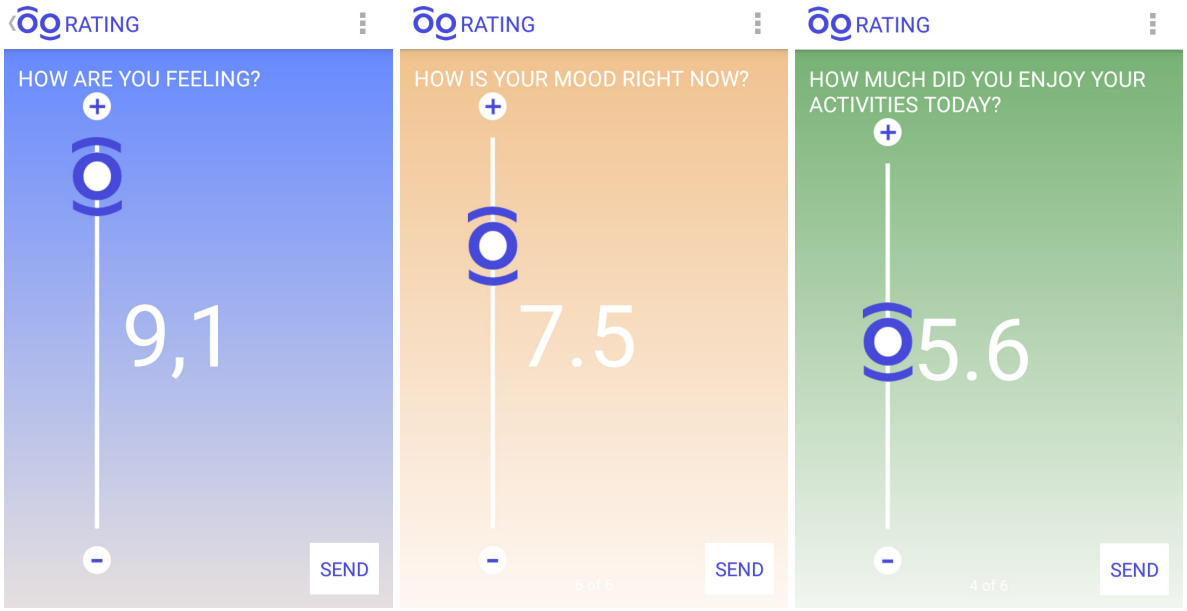

Figura 5.8: Interfaces do *MoodBuster* para Requisitar Auto-avaliações dos Pacientes.

Duas questões surgem para serem resolvidas nesse domínio:

1. *Qual o melhor momento para solicitar do paciente as informações sobre suas experiências e estados mentais?* As solicitações por auto-avaliações de experiências e estados mentais para pacientes podem ser feitas de uma maneira menos intrusiva, de maneira que o próprio paciente possa determinar as situações em que estará disponível para recebê-las;

2. *Como conhecer as situações de rotina diária vivenciadas por pacientes?* Tendo um melhor conhecimento sobre a rotina diária do paciente, um profissional de saúde

[12] `http://www.e-compared.eu/`

mental poderá discutir as causas e efeitos de sintomas depressivos. Dessa forma, a informação sobre as situações vivenciadas pelo paciente em sua rotina diária pode melhorar a efetividade da terapia. O profissional pode correlacionar as situações vivenciadas pelos pacientes com os dados de suas auto-avaliações de experiências e estados mentais, tentando identificar quais situações de rotina diária tem um impacto positivo ou negativo no estado mental do paciente.

Neste trabalho de doutorado foi desenvolvido uma solução denominada *SituMan (Situation Manager)* para abordar esses questões, a qual compreende: (i) um motor de inferência baseado no modelo conceitual descrito na seção 5.4 para identificação de situações relacionadas a rotina diária dos pacientes; (ii) um serviço Android onde fica o motor de inferência, e que também é responsável pela coleta dos dados de contexto. Uma API é também disponibilizada neste serviço para possibilitar outras aplicações se tornarem cientes de situação; e (iii) uma aplicação móvel.

O *MoodBuster* utiliza a API do serviço Android do *SituMan* para requisitar aos pacientes auto-avaliações em situações mais adequadas para eles. Para isso, o paciente (usualmente com a ajuda do profissional de saúde mental) além de definir os dados de contexto que caracterizam as situações, deve informar em quais tipos de requisição ele estará disponível para responder em cada situação definida. Adicionalmente, todas as situações identificadas dos pacientes são registradas em um sumário de situações, de maneira que seja possível os profissionais de saúde consultá-las em seus atendimentos presenciais e também correlacionar com dados auto-reportados pelos pacientes. A Figura 5.9 mostra as interfaces gráfica do *SituMan* usadas para o usuário definir suas situações e sua disponibilidade para receber requisições do *MoodBuster*.

O *SituMan* possui todos os recursos para definir e identificar situações similares ao *SelPri*. Entretanto, as informações de contexto utilizadas para identificar situações são: localização, dia da semana, período do dia, e atividade. Os conjuntos nebulosos relacionados aos períodos do dia foram ajustados para serem utilizados no contexto de Portugal (local onde foi realizada a avaliação), com diferentes valores de limiares. A co-localização não foi usada, mas adicionou-se a informação de atividade, na qual o paciente poderia informar as seguintes opções: em veículo, na bicicleta, à pé,

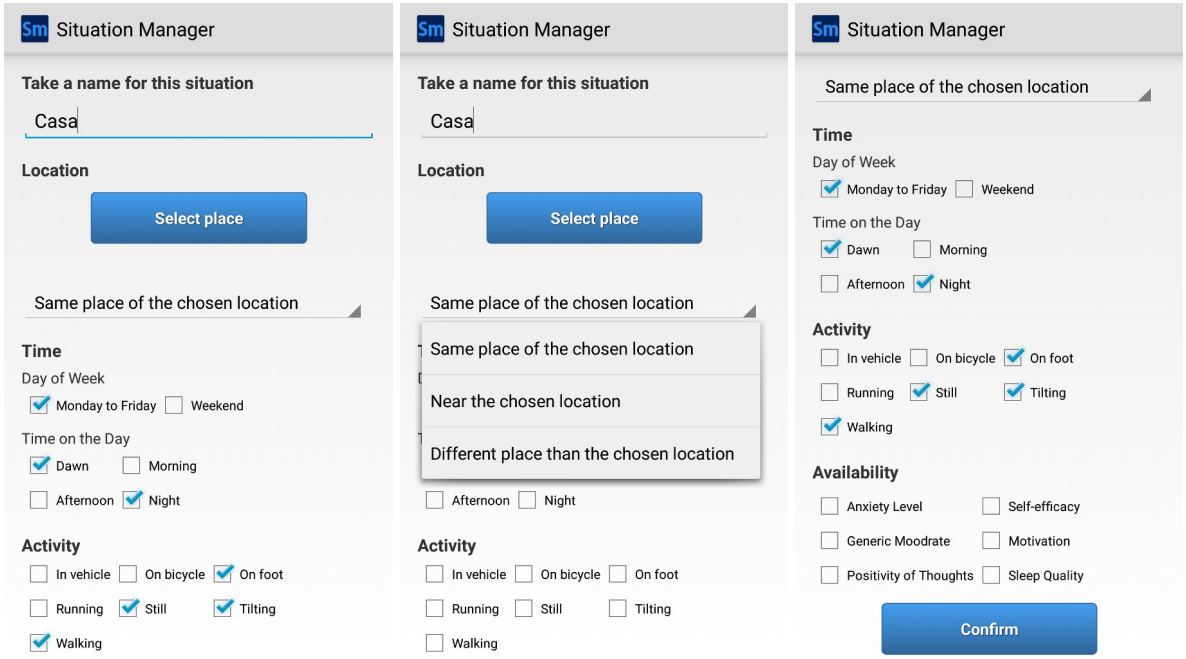

Figura 5.9: Interfaces do *SituMan* para Definição de Situações e Disponibilidade.

correndo, parado, inclinado e caminhando. A informação de atividade do usuário é obtida a partir do *Google Play Services* usando a API de reconhecimento de atividades[13].

5.9 Análise Comparativa dos Trabalhos Relacionados com a Solução Proposta

Esta seção faz uma análise comparativa, através da Tabela 5.5, da solução proposta nessa tese para a privacidade em RSMs com os trabalhos relacionados descritos anteriormente no capítulo 4. Para isso, são adotados os mesmos critérios de comparação descritos na seção 4.7.

[13] `https://developers.google.com/android/reference/com/google/android/gms/location/ActivityRecognitionApi`

Trabalho	**Tipo**	**Proposta**	**Tipo de Contexto**	**Requisitos**	**Avaliação**	**Autonomia**	**Ciência de Situação**	**Granularidade**	**Conteúdo**	**Ano**
Groba et al. [64]	A	Mecanismo	Genérico	Não	Não	Não	Não	Papéis	-	2007
Franz et al. [57]	A	Arquitetura	Genérico	Não	Não	Não	Não	Papéis	-	2008
CPE [24]	A	Mecanismo (*Engine)*	Genérico	Não	Não	Não	Não	UI/GU	-	2008
CPPL [16]	A	Linguagem	Genérico	Não	Não	Não	Sim	UI/GU	-	2012
PICOS [138]	B	*Framework* e Aplicação	Localização	Sim	Sim	Não	Não	UI/GU	Informações em geral	2011
PeopleFinder e Locaccino [120, 136]	B	Aplicação	Tempo e Localização	Sim	Sim	Não	Não	UI/GU	Localização	2009-2013
SPISM [23]	B	Aplicação	9 tipos	Sim	Não	Sim	Não	UI/GU e informação ofuscada	Localização, atividade e contatos co-localizados	2013
Fang e LeFevre [49]	C	Guia	Contexto social	Não	Sim	Sim	Não	UI/GU	Informações de perfil	2010
Squicciarini et al. [131]	C	Mecanismo	Contexto social	Não	Sim	Não	Não	UI/GU	Postagens	2014
Imran-Daud et al. [74]	C	Controle de acesso	Contexto semântico	Não	Não	Sim	Não	UI/GU e informação ofuscada	Postagens de mensagens	2016
Solução proposta	C	Aplicação	Genérico	Sim	Sim	Sim	Sim	UI/GU	Postagens	2017

Tabela 5.5: Análise Comparativa dos Trabalhos Relacionados com a Solução Proposta.

Como pode ser visto na Tabela 5.5, a solução proposta nessa tese é uma aplicação social móvel que realiza ajustes automáticos de configurações de privacidade em RSMs. Ela usa os dados de contexto de localização, tempo, co-localização e o tipo de conteúdo. Para o seu desenvolvimento, foi realizado um levantamento de requisitos com a participação de usuários brasileiros de RSMs. Com relação a avaliação, foram realizados quatro experimentos da proposta com usuários. A solução proposta possui a possibilidade de configuração de níveis de autonomia para que seja possível graduar as decisões realizadas. Além disso, ele realiza suas tomadas de decisão com base na situação do usuário. A solução proposta diferencia-se por utilizar não apenas dados de contexto isolados para tornar dinâmica as configurações de privacidade, mas dados de contexto agregados de forma a caracterizar a situação do usuário. Nela é proposto a utilização do conceito de ciência de situação ao invés de apenas possibilitar a construção de regras que levam em consideração alguma informação de contexto isolada, além de realizar a inferência da situação com o uso de lógica nebulosa. As configurações de privacidade que a solução proposta manipula são em relação ao acesso de contatos individuais ou grupo de contatos do Facebook a conteúdos postados pelo usuário dos seguintes tipos: mensagem, foto, vídeo e *check-in*.

Ao se comparar a proposta dessa pesquisa com os modelos de RBAC estendidos (seção 4.1), uma questão muito importante é que o controle de acesso a conteúdos em redes sociais normalmente não segue o modelo RBAC, o qual é muito utilizado em sistemas de informação em geral. O Facebook, por exemplo, utiliza um modelo de controle de acesso específico, como visto em [56]. Portanto, embora todos as extensões do modelo RBAC proveem controles de acesso com restrições de contexto, eles não focam em propor soluções específicas para sistemas sociais. Além disso, verifica-se que nenhuma das extensões do RBAC se preocupa com a interação do usuário com o mecanismo de controle de acesso. Estes trabalhos estão focados em propor soluções de forma a estender este modelo de controle de acesso.

A solução proposta nessa tese de doutorado é, de fato, um novo recurso a ser considerado em modelos de controle de acesso de sistemas sociais existentes. Esse recurso pode ser potencialmente usado em modelos usados atualmente em RSMs populares, tais como o Facebook e o Google+. O diferencial dele em relação aos modelos de controle de acesso propostos para redes sociais (seção 4.2) é levar em consideração questões de mobilidade, considerando que postagens realizadas

atualmente não são feitas exclusivamente através de um computador estacionário, mas sim em tempo real usando dispositivos móveis que capturam conteúdo em qualquer lugar e a qualquer momento.

Todos os trabalhos da terceira categoria (seção 4.3) são abordagens interessantes para proteger informações sensíveis dos usuários, tanto do provedor de serviços, quando de aplicações de terceiros e outros contatos. A solução proposta nessa tese é preocupada especificamente com o vazamento de privacidade para contatos não desejados. Além disso, os trabalhos dessa categoria estão mais interessados em proteger as informações de perfil do usuário (por exemplo, nome, gênero, cidade onde nasceu e onde vive atualmente), e não conteúdo de postagens. Uma limitação das soluções dessa categoria ocorre devido ao fato delas poderem diminuir a sociabilidade dos usuários, porque informações encriptadas ou falsas compartilhadas nas RSMs não favorece o estabelecimento de novos relacionamentos sociais.

Levando em consideração a categoria de trabalhos relacionados a privacidade dependente de contexto em ambientes de computação ubíqua (seção 4.4), observa-se que nenhum deles realiza avaliações com a participação do usuário na especificação das configurações de privacidade. Dessa forma, nenhum das soluções propostas objetiva dar suporte aos requisitos de privacidade dos usuários especificamente em sistemas sociais. Assim, eles não poderiam ser usados, ou mesmo aplicados com poucas alterações, diretamente em tais sistemas como solução para o problema abordado nessa tese.

Considerando a quinta categoria de trabalhos relacionados (seção 4.5), uma primeira diferença da proposta dessa tese em relação às demais dessa categoria é que nenhuma utiliza o paradigma de computação situacional para dinamizar as configurações de privacidade. Eles utilizam dados de contexto isolados para a definição de regras com restrições de contexto. Além disso, as soluções são focadas em RSMs baseadas em localização. Isso difere-se da proposta dessa pesquisa, a qual é focada na postagem de conteúdos, que é o modelo de interação entre usuários comumente usado em RSMs populares, tais como o Facebook, Google+, Twitter, Instagram e Snapchat. Dessa forma, diferente dos trabalhos descritos nessa categoria, a solução proposta não é uma aplicação social móvel com seus próprios recursos de sociabilidade, ela é uma solução que pode ser integrada com diversas RSMs já existentes.

