UM MODELO DE DESIGN DE PRIVACIDADE PARA O COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS EM REDES SOCIAIS ONLINE

MARIA LÚCIA BENTO VILLELA

UM MODELO DE DESIGN DE PRIVACIDADE PARA O COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS EM REDES SOCIAIS ONLINE

Tese apresentada ao Programa de Pós-Graduação em Ciência da Computação do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais - Departamento de Ciência da Computação como requisito parcial para a obtenção do grau de Doutor em Ciência da Computação.

Orientadora: Raquel Oliveira Prates

Belo Horizonte

Março de 2016

© 2016, Maria Lúcia Bento Villela.
Todos os direitos reservados.

Villela, Maria Lúcia Bento
V266m Um modelo de design de privacidade para o compartilhamento de informações pessoais em redes sociais online / Maria Lúcia Bento Villela. — Belo Horizonte, 2016
xxv, 157f. : il. ; 29cm

Tese (doutorado) — Universidade Federal de Minas Gerais - Departamento de Ciência da Computação
Orientadora: Raquel Oliveira Prates

1. Computação – Teses. 2. Redes sociais online – Teses. 3. Interfaces de usuário (Sistema de computador) – Teses. 4. Interação homem-máquina – Teses. 5. Direito a privacidade – Teses. I. Orientadora. II. Título.

CDU 519.6*75(043)

UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

FOLHA DE APROVAÇÃO

Um modelo de design de privacidade para o compartilhamento de informações pessoais em redes sociais online

MARIA LÚCIA BENTO VILLELA

Tese defendida e aprovada pela banca examinadora constituída pelos Senhores:

PROFA. RAQUEL OLIVEIRA PRATES - Orientadora
Departamento de Ciência da Computação - UFMG

PROF. ANTONIO AUGUSTO PEREIRA PRATES
Departamento de Sociologia e Antropologia - UFMG

PROFA. CLARISSE SIECKENIUS DE SOUZA
Departamento de Informática - PUC - RJ

PROFA. JUSSARA MARQUES DE ALMEIDA GONÇALVES
Departamento de Ciência da Computação - UFMG

PROFA. MARIA CECÍLIA CALANI BARANAUSKAS
Instituto de Computação - UNICAMP

Belo Horizonte, 18 de março de 2016.

À memória da minha mãe, exemplo para mim de força e fé.

Agradecimentos

A Deus, que está sempre comigo, e me permitiu realizar este sonho.

Ao meu marido, Severino, por todo o seu apoio, carinho e compreensão, que foram imprescindíveis para eu chegar até aqui.

Aos meus filhos - Amaury, Luiza e Vítor, pelo amor incondicional, por suportarem a minha ausência em tantos momentos importantes de suas vidas e pelo carinho que sempre me dedicaram. Tudo isso me deu grande força para enfrentar as dificuldades do caminho.

Aos meus pais, Geraldo e Consolação, pelo apoio, por torcerem sempre por mim e por terem me transmitido os bens mais valiosos na vida: a educação e a honestidade. Um agradecimento especial à minha mãe, que esteve sempre comigo, me dando forças e rezando por mim, e que agora está junto de Deus. Agradeço também aos meus irmãos - Marcos, Márcia e Mônica, aos meus cunhados e sobrinhos, e ao meu sogro, Amaury, e à minha sogra, Edméa, pelo apoio, amizade e carinho.

À Raquel Prates, minha orientadora, pelos ensinamentos, conselhos e atenção dedicada a mim durante todo este tempo. Não tenho palavras para expressar a minha gratidão por tudo o que fez e foi para mim, se mostrando não só uma grande orientadora, mas também uma amiga e um exemplo de pessoa e profissional.

À minha amiga, Simone, um anjo que Deus colocou no meu caminho, pela parceria e por toda a sua ajuda, apoio e palavras de encorajamento e carinho durante o doutorado.

Aos colegas do Pensi (Bernardo, Diego, Érica, Glívia, Júlio, Lídia, Luiz, Manoel, Natália, Pricila, Rodrigo e Soraia), pelo apoio, momentos de aprendizado,

colaboração e companheirismo. Agradeço em especial ao Diego, à Lídia e à Pricila, pela ajuda nos momentos finais. Minha gratidão também aos volutários que participaram dos meus estudos.

Aos amigos de Diamantina, que me deram força e torceram por mim, em especial à Bethe e ao Reynaldo, pela ajuda nos preparativos para o doutorado-sanduíche, e à Emiliana, pelo carinho e pela agradável companhia na fase inicial do doutorado.

Aos amigos e colegas do Doutorado, em especial ao Glauber, Henrique, Kleber, Luciana, Virgínia e Thiago, por compartilharem comigo os momentos de estudo para as provas de qualificação e pela oportunidade de convivência.

Ao professor Frank Shipman, pela oportunidade de fazer o doutorado-sanduíche na Texas A&M University.

Aos membros da banca examinadora, pelas valiosas sugestões e contribuições para melhorar a versão final deste trabalho.

Ao Departamento de Ciência da Computação da UFMG, pela infra-estrutura necessária para a realização deste trabalho, e à equipe da Secretaria do PPGCC, em especial à Sônia, Renata, Linda, Sheila e Maristela, por terem sido sempre tão atenciosas e prestativas.

Ao Departamento de Computação da UFVJM, por ter me concedido a liberação para cursar o doutorado, e aos colegas do Departamento, pelo apoio.

À Fapemig, pela bolsa do Programa Mineiro de Capacitação Docente, e à Capes, pela bolsa do doutorado-sanduíche.

Enfim, a todas as pessoas que, direta ou indiretamente, contribuíram para a realização deste trabalho.

"Sem o sofrimento da luta,
não há o prazer da vitória."
(autor desconhecido)

Resumo

Nos últimos anos, as redes sociais online (RSOs) têm experimentado considerável crescimento em número de usuários, tornando-se cada vez mais presentes na vida das pessoas. Entretanto, juntamente com esse crescimento, a possibilidade de maiores interações entre as pessoas, proporcionada pelo uso desses sistemas, tem despertado novas preocupações relacionadas à privacidade, dado o aumento do risco das pessoas terem suas informações indevidamente acessadas nesses ambientes. Diante disso, a ideia de incorporar princípios de privacidade em tempo de design apresenta-se como um requisito essencial, de forma a criar RSOs que atendam à necessidade de privacidade de seus usuários. Dessa forma, nesta tese, buscamos fornecer aos designers uma forma de pensar sobre como a privacidade relacionada ao compartilhamento de informações pessoais pode ser tratada em RSOs. Para isso, apresentamos o Modelo de Design de Privacidade (MDP), um modelo descritivo que é fundamentado na teoria de privacidade proposta por Altman e na Engenharia Semiótica. Tal modelo considera como informação pessoal em RSOs não apenas aquelas informações sobre o indivíduo que são explicitamente reveladas, mas também seus discursos e atividades dentro do sistema, que expressam, direta ou indiretamente, suas opiniões e pontos de vista, os quais o indivíduo poderia não desejar que fossem revelados. O MDP tem o propósito de ajudar designers a refletirem sobre diferentes aspectos que influenciam o nível de privacidade oferecido aos usuários, ao propor um conjunto de dimensões que estruturam o espaço de design do compartilhamento de informações pessoais em RSOs. Avaliações mostram que o MDP é expressivo o suficiente para representar aspectos relevantes de privacidade, além de ser também descritivo o suficiente para expressar diferenças em modelos de privacidade de RSOs distintas. O potencial valor epistêmico do MDP é mostrado, tendo em vista que seu uso tem o poder de fomentar discussões e reflexões relacionadas a decisões de privacidade que podem ser úteis no design de RSOs.

Palavras-chave: Privacidade, Compartilhamento de Informação Pessoal, Redes Sociais Online, Engenharia Semiótica, Interação Humano-Computador.

Abstract

In the last few years, Social Network Sites (SNSs) have experienced a growth in their number of participants, becoming an increasingly embedded part of people's daily lives. However, along with such growth, the possibility of closer interactions between people, brought by these systems, has triggered users' concerns and issues regarding privacy, given the increasingly risk of people's personal information being improperly accessed within such environments. Thus, the idea of privacy by design, i.e., incorporating privacy principles at design time rather than as an afterthought, is presented as an essential requirement, even if challenging, in order to create user interfaces that allow users to express their privacy requirements regarding personal information disclosure. Thereby, in this thesis, we intend to support designers in thinking about how privacy regarding personal information disclosure can be addressed in SNSs. In this direction, we present the Privacy Design Model (PDM) – a descriptive model that is built upon Altman's theory of privacy and Semiotic Engineering and considers as personal information in SNSs not only pieces of information about the individual, but also the individual's speech and activities that express, direct or indirectly, his/her opinions and views within the system, which he/she could not want to disclose. PDM aims at helping designers to take into consideration how different aspects influence the level of privacy being offered to users, by structuring the design space of personal information disclosure in SNSs through a number of dimensions. The evaluation of PDM expressivity shows that it is expressive enough to represent relevant aspects of privacy and also descriptive enough to express differences in the privacy models of SNSs with distinct purposes. The potential epistemic value of MDP is shown through the discussions and reflections it fosters regarding privacy decisions that could be useful for the design of SNSs' privacy models.

Keywords: Privacy, Personal Information Disclosure, Social Network Sites, Semiotic Engineering, Human-Computer Interaction.

Lista de Figuras

1.1 Etapas da pesquisa 5

2.1 Modelo de Comunicação de Jakobson 15
2.2 Espaço de design da Engenharia Semiótica 16

3.1 Nível de pessoalidade das informações, variando no eixo y de "não pessoal" (1) a "muito pessoal" (4) (a ordem em que as informações são listadas na legenda é a mesma em que aparecem no gráfico, da esquerda para a direita) 24

4.1 Estrutura do MDP, com as dimensões de privacidade 35
4.2 Relacionamentos entre as dimensões de privacidade do MDP 37
4.3 Estrutura do MDP, com as dimensões de privacidade, seus possíveis valores e os níveis de privacidade remetidos pelos mesmos 38
4.4 Compartilhamento de informação pessoal na linha do tempo do indivíduo no Facebook 40
4.5 Página "Questions" no ResearchGate 41
4.6 Compartilhamento de informação *tipada* no perfil do indivíduo no Facebook 42
4.7 Postagem de atualização de status no Facebook 42
4.8 Indivíduo compartilhando informação na linha do tempo de outro usuário, com audiência desconhecida, no Facebook 46
4.9 Notificações exibidas para o indivíduo quando usuários comentam e seguem suas publicações no ResearchGate 47
4.10 Recurso Ticker do Facebook, dando destaque à informação compartilhada sobre o indivíduo 48
4.11 Sugestão de amizade no Facebook 48
4.12 Exibição do "RGScore" na Página do Indivíduo do ResearchGate 50
4.13 (Re)compartilhamento de postagem no Facebook 51
4.14 Representação gráfica do framework *honeycomb* [Smith, 2007] 55

4.15 Disposição das dimensões de privacidade do MDP na representação visual de um tipo de comunicação 56
4.16 Representação dos níveis de privacidade da comunicação referente ao indivíduo compartilhar informação pessoal em sua linha do tempo no Facebook 59
4.17 Tela do protótipo da ferramenta de visualização do MDP 61

5.1 Audiência da informação divulgada no perfil do usuário no Facebook . . . 73
5.2 Notificação quando outro usuário curte, comenta e compartilha informação de perfil do indivíduo no Facebook 73
5.3 Compartilhamento de informação no perfil do indivíduo sendo mostrada no (a) *Feed de notícias* e na (b) seção *Novidades* do Facebook 74
5.4 Página de Ajuda sobre o *Feed de Notícias* (ou "News Feed", em inglês) do Facebook 74
5.5 Página de Ajuda sobre o recurso *Novidades* (ou "Ticker", em inglês) do Facebook 75
5.6 Sugestão de amizade no Facebook 76
5.7 Representação visual do tipo de comunicação (1) do Facebook 76
5.8 Representação visual do tipo de comunicação (2) do Facebook 78
5.9 Representação visual do tipo de comunicação (3) do Facebook 80
5.10 Representação visual do tipo de comunicação (4) do Facebook 82
5.11 Representação visual do tipo de comunicação (5) do Facebook 84
5.12 Parte da página perfil do usuário no ResearchGate 90
5.13 Configurações de privacidade no ResearchGate 91
5.14 Sugestão para seguir pesquisadores no ResearchGate 92
5.15 Representação visual do tipo de comunicação (1) do ResearchGate 92
5.16 Representação visual do tipo de comunicação (2) do ResearchGate 93
5.17 Representação visual do tipo de comunicação (3) do ResearchGate 94
5.18 Representação visual do tipo de comunicação (4) do ResearchGate 96
5.19 Representação visual do tipo de comunicação (5) do ResearchGate 97
5.20 Exibição de estatísticas (guia "Stats") na página do indivíduo no ResearchGate 98
5.21 Exibição de métrica de reputação científica (guia "RG Score") na página do indivíduo no ResearchGate 99
5.22 Compartilhando informações no perfil do CaringBridge 103
5.23 Configuração de privacidade do perfil no CaringBridge 104
5.24 Representação visual do tipo de comunicação (1) do CaringBridge 104
5.25 Representação visual do tipo de comunicação (2) do CaringBridge 106
5.26 Representação visual do tipo de comunicação (3) do CaringBridge 107

Lista de Tabelas

4.1 Escala de cinza para os hexágonos correspondentes aos valores das dimensões do MDP 57
4.2 Bordas representado o momento em que o valor para a dimensão é definio e quem tem controle sobre ela 58

5.1 Modelagem do tipo de comunicação (1) do Facebook 72
5.2 Modelagem do tipo de comunicação (2) do Facebook 77
5.3 Modelagem do tipo de comunicação (3) do Facebook 79
5.4 Modelagem do tipo de comunicação (4) do Facebook 81
5.5 Modelagem do tipo de comunicação (5) do Facebook 83
5.6 Modelagem do tipo de comunicação (1) do ResearchGate 89
5.7 Modelagem do tipo de comunicação (2) do ResearchGate 93
5.8 Modelagem do tipo de comunicação (3) do ResearchGate 94
5.9 Modelagem do tipo de comunicação (4) do ResearchGate 95
5.10 Modelagem do tipo de comunicação (5) do ResearchGate 97
5.11 Modelagem do tipo de comunicação (1) do CaringBridge 102
5.12 Modelagem do tipo de comunicação (2) do CaringBridge 105
5.13 Modelagem do tipo de comunicação (3) do CaringBridge 106
5.14 Comparação das modelagens MDP das RSOs Facebook, ResearchGate e CaringBridge 110