Os trabalhos da última categoria (seção 4.6) são abordagens interessantes que contribuem para minimizar o esforço manual do usuário para criar e manter grupos de contatos com preferências de privacidade associadas. As soluções visam prover flexibilidade e automaticidade para as configurações de privacidade em sistemas sociais. Entretanto, ressalta-se que diferentemente da proposta dessa tese, elas não intencionam atender os requisitos de privacidade dos usuários quando postando conteúdo através de dispositivos móveis, pois esses requisitos são dependentes de contexto. Além disso, embora elas objetivem automatizar as configurações de privacidade, nenhum delas provê meios para usuários delegarem autonomia ao sistema, o que pode aliviar completamente o esforço do usuário para especificar configurações de privacidade a cada postagem realizada.

5.10 Limitações da Solução Proposta

Existem várias formas através dos quais podem ocorrer o vazamento de privacidade em RSMs, por exemplo, por meio de postagens de conteúdo, informações inseridas nos perfis de usuário [103], e mesmo via curtidas [82]. Como descrito na seção 2.4, os conteúdos em RSMs podem ser acessados ou mesmo manipulados (por exemplo, curtidos, comentados, compartilhados) indevidamente por várias entidades (as origens dos vazamentos de privacidade). O escopo do *SelPri* é limitado a enfrentar o vazamento de privacidade restrito a contatos sociais quando o usuário posta conteúdo em RSMs. O *SelPri* é flexível e proposto para poder ser integrado em várias redes sociais. Entretanto, ele é limitado para ser usado somente em RSMs que tenham configurações de privacidade com granularidade fina, com controles para classificar contatos em grupos e especificar configurações de privacidade para conteúdos postados considerando estes grupos, ou mesmo contatos individuais.

Considera-se também que os recursos do *SelPri* poderiam ser absorvidos melhor se eles fossem providos pela aplicação nativa da rede social, devido os usuários estarem acostumados a usá-la. Por exemplo, os recursos do *SelPri* poderiam ser disponibilizados junto às aplicações do Facebook ou Google+. Entretanto, isso não foi realizado por questões técnicas de implementação, pois ambas aplicações possuem código fechado.

5.11 Conclusão

Este capítulo apresentou o mecanismo proposto como solução para o problema abordado nesta pesquisa de doutorado. No início foi realizado um levantamento de requisitos utilizados para o desenvolvimento do mecanismo proposto, o qual evidenciou que os usuários de RSMs possuem requisitos dinâmicos e contextuais de privacidade e quais são os principais fatores que influenciam para isso. Um modelo conceitual para a identificação de situações de usuários foi proposto. Um primeiro motor de inferência foi implementado baseado no modelo conceitual, o qual foi utilizado no domínio de privacidade em RSMs. Outros dois conceitos também foram propostos para o domínio de privacidade de RSMs: o PPS e o Gerenciamento Autônomo de Privacidade, com o uso dos níveis de autonomia. O modelo conceitual para a identificação de situações de usuários foi também usado como base para a implementação de um segundo motor de inferência, o qual foi aplicado ao domínio de saúde mental. Os trabalhos relacionados foram comparados com a proposta dessa tese de doutorado e, por fim, suas limitações foram descritas. O modelo conceitual de identificação de situações de usuários proposto é avaliado a partir de sua utilização nos domínios da privacidade em RSMs e saúde mental, bem como as aplicações desenvolvidas que fazem uso do mesmo. Todo o processo de avaliação é descrito no capítulo seguinte e será utilizado como base para validar a hipótese de investigação estabelecida para este trabalho de doutorado.

6 Avaliações Experimentais

Esse capítulo apresenta as avaliações experimentais realizadas com a solução desenvolvida nessa tese. Inicialmente dois experimentos foram feitos com o *SelPri* e, adicionalmente, outros dois com o *SituMan*. Todos experimentos foram realizados com usuários finais utilizando as soluções desenvolvidas. Portanto, as avaliações experimentais consideraram também aspectos relacionadas a Interação Humano-Computador (IHC), uma vez que apenas os usuários finais, seja os de RSMs ou os *stakeholders* da saúde mental, poderiam determinar a qualidade das aplicações móveis propostas a eles através de uma experiência de uso. Ressalta-se que as metodologias das avaliações experimentais tiveram como base os conteúdos metodológicos explanados por Steve Love [93], tais como: o processo de seleção, obtenção e caracterização de participantes, as questões relacionadas a ética, os métodos de pesquisa comumente utilizados em avaliações de IHC em ambientes móveis, como a construção e uso de questionários, e a análise e a interpretação dos dados/resultados obtidos. Os quatro experimentos são descritos detalhadamente nas próximas seções.

6.1 Acurácia do Motor de Inferência de Situação Usada no *SelPri*

O primeiro experimento com o *SelPri* objetivou verificar a acurácia do motor de inferência nebulosa para identificação de situações de usuários móveis. Nesse experimento a acurácia é uma métrica determinada pela taxa de acerto das identificações de situações corretas em que os usuários vivenciaram. Essa informação sobre a acurácia em identificar situações é importante especialmente no nível de autonomia 2, em que não é requerida a interação do usuário para a definição da configuração de privacidade adequada.

6.1.1 Metodologia e Participantes

A versão do *SelPri* usada nesse primeiro experimento foi alterada para focar principalmente na avaliação de acurácia. Com isso, as funcionalidades contidas na aplicação para postar conteúdo e definir níveis de autonomia foram removidas, limitando a aplicação ao recurso de identificação de situações. A métrica de acurácia foi calculada a partir de informações providas pelos próprios participantes, os quais ajudaram informando se o *SelPri* identificou corretamente suas situações. Quando uma nova situação nessa versão alterada do *SelPri* era identificada, uma notificação era enviada ao usuário questionando-o se a situação foi identificada corretamente. Para isso, o usuário deveria responder com um "Sim" ou "Não". A aplicação foi também adaptada para registrar em *logs* todas as situações identificadas, o momento das identificações, as respostas dos participantes, bem como todas as definições dos PPSs dos usuários. Os sujeitos foram solicitados para enviar por e-mail os *logs* após o período de uso da aplicação.

Os participantes desse primeiro experimento foram recrutados principalmente do LSDi, mas também de outros laboratórios de computação da UFMA. Os voluntários usaram o *SelPri* durante sete dias. Para participar do experimento era necessário que eles tivessem uma conta no Facebook e possuíssem um *smartphone* com o sistema operacional Android. Inicialmente os participantes foram instruídos a respeito do uso do *SelPri*, o que incluía explicações orais e demostração de cenários de exemplo. Além disso, os sujeitos podiam tirar dúvidas sobre o funcionamento do *SelPri* pessoalmente e também por e-mail.

Embora os *logs* possam mostrar verdadeiros positivos (ou seja, aquelas situações confirmadas como corretas pelos participantes) e verdadeiros negativos (ou seja, aquelas situações confirmadas como incorretas pelos participantes), eles não revelam situações de falsos negativos, ou seja, aquelas que foram definidas e os participantes vivenciaram, mas o motor de inferência falhou em identificar. Nesse sentido, questionou-se todos os sujeitos sobre estas situações definidas mas não identificadas. Para esse propósito, eles responderam um pequeno questionário através do Google Forms após o período de uso da aplicação, o qual pode ser visto no Apêndice B deste documento.

Um total de 14 participantes (sendo 13 do gênero masculino) participaram desse experimento. Todos os sujeitos eram brasileiros com idades entre 23 e 39 anos (Média = ≈28,57, DP = ≈4,34). Antes de participar do experimento, os participantes reportaram vivenciar situações variadas em suas rotinas diárias. Nesse sentido, eles foram requisitados para definirem pelo menos duas de suas situações de rotina diária no *SelPri*.

6.1.2 Resultados

A Tabela 6.1 apresenta os resultados extraídos dos *logs*. As situações definidas são aquelas configuradas pelos participantes. As situações corretas e incorretas representam a quantidade de situações confirmadas pelos participantes com "Sim" e "Não", respectivamente. A porcentagem de situações corretas é apresentada em relação ao total de situações que foram confirmadas.

Participante	***Definida***	***Correta***	***Incorreta***
1	5	78 (≈95,12%)	4
2	2	50 (≈90,9%)	5
3	3	24 (≈92,3%)	2
4	3	19 (≈82,6%)	4
5	3	25 (100%)	0
6	2	14 (100%)	0
7	2	39 (≈88,63%)	5
8	3	38 (100%)	0
9	5	58 (≈92,06%)	5
10	4	34 (≈94,44%)	2
11	4	43 (≈91,48%)	4
12	5	55 (≈96,49%)	2
13	4	57 (≈98,27%)	1
14	5	62 (100%)	0

Tabela 6.1: Resultados da Avaliação de Acurácia.

Como visto na Tabela 6.1, os participantes configuraram de 2 a 5 situações durante os sete dias do experimento. Muitas situações inferidas foram confirmadas como corretas pelos participantes: 630 confirmações, 596 (≈94,6%) corretas, e 34 incorretas. Considera-se que esse resultado de 94,6% é suficientemente bom para

o *SelPri*, uma vez que as configurações de privacidade vão ser aplicadas de acordo com a situação correta do usuário em quase todos os casos. Além disso, através do uso do primeiro nível de autonomia é possível que o usuário possa verificar a situação identificada pelo *SelPri* e decida se deseja realmente aplicar a configuração de privacidade especificada para a situação. Por outro lado, há a possibilidade de configurações de privacidade serem aplicadas erroneamente, caso o segundo nível de autonomia seja utilizado pelo usuário. Por essa razão o segundo nível é indicado para usuários que, ao utilizar o primeiro nível, verifiquem que o motor de inferência de situação tem identificado todas suas situações corretamente.

Uma notificação gerada para requisitar que um participante confirmasse como correta ou incorreta uma situação identificada era sobrescrita por outra mais nova, a medida que uma situação mais atual era inferida. Dessa forma, somente a situação identificada mais atual poderia ser confirmada como correta ou incorreta pelo participante. Isso explica a diferença entre a quantidade de situações confirmadas pelos sujeitos, pois nem sempre eles estavam disponíveis para responder as notificações.

Em relação ao questionário aplicado após o período de uso de sete dias, primeiramente foi perguntado se tinham acontecido momentos em que os participantes estiveram vivenciando as situações definidas, mas o *SelPri* não conseguiu identificá-las. Dessa forma, essa questão tenta verificar a ocorrência de falso negativos. Quatro participantes (≈28,57%) informaram que o *SelPri* falhou no processo de identificação dessas situações.

Posteriormente, questionou-se apenas aos quatro sujeitos (a questão era habilitada no Google Forms apenas para os sujeitos que respondiam "Sim" na questão anterior) se o *SelPri* conseguiu identificar a situação correta e atual após alguns poucos minutos. Decidiu-se realizar esse questionamento por acreditarmos que poderiam acontecer casos em que o atraso causado pelas frequências adaptativas originados pela abordagem utilizada para preservar energia e tráfego de rede, que é de no máximo 15 minutos (ver seção 5.7.2), pudesse causar uma sensação nos usuários de que a aplicação estava falhando para identificar suas situações. Como esperado, os quatro sujeitos confirmaram que o *SelPri* identificou suas situações após alguns minutos. Dessa forma, é possível concluir que a não identificação de algumas situações em um tempo adequado ocorreu devido ao uso da abordagem para economizar recursos,

a qual faz um balanceamento entre o consumo de recursos e a idade dos dados de contextos utilizados para identificar situações e a frequência do processo de inferência.

6.2 Experiência de Uso com o *SelPri*

A solução proposta nessa tese é diretamente relacionada com a capacidade de expressão dos usuários em relação aos seus requisitos de privacidade. Portanto, o usuário deve conseguir expressar seus desejos dinâmicos e contextuais através dos recursos propostos. Para verificar se o *SelPri* atende os requisitos de privacidade dos usuários é preciso coletar diretamente suas opiniões ao utilizá-lo. O retorno obtido a partir deles é importante para verificar como o usuário está reagindo e se sentido com a utilização de uma aplicação que tem autonomia para adaptar suas configurações de privacidade a conteúdos postados em RSMs. Além disso, o retorno dos sujeitos é usado para checar a satisfação deles com a abordagem adotada para definir e identificar situações. Dessa forma, esse segundo experimento objetivou verificar a satisfação do usuário ao usar o *SelPri* e teve dois objetivos específicos:

- **Objetivo 1**: Avaliar se a solução atendeu os requisitos dinâmicos e contextuais de privacidade dos usuários;
- **Objetivo 2**: Avaliar a satisfação dos usuários em relação às abordagens para definir e identificar situações.

6.2.1 Metodologia e Participantes

Anunciou-se o experimento através de perfis de redes sociais de membros do LSDi, listas de e-mail, bem como para estudantes e funcionários da UFMA. Os voluntários usaram o *SelPri* por pelo menos três dias. Esse tempo mínimo foi necessário para os usuários aprenderem as funcionalidades propostas pelo *SelPri* e dar suas opiniões sobre a experiência de uso. Além disso, acredita-se que esse período de tempo é suficiente para usuários expressarem e vivenciarem situações diferentes que requerem mudanças em suas configurações de privacidade, e para avaliar também se o *SelPri* identificou corretamente as situações definidas. O período em que um usuário poderia começar a participar do experimento foi de 31 dias. Entretanto, somente os

sujeitos que usaram o *SelPri* por pelo menos três dias foram habilitados a responder a um questionário *online* através do Google Forms.

Similarmente ao primeiro experimento, para que um indivíduo pudesse participar foi requerido que tivesse uma conta no Facebook e um *smartphone* com sistema operacional Android. Nesse segundo experimento, os participantes usaram a versão original do *SelPri* com todas suas funcionalidades. Inicialmente os participantes foram instruídos de várias formas em como usar o *SelPri*, o que incluiu: uma documentação *online* na página *Web* do *SelPri*, explicações orais e cenários de exemplo de uso demonstrados. Além disso, os sujeitos tinham suas questões sobre o funcionamento do *SelPri* ou problemas de uso respondidas por e-mail e, quando possível, através de contato pessoal diretamente na UFMA.

O questionário ficou disponível para os participantes e foi respondido anonimamente depois do período de uso do *SelPri*. O questionário continha 20 questões, o qual pode ser visto no Apêndice C deste documento. Primeiramente, os participantes informaram o período de uso da aplicação em dias e suas idades. As 16 questões seguintes (da 2 a 18) foram respondidas usando a escala Likert [89][1] para permitir aos participantes expressarem o quanto eles concordavam com a declaração da questão. As duas últimas questões foram qualitativas e requeriam respostas dadas de forma dissertativa, permitindo aos usuários ficarem livres para expressarem seus pensamentos e opiniões. Além desse retorno dado pelos usuários através do questionário, coletou-se as seguintes informações através de *logs* gerados na aplicação e enviados automaticamente para o servidor *SelPri*: (i) as definições de PPSs dos participantes, e (ii) mudanças nas definições dos níveis de autonomia feita pelos sujeitos.

No fim dos 31 dias da duração do experimento, um total de 21 participantes efetivos responderam o questionário, sendo 12 do gênero feminino. Considera-se um participante efetivo aquele que, além de ter utilizado o *SelPri* por um mínimo de três dias, também realizou pelo menos uma postagem de conteúdo em cada PPS definido. Eles tinham idade entre 18 e 43 anos (Média = ≈29,85, DP = ≈7,7). O tempo de uso médio dos participantes foi de ≈7 dias (Máximo = 21, Mínimo = 3, DP = ≈4.44).

[1]Uma escala que pode ser respondida com valores de 1 a 5 em que os números representam, respectivamente: muito ruim, ruim, regular, bom, e muito bom.

Os sujeitos eram todos cidadãos brasileiros e moravam em quatro diferentes estados. Ressalta-se ainda que todos os participantes afirmaram ser usuários ativos de RSMs.

6.2.2 Resultados

As primeiras 8 questões do questionário aferiram a usabilidade do *SelPri*. Ressalta-se que a avaliação a partir dessas 8 questões não objetivou prover qualquer tipo de comparação de usabilidade com outra aplicação social móvel, tais como as disponibilizadas pelos provedores de redes sociais.

Inicialmente os sujeitos informaram se a aplicação é de utilização fácil e se tiveram problemas em aprender a utilizá-la. Eles expressaram na sequência se tiveram facilidade para lembrar o uso da aplicação após um período de tempo sem utilizá-la. Depois os participantes responderam se as interfaces foram suficientes para usar as funcionalidades disponibilizadas, e se eles se sentiam satisfeitos com relação à interação com as interfaces. Posteriormente eles responderam se as notificações de erro e alerta foram expressadas em uma linguagem de entendimento simples, e se ocorreram poucos erros durante a experiência de uso. Por fim, os usuários responderam se as funcionalidades foram efetuadas rapidamente. Lembra-se que o texto exato das questões está no Apêndice C deste documento. A Figura 6.1 apresenta os resultados a partir dessas questões de usabilidade, as quais mostram que o *SelPri* foi bem avaliado.

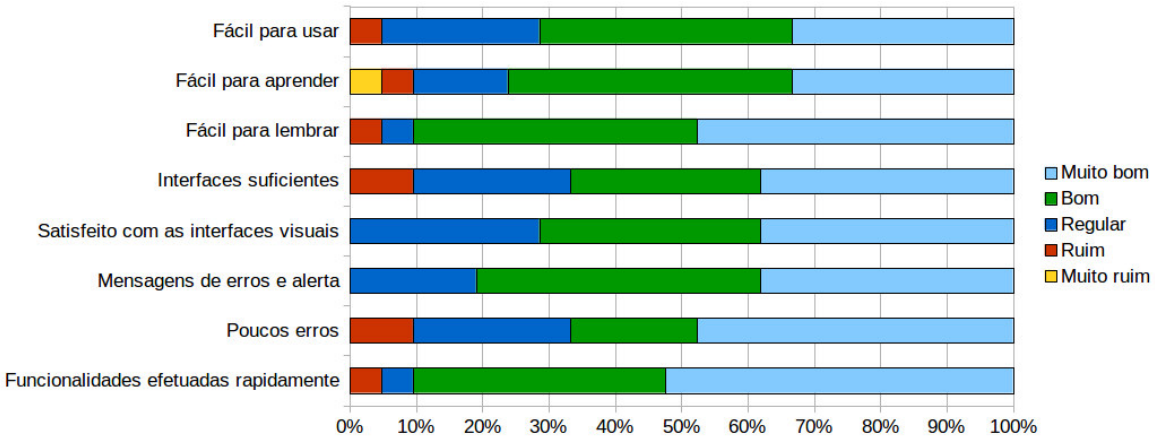

Figura 6.1: Resultados de Usabilidade.

Para observar eventuais problemas de uso ou limitações causadas pela abordagem do *SelPri* para definição de situações, os participantes informaram se eles

conseguiram expressar todas suas situações quando postando conteúdo, e se os tipos de informação de contexto usadas para expressar situações foram suficientes. Os sujeitos também informaram se o *SelPri* identificou corretamente e rapidamente suas situações a fim de avaliar o motor de inferência de situação usada. A Figura 6.2 mostra os resultados a partir dessas questões quatro questões.

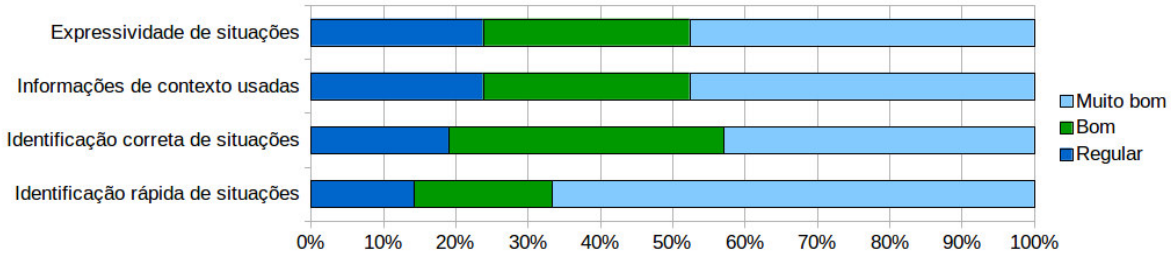

Figura 6.2: Resultados sobre Consciência de Situação.

Esses resultados mostram que o processo de definir situações foi avaliado positivamente. Algumas observações em relação ao processo de definir situações podem ser feitas a partir dos *logs* gerados na aplicação: eles revelaram que os participantes usaram ao final dos 31 dias entre 3 e 7 PPSs (Média = ≈4,61, DP = ≈1,13). Entretanto, notou-se que muitos usuários refinaram seus PPSs ao longo do tempo, fazendo mudanças nos dados de contexto e configurações de privacidade configurados previamente. Para isso, muitos PPSs foram criados e excluídos pelos usuários. Isso mostra que o recurso do *SelPri* de personalizar e modificar dinamicamente as configurações de privacidade de acordo com a situação foi de fato usado por muitos participantes. Além disso, os resultados na Figura 6.2 confirmam os obtidos no primeiro experimento, em que foi alcançada uma boa acurácia pelo motor de inferência nebulosa usada para identificar situações, pois nenhum dos participantes respondeu negativamente (muito ruim ou ruim).

Uma característica nos *logs* da aplicação é interessante. Muitos sujeitos nomearam seus PPSs com rótulos que significavam suas casas ou locais de trabalho: 18 deles criaram os PPSs com nome “No trabalho” e 17 definiram “Em casa” (ou significados similares, por exemplo, “Trabalhando”). Alguns outros nomes usados pelos participantes foram “Academia”, “Balada”, e “Estudando” (ou significados similares, por exemplo, “Treinando”). Isso indica alguns situações frequentes em que os usuários podem postar conteúdo em RSMs.

Os sujeitos também informaram se os níveis de autonomia permitiram a eles escolher adequadamente como o *SelPri* deveria se comportar quando definindo as configurações de privacidade em uma forma automática (ou autônoma). Além disso, a fim de fortalecer um questionamento dos conceitos usados, os participantes responderam se eles sentiram ter controle suficiente sobre o *SelPri*, considerando o uso dos perfis e dos níveis de autonomia. Essas questões foram usadas para avaliar a facilidade de uso e utilidade dos conceitos tanto de PPSs quanto dos níveis de autonomia, bem como as ações correspondentes feitas autonomamente pelo *SelPri* (ou seja, a definição das configurações de privacidade de postagens). A Figura 6.3 mostra os resultados dessas duas questões.

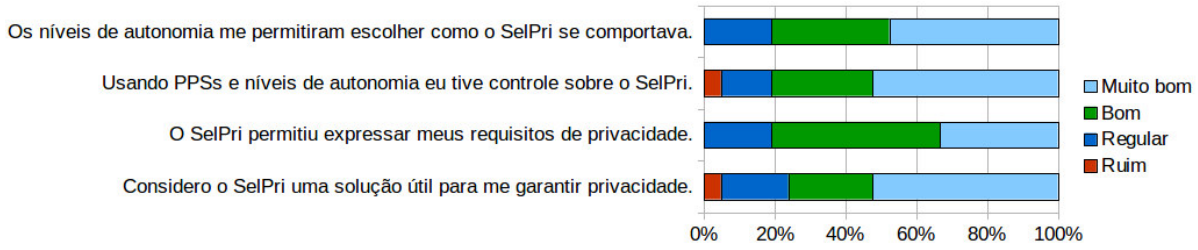

Figura 6.3: Resultados sobre Privacidade.

Adicionalmente às respostas dos participantes, analisou-se os *logs* buscando por mudanças nos níveis de autonomia (a explicação sobre os níveis de autonomia está na seção 5.6) e identificou-se o seguinte: (i) 4 usuários não mudaram do nível 1 (a configuração padrão que já vem definida desde que a aplicação é instalada) para o nível 2; (ii) 4 usuários mudaram do nível 1 para o nível 2, mas definiram de volta para o nível 1; (iii) 3 usuários mudaram muitas vezes entres os níveis 1 e 2; (iv) 10 usuários mudaram do nível 1 para o nível 2, e mantiveram no nível 2. A partir disso, observa-se que quase a metade dos participantes (10) decidiram que o melhor para eles seria o nível 2, o que indica que os usuários confiaram no *SelPri* para gerenciar autonomamente suas configurações de privacidade em postagens de conteúdo. Uma análise nos *logs* mostrou que esses 10 usuários utilizaram por mais tempo o *SelPri* em relação aos demais (Máximo = 21, Mínimo = 7), o que indica que a confiança requerida para a utilização do nível 2 demanda tempo de uso. Observa-se ainda que a maioria dos participantes experimentaram os dois níveis de autonomia, seja para poder escolher qual seria a melhor opção para eles, ou mesmo para aprender como os níveis funcionavam. Esse é um interessante resultado, pois evidencia que os participantes tiveram interesse em utilizar esse recurso da aplicação (a configuração

dos níveis de autonomia). Além disso, isso também demonstra que a avaliação desse recurso realizada com esses sujeitos tem validade, uma vez que a maioria deles o testou nas duas configurações possíveis.

Em seguida, os participantes responderam se o *SelPri* permitiu a eles expressarem seus requisitos de privacidade para postagens de conteúdo, considerando os aspectos dinâmicos e situacionais. Adicionalmente, eles foram também questionados se consideravam que o *SelPri* foi uma solução útil para garantir privacidade. O resultado foi que ≈80% responderam positivamente (bom ou muito bom) para ambas questões. Este resultado mostra a boa aceitação da abordagem do *SelPri* pelos participantes.

A primeira questão subjetiva com resposta textual questionou os participantes se ao utilizar mídias sociais tal como o Facebook antes de ter a experiência com o uso do *SelPri*, eles modificavam manualmente a configuração de privacidade a cada postagem de conteúdo. Na mesma questão, os sujeitos foram requisitados para dizer como eles faziam naturalmente quando postavam conteúdo e se eles analisavam a cada postagem qual a melhor configuração de privacidade. As repostas indicaram que 10 participantes (≈47,61%) não mudavam as configurações de privacidade padrão, afirmando que eles nunca prestavam atenção em fazer alguma alteração. Um dos sujeitos informou: "Eu nunca modifico. Normalmente procuro evitar postar qualquer conteúdo, porque perco muito tempo excluindo as pessoas que eu não quero que acessem minhas postagens". Por outro lado, 11 sujeitos (≈52,38%) reportaram que eles analisavam e modificavam as configurações de privacidade a cada postagem, e um deles escreveu: "Eu mudo as configurações de privacidade de acordo com minhas preocupações profissionais e pessoais". Um outro participantes respondeu: "Eu escolho manualmente as configurações de privacidade somente em poucas postagens, por causa do tempo necessário para essa tarefa", o que confirma que ele usualmente não está desejando configurar manualmente a configuração de privacidade para cada postagem. Além desses, um outro usuário reportou: "Eu tenho de analisar tudo manualmente, o que eu acho muito tedioso, prefiro evitar postar qualquer coisa", mostrando que o participante apenas posta algum conteúdo quando ele pode definir as configurações de privacidade adequadas, caso contrário ele decide por não postar. Em todos os casos os usuários confirmaram ter uma necessidade por um controle de privacidade que não requer muito esforço manual, o que confirma

os principais resultados do levantamento de requisitos apresentado anteriormente na seção 5.1. Portanto, as respostas dadas para essa questão indicam que usuários realmente gostariam de ter disponível soluções que, de alguma maneira, automatizem os mecanismos de controle de privacidade em RSMs.

Na última questão, os usuários foram questionados se com o uso do *SelPri*, eles passaram a conhecer mais sobre as suas próprias necessidades em relação a privacidade. O resultado mostrou que 19 participantes (≈90,47%) consideraram o *SelPri* uma experiência positiva e 17 confirmaram (≈80,95%) que eles ficaram mais preocupados com questões relacionadas a privacidade após a experiência com o *SelPri*. Um sujeito informou: "Eu comecei a prestar mais atenção nas minhas informações pessoais depois de usar a aplicação", mostrando que o *SelPri* ajudou os participantes a refletirem sobre questões de privacidade em RSMs. Um outro participante admitiu: "O uso da aplicação me fez questionar sobre em quais situações eu devo restringir uma postagem. Antes eu somente avaliava se o conteúdo era interessante para público", o que mostra que esse participante não tinha um claro entendimento de quais situações são mais sensíveis para descobrir informações pessoais em suas postagens. Ainda um outro sujeito deu a seguinte resposta: "Usando a aplicação eu pude configurar a visibilidade das minhas postagens de uma maneira mais prática, porque os perfis já estavam configurados", o que é uma opinião muito positiva, mostrando que o uso dos PPSs é útil e de uso prático.

Com essas respostas é possível concluir principalmente que o *SelPri* contribuiu em tornar esses sujeitos mais cientes de sua privacidade em RSMs e, mais importante, elas têm indicativos de que os recursos disponibilizados são realmente úteis.

6.3 Acurácia do Motor de Inferência de Situação Usado no *SituMan*

Como explicado no capítulo anterior, especificamente na seção 5.8), o motor de inferência de situação foi aplicado ao domínio de saúde mental, através do *SituMan*. Esta seção apresenta uma avaliação de acurácia realizada com o *SituMan*. Essa avaliação é importante para validar a efetividade do modelo conceitual de

identificação de situações de usuários e, mais especificamente, o quanto o motor de inferência construído para esse domínio de saúde mental acertou ao identificar situações.

6.3.1 Metodologia e Participantes

A metodologia utilizada nesse experimento foi igual à utilizada na avaliação de acurácia do *SelPri*, descrito na seção 6.1. Os participantes desse experimento foram estudantes e pesquisadores recrutados do LSDi e do INESC TEC (Portugal). Um total de 12 sujeitos (sendo 6 do gênero feminino) participaram, sendo 8 brasileiros do LSDi e 4 portugueses do INESC TEC. Os participantes tinham idade entre 23 e 51 anos (Média = ≈32.91, DP = ≈9.09).