6.1 Níveis de exposição a partir das dimensões “Fonte de Informação”, “Conteúdo” e “Audiência” do MDP 129

B.1 Descrição das dimensões do PDM 193
B.2 Descrição dos atributos das dimensões do MDP 194
B.3 Possíveis valores dos atributos das dimensões do MDP 194
B.4 Níveis de privacidade relacionados às dimensões do MDP 198

Lista de Abreviaturas

IHC Interação Humano-Computador

MDP Modelo de Design de Privacidade

RSO Rede Social Online

SiCo Sistema Colaborativo

Sumário

Agradecimentos **ix**

Resumo **xiii**

Abstract **xv**

Lista de Figuras **xvii**

Lista de Tabelas **xix**

1 Introdução **1**

1.1 Objetivo 3

1.2 Metodologia 4

1.3 Contribuições 7

1.4 Estrutura da Tese 8

2 Fundamentação Teórica **9**

2.1 Teoria de Privacidade 9

2.2 Engenharia Semiótica 13

2.2.1 Modelos da Engenharia Semiótica para o Design de Sistemas Colaborativos 16

3 Estudos Iniciais Sobre Privacidade **19**

3.1 Estudos Empíricos sobre Privacidade em RSOs 19

3.1.1 Entrevistas 20

3.1.2 Questionário 22

3.2 Levantamento da Literatura sobre Privacidade 26

3.2.1 Artefatos Conceituais para o Design de Privacidade 26

3.3 Modelos de Privacidade para RSOs 29

4 O Modelo de Design de Privacidade **33**
4.1 Estrutura do MDP 34
4.1.1 Dimensões de Privacidade 37
4.2 Decisões de Privacidade Apoiadas no MDP 51
4.2.1 Quais são as principais oportunidades nas quais informações pessoais dos usuários podem ser compartilhadas? 52
4.2.2 Para cada uma das oportunidades de compartilhamento de informação pessoal identificadas, como as dimensões de privacidade serão tratadas? 53
4.3 A Representação Visual do MDP 55

5 Avaliação **63**
5.1 Considerações Metodológicas 63
5.2 Execução 65
5.3 Avaliação com Especialista 70
5.3.1 O compartilhamento de informações pessoais no Facebook . . . 70
5.3.2 O compartilhamento de informações pessoais no ResearchGate . 87
5.3.3 O compartilhamento de informações pessoais no CaringBridge . 101
5.3.4 Usando o MDP para diferenciar RSOs sob o ponto de vista de privacidade 109
5.4 Avaliação com Potenciais Usuários 114
5.4.1 Entendimento e uso do MDP 114
5.4.2 O Uso do MDP para caracterizar RSOs distintas com relação à privacidade 118
5.4.3 Custos e benefícios do MDP 121
5.4.4 A representação visual como apoio ao entendimento e uso do MDP 122
5.5 Revisitando as Questões de Avaliação 1 e 2 124

6 Discussão **127**
6.1 Constatações e Limites do MDP 127
6.1.1 O papel das dimensões do MDP no estado de privacidade do indivíduo 127
6.1.2 Níveis de análise da privacidade através do MDP 131
6.1.3 Limites representacionais do MDP 132
6.1.4 Aspectos não Considerados no MDP 135
6.2 Considerações sobre a Avaliação do MDP 136
6.3 O MDP e outros estudos relacionados ao design de privacidade 140

7 Considerações Finais **143**
7.1 Trabalhos Futuros 144

Referências Bibliográficas **147**

Apêndice A Roteiro da Entrevista e Questionário **157**

Apêndice B Guia Prático sobre o MDP **193**

Apêndice C Material Utilizado na Avaliação com Potenciais Usuários do MDP **201**

Capítulo 1

Introdução

A Internet, com mais de três bilhões de usuários[1], tem mudado drasticamente a forma como as pessoas se relacionam socialmente, uma vez que vem sendo cada vez mais utilizada para apoiar a interação social entre seus usuários, por meio das redes sociais online (RSOs). De acordo com boyd & Ellison [2008], RSOs são sistemas baseados na web, que permitem às pessoas construírem um perfil público ou semi-público e se conectarem a outros usuários, que poderão ter acesso às suas informações. Nesse sentido, RSOs são consideradas sistemas colaborativos (SiCo's), uma vez que apoiam a *comunicação* e o *compartilhamento de informações*, que consistem em categorias de comportamento humano que contribuem para a *colaboração*[2][Grudin & Poltrock, 2016].

Ao permitirem uma interação mais rápida e fácil entre seus usuários, através do compartilhamento dos mais diversos tipos de informação, as RSOs têm experimentado um considerável crescimento em número de participantes nos últimos anos, tornando-se cada vez mais integradas à vida das pessoas [Perrin, 2015], e recebido crescente atenção de pesquisa. Entretanto, enquanto o uso desses sistemas cresce, novas preocupações relacionadas à privacidade surgem [Acquisti et al., 2015], uma vez que favorecem o compartilhamento de quantidades crescentes de informações pessoais como parte de sua funcionalidade, se apresentando como uma ameaça à privacidade de seus usuários.

Embora a maior parte das RSOs ofereçam aos seus usuários mecanismos que lhes permitem gerenciar a sua privacidade, ao estabelecerem configurações relativas ao compartilhamento de informações, disparidades têm sido observadadas entre configurações reais e desejadas, resultando em estados indesejados de privacidade [Liu et al., 2011; Netter et al., 2013]. Entretanto, tal fato nem sempre ocorre como resultado de um

[1]Dados de Internet Live Stats em janeiro de 2016 (http://www.internetlivestats.com/internet-users/).

[2]Este conceito amplia o conceito original de Sistema Colaborativo, que se refere à colaboração para execução de tarefa [Ellis et al., 1991].

gerenciamento inadequado da privacidade por parte dos usuários. Ao invés disso, tal disparidade pode ser resultado do sistema se basear em um modelo não apropriado de privacidade. Assim, a ideia de "privacidade desde o design" – isto é, incorporar princípios de privacidade em tempo de design, ao invés de deixar para se pensar em privacidade em momentos posteriores [Cavoukian, 2006] – é apresentada como um requisito importante, embora desafiador, no sentido de se criar interfaces que permitam que usuários atinjam o seu estado desejado de privacidade [Bélanger & Crossler, 2011]. Esse desafio remete à distância sócio-técnica definida por Ackerman [2000], como sendo a diferença entre o comportamento que se deve apoiar socialmente – considerando as inúmeras exceções, nuances e possibilidades que ditam a forma como as pessoas interagem no mundo físico – e o que os sistemas colaborativos podem fazer tecnicamente, considerando que o seu comportamento é restrito por regras que não conseguem cobrir toda a riqueza de possibilidades inerentes às relações sociais.

Ao longo dos últimos 10 anos, muitos estudos têm investigado como as pessoas tratam, percebem e se preocupam com privacidade em RSOs [Gross & Acquisti, 2005; Lewis et al., 2008; Debatin et al., 2009; Joinson et al., 2010; Stutzman & Hartzog, 2012; Bevan et al., 2015]. Além disso, pesquisadores também têm apresentado tecnologias voltadas para o tratamento de privacidade nas interfaces desses sistemas [Besmer & Lipford, 2010; Gao & Berendt, 2013; Paul et al., 2012; Mazzia et al., 2012; Malandrino et al., 2013; Wang & Zhou, 2015]. No plano conceitual, algumas ferramentas têm sido propostas, visando aumentar a flexibilidade que RSOs oferecem aos seus usuários, no sentido de lidarem com aspectos específicos de privacidade, como o controle de acesso e o gerenciamento de compartilhamento [Fong et al., 2009; Lederer et al., 2003; Pang & Zhang, 2015; Tierney & Subramanian, 2014]. No entanto, tais ferramentas não se propõem a apoiar designers em sua tomada de decisões, em tempo de design, sobre aspectos de privacidade que devem ser considerados nesses sistemas. Nessa direção, Romero et al. [2012] apresentam um modelo para apoiar o design de mecanismos de privacidade em RSOs, relacionado à disponibilidade dos usuários para engajarem em um processo comunicativo, dentro de um canal exclusivo. Epstein et al. [2015], por sua vez, desenvolveu um framework voltado para o design e avaliação de aspectos relacionados ao compartilhamento de informações coletadas automaticamente nas RSOs, como aquelas relacionadas à localização ou à atividade física de seus usuários, focando nas respostas e reações da audiência.

Numa perspectiva diferente da tratada por Romero et al. [2012] e Epstein et al. [2015], nós consideramos privacidade relacionada ao compartilhamento de informações pessoais em RSOs, que podem ser geradas pelo próprio indivíduo ao qual a informação se refere, ou por outros usuários do sistema. Além disso, consideramos como infor-

mações pessoais também os discursos e atividades do indivíduo, , tendo em vista que traços e atributos de privacidade podem ser inferidos a partir de registros do comportamento [Pontes et al., 2012; Kosinski et al., 2013] e sinais linguísticos [Golbeck et al., 2011; Tausczik & Pennebaker, 2010; Yarkoni, 2010] de seus usuários. Assim, privacidade em nosso estudo diz respeito à restrição de fluxos de informação sobre um indivíduo para outras pessoas em RSOs [Rubel & Biava, 2014], considerando o alcance do compartilhamento de informações pessoais nesses sistemas.

Assim, em consonância com do Desafio nº 4 (Valores Humanos) dos "Cinco Grandes Desafios de Pesquisa na área de Interação Humano-Computador (IHC) no Brasil: 2012 – 2022", [Baranauskas et al., 2015], esta tese tem o propósito de ajudar designers de RSOs a refletirem sobre como tratar privacidade nesses sistemas, no que tange especificamente ao compartilhamento de informações pessoais. A nossa intenção é apoiar designers em suas decisões sobre diferentes aspectos relacionados a tal compartilhamento, no sentido de permitir que os usuários alcancem seus estados desejados de privacidade.

Na próxima seção, descrevemos o objetivo da nossa pesquisa. Na seção 1.2, sumarizamos os passos que seguimos a fim de elaborar a questão de pesquisa que o nosso trabalho se propõe a resolver, no sentido de permitir o avanço do estado-da-arte da pesquisa em IHC. Na seção 1.3, sumarizamos as contribuições a serem trazidas pela pesquisa e, por fim, na seção 1.4, apresentamos a estrutura desta tese.

1.1 Objetivo

O objetivo da nossa pesquisa é elaborar um modelo descritivo de privacidade para apoiar o design de interação para RSOs, com foco no compartilhamento de informações pessoais. Nesse sentido, a nossa proposta é desenvolver uma ferramenta epistêmica[3], que auxilie o designer a pensar sobre como tratar tal compartilhamento. Assim, não se pretende oferecer aos designers uma solução pronta para aplicarem a seus projetos de interface, e sim auxiliá-los a elaborarem cuidadosamente suas soluções de interface, ao permitir que melhorem o seu conhecimento sobre esses aspectos. Isto está alinhado à perspectiva de reflexão em ação de Schön [1983], para a qual o processo de design consiste em explorar a situação problemática diante da qual o designer se encontra, até que ele a tenha compreendido e seja capaz de formular o problema, que é único, para o qual precisa elaborar uma solução igualmente única.

[3]Definida, neste caso, como uma ferramenta que apoia o designer em sua reflexão sobre o design que está sendo feito, ajudando-o a obter novo conhecimento ou habilidades [de Souza, 2005].

Escolhemos como base teórica de IHC para fundamentar a nossa pesquisa a Engenharia Semiótica [de Souza, 2005], que tem como proposta fornecer ferramentas epistêmicas que ajudam o designer a formular o problema e as questões de design, bem como elaborar as próprias respostas e soluções. Nesse sentido, a Engenharia Semiótica oferece um conjunto de ferramentas epistêmicas voltadas especificamente para o apoio do design de sistemas interativos, como os modelos MetaCom-G* e Marq-G* [Prates, 1998; Barbosa, 2002], a MoLIC (Modeling Language for Interaction as Conversation) [Barbosa & de Paula, 2003], a Manas [Barbosa, 2006] e a CVM (Cultural Viewpoints Metaphors) [Salgado, 2011]. Dessas ferramentas, o MetaCom-G*, o Marq-G* e a Manas foram criados com o propósito de endereçar questões de design específicas de SiCo's, enquanto que a MoLIC, apesar de ter sido originalmente criada para apoiar o design de sistemas monousuários, vem sendo estendida para considerar a modelagem também de SiCo's [Silva, 2005; de Souza & Barbosa, 2014, 2015]. Assim, através da pesquisa apresentada nesta tese, estaremos ampliando a gama de questões que a Engenharia Semiótica pode tratar, no sentido de prover uma ferramenta que apoie especificamente o design do compartilhamento de informações pessoais em RSOs, com foco na privacidade de seus usuários.

1.2 Metodologia

Iniciamos a nossa pesquisa fazendo um estudo exploratório, aplicando o Método de Inspeção Semiótica (MIS) [de Souza et al., 2006, 2010] para caracterizar estratégias de colaboração em diferentes RSOs. Assim, foi analisada a colaboração nas interfaces de três sistemas que permitem a interação entre seus usuários, baseada na troca e compartilhamento de informação: duas redes virtuais de colaboração científica, o ResearchGate[4] e o Academia.edu[5], que são sistemas que possibilitam a colaboração científica ao permitir que pesquisadores compartilhem conhecimento e encontrem potenciais parceiros de pesquisa, e uma RSO de propósito geral, o Facebook[6], que permite interação social entre seus usuários para os mais diversos fins. Esse estudo nos permitiu identificar que a privacidade relacionada ao compartilhamento de informações é comunicada e representada de formas diferentes nas interfaces desses dois tipos de sistemas, levando-nos a concluir que o propósito e contexto do sistema podem influenciar na forma como a privacidade é comunicada em sua interface [Villela et al., 2015b]. Tal fato nos despertou o interesse para o nosso objetivo de pesquisa.