6.3.2 Resultados

A Tabela 6.2 apresenta os resultados, com colunas similares a da Tabela 6.1.

Participante	*Definida*	*Correta*	*Incorreta*
1	3	45 (100%)	0
2	3	28 (≈90.32%)	3
3	4	42 (100%)	0
4	5	33 (≈86.84%)	5
5	3	38 (≈90.47%)	4
6	6	54 (100%)	0
7	5	60 (≈86.95)	9
8	5	73 (≈86.90)	11
9	4	14 (≈77,77%)	4
10	4	10 (≈90,9%)	1
11	3	43 (≈97,72%)	1
12	6	11 (≈91,66%)	1

Tabela 6.2: Resultados da Avaliação de Acurácia do *SituMan*.

Nesse experimento o motor de inferência provou também ter uma boa acurácia para identificar situações. Como visto na Tabela 6.2, os participantes

configuraram de 3 a 6 situações durante os sete dias. Como apresentado na tabela, o resultado foi: 490 confirmações, 451 (≈92,04%) corretas, e 39 incorretas. Observa-se que esse resultado foi muito próximo daquele obtido na avaliação de acurácia do *SelPri*. Atribui-se essa pequena redução na quantidade de situações corretas nessa avaliação do *SituMan* em relação ao *SelPri* ao componente de inferência de atividades (a API *activity recognition* do *Google Play Services*). Isso porque há uma imprecisão nos valores retornados por este componente para a ocorrência das atividades em porcentagem. A imprecisão é decorrente de diversos fatores, tais como: a utilização de técnica de aprendizagem de máquina supervisionada para reconhecer padrões de dados de contexto obtidos de sensores embutidos no dispositivo móvel, e aqueles relacionados a qualidade do dado de contexto, como discutido na seção 3.3.

6.4 Experiência de Uso com o *SituMan*

O *SituMan* também foi avaliado por pesquisadores envolvidos no projeto E-Compared. O objetivo dessa segunda avaliação foi verificar a satisfação dos usuários com as funcionalidade para definir e identificar situações, o que consequentemente acarreta o envio de notificações que requisitam a pacientes responderem auto-avaliações em momentos mais adequados. Apesar dessa avaliação não estar diretamente relacionada ao domínio de privacidade em RSMs, a descrição dessa avaliação é importante para verificar a satisfação dos usuários em relação as abordagens para definir e identificar situações no domínio em que o modelo conceitual proposto nesta tese foi aplicado.

6.4.1 Metodologia e Participantes

Esse experimento foi realizado com usuários portugueses na cidade de Porto. Os participantes foram recrutados do INESC TEC e do Instituto Universitário da Maia (ISMAI) através de reuniões de projeto e apresentações. Um total de 9 pessoas participaram do experimento, sendo 4 deles pesquisadores da área de tecnologia da informação e 5 psicólogos. Ressalta-se que todos participantes tinham doutorado ou eram estudantes de doutorado em suas áreas. Além disso, eles eram fluentes no idioma inglês. Isso era um requisito para participar do experimento, pois as aplicações

MoodBuster e *SituMan* foram desenvolvidas nesse idioma. Os participantes tinham as seguintes idades: dois tinham menos de 26 anos, um entre 26 e 30, dois entre 36 e 40, três entre 41 e 45, e um entre 51 e 55. Em relação ao gênero, sete eram homens.

Os participantes não eram pacientes em um tratamento de depressão, mas conheciam os objetivos do projeto e tinham conhecimento aprofundado das áreas de pesquisa: tecnologias da informação e comunicação aplicadas à saúde mental. Na verdade, os participantes com essas características são os mais apropriados para atender o objetivo desse experimento, pois nesse momento o objetivo foi de verificação da viabilidade de uso do *SituMan* em cenários reais em que pacientes depressivos e psicólogos ou psiquiatras o usariam, permitindo que os participantes com conhecimento na área de pesquisa pudessem indicar problemas e dar sugestões de melhorias para a solução antes dela ser usada por pacientes reais. Todos os participantes responderam um questionário *online* através do Google Forms ao final de sete dias usando a aplicação, o qual pode ser visto no Apêndice D deste documento.

Inicialmente os sujeitos foram instruídos por vários meios em como usar as duas aplicações, o que incluiu: a documentação *online* em uma página *Web* dedicada ao experimento, explicações orais e demonstração de cenários de uso realísticos. Além disso, os sujeitos tinham suas questões respondidas por e-mail e contato pessoal direto, quando possível.

O questionário ficou disponível *online* para participantes responderem anonimamente depois dos sete dias de uso. Mesmo sendo anônimo, os sujeitos deveriam informar no questionário suas idades e gêneros. O questionário tinha nove questões para avaliar o *SituMan* que foram respondidas usando a escala Likert, similar ao segundo experimento do *SelPri*. Uma última questão foi opcional, a qual requeria respostas de forma dissertativa para permitir que os participantes se sentissem livres para expressar seus pensamentos e opiniões.

6.4.2 Resultados

A Figura 6.4 apresenta os resultados das nove questões. As primeiras cinco questões avaliaram a usabilidade do *SituMan*. Em geral, todos participantes consideraram o *SituMan* fácil de usar, gostaram de usar as interfaces providas, e não tiveram problemas em aprender como usar a aplicação. Os participantes responderam

positivamente (bom ou muito bom) quando questionados se as mensagens de erro e alerta eram expressas em uma linguagem simples e fácil de entender. Na quinta questão, os usuários também consideraram que ocorreram poucos erros causados pelo *SituMan*.

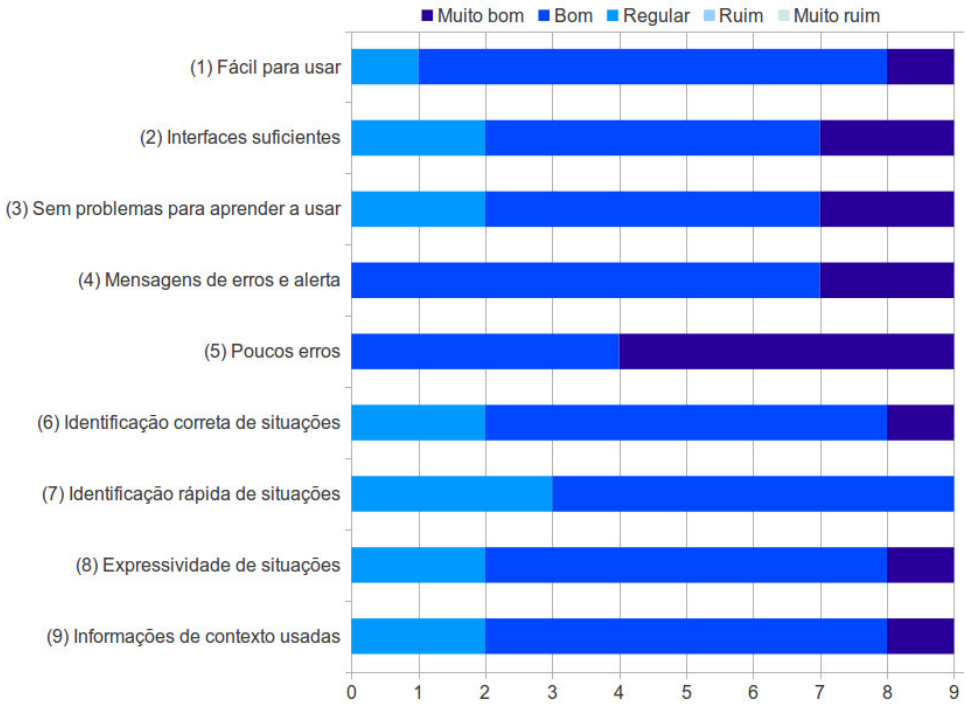

Figura 6.4: Resultados do Questionário.

Para avaliar o motor de inferência nebulosa de situação, os participantes informaram se o *SituMan* identificou corretamente suas situações. Em seguida, os sujeitos reportaram se o *SituMan* identificou suas situações em um tempo aceitável. As respostas para essas duas questões foram regular e bom. Os sujeitos foram também questionados se o *SituMan* permitiu a eles expressarem todas as situações desejadas, e se os tipos de informações de contexto usadas para expressar situações foram suficientes. Em ambas questões, o resultado foi que 7 deles responderam positivamente (bom ou muito bom) e 2 responderam regular – as respostas foram as mesmas em ambas questões.

A última questão requisitou os participantes que descrevessem mais sobre sua experiência com o uso das aplicações, e dizia que o espaço era livre para eles escreverem qualquer coisa que considerassem importante. Além disso, recomendou-se aos participantes informarem os problemas enfrentados durante o experimento. Um participante respondeu “Eu criei situações que não foram reconhecidas”, e um outro escreveu “Problemas com a identificação da minha situação dirigindo”. Conversou-

se com os participantes após a análise destas respostas e identificou-se duas razões possíveis para essas respostas: (1) a situação pode ter sido definida incorretamente pelo usuário: identificou-se que um dos sujeitos teve problemas em criar uma situação, por ter definido uma informação de localização em um lugar que nunca esteve no período do experimento; e (2) o componente responsável pela identificação das atividades do usuário (a API *activity recognition* do *Google Play Services*) inferiu mais de uma atividade sendo realizada concorrentemente, os quais são chamados "casos de dúvida", e dessa forma habilitando a ativação de várias regras nebulosas de situação. Particularmente, a situação "dirigindo" foi definida pelo participante com a informação "em veículo", então ela somente poderia ser ativada se essa atividade foi inferida pelo componente de reconhecimento de atividades. Entretanto, o componente pode ter retornado que o usuário estaria também realizando outra atividade.

6.5 Conclusão

Esse capítulo apresentou duas avaliações realizadas com o *SelPri* e duas com o *SituMan*. Como já descrito no capítulo de introdução, a hipótese de pesquisa desta tese de doutorado é: *O paradigma de computação situacional possibilita o desenvolvimento de mecanismos mais eficazes para o atendimento dos requisitos dinâmicos e dependentes de contexto de privacidade dos usuários em aplicações sociais móveis*. A avaliação da experiência de uso realizada com o *SelPri* principalmente comprovou esta hipótese de pesquisa. A avaliação destacou que a abordagem do *SelPri* para atender os requisitos dinâmicos e dependentes de contexto de privacidade teve uma boa aceitação pelos participantes e provou ser de uso prático. Por meio das avaliações realizadas com o *SelPri* foi possível mostrar sua importância e o quanto os recursos oferecidos são úteis para usuários de RSMs.

As avaliações de experiência de uso também mostraram que ambas aplicações (*SelPri* e *SituMan*) foram bem avaliadas com relação a usabilidade. Esses resultados são importantes por terem mostrado que os recursos oferecidos pelas aplicações foram facilmente usados. O *SituMan* também teve uma boa aceitação pelos usuários e mostrou sua viabilidade de ser testado em cenários reais de uso para auxiliar profissionais de saúde em tratamentos de pacientes com transtorno mental, mais especificamente a depressão.

As avaliações de acurácia mostraram uma taxa de acerto elevada dos motores de inferência para identificar situações. Uma vez que as situações são identificadas corretamente e a maioria dos usuários confirmaram que elas são identificadas em tempo hábil, as ações realizadas a partir das identificações são também realizadas de forma correta. No domínio de RSMs, a postagem de um conteúdo utiliza uma configuração automática de privacidade adequada à situação em que o usuário se encontra. Já no domínio de saúde mental, a requisição de auto-avaliações para pacientes em tratamentos de depressão é feita em momentos mais convenientes para o paciente.

Apesar da alta taxa de acerto na identificação das situações especificadas pelos usuários (≈94,6% e ≈92,04%, para o *SelPri* e *SituMan*, respectivamente), analisou-se os fatores que influenciaram negativamente estes resultados, destacando-se os seguintes: (i) qualidade baixa dos dados de contexto obtidos de sensores, ou seja, imprecisões no hardware; (ii) atualidade dos dados de contexto, ou seja, a idade das informações de contexto. As identificações de situação que devem ser feitas em tempo real requerem que os dados de contexto utilizados no processo de inferência também sejam de tempo real. Apesar da implementação do motor de inferência do *SelPri* ter tratado questões de qualidade relacionada a idade da informação de co-localização, qualquer outro dado de contexto pode sofrer de questões relacionadas a diferença entre o tempo de sua medição e o instante em que ela é de fato utilizada pelo motor de inferência; (iii) definição errada de situações pelos usuários, pois observou-se que alguns participantes definiram equivocadamente suas situações e tiveram que redefini-las, corrigindo os erros identificados. Entretanto, em alguns casos não houve a identificação de erros no processo de definição de situações, o que fez com que os participantes marcassem algumas situações como identificação incorreta.

7 Conclusões

Este documento apresentou uma proposta de solução com o objetivo de abordar o problema em aberto de atender os requisitos de privacidade de usuários em RSMs. Um modelo conceitual para a identificação de situações de usuários móveis foi desenvolvido e utilizado como base para a construção de um motor de inferência implementado na solução proposta para a privacidade em RSMs. Considera-se uma importante contribuição desta tese a concepção deste modelo conceitual baseado em lógica nebulosa, que é flexível para ser aplicado em diversos domínios. A solução é chamada de *Selpri*, a qual foi desenvolvida com base em uma elicitação de requisitos feita diretamente com usuários de RSMs. Os resultados do levantamento evidenciaram que os usuários necessitam de uma solução que atenda seus requisitos dinâmicos e contextuais de privacidade.

O *SelPri* mitiga a carga de trabalho necessária para o usuário especificar configurações de privacidade a cada postagem realizada, o que está associado com a falta de flexibilidade das configurações de privacidade providas pelas RSMs atuais. O processo de especificação de configurações de privacidade requer conhecimento dos usuários sobre os riscos de privacidade inerentes ao conteúdo que está sendo postado, o qual normalmente está relacionado ao contexto/situação atual do usuário. Mesmo tendo esse conhecimento, os usuários podem não estar habilitados ou não desejarem definir manualmente as configurações de privacidade a cada postagem. Como resultado dessas limitações, os usuários tipicamente não estão satisfeitos com a maneira disponibilizada para configurar suas preferências de privacidade [92]. Consequentemente, eles acabam usando estratégias alternativas para obter privacidade [149], tal como o bloqueio de qualquer tipo de interação com contatos não desejados.

À medida que novos mecanismos de granularidade fina usados para selecionar a audiência de postagens são disponibilizados, os usuários de RSMs têm se tornado mais privados para as audiências não desejadas [42] e têm postado uma quantidade muito maior de conteúdo para as audiências desejadas [129]. O *SelPri* permite que usuários definam configurações de privacidade dependentes de contexto,

possibilitando a postagem de conteúdos de forma seletiva com granularidade fina baseada na situação do usuário. Ao mesmo tempo, ele permite que os próprios usuários controlem as permissões que são dadas para todos conteúdos postados em cada situação. Como resultado, o suporte de automatização dado às configurações de privacidade é transparente tanto para os próprios usuários como para seus contatos.

O *SelPri* provê níveis em que o usuário pode delegar autonomia à aplicação para escolher qual configuração de privacidade é mais adequada aos conteúdos postados em RSMs. Para isso, o usuário deve escolher o nível de autonomia que a aplicação deve funcionar, como também configurar os perfis de privacidade situacionais. Nesse sentido, devido requerer pouco esforço administrativo, o *SelPri* provê uma abordagem para mitigar o paradoxo de privacidade, por reduzir a distância existente entre as atitudes e comportamentos de privacidade dos usuários.

O *SelPri* foi concebido para atender os requisitos de privacidade dos usuários, de acordo com as situações vivenciadas, sem afetar negativamente sua sociabilidade. Consequentemente, o *SelPri* tenta alcançar o chamado *Privacy Fit* [147] em RSMs. Ou seja, ele visa alcançar uma combinação entre os níveis de privacidade desejado e alcançado pelo usuário, considerando os requisitos dinâmicos e contextuais de privacidade do mesmo. Dessa forma, através do desenvolvimento do *SelPri*, o objetivo geral dessa tese de doutorado foi atendido, o qual é contribuir com uma solução que atenda os requisitos dinâmicos e contextuais de privacidade de usuários em aplicações sociais móveis. Além disso, comprovando a hipótese de pesquisa desta tese, o paradigma de computação situacional facilitou o atendimento dos requisitos dinâmicos e contextuais de privacidade dos usuários de RSMs. Isso ocorreu porque a aplicação proposta aos usuários, o *SelPri*, tem a habilidade para interagir e aprender com o usuário sobre suas situações, e autonomamente adaptar as configurações de privacidade de postagens de acordo com o contexto situacional do usuário.

Adicionalmente, o modelo conceitual de identificação de situações do usuário foi aplicado ao domínio de saúde mental, através do desenvolvimento do então o *SituMan*. O *SituMan* explora o uso do paradigma de computação situacional como mecanismo para prover requisições adaptativas por auto-avaliações para pacientes com transtornos mentais. Isso significa que o paciente escolhe receber (ou evitar o recebimento) tipos específicos de requisições por auto-avaliações de acordo com a situação atual. Além disso, o *SituMan* pode registrar situações vivencias

pelo paciente para ajudar profissionais de saúde mental em suas tomadas de decisão durante o tratamento. O *SituMan* trabalhando juntamente com o *MoodBuster* abrangem uma nova classe de aplicações móveis de EMA/EMI, chamada de *Situation-Aware EMA/I (SA-EMA/I)*, a qual possibilita o envio de requisições por auto-avaliação e intervenções mais adequadas e não intrusivas. Essa solução vai de encontro à visão de Stephen Intille [75], por coletar informações de contexto relacionadas ao paciente continuamente e passivamente, e requisitar auto-avaliações em situações convenientes. Com a aplicação do modelo conceitual a saúde mental foi possível mostrar sua flexibilidade, de modo a ficar comprovado que ele pode ser utilizado em diferentes domínios de aplicação.

7.1 Contribuições

As principais contribuições deste trabalho de doutorado são as seguintes:

- Uma elicitação para identificação de requisitos de privacidade específicos de aplicações sociais móveis;
- Um modelo conceitual com a utilização de lógica nebulosa para a identificação de situações do usuário a partir de informações de contexto obtidas a partir de sensores embutidos em dispositivos móveis;
- Uma solução que faz uso do modelo conceitual para contribuir com os requisitos de privacidade identificados na elicitação realizada com os usuários de RSMs;
- Uma avaliação com a solução proposta para o domínio de privacidade em RSMs para verificar a viabilidade de uso, analisando aspectos de usabilidade e atendimento das necessidades de usuários;
- Uma aplicação do modelo conceitual no domínio de saúde mental;
- Uma avaliação com a solução para saúde mental, mostrando sua viabilidade de ser testada por profissionais em cenários reais, com pacientes depressivos;
- Avaliações com os motores de inferência em ambos domínios de aplicação, visando estimar a acurácia para identificar corretamente as situações dos usuários.

7.2 Trabalhos Futuros

A partir desta tese outros trabalhos podem ser desenvolvidos para dar continuidade a esta pesquisa:

- O modelo conceitual pode ser evoluído e implementar novos motores de inferência de forma a permitir a identificação de novas situações em que o usuário passou a vivenciar mas não definiu previamente. A solução pode ser capaz de aprender e criar dinamicamente ao passar do tempo novas situações vivenciadas pelo usuário. Dessa forma, um motor de inferência funcionaria com uma técnica híbrida para identificação de situações, aproveitando-se do melhor da lógica nebulosa (uma técnica baseada em especificação) e de alguma solução de aprendizagem de máquina ou mineração de dados (técnicas baseadas em aprendizagem). Além disso, algum mecanismo de aprendizagem por reforço poderia ser incorporado ao motor de inferência, na intenção de minimizar erros nas identificações de situações.

- Uma possibilidade de trabalho futuro é a criação de mecanismos para tratar e/ou melhorar a qualidade dos dados de contexto. Apesar de isso ter sido feito com o dado de co-localização, em que considerou-se o tempo de vida da informação, a solução pode ser aprimorada para ter mecanismos que tratem a qualidade de contexto. Dessa forma, ela poderá tratar incerteza, considerar aspectos de completude do dado, bem como possuir mecanismos para o tratamento de falhas que não permitam a obtenção do dado de contexto.

- Com base em situações aprendidas, o *SelPri* poderia recomendar a definição de novos PPSs ao usuário. Em um próximo passo mais avançado, a solução pode também ser melhorada para identificar quais configurações de privacidade são mais adequadas para certas situações e as sugerir ao usuário. Isso iria reduzir o esforço de configuração de privacidade manual, permitindo a extensão da solução na direção de aliviar os usuários da tarefa de especificar completamente seus requisitos dinâmicos e contextuais de privacidade. Uma outra possibilidade de trabalho futuro é utilizar outras fontes de informação para escolha automática das configurações de privacidade, tal como a semântica do conteúdo da postagem.

- Em relação ao *SituMan*, uma importante pesquisa a ser realizada como trabalho futuro é a realização de experimentos em larga escala com pacientes que estão realmente em tratamentos de transtorno mental. Consequentemente, isso requereria o recrutamento de um grupo de pacientes maior e mais representativo, abrangendo os principais níveis de severidade dos transtornos mentais e um maior tempo de exposição para o uso da aplicação. Dessa forma, seria possível mensurar a efetividade da solução, comparando-se a tratamentos que não a utilizam como ferramenta de suporte aos profissionais de saúde mental.

- Como o modelo conceitual de identificação de situações foi aplicado a dois domínios, ele também pode ser usado para contribuir em outros domínios de aplicação, tais como a Internet das Coisas, os Ambientes Inteligentes, e as Cidades Inteligentes. De uma forma geral, outras aplicações que também necessitem de situações de rotina diária de seus usuários podem usufruir dos recursos fornecidos pelo modelo.

7.3 Publicações

Durante o doutorado, desenvolveu-se trabalhos científicos para divulgar a pesquisa e o conhecimento adquirido e amadurecido dentro das linhas de pesquisa envolvidas. Alguns desses trabalhos têm uma relação direta com essa pesquisa, em que os seus conteúdos encontram-se nesse documento de tese. Outros trabalhos foram desenvolvidos durante o doutorado, mas em parceria com outros alunos do LSDi ou a partir de projetos conduzidos no laboratório e, portanto, são relacionados indiretamente com essa pesquisa. Seguindo essa classificação, a seguir eles são listados.

7.3.1 Publicações Relacionadas Diretamente com esta Pesquisa

1 ARIEL SOARES TELES; ROCHA, A.; SILVA, F. J. S. E.; LOPES, J. A. C.; O'SULLIVAN, D.; VEN, P. V.; ENDLER, M. Enriching Mental Health Mobile Assessment and Intervention with Situation Awarenes. Sensors (Basel). MDPI. 2017.

Este artigo apresenta detalhadamente o *SituMan* e as avaliações experimentais

realizadas com ele.

Extrato Qualis CAPES (2015): A1 em Engenharias IV. Fator de Impacto (2015): 2.033

2 ARIEL SOARES TELES; SILVA, F. J. S. E.; ENDLER, M. Situation-based Privacy Autonomous Management for Mobile Social Networks. Computer Communications. Elsevier.

Este artigo apresenta detalhadamente o *SelPri* e as avaliações experimentais realizadas com ele. Artigo submetido em 26 de abril de 2016 e ainda sem resultado final até a data da versão final desta Tese de Doutorado.

Extrato Qualis CAPES (2015): A1 em Engenharias IV. Fator de Impacto (2015): 2.099

3 ARIEL SOARES TELES; PINHEIRO, D. N.; GONCALVES, J. F.; BATISTA, R. C.; PINHEIRO, V.; SILVA, F. J. S. E.; ENDLER, M.. *Redes Sociais Móveis: Conceitos, Aplicações e Aspectos de Segurança e Privacidade*. Minicurso do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. 31ed. Sociedade Brasileira de Computação, 2013, Brasília-DF.

Este capítulo de livro apresenta uma fundamentação e revisão da literatura sobre Redes Sociais Móveis, apresentando seus conceitos, aplicações e aspectos de segurança e privacidade. Capítulo de livro relativo a minicurso apresentado no Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos de 2013.

4 ARIEL SOARES TELES; SILVA, F. J. S. E.; BATISTA, R. C. *Security and Privacy in Mobile Social Networks*. Security and Privacy Preserving in Social Networks. Lecture Notes in Social Networks. Springer, 2013.

Este capítulo de livro apresenta o estado da arte especificamente sobre segurança e privacidade em RSMs, o qual é tema deste trabalho.

5 ARIEL SOARES TELES; SILVA, F. J. S. E.; ENDLER, M. *How to support the user's dynamic and contextual desires regarding privacy in UbiComp? An intersection between issues: ubiquity and privacy*. In: XIII Simpósio Brasileiro Sobre Fatores Humanos em Sistemas Computacionais, 2014, Foz do Iguaçu - PR. Anais do XIII Simpósio Brasileiro Sobre Fatores Humanos em Sistemas Computacionais, 2014.

Este artigo é um *position paper* que relatada a dificuldade de se atender os desejos dinâmicos e contextuais em ambientes de computação ubíqua e, além disso, ele

faz uma relação de interseção entre dois desafios do primeiro relatório técnico dos Grandes Desafios de Pesquisa em Interação Humano-Computador no Brasil (I GranDIHC-BR) [12]. Este trabalho descreve a problemática desta pesquisa de doutorado, a qual foi considerada um dos grandes desafios em IHC no Brasil.

6 ARIEL SOARES TELES; ROCHA, A.; SILVA, F. J. S. E.; LOPES, J. A. C.; O'SULLIVAN, D.; VEN, P. V.; ENDLER, M. Towards Situation-aware Mobile Applications in Mental Health. In: 29th IEEE International Symposium on Computer-Based Medical Systems – IEEE CBMS. Dublin and Belfast, 2016.
Este artigo apresenta resumidamente o *SituMan*.

7.3.2 Publicações Relacionadas Indiretamente com esta Pesquisa

7 PINHEIRO, D. N.; ARIEL SOARES TELES; GOMES, B. T. P.; SILVA, F. J. S. E. *A Middleware for Developing Context-aware Mobile Applications in Low-cost Acquisition Devices*. In: The 7th FTRA International Conference on Human-centric Ubiquitous Computing and Applications, Ostrava - Czech Republic. Proceedings of the 7th FTRA International Conference on Human-centric Ubiquitous Computing and Applications. Lecture Notes in Electrical Engineering (LNEE). Springer, 2014.

8 ARIEL SOARES TELES; GONCALVES, J. F.; SILVA, F. J. S. E.; PINHEIRO, V.; ENDLER, Markus. *Infraestrutura e Aplicações de Redes Sociais Móveis para Colaboração em Saúde*. XIII Congresso Brasileiro de Informática em Saúde - CBIS, Curitiba - Paraná. 2012.

9 ARIEL SOARES TELES; PINHEIRO, D. N.; GONCALVES, J. F.; BATISTA, R. C.; SILVA, F. J. S. E.; PINHEIRO, V.; Haeusler, E.; ENDLER, Markus. *MobileHealthNet: A Middleware for Mobile Social Networks in m-Health*. 3rd International Conference on Wireless Mobile Communication and Healthcare - MobiHealth, Paris. 2012.

10 GONCALVES, J. F.; ARIEL SOARES TELES; SILVA, F. J. S. E. *Um Modelo de Segurança e Privacidade para Redes Sociais Móveis Aplicadas à Área da Saúde*. Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, 2012, Curitiba-PR.

11 FERREIRA, A. O.; ARIEL SOARES TELES; SILVA, F. J. S. E. *MHNSS: A Middleware for Developing Speech-based Interaction Mobile Applications*. In: XIII Simpósio Brasileiro Sobre Fatores Humanos em Sistemas Computacionais, 2014, Foz do Iguaçu - PR. Anais do XIII Simpósio Brasileiro Sobre Fatores Humanos em Sistemas Computacionais, 2014.

Referências Bibliográficas

[1] B. Adams, D. Q. Phung, and S. Venkatesh. Sensing and using social context. *TOMCCAP*, 5(2), 2008.

[2] I. Altman. *The environment and social behavior: privacy, personal space, territory, crowding*. Brooks/Cole Pub. Co., 1975.

[3] C. Anagnostopoulos and S. Hadjiefthymiades. Enhancing situation-aware systems through imprecise reasoning. *IEEE Transactions on Mobile Computing*, 7(10):1153–1168, Oct 2008.

[4] C. Anagnostopoulos and S. Hadjiefthymiades. Advanced inference in situation-aware computing. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 39(5):1108–1115, 2009.

[5] C. Anagnostopoulos and S. Hadjiefthymiades. Advanced fuzzy inference engines in situation aware computing. *Fuzzy Sets and Systems*, 161(4):498–521, 2010.

[6] C. B. Anagnostopoulos, Y. Ntarladimas, and S. Hadjiefthymiades. Situation awareness: Dealing with vague context. In *ACS/IEEE International Conference on Pervasive Services*, pages 131–140, 2006.

[7] C. B. Anagnostopoulos, Y. Ntarladimas, and S. Hadjiefthymiades. Situational computing: An innovative architecture with imprecise reasoning. *Journal of Systems and Software*, 80(12):1993–2014, 2007.

[8] D. Anthony, T. Henderson, and D. Kotz. Privacy in location aware computing environments. *IEEE Pervasive Computing*, 6(4):64–72, 2007.

[9] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati. Privacy-enhanced location services information. In *Digital Privacy: Theory, Technologies and Practices*, pages 307–326. Auerbach Publications (Taylor and Francis Group), 2007.

[10] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin. Persona: An online social network with user-defined privacy. *ACM SIGCOMM Computer Communication Review*, 39(4):135–146, 2009.

[11] M. Baldauf, S. Dustdar, and F. Rosenberg. A survey on context-aware systems. *International Journal Ad Hoc Ubiquitous Computing*, 2(4):263–277, June 2007.