[4] www.researchgate.net
[5] www.academia.edu
[6] www.facebook.com

Assim, a primeira etapa da pesquisa consistiu em efetuar outros estudos exploratórios empíricos e levantamento bibliográfico, que nos permitiram definir a questão de pesquisa, com base no objetivo previamente estabelecido. Com base nos resultados desses estudos, propomos o Modelo de Design de Privacidade (MDP), um modelo descritivo para apoiar o design de privacidade em RSOs. Em seguida, fizemos a avaliação do modelo que propomos, com o foco em sua expressividade. A Figura 1.1 mostra as etapas que fizeram parte da nossa pesquisa.

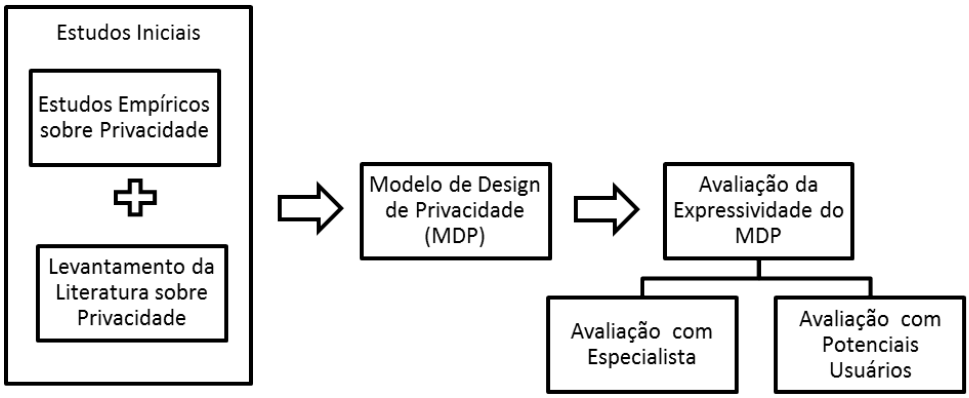


Figura 1.1. Etapas da pesquisa

Os estudos empíricos que consistiram no passo inicial da nossa pesquisa abrangeram entrevistas e questionários, a partir dos quais obtivemos resultados qualitativos e quantitativos que nos permitiram identificar e contrastar como questões de privacidade relacionadas ao compartilhamento de informações pessoais são tratadas pelas pessoas, no mundo físico, das interações face-a-face, e no mundo virtual, das RSOs de propósito geral [Xavier et al., 2014; Villela et al., 2015a,c,d]. A partir desses estudos, identificamos alguns aspectos relacionados à privacidade no compartilhamento de informações pessoais interessantes para serem considerados em nossa pesquisa. Em particular, os resultados mostram que as pessoas entendem que o contexto das interações face-a-face e as RSOs exigem comportamentos distintos, e que elas levam em consideração o quão pessoal julgam ser uma informação, ao decidirem sobre como irão compartilhá-la nesses diferentes contextos.

De posse do conhecimento prático obtido a partir dos estudos empíricos que realizamos, fizemos um amplo levantamento da literatura sobre privacidade, abrangendo teorias de privacidade em geral, abordagens teóricas de privacidade no contexto de

sistemas de informação e estudos empíricos de privacidade em RSOs. Buscamos, com esse levantamento, investigar elementos presentes nesses estudos que poderiam ser considerados no compartilhamento de informações pessoais em RSOs, ao impactarem, de alguma forma, a privacidade dos seus usuários.

A fim de tratar privacidade em RSOs sob a perspectiva da Engenharia Semiótica, utilizamos o seu espaço de design para organizar o compartilhamento de informações pessoais nesses sistemas, como será explicado no Capítulo 4. Incorporamos ou adaptamos ao mesmo diferentes elementos, provenientes de teorias gerais de privacidade [Altman, 1975; DeCew, 1997; Westin, 2003; Nissenbaum, 2004; Solove, 2008; Petronio, 2002], de abordagens teóricas que consideram privacidade no contexto de sistemas de informação [Palen & Dourish, 2003; Boyle & Greenberg, 2005] e de estudos empíricos sobre privacidade em RSOs [Villela et al., 2015a; Emanuel et al., 2013; Hoadley et al., 2010].

Dessa forma, foi definido o espaço de design do compartilhamento de informações pessoais em RSOs para o qual a Engenharia Semiótica pode contribuir. Ao conceituar IHC como um fenômeno de metacomunicação designer–usuário, como será visto no Capítulo 2, a Engenharia Semiótica nos oferece a oportunidade de estudar, entre outros tópicos de interesse, o **conteúdo** relacionado ao compartilhamento de informações pessoais em RSOs que impacta a privacidade dos seus usuários e que deverá ser comunicado pelo designer através de sua interface. Em particular, com esta teoria podemos estudar como designers podem oferecer oportunidades para os usuários alcançarem seus estados desejados de privacidade dentro do sistema, levando-nos à seguinte questão de pesquisa:

Quais são os elementos de privacidade a serem considerados no projeto de metacomunicação do compartilhamento de informações pessoais em RSOs, e como eles deverão ser tratados, no sentido de permitir que os usuários alcancem estados desejados de privacidade?

Esta questão de pesquisa foi enquadrada dentro de uma área específica de interesse, que é o processo de design de IHC de RSOs, considerando a privacidade relacionada ao compartilhamento de informações pessoais.

Os resultados teóricos e empíricos obtidos a partir da primeira etapa de nossa pesquisa nos levou a propor o Modelo de Design de Privacidade (MDP), que consiste em um modelo descritivo para guiar o design (ou crítica) do compartilhamento de informações pessoais em RSOs, considerando o seu impacto na privacidade de seus usuários [Villela & Prates, 2015b].

Na segunda etapa da pesquisa, nós realizamos a avaliação da expressividade do MDP, ao analisar a sua capacidade de expressar decisões de privacidade em RSOs

e verificar se ele é descritivo o suficiente para representar diferenças em modelos de privacidade de RSOs com diferentes propósitos [Villela & Prates, 2016]. Assim, conduzimos uma avaliação qualitativa analítica em dois passos. O primeiro passo consistiu em realizarmos a análise de três diferentes RSOs, fazendo as modelagens reversas de sua privacidade de acordo com as dimensões do MDP. Tal avaliação foi chamada de "avaliação com especialista" tendo em vista que foi realizada pela autora desta tese, considerada especialista no MDP, com os resultados obtidos tendo sido discutidos com a sua orientadora nesta pesquisa. Feito isso, o segundo passo consistiu da "avaliação com potenciais usuários", quando avaliamos o uso do MDP por designers de sistemas, que representam os seus potenciais usuários. Com essa avaliação da expressividade do MDP, demos o primeiro passo no sentido de mostrar que o mesmo alcança o seu propósito de apoiar designers na reflexão sobre níveis de privacidade a serem oferecidos aos usuários de RSOs, relacionados ao compartilhamento de informações pessoais nesses sistemas.

1.3 Contribuições

Esta tese apresenta contribuições para a área de IHC em geral e para a teoria da Engenharia Semiótica, no sentido de produzir novo conhecimento e novas questões de pesquisa.

Em relação à área de IHC, esta tese contribui com a proposição do MDP, que consiste em uma ferramenta conceitual de design. Tal ferramenta pode ser utilizada por designers de RSOs, ao projetarem o compartilhamento de informações pessoais nesses sistemas, considerando o seu impacto na privacidade dos seus usuários.

Os resultados nos nossos estudos de caso mostram o valor epistêmico do MDP como ferramenta de análise, tendo em vista a sua capacidade de caracterizar RSOs sob o ponto de vista de privacidade, além de despertar reflexões sobre aspectos de privacidade relacionados ao compartilhamento de informações pessoais nesses sistemas. Podemos dizer também que o MDP ajuda os profissionais de IHC a explorarem o espaço de design relacionado ao compartilhamento de informações em RSOs, independente do seu nível de conhecimento de Engenharia Semiótica.

Em tempo de design, o MDP pode ajudar designers a projetarem RSOs refletindo sobre os estados de privacidade que podem ser atingidos pelos seus usuários, de acordo com o contexto. Em tempo de avaliação, tal modelo guia avaliadores de IHC a analisarem de modo sistemático e avaliarem a forma como o sistema trata níveis de privacidade no compartilhamento de informações pessoais de seus usuários.

Finalmente, para a teoria da Engenharia Semiótica, esta tese contribui ao expandir o conjunto de questões que a mesma pode tratar. Apesar desta teoria já apresentar uma ferramenta epistêmica para a modelagem da comunicação entre usuários em SiCo's - a Manas, com o MDP nós focamos na comunicação que caracteriza o compartilhamento de informações pessoais e no seu impacto na privacidade.

1.4 Estrutura da Tese

O restante desta tese está organizado conforme descrito a seguir. O Capítulo 2 apresenta os fundamentos teóricos que caracterizam o fenômeno de interesse desta tese. O Capítulo 3 apresenta os estudos iniciais sobre privacidade que realizamos e serviram de base para o Modelo de Design de Privacidade, que é apresentado no Capítulo 4. O Capítulo 5 mostra a avaliação que realizamos da expressividade do MDP. No Capítulo 6 é apresentada nossa discussão sobre os resultados que obtivemos com a pesquisa e, finalmente, no Capítulo 7, são apresentadas nossas conclusões e delineamentos de trabalhos futuros.

Capítulo 2

Fundamentação Teórica

O Modelo de Design de Privacidade (MDP) foi elaborado usando como base teorias gerais de privacidade [Altman, 1975; Nissenbaum, 2004; Petronio, 2002; Solove, 2008; Westin, 2003], a teoria da Engenharia Semiótica [de Souza, 2005] e estudos empíricos comparativos sobre privacidade no contexto online e off-line [Villela et al., 2015a,c]. Neste capítulo, falaremos sobre as teorias de privacidade nas quais nos baseamos e a Engenharia Semiótica. Os estudos empíricos serão descritos no Capítulo 3. Iniciaremos nossa fundamentação téorica apresentando, na seção 2.1, as teorias de privacidade nas quais nos baseamos para derivar os aspectos de privacidade a serem considerados no compartilhamento de informações pessoais em nosso modelo, usando como ponto de partida a teoria de regulação de privacidade de Altman [1975]. Tal teoria tem exercido importante influência na forma como pesquisadores na área de interação humano-computador consideram privacidade no contexto dos sistemas de informação, como usado, por exemplo, por Palen & Dourish [2003]. Em seguida, na seção 2.2, apresentaremos os conceitos da Engenharia Semiótica utilizados na elaboração do MDP, concentrando-se no modo como tal teoria estrutura o espaço de design de IHC, e suas ferramentas para modelagem da interação usuário-sistema em SiCo's, que é o contexto da pesquisa apresentada nesta tese.

2.1 Teoria de Privacidade

Em nosso estudo, consideramos privacidade em função do compartilhamento de informação em RSOs, feito pelo próprio indivíduo ao qual a informação se refere e também por outras pessoas[boyd, 2007]. Assim, a privacidade está relacionada a restringir fluxos de informação sobre um indivíduo para outros usuários em RSOs, considerando o alcance do compartilhamento de informação pessoal dentro desses sistemas.

Para elaborarmos o MDP, nos baseamos primariamente na teoria de regulação de privacidade de Altman [1975], que definiu privacidade como *"um controle seletivo de acesso ao indivíduo"* (p.18). Nesse sentido, privacidade não é estática, mas um processo dialético e dinâmico de regulação de limites, em que as pessoas aumentam ou diminuem seus limites de acesso, de acordo com o contexto. O termo "dialético" na definição de privacidade de Altman se refere à abertura ou ao fechamento do indivíduo a outras pessoas, no sentido de buscar ou evitar interação social. O termo "dinâmico", por sua vez, indica que o nível desejado de privacidade (ou seja, o nível ideal de contato em um momento específico), que varia de acordo com diferenças individuais e culturais, move-se ao longo de um contínuo de abertura e fechamento, em resposta a diferentes circunstâncias. Isso significa que as pessoas modificam e continuamente reavaliam seus limites de acesso em resposta ao ambiente e às suas próprias necessidades de interação social.

Essa definição de privacidade de Altman afasta-se da noção tradicional de privacidade em que a interação do indivíduo com outras pessoas é evitada [Westin, 1967]. Ao contrário, de acordo com Altman, o indivíduo ter mais privacidade não necessariamente é melhor, tendo em vista que a necessidade de privacidade das pessoas pode mudar, dependendo da situação pela qual estão passando.

Dessa forma, raciocinando sobre a definição de Altman, identificamos três características de privacidade que consideramos no MDP: *controle*, *estado de privacidade* e *contexto*. Como veremos a seguir, o *controle* está relacionado ao processo de regulação de limites de acesso do indivíduo, o *estado de privacidade* é visto como resultado do aumento ou diminuição desses limites de acesso, e o *contexto* está relacionado ao dinamismo no qual esses limites são modificados.

O controle de privacidade O controle do fluxo de informação sobre o indivíduo para outras pessoas está associado ao processo de regulação de limites de acesso, na definição de privacidade de Altman. Outros teóricos, como DeCew [1997] e Westin [2003], também consideram o controle sobre quais informações pessoais estão sendo coletadas, além de como e com quem elas são compartilhadas, como sendo central no sentido de manter a privacidade do indivíduo. No mundo físico, este tipo de controle é normalmente óbvio, uma vez que nós sabemos com quem estamos conversando e quem está tendo acesso à nossa informação. Entretanto, controlar esses limites de acesso e o fluxo de informação entre pessoas em uma RSO pode ser mais complexo, devido a características específicas desses sistemas.

Embora possa acontecer no mundo físico, em RSOs aumenta a possibilidade da privacidade do indivíduo ser comprometida, uma vez que informações sobre ele podem

ser compartilhadas por outros usuários, ou até mesmo pelo próprio sistema, sem o seu conhecimento ou consentimento. Além disso, até mesmo quando a informação é compartilhada voluntariamente pelo indivíduo, problemas de privacidade podem surgir, caso o mesmo não seja capaz de controlar efetivamente a audiência da informação ou o uso que pode ser feito dela[Joinson & Paine, 2007].

O MDP permite que o designer decida sobre o quanto de controle deve ser concedido aos usuários no sentido de definir aspectos específicos do compartilhamento de suas informações pessoais, como, por exemplo, quem pode compartilhá-las e qual será a sua audiência. Essa decisão ocorre no sentido de determinar qual será a parcela de contribuição do sistema e qual será a parcela de contribuição dos usuários na configuração de sua privacidade.