[12] M. C. C. Baranauskas, C. S. Souza, and R. Pereira. I grandihc-br — grandes desafios de pesquisa em interação humano-computador no brasil. Technical report, Comissão Especial de Interação Humano-Computador da Sociedade Brasileira de Computação, 2014.

[13] J. Barwise. Scenes and other situations. *Journal of Philosophy*, 78(7):369–397, 1981.

[14] A. Beach, B. Raz, and L. Buechley. Touch me wear: Getting physical with social networks. In *Proceedings of the International Conference on Computational Science and Engineering*, volume 4 of *CSE '09*, pages 960–965. IEEE Computer Society, 2009.

[15] F. Beato, M. Kohlweiss, and K. Wouters. Scramble! your social network data. In *Proceedings of the 11th International Symposium on Privacy Enhancing Technologies*, PETS '11, pages 211–225. Springer Berlin Heidelberg, 2011.

[16] A. Behrooz and A. Devlic. A context-aware privacy policy language for controlling access to context information of mobile users. In R. Prasad, K. Farkas, A. Schmidt, A. Lioy, G. Russello, and F. Luccio, editors, *Security and Privacy in Mobile Information and Communication Systems*, volume 94 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 25–39. Springer Berlin Heidelberg, 2012.

[17] P. Bellavista, A. Corradi, M. Fanelli, and L. Foschini. A survey of context data distribution for mobile ubiquitous systems. *ACM Computing Surveys*, 44(4):24:1–24:45, sep 2012.

[18] M. Benisch, P. G. Kelley, N. Sadeh, and L. F. Cranor. Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs. *Personal Ubiquitous Computing*, 15(7):679–694, Oct. 2011.

[19] E. Bertino, P. A. Bonatti, and E. Ferrari. Trbac: A temporal role-based access control model. *ACM Transactions on Information and System Security*, 4(3):191–233, Aug. 2001.

[20] E. Bertino, B. Catania, M. L. Damiani, and P. Perlasca. Geo-rbac: A spatially aware rbac. In *Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies*, SACMAT '05, pages 29–37, New York, NY, USA, 2005. ACM.

[21] C. Bettini, O. Brdiczka, K. Henricksen, J. Indulska, D. Nicklas, A. Ranganathan, and D. Riboni. A survey of context modelling and reasoning techniques. *Pervasive and Mobile Computing*, 6(2):161–180, 2010.

[22] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: automated identity theft attacks on social networks. In *Proceedings of the 18th international conference on World wide web*, WWW '09, pages 551–560, New York, NY, USA, 2009. ACM.

[23] I. Bilogrevic, K. Huguenin, B. Agir, M. Jadliwala, and J.-P. Hubaux. Adaptive information-sharing for privacy-aware mobile social networks. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '13, pages 657–666. ACM, 2013.

[24] M. Blount, J. Davis, M. Ebling, W. Jerome, B. Leiba, X. Liu, and A. Misra. Privacy engine for context-aware enterprise application services. In *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, volume 2 of *EUC '08*, pages 94–100, 2008.

[25] C. Bolchini, C. Curino, G. Orsi, E. Quintarelli, R. Rossato, F. A. Schreiber, and L. Tanca. And what can context do for data? *Communications of the ACM*, 52(11):136–140, 2009.

[26] D. Boyd and N. B. Ellison. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13, 2007.

[27] A. Boytsov. *Context reasoning, context prediction and proactive adaptation in pervasive computing systems*. PhD thesis, 2011.

[28] T. Buchholz, A. Küper, and M. Schiffers. Quality of context: What it is and why we need it. In *In Proceedings of the 10th Workshop of the OpenView University Association: (HPOVUA)*, 2003.

[29] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. Semantic web-based social network access control. *Computers & Security*, 30(2–3):108–115, 2011. Special Issue on Access Control Methods and Technologies.

[30] G. Chen and D. Kotz. Solar: A pervasive-computing infrastructure for context-aware mobile applications. Technical Report TR2002-421, Dartmouth College, 2002.

[31] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. M. Leung. Body area networks: A survey. *Mobile Networks and Applications*, 16(2):171–193, 2011.

[32] P. Cingolani and J. Alcalá-Fdez. jfuzzylogic: a robust and flexible fuzzy-logic inference system language implementation. In *IEEE International Conference on Fuzzy Systems*, pages 1–8. IEEE, 2012.

[33] P. Cingolani and J. Alcalá-Fdez. jfuzzylogic: a java library to design fuzzy logic controllers according to the standard for fuzzy control programming. pages 61–75, 2013.

[34] M. Conti, A. Hasani, and B. Crispo. Virtual private social networks. In *Proceedings of the First ACM Conference on Data and Application Security and Privacy*, CODASPY '11, pages 39–50, New York, NY, USA, 2011. ACM.

[35] M. Conti, A. Hasani, and B. Crispo. Virtual private social networks and a facebook implementation. *ACM Transactions on the Web*, 7(3):14:1–14:31, 2013.

[36] A. Corradi, R. Montanari, and D. Tibaldi. Context-based access control management in ubiquitous environments. In *Proceedings of the Third IEEE International Symposium on Network Computing and Applications*, NCA '04, pages 253–260, 2004.

[37] L. A. Cutillo, R. Molva, and T. Strufe. Safebook: A privacy-preserving online social network leveraging on real-life trust. *IEEE Communications Magazine*, 47(12):94–101, 2009.

[38] F. S. da Silva, K. C. N. da Silva, and G. Bressan. Análise de informações contextuais através de técnicas de aprendizagem de máquina. In *WebMedia '12: Anais dos Minicursos do Simpósio Brasileiro de Sistemas Multimída e Web*, pages 117–152. SBC, 2012.

[39] L. David, R. Vasconcelos, L. Alves, R. Andre, G. Baptista, and M. Endler. A communication middleware for scalable real-time mobile collaboration. In *IEEE 21st International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, WETICE '12, pages 54–59, June 2012.

[40] L. David, R. O. Vasconcelos, L. Alves, R. Andre, and M. Endler. A dds-based middleware for scalable tracking, communication and collaboration of mobile nodes. *Journal of Internet Services and Applications*, (13):4–16, 2013.

[41] A. K. Dey. Understanding and using context. *Personal Ubiquitous Computing*, 5(1):4–7, Jan. 2001.

[42] R. Dey, Z. Jelveh, and K. Ross. Facebook users have become much more private: A large-scale study. In *Proceedings of the International Conference on Pervasive Computing and Communications*, PERCOM Workshops, pages 346–352. IEEE, March 2012.

[43] V. J. do Sacramento Rodrigues. *Gerêencia de Privacidade para Aplicações Sensíveis ao Contexto em Redes Móveis*. PhD thesis, Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Informática, Rio de Janeiro, RJ, Setembro 2006.

[44] W. Dong, V. Dave, L. Qiu, and Y. Zhang. Secure friend discovery in mobile social networks. In *Proceedings of 30th IEEE International Conference on Computer Communications*, INFOCOM '11, pages 1647–1655. IEEE Computer Society, 2011.

[45] J. R. Douceur. The sybil attack. In *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, IPTPS '01, pages 251–260, London, UK, UK, 2002. Springer-Verlag.

[46] P. Dourish and K. Anderson. Collective information practice: Exploring privacy and security as social and cultural phenomena. *Journal Human-Computer Interaction*, 21(3):319–342, 2006.

[47] C. Emmanouilidis, R.-A. Koutsiamanis, and A. Tasidou. Mobile guides: Taxonomy of architectures, context awareness, technologies and applications. *Journal of Network and Computer Applications*, 36(1):103–125, 2013.

[48] M. R. Endsley. Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37:32–64, 1995.

[49] L. Fang and K. LeFevre. Privacy wizards for social networking sites. In *Proceedings of the 19th International Conference on World Wide Web*, WWW '10, pages 351–360, New York, NY, USA, 2010. ACM.

[50] D. Ferraiolo and R. Kuhn. Role-based access control. In *15th NIST-NCSC National Computer Security Conference*, pages 554–563, 1992.

[51] J. B. Filho, J. Gensel, W. Viana, and H. Martin. A contextual annotation-based access control model for pervasive environments. In *Second International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use*, IWSSI/SPMU '10, 2010.

[52] J. B. Filho and H. Martin. A generalized context-based access control model for pervasive environments. In *Proceedings of the 2nd SIGSPATIAL ACM GIS 2009 International Workshop on Security and Privacy in GIS and LBS*, SPRINGL '09, pages 12–21. ACM, 2009.

[53] A. M. P. Fleischmann. *Sensibilidade à Situação em Sistemas Educacionais na Web*. PhD thesis, Universidade Federal do Rio Grande do Sul. Instituto de Informática. Programa de Pós-graduação em Computação, Julho 2012.

[54] P. W. Fong. Relationship-based access control: Protection model and policy language. In *Proceedings of the First ACM Conference on Data and Application Security and Privacy*, CODASPY '11, pages 191–202, New York, NY, USA, 2011. ACM.

[55] P. W. Fong and I. Siahaan. Relationship-based access control policies and their policy languages. In *Proceedings of the 16th ACM Symposium on Access Control Models and Technologies*, SACMAT '11, pages 51–60, New York, NY, USA, 2011. ACM.

[56] P. W. L. Fong, M. Anwar, and Z. Zhao. A privacy preservation model for facebook-style social network systems. In *Proceedings of the 14th European Conference on Research in Computer Security*, ESORICS '09, pages 303–320, Berlin, Heidelberg, 2009. Springer-Verlag.

[57] E. Franz, C. Groba, T. Springer, and M. Bergmann. A comprehensive approach for context-dependent privacy management. In *International Conference on Availability, Reliability and Security - ARES*, pages 903–910, 2008.

[58] G. Friedland and R. Sommer. Cybercasing the joint: on the privacy implications of geo-tagging. In *Proceedings of the 5th USENIX conference on Hot topics in security*, HotSec'10, pages 1–8. USENIX Association, 2010.

[59] A. Gaddah and T. Kunz. A survey of middleware paradigms for mobile computing. Technical report, Carleton University, 2003.

[60] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen. Security issues in online social networks. *IEEE Internet Computing*, 15(4):56–63, 2011.

[61] J. F. Goncalves, F. J. da Silva e Silva, R. O. Vasconcelos, G. L. B. Baptista, and M. Endler. A security infrastructure for massive mobile data distribution. In *Proceedings of the 11th ACM International Symposium on Mobility Management and Wireless Access*, MobiWac '13, pages 41–50, New York, NY, USA, 2013. ACM.

[62] F. Gravenhorst, A. Muaremi, J. Bardram, A. Grünerbl, O. Mayora, G. Wurzer, M. Frost, V. Osmani, B. Arnrich, P. Lukowicz, and G. Tröster. Mobile phones as medical devices in mental disorder treatment: An overview. *Personal Ubiquitous Computing*, 19(2):335–353, 2015.

[63] C. Grier, K. Thomas, V. Paxson, and M. Zhang. @spam: the underground on 140 characters or less. In *Proceedings of the 17th ACM conference on Computer and communications security*, CCS '10, pages 27–37, New York, NY, USA, 2010. ACM.

[64] C. Groba, S. Grob, and T. Springer. Context-dependent access control for contextual information. In *Proceedings of the 2nd International Conference on Availability, Reliability and Security*, ARES '07, pages 155–161, Washington, DC, USA, 2007.

[65] O. M. Group. Data distribution service for real-time systems specification, July 2001.

[66] S. Guha, K. Tang, and P. Francis. Noyb: Privacy in online social networks. In *Proceedings of the First Workshop on Online Social Networks*, WOSN '08, pages 49–54, New York, NY, USA, 2008. ACM.

[67] W. He, X. Liu, and M. Ren. Location cheating: A security challenge to location-based social network services. In *Proceedings of the 31st International Conference on Distributed Computing Systems*, ICDCS '11, pages 740–749. IEEE Computer Society, 2011.

[68] K. Henricksen and J. Indulska. Modelling and using imperfect context information. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications – Workshops*, pages 33–37, 2004.

[69] K. E. Heron and J. M. Smyth. Ecological momentary interventions: Incorporating mobile technology into psychosocial and health behaviour treatments. *British Journal of Health Psychology*, 15(1):1–39, 2010.

[70] H. Hu, G.-J. Ahn, and J. Jorgensen. Multiparty access control for online social networks: Model and mechanisms. *IEEE Transactions on Knowledge and Data Engineering*, 25(7):1614–1627, 2013.

[71] X. Hu, T. Chu, V. Leung, E.-H. Ngai, P. Kruchten, and H. Chan. A survey on mobile social networks: Applications, platforms, system architectures, and future research directions. *IEEE Communications Surveys Tutorials*, 17(3):1557–1581, 2015.

[72] Q. Huang and Y. Liu. On geo-social network services. In *Proceedings of the 17th International Conference on Geoinformatics*, pages 1–6, 2009.

[73] R. Hull, B. Kumar, D. Lieuwen, P. Patel-Schneider, A. Sahuguet, S. Varadarajan, and A. Vyas. Enabling context-aware and privacy-conscious user data sharing. In *Proceedings of the IEEE International Conference on Mobile Data Management*, MDM '04, pages 187–198, 2004.

[74] M. Imran-Daud, D. Sánchez, and A. Viejo. Privacy-driven access control in social networks by means of automatic semantic annotation. *Computer Communications*, 76:12–25, 2016.

[75] S. S. Intille. Technological innovations enabling automatic, context-sensitive ecological momentary assessment. In A. S. et al., editor, *The science of real-time data capture: self-reports in health research*, pages 308–337. Oxford: Oxford University Press, 2007.

[76] J. B. D. Joshi, E. Bertino, U. Latif, and A. Ghafoor. A generalized temporal role-based access control model. *IEEE Transactions on Knowledge and Data Engineering*, 17(1):4–23, 2005.

[77] N. Kayastha, D. Niyato, P. Wang, and E. Hossain. Applications, architectures, and protocol design issues for mobile social networks: A survey. *Proceedings of the IEEE*, 99(12):2130–2158, 2011.

[78] M. Kirkpatrick and E. Bertino. Context-dependent authentication and access control. In J. Camenisch and D. Kesdogan, editors, *iNetSec 2009 – Open Research Problems in Network Security*, volume 309 of *IFIP Advances in Information and Communication Technology*, pages 63–75. Springer Berlin Heidelberg, 2009.

[79] A. Kleiboer, J. Smit, J. Bosmans, J. Ruwaard, G. Andersson, N. Topooco, T. Berger, T. Krieger, C. Botella, R. Baños, K. Chevreul, R. Araya, A. Cerga-Pashoja, R. Cieślak, A. Rogala, C. Vis, S. Draisma, A. van Schaik, L. Kemmeren, D. Ebert, M. Berking, B. Funk, P. Cuijpers, and H. Riper. European comparative effectiveness research on blended depression treatment versus treatment-as-usual (e-compared): study protocol for a randomized controlled, non-inferiority trial in eight european countries. *Trials*, 17(1), 2016.

[80] S. Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 2015.

[81] B. Konings, F. Schaub, and M. Weber. Who, how, and why? enhancing privacy awareness in ubiquitous computing. In *IEEE International Conference on Pervasive Computing and Communications Workshops*, PERCOM Workshops, pages 364–367, 2013.