O estado de privacidade O estado de privacidade, relacionado à teoria de Altman, é obtido como resultado da possibilidade do indivíduo aumentar ou diminuir os seus limites de acesso, no sentido de alcançar o seu estado desejado de privacidade. Conforme já mencionado, essa noção de estado de privacidade é diferente da ideia de privacidade introduzida por [Westin, 1967, p.7], definida como uma "retirada voluntária e temporária da sociedade, por parte da pessoa", através da qual a mesma pode atingir um *estado* de anonimato, solidão, reserva ou intimidade.

De acordo com Altman, o objetivo da regulação de privacidade permitir que o indivíduo alcance o seu estado desejado de privacidade, ao longo de um espectro que varia desde uma total abertura até um total fechamento a outras pessoas. A implicação disso é que deve existir um contínuo de estados de privacidade que podem ser alcançados pelo indivíduo, variando desde o estado de privacidade mínimo, onde todas as suas informações estão acessíveis para uma ampla audiência, até o estado de privacidade total, onde nenhuma informação é compartilhada.

Essa perspectiva de estado de privacidade vem ao encontro da abordagem utilizada no MDP, considerando que as RSOs podem permitir que seus usuários atinjam diferentes estados de privacidade, dependendo de diferentes elementos envolvidos no compartilhamento de suas informações. Esses elementos estão relacionados a quem compartilha, o que é compartilhado e para quem, em que local e por quanto tempo a informação fica disponível, além dos efeitos gerados por tal compartilhamento.

A natureza contextual de privacidade A natureza contextual de privacidade está relacionada ao dinamismo com o qual as pessoas movem os seus limites de acesso [Altman, 1975]. Assim, privacidade não tem um significado universal, que é válido em

todos os contextos, ou seja, não existem normas universais de privacidade, sendo as mesmas distintas para cada situação ou contexto [Nissenbaum, 2004; Solove, 2008].

Nós associamos o dinamismo relacionado aos limites de acesso das pessoas, colocado na teoria de privacidade de Altman, com a teoria de integridade contextual de Nissenbaum [2004], que considera que esses limites são regidos por um conjunto de normas relacionadas à adequação social e ao fluxo de informação, que dependem do contexto. A norma de *adequação social* determina que tipo de informação pessoal é apropriado compartilhar em determinada circunstância, considerando que cada ambiente social determina que tipo de informação se espera que seja compartilhado, distinguindo entre diferentes relacionamentos e papeis sociais. Normas de *fluxo de informação*, por sua vez, ajudam a definir relacionamentos pela quantidade de informação que é compartilhada entre as pessoas, ou seja, pessoas compartilham informações mais íntimas com amigos mais íntimos e informação mais geral com conhecidos, com os quais não possuem intimidade. De acordo com essa teoria, as regras que governam tais normas mudam com o tempo, ou seja, o que era apropriado compartilhar em um dado momento pode não mais ser considerado apropriado em outro momento posterior. Isso é exemplificado pelas mudanças no comportamento das pessoas no que tange à forma como compartilham suas informações pessoais, causadas por experiências prévias positivas ou negativas em relação a esse aspecto.

O MDP considera o contexto como sendo o "pano–de–fundo" que irá guiar as decisões do designer, no sentido de definir aspectos específicos relacionados a como deverá ocorrer o compartilhamento de informações pessoais dentro do sistema, a fim de permitir que seus usuários alcancem os seus estados desejados de privacidade.

Privacidade como Comunicação A perspectiva de privacidade de Altman caracteriza elementos importantes de privacidade, conforme discutimos anteriormente, porém não considera explicitamente as interações interpessoais subjacentes ao compartilhamento de informações, que estão presentes nos contextos mediados. Nesse sentido, Petronio [2002] estendeu a teoria de Altman, ao apresentar a sua teoria chamada "Gerenciamento da Privacidade da Comunicação"[1]. Tal teoria considera privacidade como consequência de um processo de negociação entre pessoas, tendo em vista que seus limites de privacidade são regulados por ambas as partes que estão se comunicando durante o compartilhamento de informação.

Assim, a teoria de Petronio aborda a perspectiva de privacidade como comunicação, inserindo o elemento "colaboração" no processo de regulação de limites. Tal teoria

[1]tradução do nome original em inglês "Communication Privacy Management" (CPM)

considera que ambos, o emissor e o receptor, são mutuamente responsáveis pela informação compartilhada, no sentido de que o receptor, a partir do momento em que tem acesso à informação compartilhada pelo emissor, adquire também a responsabilidade sobre a sua privacidade. De acordo com Petronio [2002], isso explica o porquê das pessoas fazerem certas decisões sobre se compartilham ou não informações que consideram privadas.

Essa perspectiva de privacidade como comunicação, que considera o emissor e o receptor da comunicação referente ao compartilhamento de informação pessoal como corresponsáveis pela privacidade do indivíduo ao qual a informação se refere, vai ao encontro da perspectiva que usamos na definição da estrutura do MDP. No entanto, além de considerar as partes envolvidas no compartilhamento de informação, o MDP, ao configurar tal compartilhamento como uma comunicação, considera outros elementos presentes da mesma, conforme veremos na Seção 2.2, e que também impactam o estado de privacidade que pode ser alcançado pelo indivíduo nas RSOs.

2.2 Engenharia Semiótica

A Engenharia Semiótica [de Souza, 2005] consiste em uma teoria explicativa, da área de Interação Humano-Computador (IHC), que caracteriza a interação humano-computador como um processo de comunicação humana mediada pelo computador, em que designers, através das interfaces dos sistemas, estão indiretamente dizendo aos usuários a quem o sistema se destina, que problemas ele é capaz de resolver e como interagir com ele para resolvê-los. Assim, à medida que o usuário interage com o sistema, ele vai entendendo a mensagem transmitida pelo designer, o que faz com que a interface de um sistema seja considerada um artefato de metacomunicação, uma vez que a comunicação designer-usuário ocorre através da comunicação usuário-sistema.

A Engenharia Semiótica conta com uma ontologia que reflete o modo como ela caracteriza a interação humano-computador e estrutura o seu espaço de design. Tal ontologia contém os elementos necessários para fornecer uma explicação para os fenômenos envolvidos no projeto, uso e avaliação de sistemas computacionais interativos. Esses elementos estão distribuídos em quatro categorias gerais: *processos de significação*, *processos de comunicação*, *interlocutores* envolvidos nesses processos e *espaço de design* [de Souza, 2005].

Os processos de *significação* e de *comunicação* são provenientes da teoria semiótica de Eco [1976, 1986], na qual a Engenharia Semiótica se baseia, a fim de caracterizar a interação humano-computador como processo comunicativo entre designers

e usuários, conforme mencionado anteriormente. De acordo com essa teoria de Eco, *significação* é o processo pelo qual conteúdos são sistematicamente associados a expressões, de acordo com convenções sociais e culturais, resultando na criação de um sistema de signos, sendo um signo qualquer coisa que significa algo para alguém [Peirce, 1998]. *Comunicação*, por outro lado, é o processo pelo qual indivíduos usam sistemas de significação e outros códigos para alcançarem diferentes propósitos. A partir dessa teoria, tem-se que os elementos fundamentais da comunicação são: a *intenção*, que diz respeito a o que se deseja alcançar com a comunicação, o *conteúdo*, que consiste na informação transmitida durante a comunicação, e a *expressão*, que diz respeito às formas e aos meios pelos quais a comunicação ocorre.

Assim, de acordo com a Engenharia Semiótica, a interface de um sistema significa (ou expressa) a *intenção* de design através de um conjunto finito de elementos e estruturas associados aos estados e comportamento do sistema. Isto forma um sistema de significação propositadamente projetado, em que certos tipos de signos são associados a certos tipos de conteúdo, no sentido de apoiar a comunicação das intenções de design. Nesse processo de comunicação, usuários acessam a informação (*conteúdo*) que os sistemas interativos transmitem através de signos (*expressão*) disponíveis na interface. Dessa forma, além dos elementos *intenção*, *conteúdo* e *expressão*, os dois níveis de comunicação envolvidos na interação humano-computador - a *metacomunicação designer-usuário* e a *comunicação usuário-sistema* - também compõem a categoria *processos de comunicação*.

A categoria *interlocutores* é composta pelos três agentes envolvidos no processo de comunicação que caracteriza a interação humano-computador: *designers*, *usuários* e *sistema*. Conforme falado no início desta seção, esses elementos se fazem presentes em tempo de interação, através da metacomunicação. Como a interface representa o designer em tempo de interação, o sistema é considerado o *preposto do designer* no processo de comunicação. A mensagem do designer para o usuário, transmitida através da interface, é conhecida como metamensagem e pode ser parafraseada da seguinte forma:

"Eis aqui a minha compreensão de quem você é, do que eu aprendi sobre o que você quer ou necessita fazer. Este é o sistema que eu projetei consequentemente para você, e esta é a maneira que você pode ou deve usá-lo, a fim de cumprir um conjunto de objetivos que cabem dentro dessa visão." [de Souza, 2005, p.84] (tradução do autor)

Especialmente no contexto de SiCo's, ao qual se aplica o modelo apresentado nesta tese, vale salientar que essa metamensagem se destina não apenas a um único usuário, mas para todo o grupo que utilizará o sistema para interagir entre si. Neste caso, tal metamensagem também transmite aos usuários as decisões do designer em

relação a quem (emissor) pode falar com quem (receptor), sobre o quê, e usando que códigos e meios. Nesse sentido, o compartilhamento de informações pessoais em RSOs, que é o foco da nossa pesquisa sobre privacidade, é visto como um caso de comunicação entre usuários mediada pelo sistema.

A Engenharia Semiótica estrutura o *espaço de design* de IHC através do modelo de comunicação de Jakobson [1960]. Neste modelo, como pode ser visto na Figura 2.1, seis elementos estruturam o espaço de comunicação: *emissor*, *receptor*, *mensagem*, *código*, *canal* e *contexto*. O espaço de design da Engenharia Semiótica expressa os elementos do modelo de Jakobson da seguinte forma: o designer é o emissor da metamensagem, o usuário é o receptor, o computador é o canal, a mensagem é a interface do sistema, mensagens são codificadas em códigos computacionais, e o contexto representa onde a comunicação ocorre. A Figura 2.2 ilustra a caracterização do espaço de design da Engenharia Semiótica.

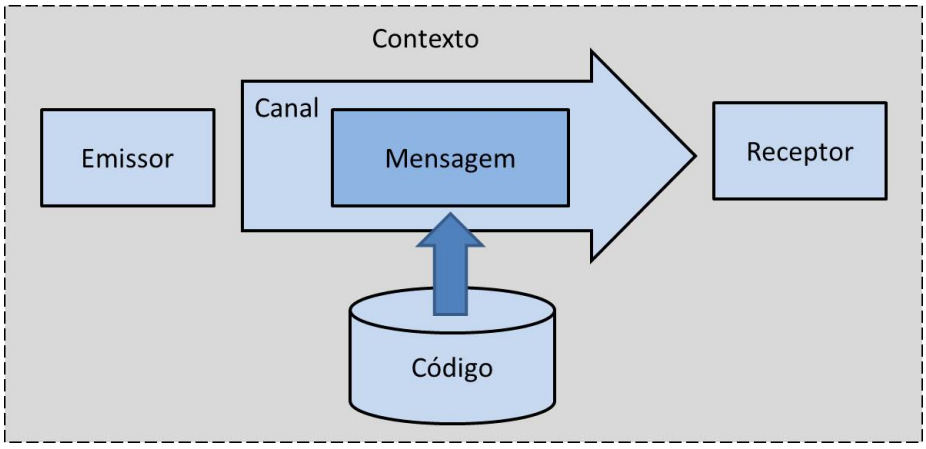


Figura 2.1. Modelo de Comunicação de Jakobson

Designers devem tomar decisões sobre cada um desses aspectos do espaço de design da Engenharia Semiótica, durante a construção de seu discurso, ou seja, durante o processo de design. Assim, é importante que eles reflitam sobre esses elementos, uma vez que tal reflexão os leva a se aprofundarem e compreenderem melhor as possíveis implicações de suas decisões de design [de Souza, 2005].

Para apoiar os designers em suas reflexões durante a atividade de design, a Engenharia Semiótica propõe que lhes sejam oferecidas *ferramentas epistêmicas*. Essas ferramentas são utilizadas pelo designer, não para obter respostas diretas para um problema, mas para aumentar a sua compreensão sobre o problema em si e suas implicações [de Souza, 2005], bem como elaborar suas próprias respostas e soluções. Assim, essas ferramentas ampliam o conhecimento do designer, o que leva ao potencial aperfeiçoa-

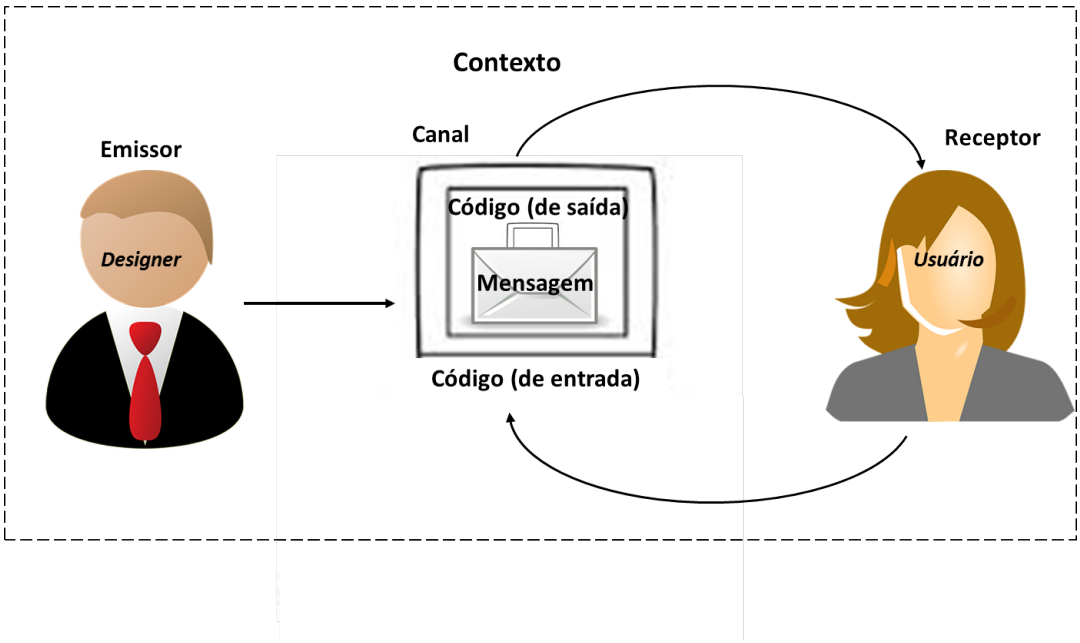


Figura 2.2. Espaço de design da Engenharia Semiótica

mento do processo de tomada de decisões inerente à atividade de design, possibilitando a melhoria da qualidade dos produtos desenvolvidos.

Engenharia Semiótica oferece aos designers algumas ferramentas epistêmicas voltadas especificamente para o design de SiCo's, que serão mostradas a seguir.

2.2.1 Modelos da Engenharia Semiótica para o Design de Sistemas Colaborativos

A Engenharia Semiótica oferece a designers ferramentas epistêmicas que consistem em linguagem e modelos conceituais para o design de SiCo's, a saber: a MoLIC (Modeling Language for Interaction as Conversation)[Barbosa & de Paula, 2003; de Souza & Barbosa, 2014, 2015] e os modelos MetaCom-G* e Marq-G* [Prates, 1998; Barbosa, 2002] e a Manas [Barbosa, 2006].

A MoLIC [Barbosa & de Paula, 2003; Silva, 2005] é uma linguagem de modelagem da interação dos usuários com o sistema, que segue a metáfora que caracteriza a interação usuário-sistema como uma conversa entre essas partes. A MoLIC permite ao designer definir e representar detalhadamente todas as possíveis conversas que os usuários podem ou devem ter com o sistema para alcançar seus objetivos. A sua extensão para considerar a modelagam de SiCo's se propõe a permitir a caracterização da comunicação entre diferentes usuários [Silva, 2005], e vem sendo aperfeiçoada, no sentido de permitir uma representação eficaz das interações dos usuários com o sistema

e também entre usuários, no design de SiCo's [de Souza & Barbosa, 2014, 2015].

O MetaCom-G* [Prates, 1998], o Marq-G* [Barbosa, 2002] e a Manas [Barbosa, 2006] consistem em modelos de apoio ao design de SiCo's, que oferecem ao designer uma forma de descrever a sua mensagem que será transmitida aos usuários através da interface. Além disso, esses modelos também geram indicadores qualitativos de potenciais problemas que podem ocorrer a partir desta descrição, auxiliandoo designer a tomar decisões de design mais conscientes. O MetaCom-G* tem o seu foco no trabalho colaborativo de um grupo, permitindo que o designer planeje a colaboração e a comunicação de grupos de usuários reunidos em um sistema para executarem uma determinada tarefa. O Marq-G* [Barbosa, 2002] é fundamentado no MetaCom-G*, e permite que o designer represente sua interpretação sobre a maneira como um grupo de usuários se organiza para executar atividades no sistema. Já a Manas tem como foco o processo de comunicação entre usuários dentro de um SiCo, e seu objetivo é permitir que designers modelem como se dará tal comunicação. Assim, com base na modelagem da comunicação, a Manas é capaz de apontar problemas de sociabilidade que podem acontecer durante a comunicação interpessoal que ocorre através do sistema, incluindo alguns problemas de privacidade.

Essas três ferramentas consistem em modelos que permitem que o designer reflita sobre suas decisões de projeto, além de o permitirem descrever alguns aspectos do sistema a ser projetado, fazendo uso de uma linguagem de design. Com base nessa descrição do sistema, esses modelos geram indicadores qualitativos de potenciais problemas que podem ocorrer, ampliando o conhecimento do designer sobre as potenciais inconsistências de sua representação, e de possíveis consequências de suas decisões de design nas atividades que são apoiadas pelo sistema. As linguagens de design oferecidas por esses modelos são separáveis de contexto, ou seja, definem características básicas do sistema, e não levam em consideração o contexto no qual o mesmo está sendo desenvolvido, ficando a cargo do designer fazer tais considerações. Outras características dessas linguagens de design é que elas são descritivas, no sentido de que chamam a atenção do designer para possíveis situações problemáticas, mas cabe a ele decidir, considerando o contexto, se tais situações realmente representam problemas ou não.

Assim como esses modelos, o MDP também tem o propósito de ser uma ferramenta epistêmica para levar o designer a refletir sobre suas decisões de projeto. No entanto, diferente do modelos anteriores, o MDP explora especificamente as dimensões relacionadas à privacidade na comunicação que é caracterizada a partir do compartilhamento de informações pessoais em RSOs. Como será visto no Capítulo 4, os elementos da ontologia da Engenharia Semiótica pertencentes à categoria *espaço de design* são a base utilizada pelo MDP para a estruturação do espaço de compartilhamento de

informações pessoais em RSOs.

Na verdade, a Manas pode modelar não apenas a comunicação direta, mas indireta também. Se um user faz uma tarefa que requer que outro faça outra no sistema isso pode ser modelado como uma comunicação. Talvez dizer que o MDP explora especificamente as dimensões relacionadas a privacidade (ou algo nesta direção).

Capítulo 3

Estudos Iniciais Sobre Privacidade

Os estudos exploratórios realizados nos estágios iniciais da nossa pesquisa nos permitiram identificar aspectos importantes relacionados à privacidade no compartilhamento de informações em RSOs. Tais estudos ocorreram inicialmente na forma de estudos empíricos, através da condução de entrevistas e aplicação de questionários, a partir dos quais obtivemos resultados qualitativos e quantitativos que forneceram indicadores dque fundamentaram algumas de nossas decisões sobre o MDP. Em seguida, realizamos um levatamento da literatura sobre privacidade, abrangendo teorias de privacidade em geral, abordagens teóricas de privacidade em sistemas de informação, e estudos empíricos de privacidade em RSOs. Buscamos, com esse levantamento, investigar elementos presentes nesses estudos que poderiam ser considerados no compartilhamento de informações pessoais em RSOs, como aspectos que impactam a privacidade dos seus usuários. Os resultados desses estudos são apresentados nas seções 3.1 e 3.2, respectivamente.

3.1 Estudos Empíricos sobre Privacidade em RSOs

Os estudos exploratórios empíricos foram conduzidos no início de nossa pesquisa com a finalidade de contribuir para melhorar a nossa compreensão sobre os valores, comportamentos e percepções dos usuários de RSOs, no que tange à privacidade relacionada ao compartilhamento de informação pessoal nesses ambientes. A partir do contraste entre a forma como tal compartilhamento ocorre tanto nesses sistemas quanto no mundo físico, das interações face-a-face [Xavier et al., 2014; Villela et al., 2015d,a,c], obtivemos uma visão mais ampliada da questão e pudemos perceber como as RSOs acarretaram mudanças na forma como as pessoas entendem o conceito de privacidade. Apresentaremos os principais resultados qualitativos e quantitivos desses estudos, que

fundamentaram algumas de nossas decisões sobre o MDP, nas subseções 3.1.1 e 3.1.2, respectivamente.

3.1.1 Entrevistas

Iniciamos o nosso estudo exploratório buscando descobrir opiniões, atitudes e conflitos que as pessoas possuem em relação à privacidade em RSOs. A fim de proceder a coleta dos dados para a pesquisa, foram realizadas entrevistas presenciais e semiestruturadas, contrastando privacidade online e off-line. Os pré-requisitos para participar da pesquisa eram ser usuário do Facebook e ser aluno ou professor da Universidade Federal de Minas Gerais. Esta última exigência foi estabelecida como uma forma de tentar amenizar as diferenças entre os participantes e os fatores externos que influenciem as respostas. O pré-requisito de ser usuário do Facebook foi exigido não só para homogeneizar o perfil, mas também para possibilitar a realização de perguntas mais específicas sobre a experiência com redes sociais durante as entrevistas.

Além da definição dos requisitos citados acima, foram definidos quatro perfis de entrevistados, que se diferenciavam em relação à área de atuação e faixa etária. Em relação à área de atuação, diferenciamos pessoas que estudavam ou atuavam na área de tecnologia da informação (TI) das que atuavam em outras áreas, pois, por possuírem maior conhecimento no que concerne à tecnologia, as pessoas da área de TI poderiam ter uma percepção diferente sobre privacidade online [Hargittai et al., 2010]. Em relação à faixa etária, diferenciamos pessoas entre 18 e 35 anos e aquelas acima de 35 anos, tendo em vista que a idade também pode influenciar a percepção e as atitudes das pessoas do que concerne à privacidade [Kisilevich et al., 2011]. Assim, foram selecionados 20 participantes, com cinco deles se encaixando em cada um dos seguintes grupos: pessoas que não são da área de TI com menos de 35 anos; pessoas da área de TI com menos de 35 anos; pessoas da área de TI com mais de 35 anos; e pessoas que não são de TI com mais de 35 anos.

O roteiro da entrevista abordava 23 perguntas abertas, divididas em quatro blocos temáticos, que tratavam diversas questões relativas a privacidade, conforme mostrado no Apêndice A. O primeiro bloco trazia perguntas sobre o que se entende por privacidade, o quanto a pessoa se preocupa e como compartilha suas informações no mundo físico. No segundo havia perguntas que exploravam se o participante considerava a privacidade no mundo físico diferente da que existe no mundo virtual. O terceiro bloco tinha como objetivo obter informações sobre a experiência em RSOs e como o respondente lidava com sua privacidade nesse ambiente. Assim, esse bloco possuía perguntas sobre o uso de recursos de gerenciamento de privacidade e com quem ele compartilha

suas informações no Facebook. Por fim, o último bloco tinha perguntas associadas à privacidade na sociedade, como sua opinião sobre a privacidade ser um direito essencial e se acredita que pode acontecer das pessoas se exporem em excesso de forma involuntária.

A partir da análise dos discursos dos participantes em resposta às questões da entrevista, realizada a partir da aplicação do Método de Explicitação do Discurso Subjacente (MEDS) [Nicolaci-da Costa et al., 2004], identificamos as seguintes categorias [Xavier et al., 2014; Villela et al., 2015d]: (1) as informações mais pessoais são as diretamente associadas à segurança, relações e sentimentos; (2) as informações consideradas muito privativas podem não estar nas RSOs; (3) os níveis de compartilhamento off-line não se refletem online; (4) as RSOs e a internet, de uma forma geral, acarretaram mudanças em relação à forma como as pessoas lidam com privacidade; (5) o gerenciamento da privacidade online é mais difícil; (6) exposição fora de controle nas RSOs; e (7) hiperexposição das pessoas nas RSO. Dentre essas categorias de análise, algumas nos despertaram reflexões durante a elaboração do MDP, conforme detalharemos a seguir.

Primeiramente, identificamos que as pessoas não refletem nas RSOs a forma como compartilham suas informações no mundo físico. No mundo físico, os participantes possuem diferentes níveis de compartilhamento, caracterizados por compartilharem diferentes tipos de informação com diferentes pessoas, de acordo com o seu grau de confiança nas mesmas. Entretanto, de uma forma geral, esses níveis de compartilhamento não são refletidos nas RSOs. Assim, dependendo do quão pessoal consideram ser a informação, as pessoas optam por uma entre duas estratégias para o seu compartilhamento nesses sistemas: (a) na primeira, todos os grupos (amigos, ou mesmo todos usuários do sistema) são tratados como menos confiáveis e informação não é compartilhada na rede; (b) na segunda estratégia, pessoas pertecentes a diferentes níveis de confiança do indivíduo são tratadas como se pertencessem ao seu nível maior confiança, e a informação é postada para todos os grupos, sem distinções. Em ambos os casos, as pessoas possuem comportamentos diferentes ao compartilharem suas informações nas RSOs, do que possuem no mundo físico, o que nos faz concluir que nenhuma dessas duas estratégias é ideal. Na primeira, pode ocorrer uma perda de oportunidades de interação, uma vez que o usuário deixa de interagir para não ter que restringir corretamente o acesso às suas informações por parte de outros usuários do sistema. A segunda estratégia, por outro lado, remete a uma exposição maior do indivíduo na RSO, uma vez que informações são compartilhadas com um determinado conjunto de pessoas, com as quais ele não compartilharia no mundo físico. Dessa forma, tais estratégias indicam que as decisões feitas pelos designers do Facebook têm influenciado o comportamento

de seus usuários, levando-os a agir muitas vezes de forma diferente da habitual ou desejada. Isso fica mais evidente a partir do relato dos participantes, que expuseram como um dos motivos associados à adoção dessas estratégias o fato de considerarem muito alto o **custo de configurarem adequadamente sua privacidade** em RSOs.

Os resultados das entrevistas também mostraram experiências negativas vivenciadas pelos participantes quanto à sua privacidade no Facebook, que nos apontaram elementos importantes que impactam a privacidade relacionada ao compartilhamento de informações pessoais em RSOs. Um dos problemas relatados consiste nos inconvenientes que são causados pelas **ações de terceiros sobre as informações pessoais** do participante. Isso diz respeito ao fato das pessoas não terem controle sobre o que outros usuários podem compartilhar sobre elas no sistema, como, por exemplo, quando postam fotos ou vídeos que as incluem, sem o seu consentimento.

Além disso, algumas das experiências negativas relatadas pelos participantes estão diretamente relacionadas a decisões de design da interface do Facebook, como a falta de controle sobre a exposição das suas informações pessoais que são compartilhadas no sistema. De acordo com os participantes, isso é ocasionado pelo **discurso que o sistema** faz sobre tal compartilhamento. Um exemplo desse discurso, apontado como causa de preocupações com privacidade, é o recurso "Novidades" do Facebook, que mostra aos usuários, em tempo real, as atividades de seus amigos no sistema. Conforme explicado na "Ajuda" sobre este recurso, os usuários vêem através do mesmo apenas informações às quais eles já possuem acesso de outra forma no sistema. Entretanto, neste caso, a informação é destacada em tempo real a outros usuários da rede, sem que estes necessitam de procurar explicitamente por ela. Além disso, ao usuário não é oferecida a oportunidade de restringir ou configurar o que ele deseja ou não que o sistema "fale" sobre ele com outros usuários.