[82] M. Kosinski, D. Stillwell, and T. Graepel. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, 110(15):5802–5805, 2013.

[83] B. Krishnamurthy and C. E. Wills. Privacy leakage in mobile online social networks. In *Proceedings of the 3rd conference on Online social networks*, WOSN'10, pages 1–9, 2010.

[84] D. Kulkarni and A. Tripathi. Context-aware role-based access control in pervasive computing systems. In *Proceedings of the 13th ACM symposium on Access control models and technologies*, SACMAT '08, pages 113–122, New York, NY, USA, 2008. ACM.

[85] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell. A survey of mobile phone sensing. *IEEE Communications Magazine - Ad Hoc and Sensor Networks*, 48(9):140–150, 2010.

[86] M. Langheinrich. Privacy in ubiquitous computing. In J. Krumm, editor, *Ubiquitous Computing Fundamentals*, chapter 3, pages 95–159. Chapman & Hall/CRC, Boca Raton, FL, 2010.

[87] J. Li and Q. Li. Decentralized self-management of trust for mobile ad hoc social networks. *International Journal of Computer Networks & Communications (IJCNC)*, 3(6):1–17, 2011.

[88] Y. Li, Y. Li, Q. Yan, and R. H. Deng. Privacy leakage analysis in online social networks. *Computers & Security*, 49(C):239–254, 2015.

[89] R. Likert. A technique for the measurement of attitudes. *Archives of Psychology*, 22(140):1–55, 1932.

[90] J. Lin, M. Benisch, N. Sadeh, J. Niu, J. Hong, B. Lu, and S. Guo. A comparative study of location-sharing privacy preferences in the united states and china. *Personal and Ubiquitous Computing*, 17(4):697–711, Apr. 2013.

[91] X. Lin, B. Cheng, and J. Chen. A situation-aware approach for dealing with uncertain context-aware paradigm. In *Proceedings of the 28th IEEE Conference on Global Telecommunications*, GLOBECOM'09, pages 1880–1885, Piscataway, NJ, USA, 2009. IEEE Press.

[92] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing facebook privacy settings: User expectations vs. reality. In *Proceedings of the ACM SIGCOMM Conference on Internet Measurement Conference*, IMC '11, pages 61–70, New York, NY, USA, 2011. ACM.

[93] S. Love. *Understanding mobile human-computer interaction*. Elsevier, 2005.

[94] R. Lubke, D. Schuster, and A. Schill. Mobilisgroups: Location-based group formation in mobile social networks. In *Proceedings of the 9th Annual IEEE International Conference on Pervasive Computing and Communications, Workshop Proceedings*, PerCom '11, pages 502–507, Seattle, WA, USA, 2011. IEEE.

[95] M. M. Lucas and N. Borisov. Flybynight: Mitigating the privacy risks of social networking. In *Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society*, WPES '08, pages 1–8, New York, NY, USA, 2008. ACM.

[96] W. Luo, Q. Xie, and U. Hengartner. Facecloak: An architecture for user privacy on social networking sites. In *Proceedings of the International Conference on Computational Science and Engineering*, volume 3 of *CSE '09*, pages 26–33, 2009.

[97] A. Manzoor. *Quality of context in pervasive systems: models, techniques, and applications*. PhD thesis, TU Wien, November 2010.

[98] A. Manzoor, H.-L. Truong, and S. Dustdar. On the evaluation of quality of context. In *Smart Sensing and Context*, pages 140–153. Springer, 2008.

[99] A. Manzoor, H.-L. Truong, and S. Dustdar. Quality of context: models and applications for context-aware systems in pervasive environments. *The Knowledge Engineering Review*, 29:154–170, 3 2014.

[100] A. Masoumzadeh and J. Joshi. Osnac: An ontology-based access control model for social networking systems. In *Proceedings of the IEEE Second International Conference on Social Computing*, SocialCom '10, pages 751–759, 2010.

[101] A. Masoumzadeh and J. Joshi. Ontology-based access control for social network systems. *International Journal of Information Privacy, Security and Integrity (IJIPSI)*, 1(1):59–78, 2011.

[102] M. L. Mazurek, P. F. Klemperer, R. Shay, H. Takabi, L. Bauer, and L. F. Cranor. Exploring reactive access control. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, pages 2085–2094, New York, NY, USA, 2011. ACM.

[103] A. Mislove, B. Viswanath, K. P. Gummadi, and P. Druschel. You are who you know: Inferring user profiles in online social networks. In *Proceedings of the Third ACM International Conference on Web Search and Data Mining*, WSDM '10, pages 251–260, New York, NY, USA, 2010. ACM.

[104] T. M. Mitchell. *Machine learning*. McGraw-Hill, New York, NY [u.a., 1997.

[105] S. Moncrieff, S. Venkatesh, and G. West. Dynamic privacy assessment in a smart house environment using multimodal sensing. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 5(2):10:1–10:29, 2008.

[106] M. J. Moyer and M. Abamad. Generalized role-based access control. In *21st International Conference on Distributed Computing Systems*, pages 391–398, 2001.

[107] Y. Najaflou, B. Jedari, F. Xia, L. Yang, and M. Obaidat. Safety challenges and solutions in mobile social networks. *Systems Journal, IEEE*, 9(3):834–854, 2015.

[108] A. Narayanan and V. Shmatikov. De-anonymizing social networks. In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, SP '09, pages 173–187, Washington, DC, USA, 2009. IEEE Computer Society.

[109] L. Palen and P. Dourish. Unpacking "privacy" for a networked world. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems*, CHI '03, pages 129–136, New York, NY, USA, 2003.

[110] G. Pardo-Castellote. Omg data-distribution service: Architectural overview. In *Proceedings of the 2003 IEEE Conference on Military Communications - Volume I*, MILCOM '03, pages 242–247, Washington, DC, USA, 2003. IEEE Computer Society.

[111] W. Pedrycz and F. Gomide. *Fuzzy Systems Engineering: Toward Human-Centric Computing*. Wiley-IEEE Press, 2007.

[112] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos. Context aware computing for the internet of things: A survey. *IEEE Communications Surveys & Tutorials*, 16(1):414–454, 2014.

[113] J. Perry. *The Problem of the Essential Indexical: And Other Essays*. CSLI Publications. Center for the Study of Language & Information, 2 edition, 2000.

[114] S. Poslad. *Ubiquitous Computing: Smart Devices, Environments and Interactions*. John Wiley and Sons, 2009.

[115] J. Rana, J. Kristiansson, J. Hallberg, and K. Synnes. Challenges for mobile social networking applications. In *Proceedings of the International ICST Conference on Communications Infrastructure, Systems and Applications in Europe*, volume 16 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 275–285. Springer Berlin Heidelberg, 2009.

[116] R. Ravichandran, M. Benisch, P. G. Kelley, and N. M. Sadeh. Capturing social networking privacy preferences. In *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies*, PETS '09, pages 1–18, Berlin, Heidelberg, 2009. Springer-Verlag.

[117] A. Rocha, M. Henriques, J. Correia Lopes, R. Camacho, M. Klein, G. Modena, P. Van de Ven, E. McGovern, E. Tousset, T. Gauthier, and L. Warmerdam. ICT4Depression: Service oriented architecture applied to the treatment of depression. In *25th International Symposium on Computer-Based Medical Systems*, CBMS'12, pages 1–6, 2012.

[118] T. J. Ross. *Fuzzy Logic with Engineering Applications*. Wiley, 2010.

[119] S. J. Russell and P. Norvig. *Artificial Intelligence: A Modern Approach*. Prentice Hall, Upper Saddle River, NJ, USA, 3 edition, 2010.

[120] N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal Ubiquitous Computing*, 13(6):401–412, Aug. 2009.

[121] P. Samarati and S. C. Vimercati. Access control: Policies, models, and mechanisms. In R. Focardi and R. Gorrieri, editors, *Foundations of Security*

Analysis and Design: Tutorial Lectures, pages 137–196, Berlin, Heidelberg, 2001. Springer-Verlag.

[122] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-based access control models. *Computer*, 29(2):38–47, Feb. 1996.

[123] R. Sayaf and D. Clarke. Access control models for online social networks. In L. Caviglione, M. Coccoli, and A. Merlo, editors, *Social Network Engineering for Secure Web Data and Services*, pages 32–65. IGI Global, 2013.

[124] F. Schaub, B. Könings, S. Dietzel, M. Weber, and F. Kargl. Privacy context model for dynamic privacy adaptation in ubiquitous computing. In *6th International Workshop on Context-Awareness for Self-Managing Systems, ACM UbiComp workshops*, Casemans 2012, pages 752–757, 2012.

[125] F. Schaub, B. Könings, M. Weber, and F. Kargl. Towards context adaptive privacy decisions in ubiquitous computing. In *IEEE International Conference on Pervasive Computing and Communications, Work in Progress*, PerCom '12. IEEE, 2012.

[126] D. Schuster, A. Rosi, M. Mamei, T. Springer, M. Endler, and F. Zambonelli. Pervasive social context - taxonomy and survey. *ACM Transactions on Intelligent Systems and Technology*, 9(4):1–22, 2012.

[127] M. Shehab, A. Squicciarini, G.-J. Ahn, and I. Kokkinou. Access control for online social networks third party applications. *Computers & Security*, 31(8):897–911, 2012.

[128] S. Shiffman, A. A. Stone, and M. R. Hufford. Ecological momentary assessment. *Annual Review of Clinical Psychology*, 4(1):1–32, 2008.

[129] M. Sleeper, R. Balebako, S. Das, A. L. McConahy, J. Wiese, and L. F. Cranor. The post that wasn't: exploring self-censorship on facebook. In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work*, CSCW '13, pages 793–802. ACM, 2013.

[130] A. Sorniotti and R. Molva. Secret interest groups (sigs) in social networks with an implementation on facebook. In *Proceedings of the 2010 ACM Symposium on Applied Computing*, SAC '10, pages 621–628, New York, NY, USA, 2010. ACM.

[131] A. Squicciarini, S. Karumanchi, D. Lin, and N. DeSisto. Identifying hidden social circles for advanced privacy configuration. *Computers & Security*, 41:40–51, 2014.

[132] A. Teles, F. J. da Silva e Silva, and R. Batista. *Security and Privacy in Mobile Social Networks*. Lecture Notes in Social Networks. Security and Privacy Preserving in Social Networks, Springer, 2013.

[133] A. Teles, J. Gonçalves, V. Pinheiro, F. J. da Silva e Silva, and M. Endler. Infraestrutura e aplicações de redes sociais móveis para colaboração em saúde. In *Congresso Brasileiro de Informática em Saúde*, CBIS '12, 2012.

[134] A. Teles, D. Pinheiro, J. Gonçalves, R. Batista, F. Silva, V. Pinheiro, E. Haeusler, and M. Endler. Mobilehealthnet: A middleware for mobile social networks in m-health. In *Proceedings of the 3rd International Conference on Wireless Mobile Communication and Healthcare*, MobiHealth '12, 2012.

[135] A. S. Teles, D. Pinheiro, J. Gonçalves, R. Batista, V. Pinheiro, F. J. da Silva e Silva, and M. Endler. Redes sociais móveis: Conceitos, aplicações e aspectos de segurança e privacidade. In *SBRC '13: Anais dos Minicursos do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 51–100. SBC, 2013.

[136] E. Toch, J. Cranshaw, P. Hankes-Drielsma, J. Springfield, P. G. Kelley, L. Cranor, J. Hong, and N. Sadeh. Locaccino: A privacy-centric location sharing application. In *Proceedings of the 12th ACM International Conference Adjunct Papers on Ubiquitous Computing - Adjunct*, Ubicomp '10 Adjunct, pages 381–382, New York, NY, USA, 2010. ACM.

[137] J. Y. Tsai, P. Kelley, P. Drielsmal, L. F. Cranor, J. Hong, and N. Sadeh. Who's viewed you?: the impact of feedback in a mobile location-sharing application. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, pages 2003–2012, New York, NY, USA, 2009. ACM.

[138] M. Tschersich, C. Kahl, S. Heim, S. Crane, K. BöTtcher, I. Krontiris, and K. Rannenberg. Towards privacy-enhanced mobile communities-architecture, concepts and user trials. *The Journal of Systems and Software*, 84(11):1947–1960, 2011.

[139] P. van de Ven, M. R. Henriques, M. Hoogendoorn, M. Klein, E. McGovern, J. Nelson, H. Silva, and E. Tousset. A mobile system for treatment of depression. In *International Joint Conference on Biomedical Engineering Systems and Technologies*, BIOSTEC'12, 2012.

[140] N. Vastardis and K. Yang. Mobile social networks: Architectures, social properties, and key research challenges. *IEEE Communications Surveys Tutorials*, 15(3):1355–1371, Third 2013.

[141] C. Vicente, D. Freni, C. Bettini, and C. Jensen. Location-related privacy in geo-social networks. *IEEE Internet Computing*, 15:20–27, may-june 2011.

[142] S. Wasserman and K. Faust. *Social Network Analysis: Methods and Applications*. Structural Analysis in the Social Sciences. Cambridge University Press, 1 edition, 1994.

[143] R. S. Wazlawick. *Metodologia de Pesquisa para Ciência da Computação*. Elsevier Brasil, 2 edition, 2014.

[144] M. Weiser. The computer for the 21st century. *Scientific American*, 265(3):66–75, 1991.

[145] C. D. Wickens. Situation awareness: Review of mica endsley's 1995 articles on situation awareness theory and measurement. *Human Factors*, 50(3):397–403, 2008.

[146] S. Wilson, J. Cranshaw, N. Sadeh, A. Acquisti, L. F. Cranor, J. Springfield, S. Y. Jeong, and A. Balasubramanian. Privacy manipulation and acclimation in a location sharing application. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '13, pages 549–558, New York, NY, USA, 2013. ACM.

[147] P. Wisniewski, A. N. Islam, B. P. Knijnenburg, and S. Patil. Give social network users the privacy they want. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, CSCW '15, pages 1427–1441, New York, NY, USA, 2015. ACM.

[148] P. Wisniewski, B. P. Knijnenburg, and H. R. Lipford. Profiling facebook users' privacy behaviors. In *Workshop on Privacy Personas and Segmentation at the Symposium On Usable Privacy and Security*, SOUPS '14, 2014.

[149] P. Wisniewski, H. Lipford, and D. Wilson. Fighting for my space: Coping mechanisms for sns boundary regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, pages 609–618, New York, NY, USA, 2012. ACM.

[150] M. Wu. *Adaptive Privacy Management for Distributed Applications*. PhD thesis, Lancaster University, United Kingdom, June 2007.

[151] W. Xu, F. Zhang, and S. Zhu. Toward worm detection in online social networks. In *Proceedings of the 26th Annual Computer Security Applications Conference*, ACSAC '10, pages 11–20. ACM, 2010.

[152] Y. Yang, S. J. Read, and L. C. Miller. The concept of situations. *Social and Personality Psychology Compass*, 3(6):1018–1037, 2009.