3.1.2 Questionário

A partir dos resultados qualitativos obtidos com as entrevistas, e com o objetivo de obter um entendimento mais amplo sobre quão similares ou diferentes são as atitudes relacionadas à privacidade nas RSOs e no mundo físico, preparamos e aplicamos um questionário. Este questionário gerou resultados quantitativos que nos permitiram analisar e contrastar as atitudes das pessoas relacionadas ao compartilhamento de suas informações pessoais nesses dois contextos [Villela et al., 2015a,c]. Entender essas diferenças é importante no sentido de avaliar como as RSOs apoiam as necessidades de privacidade de seus usuários, bem como alteram a forma como eles interagem. Assim, o foco do nosso estudo, nesse caso, foi investigar, a partir dos dados coletados com o

questionário, as duas seguintes questões: (1) Quais informações as pessoas consideram como sendo pessoais e em que nível? e (2) Com quem elas se sentem confortáveis para compartilharem tais informações nas RSOs e no mundo físico?

A fim de verificar se a cultura exerce influência na forma como as pessoas classificam as informações em relação ao grau em que as consideram pessoais e na forma como as compartilham, tal questionário foi aplicado no Brasil e nos EUA. Assim como nas entrevistas, usamos o Facebook como o sistema representativo das RSOs, dado que era o mais popular em ambos os países na época da pesquisa[1], e continua sendo até os dias de hoje. O questionário foi projetado para coletar dados sobre perfil dos respondentes, sua experiência em RSOs, classificação da informação em relação ao grau em que é considerada pessoal e seu compartilhamento (online e off-line), bem como suas atitudes relacionadas à privacidade online e off-line. As versões em português e em inglês do questionário são mostradas no Apêndice A.

No Brasil, o questionário foi distribuído na UFMG, para a sua comunidade de professores, funcionários e alunos, e coletou 1038 respostas válidas, no período de abril a maio de 2014. Nos EUA, foi utilizado o *Mechanical Turk* para coletar respostas válidas de 581 participantes americanos, no período de março a abril de 2014. Neste caso, foram seguidas diretrizes de melhores práticas para utilização do *Mechanical Turk* descritas na literatura [Marshall & Shipman, 2013; Jakobsson, 2009; Downs et al., 2010].

A partir da análise dos dados coletados por meio da aplicação do questionário, identificamos que os participantes classificam diferentes tipos de informação em diferentes níveis, de acordo com o seu julgamento sobre quão pessoal estes sejam, e estes níveis parecem impactar seu desejo de compartilhar informação tanto no mundo físico quanto nas RSOs [Villela et al., 2015a]. Denominamos o nível em que uma informação pode ser classificada como sendo o seu *"nível de pessoalidade"*.

Esses níveis de pessoalidade das informações foram obtidos da seguinte forma: apresentamos aos participantes dezessete diferentes tipos de informação, escolhidos com base nas informações de perfil do Facebook e nos resultados que obtivemos com as entrevistas [Xavier et al., 2014; Villela et al., 2015d], e perguntamos quem eles consideravam ser as pessoas mais próximas com as quais eles compartilham suas informações pessoais e de que tipo são essas informações. Então, solicitamos aos participantes que classificassem esses tipos de informação de acordo com quão pessoal eles as consideravam, dentro de uma escala de 4 pontos, variando de "não pessoal" a "muito pessoal". Com base em como os participantes classificaram os tipos de informação, foram criados cinco grupos de informação, obtidos através do método *k-means* [MacQueen, 1967], que

[1]De acordo com http://www.alexa.com - acessado em fevereiro de 2014

coincidiram para os dados coletados com participantes americanos [Villela et al., 2015a] e brasileiros [Xavier, 2014], embora tenham apresentado algumas poucas diferenças nas informações dentro de cada grupo [Villela et al., 2015c]. A Figura 3.1 mostra a resposta média para cada tipo de informação e seu intervalo de confiança de 95%, para os dados coletados com participantes americanos[2]. A separação visual da média das categorias, representada pelas caixas nessa figura, coincide com a classificação de grupo obtida pelo método *k-means*.

Como ele está ordenado as informações aparecem listadas na ordem que aparecem no gráfico (da esquerda para a dirieta). Não é isso?

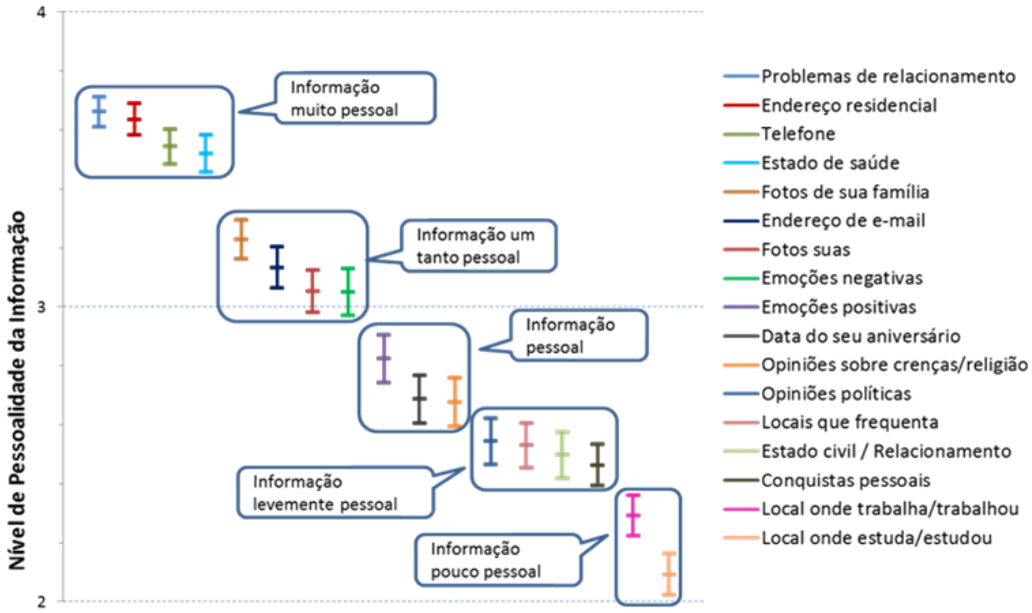


Figura 3.1. Nível de pessoalidade das informações, variando no eixo y de "não pessoal" (1) a "muito pessoal" (4) (a ordem em que as informações são listadas na legenda é a mesma em que aparecem no gráfico, da esquerda para a direita)

Como mostrado na Figura 3.1, podemos distinguir dois grupos de informação na parte superior do gráfico (entre os valores 3 e 4). Assim, nós denominamos o grupo que está no nível mais superior (cuja média está próxima do valor 4) como o grupo das "informações muito pessoais", composto pelos seguintes tipos de informação: *problemas de relacionamento*, *endereço residencial*, *telefone* e *estado de saúde*. O outro grupo localizado nessa parte do gráfico nós denominamos o grupo das "informações um

[2]Mostramos apenas os dados referentes à amostragem composta de participantes americanos, tendo em vista que os dados coletados com participantes brasileiros foram bastante semelhantes a estes, coincidindo os grupos de informações encontrados e ocorrendo apenas pequenas diferenças nas informações pertencentes a cada grupo.

tanto pessoais", composto por *fotos de família*, *endereço de e-mail*, *fotos suas* e *emoções negativas*.

Os demais grupos identificados estão localizados entre as médias de valores 2 e 3, e não estão tão claramente separados entre si, como no caso dos dois primeiros grupos. O terceiro grupo, mais próximo ao valor 3, foi denominado o grupo das "informações pessoais" e é composto por *emoções positivas*, *data de aniversário* e *opiniões sobre crenças/religião*. Denominanos o próximo grupo dentro dessa faixa como o grupo das "informações levemente pessoais", composta pelos seguintes tipos de informação: *opiniões políticas*, *locais frequentados*, *estado civil/relacionamento* e *conquistas pessoais*. Por fim, o último grupo (cuja média é mais próxima do valor 2) foi denominado o grupo das "informações pouco pessoais" e é composto por *local onde trabalha/trabalhou* e *local onde estuda/estudou*.

A partir do resultado inicial, mostrado em [Villela et al., 2015a], investigamos se o nível de pessoalidade de fato impacta a forma como as pessoas compartilham suas informações pessoais [Villela et al., 2015c]. Para isso, após identificar os diferentes níveis de pessoalidade associados a diferentes tipos de informação pelos participantes dos EUA e do Brasil, analisamos se tal diferença impactou as suas atitudes, no sentido de restringir ou compartilhar publicamente esses tipos de informação. Os resultados mostram que, para cada um dos grupos de participantes americanos e brasileiros, há uma correlação entre os níveis de pessoalidade associados a diferentes tipos de informação e as suas atitudes no sentido de compartilhá-los. Assim, quanto maior for o nível de pessoalidade da informação, maior é a possibilidade dos usuários não a compartilharem com ninguém. Por outro lado, quanto menor for o nível de pessoalidade da informação, maior é a possibildiade dos usuários a compartiharem publicamente.

Dentre outras contribuições, os resultados obtidos com o questionário, especificamente no que diz respeito aos níveis de pessoalidade identificados, mostram-se úteis para serem utilizados por designers de RSOs no apoio a suas decisões relacionadas a quais tipos de informação usuários deveriam poder compartilhar no sistema, além de decisões sobre configurações para permitir ou restringir o acesso a esses tipos de informação, ou estratégias para encorajar o compartilhamento dos mesmos. Isso nos levou a pensar no **nível de pessoalidade** como sendo um aspecto importante a ser considerado no MDP.

3.2 Levantamento da Literatura sobre Privacidade

O interesse de pesquisa em privacidade no contexto de RSOs começou em meados da década de 2000, quando o uso desses sistemas começou a disseminar em todo o mundo [Perrin, 2015]. A facilidade das interações e o favorecimento do compartilhamento de informações pessoais, proporcionados por esses sistemas, têm despertado crescente preocupação com privacidade, aumentando assim os desafios para a pesquisa de privacidade em IHC.

Nesse sentido, alguns pesquisadores se basearam em teorias bem estabelecidas sobre privacidade no contexto geral [Altman, 1975; Nissenbaum, 2004], para buscarem um melhor entendimento de privacidade no contexto dos sistemas de informação que permitem a interação social entre seus usuários [Palen & Dourish, 2003; Boyle & Greenberg, 2005; Barkhuus, 2012]. No entanto, a maior parte das pesquisas sobre privacidade nesses sistemas consiste em estudos empíricos e tem principalmente se dedicado à compreensão de diferentes aspectos relacionados à privacidade no compartilhamento de informação pessoal. Especificamente no que tange ao design de privacidade em RSOs, a maior parte das pesquisas está relacionada ao desenvolvimento de tecnologias que se propõem a tratar algum aspecto relacionado à privacidade na interface desses sistemas. Por outro lado, poucos estudos têm contribuído com modelos teóricos ou ferramentas conceituais para considerar privacidade no design de tecnologias online [Bélanger & Crossler, 2011].

Esta seção apresenta uma visão geral da literatura sobre o design de privacidade em RSOs, com foco em modelos teóricos e conceituais, que é o escopo da nossa pesquisa. A seguir, apresentamos as principais propostas de *frameworks* teóricos que consideram privacidade no contexto dos sistemas de informação com enfoque social, na subseção 3.2.1. Por fim, na subseção 3.3, estreitando o foco da revisão de literatura no sentido de se aproximar do foco da nossa pesquisa, apresentamos os modelos conceituais propostos para o tratamento de aspectos relacionados à privacidade no design de RSOs.

3.2.1 Artefatos Conceituais para o Design de Privacidade

Com base em teorias de privacidade, alguns estudos têm focado em fornecer um melhor entendimento sobre a relação entre privacidade e tecnologia. A motivação para esses estudos vem das questões de privacidade introduzidas pelo uso intensificado de sistemas de informação voltados para proporcionar interação social entre seus usuários. Nesse sentido, Palen & Dourish [2003] propõem um *framework* conceitual que enquadra privacidade dentro do contexto desses sistemas, apontando aspectos específicos a

serem considerados em análises de IHC. Esses autores dão destaque à disparidade que existe entre a tecnologia, que é essencialmente baseada em regras, e a privacidade, cujo gerenciamento por parte dos indivíduos ocorre normalmente de forma dinâmica em resposta a contextos ou situações específicas. Apoiando-se na teoria de Altman [1975], Palen & Dourish [2003] analisam o impacto da tecnologia no gerenciamento de privacidade, visto como um processo contínuo de gerenciamento de limites que se movem de forma dinâmica, de acordo com o contexto, ao invés de uma aplicação estática de regras. Esses limites refletem tensões entre objetivos essencialmente conflitantes, com a tecnologia da informação exercendo importante impacto tanto no sentido de rompê-los ou desestabilizá-los, quanto como uma forma de gerenciá-los. Palen & Dourish [2003] descrevem três limites que consideram centrais para a caracterização do gerenciamento de privacidade: *divulgação* ("disclosure boundary"), *identidade* ("identity boundary") e *temporalidade* ("temporality boundary").

De acordo com Palen & Dourish [2003], o *limite de divulgação* é definido como a tensão entre o privado e o público. Isso surge a partir da exigência de divulgação de informações pessoais para a participação no mundo social, o que faz com que o gerenciamento de privacidade não seja apenas uma questão de não divulgar uma informação privada, mas também de efetuar uma divulgação seletiva dessa informação. O *limite de identidade*, por sua vez, é definido como sendo o limite entre o "indivíduo" e os "outros". Nesse caso, considerando o contexto dos sistemas de informação, o papel mediador da tecnologia faz com que a interação entre pessoas ocorra através de suas representações no sistema. Assim, tendo em vista as falhas que podem ocorrer em tais representações, pode não ser possível compreender quem são as pessoas e como desejam ser percebidas, além de proporcionar uma diminuição do seu controle direto sobre a sua identidade construída dentro do sistema, proporcionando falhas relativas à privacidade. Por fim, o *limite da temporalidade* é visto como a tensão entre passado, presente e futuro. Nesse caso, a capacidade da tecnologia de tornar persistente a informação que é compartilhada pode trazer consequências indesejáveis na privacidade do indivíduo. De acordo com Palen & Dourish [2003], as tensões representadas por esses limites não são resolvidas de maneira independente, mas fazem parte de um único processo de gerenciamento de privacidade.

Outra abordagem teórica relevante que relaciona privacidade e tecnologia é o vocabulário desenvolvido por Boyle & Greenberg [2005]. Tal vocabulário também se baseia na teoria de privacidade de Altman e, com a finalidade de facilitar o entendimento da relação entre privacidade e design, fornece uma descrição de como indivíduos controlam a sua privacidade em sistemas de interação por vídeo. Em um alto nível de abstração, os autores descrevem o processo de gereneciamento de privacidade por meio

de controles de *solitude*, *autonomia* e *confidencialidade*.

Solitude refere-se à necessidade das pessoas controlarem seus níveis desejados de interação social. Nesse sentido, a tecnologia pode impactar a solitude, uma vez que dificulta o controle, por parte do indivíduo, sobre como se dará o interação que parte da iniciativa de outras pessoas. *Autonomia*, por sua vez, está relacionada ao entendimento de como a pessoa escolhe se apresentar quando estão sozinhas ou socialmente. Nesse caso, a tecnologia exerce um importante papel na autonomia do indivíduo, tendo em vista que pode exigir que o mesmo desempenhe diferentes e conflitantes papeis em suas interações mediadas pelo sistema. Por fim, *confidencialidade* está relacionada a compreender como um pessoa controla o acesso de outras pessoas à sua informação. Assim como no caso da *solitude*, a *confidencialidade* pode ser altamente impactada pela tecnologia, tendo em vista que, devido às características inerentes das aplicações que permitem a interação social entre seus usuários, a informação é facilmente disseminada e acessada nesses ambientes. Boyle & Greenberg [2005] relacionam essas três modalidades de controle como congruentes com os três limites mostrados no *framework* téorico de Palen & Dourish [2003] da seguinte forma: o *limite de divulgação* é regulado principalmente pelo controle de *confidencialidade*, mas também pelo controle de *solitude*; o *limite de identidade* é regulado pelo controle de *autonomia*; e o *limite de temporalidade* é regulado por normas e preferências que fazem parte dos controles de *solitude*, *confidencialidade* e *autonomia*.

Barkhuus [2012] apresenta uma reconsideração do conceito de privacidade relacionada ao compartilhamento de informação pessoal em sistemas de informação com enfoque social, chamando atenção para um tratamento mais específico da noção de privacidade em IHC. O autor usou a teoria de integridade contextual de Nissenbaum [2004], examinando as normas de *adequação social* e *fluxo de informação*, bem como as *mudanças de normas* no decorrer do tempo, com o objetivo de fornecer exemplos reais de como privacidade é percebida, negociada e articulada no compartilhamento de informações nesses sistemas. Assim, com base em dados empíricos focados no gerenciamento de informação pessoal em RSOs, o autor explica a teoria de integridade contextual, enfatizando que privacidade deve ser tratada como uma noção mais flexível, tendo em vista que os usuários ajustam suas práticas referentes ao compartilhamento de informação pessoal de acordo com normas sociais. Tais normas definem razões para compartilhar ou não informações, podendo mudar no decorrer do tempo, tornando inapropriado o que antes era apropriado saber sobre uma pessoa.

Por fim, voltado para o escopo mais geral de SiCo's, sem focar especificamente nas interações sociais, Skinner et al. [2006] apresentou uma taxonomia de privacidade, que pode ser usada na formulação de políticas, bem como de práticas e tecnologias

voltadas para a privacidade nesses sistemas. Tal taxonomia classifica hierarquicamente e categoriza os conceitos e princípios de privacidade, produzindo uma representação organizada dos mesmos de acordo com três dimensões interrelacionadas: *tempo*, *assunto* e *espaço*. Essas três dimensões exercem diferentes influências sobre a privacidade e se traduzem em três visões de privacidade: *visão computacional*, *visão de conteúdo* e *visão estrutural*, respectivamente.

A *visão computacional* reflete o nível de proteção de privacidade concedido ao usuário e está relacionada à dimensão *tempo*, no sentido de definir a quantidade de tempo e recursos necessários para ajustar o nível adequado de proteção de privacidade. A *visão de conteúdo* reflete a privacidade das informações compartilhadas no sistema e está relacionada à dimensão *assunto* no sentido de identificar diferentes necessidades de privacidade de acordo com características específicas dessas informações. Por fim, a *visão estrutural* reflete a privacidade dentro do sistema nos níveis individual, de grupo e organizacional, e está relacionada à dimensão *espaço* no sentido de determinar diferentes necessidades de privacidade para cada um desses níveis.

Como vimos, esses trabalhos identificam aspectos relevantes a serem considerados no tratamento de privacidade em sistemas de informação que permitem a interação social entre seus usuários. Assim, estes aspectos fornecem um entendimento mais amplo de privacidade, permitindo considerações sobre como incorporá-la no design desse tipo de sistema. Dessa forma, essas abordagens teóricas estabelecem uma base para a articulação de idéias de design que irão guiar o projeto e a avaliação de tecnologias sociais que suportam a privacidade de seus usuários. Nesse sentido, as ideias presentes esses estudos podem ser consideradas na criação de ferramentas epistêmicas, como o MDP, a fim de auxiliar o designer a refletir sobre como tratar privacidade em RSOs.

3.3 Modelos de Privacidade para RSOs

Algumas ferramentas conceituais têm sido propostas com o objetivo de tratar diferentes aspectos relacionados à privacidade no design de RSOs, como o controle de acesso às informações compartilhadas dentro do sistema, bem como o gerenciamento da forma como tal compartilhamento ocorre. Modelos de controle de acesso definem a forma como usuários poderão criar políticas para controlar o acesso às informações que compartilham nesses sistemas. Nesse sentido, Pang & Zhang [2015] definem um modelo de RSO que considera, além dos relacionamentos entre seus usuários, as informações públicas compartilhadas nesses ambientes, tratando estas últimas como uma nova dimensão que usuários podem utilizar na formulação de políticas de controle de acesso

que proporcionem a proteção de sua informação privada. Esse trabalho se apresenta como uma extensão de outros modelos de controle de acesso que se baseiam apenas no relacionamento entre seus usuários, com foco no relacionamento entre o dono da informação e aquele que a requisita [Carminati et al., 2009a,b; Fong et al., 2009], ou baseados na estrutura de grafo de RSOs, como n-amigos em comum e clique [Fong, 2011; Fong & Siahaan, 2011; Bruns et al., 2012]. Com uma fundamentação mais ampla do que o relacionamento entre usuários, Cheng et al. [2012] propôs um modelo que considera também os recursos e ações executadas pelos mesmos para a formulação de esquemas de controle de acesso a informações em RSOs.

No sentido de permitir que usuários gerenciem de forma eficiente o compartilhamento de suas informações pessoais em ambientes sociais online, considerando o impacto de tal compartilhamento em sua privacidade, Lederer et al. [2003] descreveram um *framework* conceitual que permite que usuários ajustem a precisão da informação compartilhada, de acordo com sua situação atual e com a audiência. Tierney & Subramanian [2014], por sua vez, utilizam uma abstração de contexto derivada da teoria de integridade contextual de Nissenbaum [2004] e propõem um modelo de compartilhamento de informação em RSOs que leva em consideração o papel do usuário, a informação postada, bem como as normas definidas de acordo com o papel do usuário e os atributos da postagem, para definir como as informações serão compartilhadas nesses sistemas.

Como podemos perceber, esses modelos e ferramentas conceituais visam aumentar a flexibilidade que esses sistemas oferecem aos **usuários**, no sentido de lidar com aspetos específicos de privacidade. Por outro lado, com o propósito específico de apoiar designers em suas decisões relacionadas a aspectos de privacidade que devem ser considerados no design de RSOs, alguns autores apresentam diretrizes e sugestões de design. Lipford et al. [2009] propõem um conjunto de diretrizes para o tratamento de privacidade nesses sistemas, a partir da análise de privacidade de RSOs de acordo com a teoria de integridade contextual de Nissenbaum [2004]. Tal análise identificou e explicou diferentes problemas de privacidade nesses sistemas, devido à impossibilidade ou à dificuldade de entender completamente os fluxos de informação sobre seus usuários. Assim, os autores chegam à conclusão de que uma forma de ajudar os usuários a alcançarem seus níveis desejados de privacidade seria tornar esses fluxos mais visíveis, de forma que usuários possam apresentar comportamentos consistentes com suas normas de adequação e distribuição da informação.

Ainda nessa linha de diretrizes para o design de RSOs com foco na privacidade de seus usuários, Lederer et al. [2004] descrevem cinco armadilhas com implicações na privacidade pessoal a que designers estão sujeitos ao projetarem sistemas interativos

e apresentam sugestões de como evitá-las. Essas armadilhas estão ligadas ao entendimento do usuário sobre como as informações pessoais são tratadas no sistema, e às suas ações dentro do mesmo. Em relação ao entendimento, esses autores sugerem que o sistema não deve ocultar a natureza e a extensão de uma potencial divulgação de informações, e nem ocultar o fluxo de informações presente no sistema. Em relação às ações dos usuários dentro do sistema, Lederer et al. [2004] propõem que o sistema não deve exigir uma excessiva configuração por parte dos mesmos no sentido de gerenciarem sua privacidade, mas deve permitir que estes transfiram suas práticas sociais já bem estabelecidas no mundo físico para as novas tecnologias.

Aproximando-se do propósito do MDP, existe na literatura também a proposta de modelos conceituais voltados para apoiar a decisão de designers no que tange ao tratamento de aspectos de privacidade em RSOs. Porém, tratando privacidade sob uma ótica diferente da tratada pelo MDP, Romero et al. [2012] propôs o "Modelo Fundamentado em Privacidade"[3], que visa apoiar o design de mecanismos que permitem a indivíduos coordenarem sua privacidade relacionada especificamente às suas disponibilidades para engajarem em um processo comunicativo com outras pessoas, dentro de um canal exclusivo, em plataformas digitais sociais. Esse modelo de Romero et al. [2012] se baseia em teoria de uso da linguagem que considera o conhecimento, crenças e suposições mútuos entre as partes comunicantes, bem como na teoria de privacidade de Altman [1975], no sentido de descrever como indivíduos que se comunicam nesses ambientes criam e adaptam seus limites de privacidade de forma dinâmica e dentro de um processo colaborativo.

Ainda dentro do propósito de apoiar a decisão de designers sobre como projetar aspectos específicos de RSOs, Epstein et al. [2015] desenvolveram um *framework* para projetar e avaliar aspectos relacionados ao compartilhamento de informações que são coletadas automaticamente nesses sistemas. Tal *framework* tem o propósito de ajudar designers a refletirem sobre suas decisões relacionadas a tal compartilhamento a partir de uma perspectiva multidimensional, como é a proposta da nossa pesquisa. Entretanto, a proposta de Epstein et al. [2015] foca especificamente nas respostas e reações da audiência à informação compartilhada, e não nos diferentes aspectos relacionados ao compartilhamento e seus impactos nos níveis de privacidade oferecidos aos usuários pelo sistema, que é o foco do MDP.

[3]Tradução do nome original em inglês "Privacy Grounded Model" (PGM).

Capítulo 4

O Modelo de Design de Privacidade

Neste capítulo, apresentamos o Modelo de Design de Privacidade (MDP), que consiste em uma ferramenta epistêmica para apoiar o designer na elaboração e avaliação do discurso designer-usuário em RSOs, com foco na privacidade relacionada ao compartilhamento de informações pessoais. Como uma ferramenta epistêmica, o MDP não se propõe a fornecer diretamente uma solução para tratar questões de privacidade em RSOs, e sim a aumentar o entendimento do designer sobre o problema e suas implicações, a fim de permitir-lhe gerar soluções alternativas e compará-las entre si.

O MDP é um modelo descritivo que considera o compartilhamento de informações pessoais em RSOs como uma comunicação entre usuários mediada pelo sistema. Tal comunicação pode ocorrer tanto na forma direta (quando o próprio indivíduo[1] compartilha informações sobre ele no sistema) quanto na forma indireta (quando outro usuário compartilha informações sobre o indivíduo). Além da informação sobre o indivíduo que é explicitamente compartilhada, o MDP também considera como informação pessoal seus discursos e atividades dentro do sistema, uma vez que podem levar à inferência de características e atributos pessoais, que impactam a sua privacidade [Golbeck et al., 2011; Kosinski et al., 2013]. Além disso, o MDP considera privacidade no contexto "um-para-muitos" das RSOS, em que as informações pessoais dos seus usuários são compartilhadas em espaços acessíveis a um grupo limitado ou ilimitado de pessoas, não levando em consideração as informações que são compartilhadas em interações envolvendo duas ou mais pessoas que se comunicam exclusivamente entre si, em um canal exclusivo.

[1]Nesta tese, usamos o termo "indivíduo" para nos referirmos ao usuário cuja informação está sendo compartilhada dentro da RSO.

O MDP estrutura o espaço de design do compartilhamento de informações pessoais em RSOs, definindo elementos de privacidade, os relacionamentos entre eles, atributos dos elementos e possíveis valores dos mesmos. Tal modelo consiste em uma ferramenta que permite ao designer expressar o seu modelo conceitual referente ao compartilhamento de informações pessoais dentro do sistema, ajudando-o na reflexão sobre o impacto desse compartilhamento na privacidade dos seus usuários. Tal ajuda ocorre através do fornecimento de informações qualitativas sobre os níveis de privacidade associados aos elementos do modelo. Os elementos e atributos do MDP constituem as estruturas descritivas básicas que permitem ao designer representar o seu projeto do compartilhamento de informações pessoais.

Na próxima seção, apresentamos a estrutura do espaço de design do compartilhamento de informações pessoais em RSOs considerada pelo MDP, bem como a descrição da sua lógica de design, com a explicação dos seus elementos, atributos e seus possíveis valores, bem como os níveis de privacidade remetidos por esses. Em seguida, na seção 4.2, mostramos uma sugestão de como o MDP pode ser utilizado no design de privacidade de RSOs. Por fim, na seção 4.3, mostramos como a modelagem do compartilhamento de informação pessoal, considerando aspectos de privacidade, é representada visualmente no MDP.

4.1 Estrutura do MDP

O MDP usa como base o espaço de design da Engenharia Semiótica para estruturar o espaço de compartilhamento de informações pessoais em RSOs. Vimos, no Capítulo 2, que a Engenharia Semiótica se baseia no modelo de comunicação de Jakobson [1960] para estruturar o seu espaço de design, caracterizado por meio da metamensagem enviada pelo designer ao usuário através da interface. Vimos que em sistemas colaborativos, como as RSOs, o designer inclui em sua metamensagem informações sobre como a comunicação entre usuários poderá ocorrer dentro do sistema, bem como sobre o que se pode falar e os códigos a serem utilizados para tal. Assim, podemos considerar que, neste caso, o designer está estruturando o espaço de comunicação entre os usuários, ao definir quem pode ser o emissor e o receptor, sobre o que podem falar, através de que canal e usando que códigos. Dessa forma, no MDP, utilizamos o modelo de Jakobson para estruturar a comunicação usuário-sistema-usuário.