[153] J. Ye, S. Dobson, and S. McKeever. Situation identification techniques in pervasive computing: A review. *Pervasive and Mobile Computing*, 8(1):36–66, 2012.

[154] J. Ye, S. McKeever, L. Coyle, S. Neely, and S. Dobson. Resolving uncertainty in context integration and abstraction: Context integration and abstraction. In *Proceedings of the 5th International Conference on Pervasive Services*, ICPS '08, pages 131–140, New York, NY, USA, 2008. ACM.

[155] L. Zadeh. Fuzzy sets*. *Information and Control*, 8(3):338–353, 1965.

[156] L. A. Zadeh. The concept of a linguistic variable and its application to approximate reasoning—i. *Information Sciences*, 8(3):199–249, 1975.

[157] L. A. Zadeh. Fuzzy logic = computing with words. *IEEE Transactions on Fuzzy Systems*, 4(2):103–111, 1996.

[158] C. Zhang, J. Sun, X. Zhu, and Y. Fang. Privacy and security for online social networks: challenges and opportunities. *IEEE Network*, 24(4):13–18, 2010.

A Questionário da Elicitação de Requisitos

Pesquisa sobre Privacidade em Redes Sociais Móveis

Etapa 1

Este questionário faz parte de um projeto de pesquisa realizado pelo Laboratório de Sistemas Distribuídos da Universidade Federal do Maranhão (http://lsd.ufma.br/). Ele tem por objetivo conhecer mais profundamente as necessidades de usuários em relação a privacidade ao utilizar Redes Sociais Online (também chamadas de Mídias Sociais) através de dispositivos móveis (smartphones, tablets, etc).

Gostaríamos de agradecer a sua participação e informar que você está contribuindo para que sejam construídas soluções mais próximas dos requisitos de privacidade dos usuários.

O questionário respondido por você apenas terá validade caso tenha sido respondido completamente. Portanto, pedimos gentilmente que assim o faça, são apenas 20 questões que levam em média somente 10 minutos para responder.

Informamos ainda que você não é identificado ao responder este questionário. Portanto qualquer informação prestada aqui por você é anônima. As informações que você prestar aqui serão utilizadas apenas para fins de pesquisa.

Você estará apto a responder o questionário completo caso seja maior de idade, possua uma conta no Facebook com no mínimo 50 amigos e utilize algum dispositivo móvel como um dos meios de acesso a ela.

1. Qual sua idade?

2. Você possui uma conta no Facebook com no mínimo 50 amigos e utiliza algum dispositivo móvel como um dos meios de acesso a ela?

(a) Sim

(b) Não

Etapa 2

Diga-nos mais sobre você.

3. Qual seu gênero?

(a) Masculino

(b) Feminino

4. Qual seu nível escolar mais alto?

(a) Ensino Fundamental

(b) Ensino Médio / Técnico

(c) Superior (cursando)

(d) Superior (concluído)

(e) Pós-graduação (especialização)

(f) Pós-graduação (mestrado)

(g) Pós-graduação (doutorado)

5. Onde você mora atualmente? (Cidade, Estado e País)

Etapa 3

Fale mais sobre a sua utilização de mídias sociais (considere o Facebook).

6. Com qual frequência você utiliza mídias sociais por meio de dispositivos móveis? Considere apenas o acesso utilizando algum dispositivo móvel.

(a) 1 vez por semana

(b) 2 a 5 vezes por semana

(c) 1 vez por dia

(d) 2 a 5 vezes por dia

(e) Mais de 5 vezes por dia

7. Você se julga preocupado com sua privacidade em mídias sociais?

(a) Sim

(b) Não

8. Você acha que o fato de acessar mídias sociais através de dispositivos móveis faz com que você esteja sujeito a uma quantidade maior de problemas relacionados a sua privacidade?

(a) Sim

(b) Não

Etapa 4

Se imagine nas situações descritas e analise qual a melhor resposta para as questões. Caso você não consiga se imaginar na situação por nunca ter realizado, não responda a questão, todas elas são opcionais.

O termo "conteúdo"é utilizado para qualquer informação que, ao ser publicada na mídia social, caracterize a situação que você está, tais como uma foto, um vídeo, um comentário ou sua localização (check-in).

Para responder as questões abaixo, considere que você organiza seus contatos (amigos do Facebook) em grupos. Por exemplo, família, amigos, colegas de trabalho, colegas de estudo, colegas de alguma atividade que você realiza (por exemplo, academia, treino de algum esporte, pescaria, etc), apenas conhecidos, etc.

LEGENDA DE RESPOSTAS

Contato ou grupo: Quando você deseja que (i) apenas um contato específico acesse o conteúdo ou (ii) apenas os contatos de um ou mais grupos específicos acessem o conteúdo.

Exceção de contato ou grupo: Quando você deseja que todos seus contatos possam acessar o conteúdo, com exceção de (i) um ou mais contatos ou (ii) um ou mais grupos de contatos.

Para todos contatos: Quando você deseja que todos seus contatos possam acessar o conteúdo.

Público: Quando qualquer usuário da Rede Social Online, inclusive os que não são seus contatos, pode acessar o conteúdo.

Igual a questão anterior: Quando você deseja não modificar (em relação a questão anterior) os contatos que têm acesso ao conteúdo publicado e, portanto, deseja manter a mesma configuração de privacidade da situação anterior. Por exemplo, na situação anterior você determinou que apenas contatos do grupo família tivessem acesso ao conteúdo publicado, na questão atual você deseja que esta configuração seja mantida.

9. Você está em uma festa pela madrugada com um grupo de amigos e publica uma foto sua com eles. Quem você deseja que acesse esse conteúdo?

(a) Contato ou grupo

(b) Para todos contatos

(c) Público

(d) Exceção de contato ou grupo

10. Você está em uma viagem de passeio durante suas férias com seu namorado(a) ou esposo(a) e publica uma mensagem sobre o que está achando do local visitado. Quem você deseja que acesse esse conteúdo?

(a) Contato ou grupo

(b) Para todos contatos

(c) Público

(d) Exceção de contato ou grupo

(e) Igual a questão anterior

11. Você está trabalhando em seu expediente e publica um vídeo curto que representa um pouco de sua rotina de trabalho. Quem você deseja que acesse esse conteúdo?

(a) Contato ou grupo

(b) Para todos contatos

(c) Público

(d) Exceção de contato ou grupo

(e) Igual a questão anterior

12. Você está estudando na universidade (ou escola) e publica um comentário sobre o assunto estudado. Quem você deseja que acesse esse conteúdo?

(a) Contato ou grupo

(b) Para todos contatos

(c) Público

(d) Exceção de contato ou grupo

(e) Igual a questão anterior

13. Você está sozinho comendo em um restaurante conhecido no horário do almoço ou janta e publica uma foto do prato. Quem você deseja que acesse esse conteúdo?

(a) Contato ou grupo

(b) Para todos contatos

(c) Público

(d) Exceção de contato ou grupo

(e) Igual a questão anterior

14. Você está em um momento de lazer com sua família e publica um vídeo da atividade que vocês estão realizando. Quem você deseja que acesse esse conteúdo?

(a) Contato ou grupo

(b) Para todos contatos

(c) Público

(d) Exceção de contato ou grupo

(e) Igual a questão anterior

15. Você está em um momento de descanso durante o final de semana (sábado ou domingo) e publica um comentário mostrando o quanto é bom ter momentos de descanso. Quem você deseja que acesse esse conteúdo?

(a) Contato ou grupo

(b) Para todos contatos

(c) Público

(d) Exceção de contato ou grupo

(e) Igual a questão anterior

16. Você está em uma viagem de trabalho com seu chefe durante a semana e publica uma foto da atividade profissional que está realizando durante a viagem. Quem você deseja que acesse esse conteúdo?

(a) Contato ou grupo

(b) Para todos contatos

(c) Público

(d) Exceção de contato ou grupo

(e) Igual a questão anterior

17. Você está em uma comemoração com seus amigos em uma choperia (bar ou pub) e publica sua localização (check-in) fazendo marcação de seus amigos mostrando que eles estão co-localizados. Quem você deseja que acesse esse conteúdo?

(a) Contato ou grupo

(b) Para todos contatos

(c) Público

(d) Exceção de contato ou grupo

(e) Igual a questão anterior

18. Você está realizando uma prática de atividade física no horário noturno com nenhum contato da sua Rede Social Online presente (co-localizado) e publica uma foto que retrata essa atividade. Quem você deseja que acesse esse conteúdo?

(a) Contato ou grupo

(b) Para todos contatos

(c) Público

(d) Exceção de contato ou grupo

(e) Igual a questão anterior

19. Ao responder as questões anteriores, que fatores lhe influenciaram a mudar sua definição de quais contatos podem acessar seus conteúdos publicados (ou seja, motivou a mudança de suas configurações de privacidade)? Além desses, podem haver outros fatores que influenciaram você, e que poderá listar na questão seguinte.

(a) A sua localização (como no trabalho, em casa, em um bar, em uma outra cidade,

etc) - Influenciou ou Não influenciou?

(b) O fator tempo (horário no dia, dia da semana, período do ano, etc) - Influenciou ou Não influenciou?

(c) As pessoas co-localizadas (próximas a você) - Influenciou ou Não influenciou?

(d) O tipo de conteúdo (foto, vídeo, comentário, sua localização) - Influenciou ou Não influenciou?

20. Você considera que algum outro fator influenciou as suas respostas? Se sim, diga qual(is). (Resposta em texto livre)

B Questionário da Avaliação de Acurácia do *SelPri*

Pesquisa sobre experiência de uso do *SelPri*

Este questionário deve ser respondido após a experiência de ter utilizado o *SelPri* - Identificador de Situações.

1. Qual sua idade?

2. Qual seu gênero?

(a) Masculino

(b) Feminino

3. Aconteceram momentos em que você estava em uma determinada situação definida mas o *SelPri* não identificou que você estava nela?

(a) Sim

(b) Não

4. Se sim, após alguns minutos o *SelPri* conseguiu identificar a situação?

(a) Sim

(b) Não

C Questionário da Experiência de Uso do *SelPri*

Este questionário faz parte de um projeto de pesquisa realizado pelo Laboratório de Sistemas Distribuídos da Universidade Federal do Maranhão (http://lsd.ufma.br/). O projeto tem por objetivo conhecer mais profundamente as necessidades de usuários em relação a privacidade ao utilizar Redes Sociais Online (também chamadas de Mídias Sociais) através de dispositivos móveis (smartphones, tablets, etc) e contribuir na construção de soluções mais próximas dos requisitos de privacidade dos usuários.

O questionário respondido por você apenas terá validade caso tenha sido respondido completamente. Portanto, pedimos gentilmente que assim o faça. Você estará apto a responder o questionário completo caso tenha utilizado o SelPri (http://lsd.ufma.br/selpri/) por pelo menos 3 dias. Informamos ainda que você não é identificado ao responder este questionário. Portanto qualquer informação prestada aqui por você é anônima. As informações que você prestar aqui serão utilizadas apenas para fins de pesquisa.

Agradecemos a sua participação.

Etapa 1

1. Quanto tempo (em dias) você usou o *SelPri*?
2. Qual sua idade?

Etapa 2

Utilize a escala de 1 a 5 para confirmar a sua concordância com a afirmação.

3. É fácil a utilização da aplicação.
4. Não tive problemas em aprender a utilizar a aplicação.
5. Tive facilidade para lembrar o uso da aplicação após um período de tempo sem utilizá-la.
6. Para usar as funcionalidades disponíveis pela aplicação, as interfaces apresentadas são suficientes.
7. Me sinto satisfeito a respeito da interação com as interfaces da aplicação.
8. As mensagens de erro ou alerta na aplicação são expressas em linguagem simples de entendimento.

9. Ocorreram poucos erros (*bugs*) provocados pela aplicação.

10. As funcionalidades disponibilizadas pela aplicação são efetuadas rapidamente.

11. Consegui expressar todas minhas situações ao realizar postagem de conteúdo.

12. Os tipos de informações contextuais (localização, contatos co-localizados, dias da semana, horário no dia) utilizados para expressar as situações são suficientes. 13. A aplicação identificou minhas situações corretamente.

14. A aplicação identificou minhas situações em tempo hábil.

15. Os níveis de autonomia me permitiram escolher como a aplicação deve se comportar ao definir configurações de privacidade automáticas.

16. Através das configurações dos perfis de privacidade situacionais e dos níveis de autonomia, tenho controle sobre as ações realizadas pela aplicação.

17. A aplicação permite expressar meus requisitos dinâmicos e situacionais de privacidade para postagem de conteúdos através dos recursos disponibilizados.

18. Considero a aplicação útil para me garantir privacidade em redes sociais móveis.

Etapa 3

Questões subjetivas.

19. Ao utilizar mídias sociais tal como o Facebook antes de ter essa experiência com o uso do *SelPri*, você modificava manualmente a configuração de privacidade a cada postagem de conteúdo? Nos diga como você fazia naturalmente e se você analisava a cada postagem qual a melhor configuração de privacidade.

20. Muitos são os casos em que o próprio usuário não tem noção ou consciência das implicações que a falta de privacidade em mídias sociais causam para si, e muitas pesquisas tem mostrado isso. Com o uso do *SelPri*, você passou a conhecer mais sobre as suas próprias necessidades em relação a privacidade? Nos diga mais como foi sua experiência ao utilizar a aplicação.

D Questionário da Experiência de Uso do *SituMan*

Research about Situation Awareness in Mobile Mental Health Applications

This questionnaire is part of a research project carried out by INESC TEC. The questionnaire aims to know how was your experience using the Situation Manager application together with the MoodBuster application.

The answer to the questionnaire is only valid if you answer all questions. Therefore, we kindly ask you to answer them all.

We also inform that you are not identified by answering this questionnaire. The information provided is anonymous and will be only used for this investigation.

You are able to answer the full questionnaire if you used the Situation Manager along with MoodBuster for 7 days.

In the first item you should confirm that you sent us your log situations. You will be confirming that sent us by e-mail (situman@googlegroups.com) the file log.txt saved by Situation Manager application using the Log Manager option menu.

We appreciate your participation in this evaluation process.

Step 1

1. How old are you?

2. What is your gender?

Step 2

Tell us about your experience with the use of Situation Manager.

Use the scale from 1 to 5 to confirm your agreement with the affirmation.

3. The use of the Situation Manager application is easy.

4. The interfaces shown in the Situation Manager application are sufficient to use the available features.

5. I had no problem in learning how to use the Situation Manager application.

6. Error and alert messages in the Situation Manager application are expressed in a simple and easy language for understanding.

7. Few errors (bugs) caused by the Situation Manager application occurred.

8. The Situation Manager application correctly identified my situations.

9. The Situation Manager application identified my situation at the right time.

10. I was able to express all my situations.

11. The types of contextual information (location, day of week, time on the day, and activity) used to express the situations are sufficient.

12. Tell us more about your experience with the use of these applications. This space can be used to tell us something that you consider important. This question is not mandatory.