O MDP é estruturado por meio das seguintes *dimensões de privacidade*: **fonte de informação**, **espaço de comunicação**, **informação do indivíduo**, **persistência**

temporal, **audiência**, **notificação para o indivíduo**[2], **discurso sobre o indivíduo**[3] e **disseminação da informação**. Tais dimensões descrevem diferentes aspectos relacionados ao compartilhamento de informações pessoais em RSOs, conforme mostrado na Figura 4.1 e representam aspectos sobre os quais o designer deve pensar, e que podem impactar o estado de privacidade dos usuários. Para cada uma dessas dimensões, um conjunto de possíveis valores é definido, remetendo a níveis distintos de privacidade para o indivíduo, como será mostrado adiante. O Apêndice B apresenta um guia sobre as dimensões de privacidade do MDP.

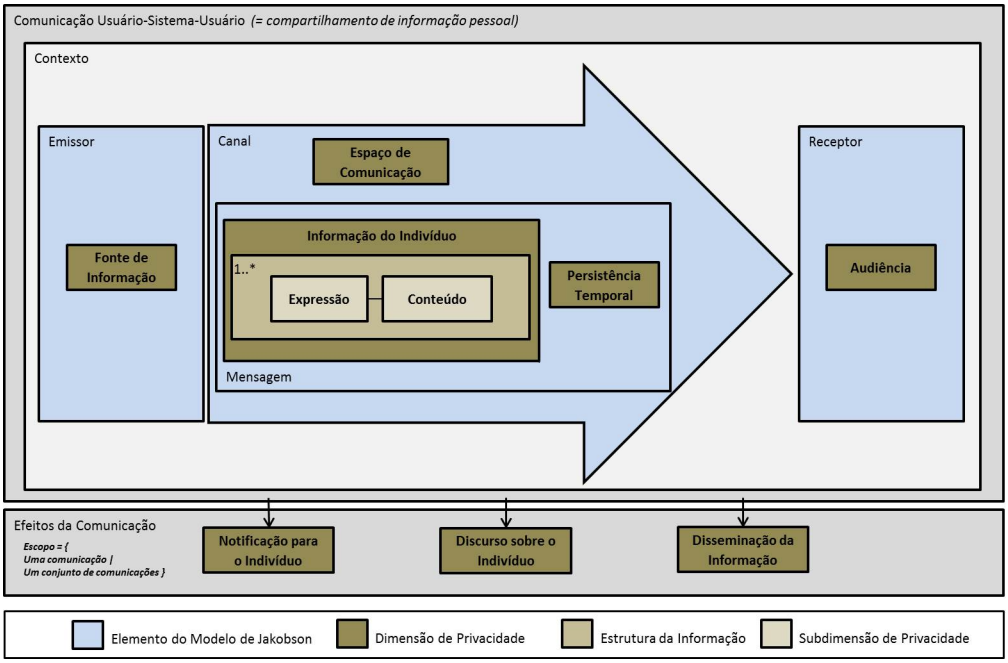


Figura 4.1. Estrutura do MDP, com as dimensões de privacidade

O MDP fundamenta-se basicamente na teoria de privacidade de Altman [1975] para derivar as características de privacidade a serem consideradas no compartilhamento de informações pessoais. Essas características estão presentes diretamente no modelo em questão através dos elementos **controle** e **estado de privacidade**, e indiretamente através do elemento **contexto**. O **controle** está relacionado a quem possui o poder de decisão sobre os valores a serem atribuídos a cada uma das dimensões de privacidade. Isso significa que, em tempo de design, o designer deve decidir, para cada

[2]O nome desta dimensão foi alterado com base nos resultados obtidos na avaliação com potenciais usuários e na revisão efetuada pelos membros da comissão examinadora desta tese. Assim, a dimensão **notificação para o indivíduo** é equivalente à dimensão **notificação** em Villela & Prates [2015b] e Villela & Prates [2016].

[3]O nome desta dimensão também foi alterado, pelo mesmo motivo anterior. Assim, a dimensão **discurso sobre o indivíduo** é equivalente à dimensão **discurso do sistema** em Villela & Prates [2015b] e Villela & Prates [2016].

uma das dimensões, a quem deverá ser concedido o controle sobre o valor da mesma: ao *usuário* ou ao *sistema*. No primeiro caso, o designer permite que o usuário defina o valor para a dimensão, em tempo de uso, concedendo ao mesmo o controle sobre o nível de privacidade relacionado à dimensão. No caso do controle ser do sistema, o designer determina, em tempo de design, como será definido o valor para a dimensão, determinando assim o nível (ou o intervalo definido pelo nível mínimo e máximo) de privacidade proporcionado através da mesma. Neste caso, o designer pode determinar um valor fixo para a dimensão, em tempo de design, ou definir que o valor da dimensão será definido pelo próprio sistema, mas em tempo de uso, podendo a mesma assumir um conjunto de valores com base em um processo de decisão, que pode levar em conta decisões tomadas pelo usuário.

O **estado de privacidade** é obtido a partir dos níveis de privacidade relacionados a cada uma das dimensões do modelo. Assim, a combinação de valores atribuídos a cada uma das dimensões de privacidade, em tempo de design ou em tempo de uso, considerando diferentes oportunidades de compartilhamento de informação pessoal, pode levar o indivíduo a atingir diferentes estados de privacidade dentro do sistema.

No MDP, o controle e o espaço de design de privacidade são ortogonais, no sentido de que, para cada uma das dimensões de privacidade propostas pelo modelo, o designer deverá tomar decisões relacionadas a quem terá o controle sobre as mesmas, se o usuário ou o sistema. Assim, a partir das decisões do designer em relação ao controle e valor para as dimensões de privacidade, no momento em que está fazendo a modelagem do compartilhamento de informações pessoais de um sistema, é concedido ao usuário a possibilidade de atingir determinados estados de privacidade. Nesse sentido, consideramos que o estado de privacidade alcançado pelo indivíduo dentro de uma RSO consiste em uma instância do que pode ser representado pelo MDP, a partir dos valores atribuídos às suas dimensões, tanto em tempo de design quanto em tempo de uso.

Diferente dos elementos anteriores, o **contexto** não é tratado diretamente no MDP. Entretanto, ele exerce um papel fundamental no sentido de guiar as decisões do designer sobre como tratar as dimensões de privacidade, no que se refere à forma como serão atribuídos valores às mesmas. Assim, com base no contexto de design, cabe ao designer decidir, para cada uma das dimensões de privacidade do MDP, se o nível de privacidade a ser oferecido aos usuários pela mesma será dependente do contexto de design ou do contexto de uso.

As dimensões de privacidade do MDP estão relacionadas entre si, a fim de formar a estrutura de comunicação referente ao compartilhamento de informação pessoal em RSOs. Assim, conforme mostrado na Figura 4.2, o compartilhamento de informa-

ção pessoal é caracterizado como uma *comunicação usuário-sistema-usuário*, em que a **fonte de informação** compartilha uma **unidade de informação sobre indivíduo**, que pode ser composta por uma ou mais **estruturas de informação**. Cada unidade de informação do indivíduo é compartilhada com uma **audiência**, dentro de um **espaço de comunicação** e possui uma **persistência temporal**, que está relacionada ao seu tempo de existência dentro do sistema. Essa comunicação pode ou não gerar *efeitos comunicativos*, caracterizados pela **notificação** que o sistema fornece ao indivíduo relacionada à ação de outros usuários sobre a sua informação, pelo **discurso sobre o indivíduo**, que o sistema faz sobre o compartilhamento realizado, e pela **disseminação da informação** compartilhada sobre o indivíduo por parte de outros usuários.

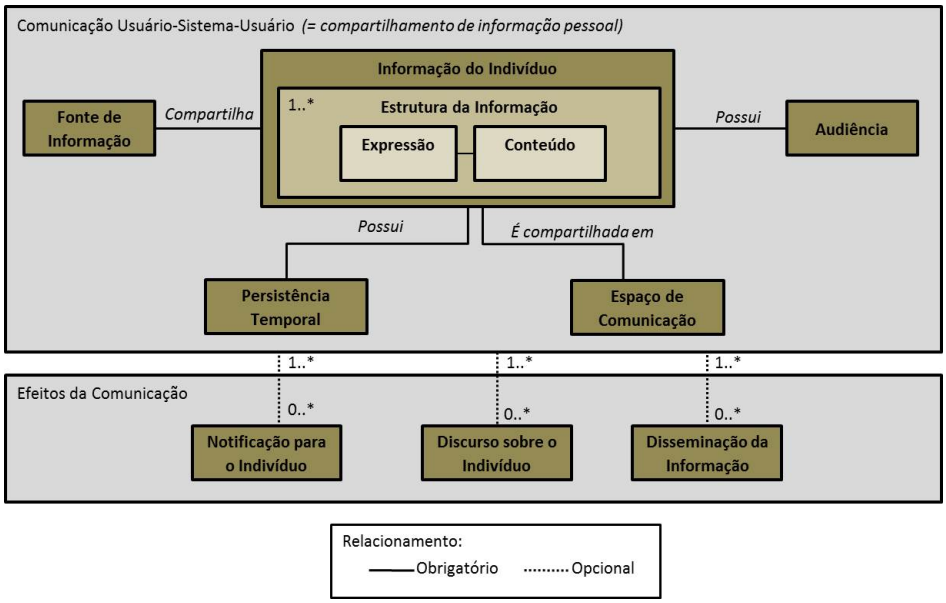


Figura 4.2. Relacionamentos entre as dimensões de privacidade do MDP

A seguir, na subseção 4.1.1, descrevemos detalhadamente cada uma das dimensões de privacidade do MDP, com os valores que as mesmas podem assumir e seus níveis de privacidade correspondentes, conforme mostrado na Figura 4.3.

4.1.1 Dimensões de Privacidade

As dimensões de privacidade do MDP foram definidas com base na literatura sobre compartilhamento de informação e privacidade em RSOs, e em estudos empíricos que foram realizados em estágios anteriores da nossa pesquisa. Essas dimensões são estruturadas em dois níveis: *comunicação usuário-sistema-usuário* e *efeitos da comunicação*. A *comunicação usuário-sistema-usuário* diz respeito à comunicação entre usuários que

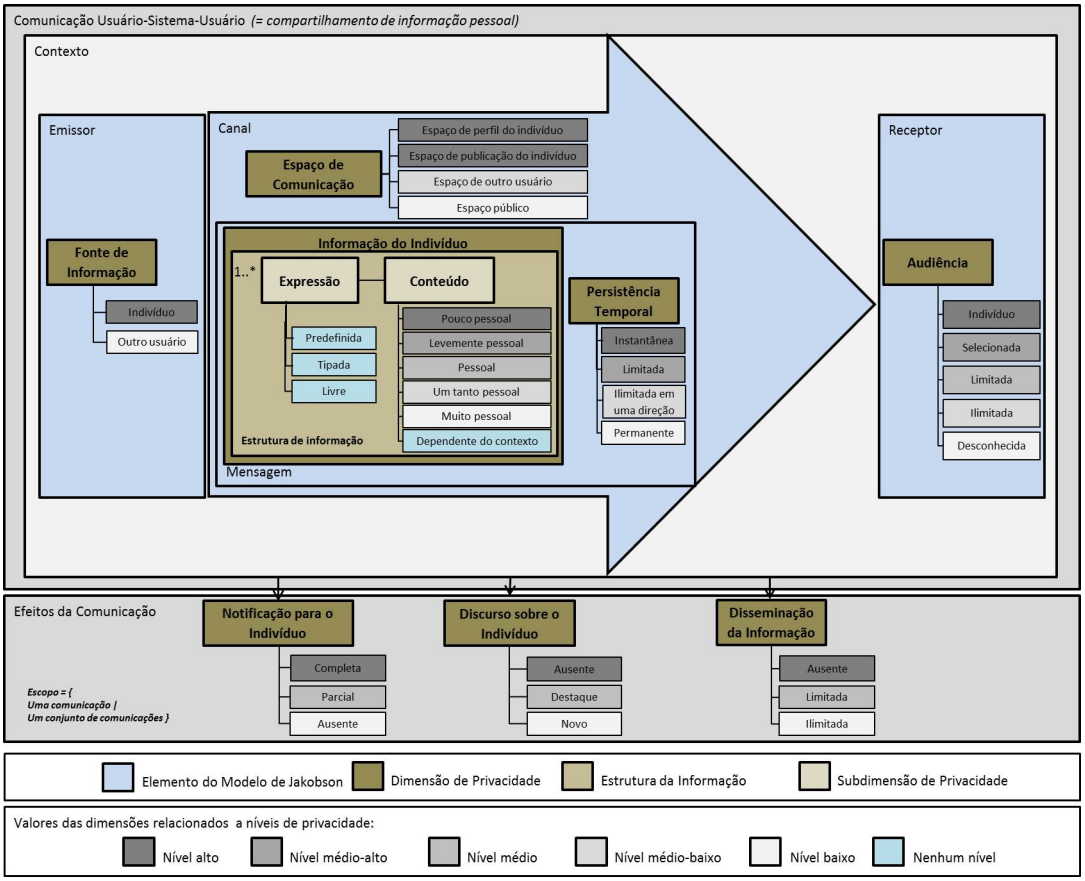


Figura 4.3. Estrutura do MDP, com as dimensões de privacidade, seus possíveis valores e os níveis de privacidade remetidos pelos mesmos

ocorre através do sistema, com o seu conteúdo consistindo de informações pessoais. Os *efeitos da comunicação*, por sua vez, consistem de informações que podem ser geradas a partir da comunicação usuário-sistema-usuário, referente ao compartilhamento de informações pessoais do indivíduo, e que também estão relacionadas a questões de privacidade. A seguir, serão detalhadas as dimensões em cada um desses níveis.

4.1.1.1 Dimensões de Comunicação Usuário-Sistema-Usuário

As dimensões de comunicação usuário-sistema-usuário, descritas a seguir, são estruturadas com base no modelo de comunicação de Jakobson [1960], e modelam os elementos que constituem o compartilhamento de informação pessoal em RSOs.

Fonte de Informação Esta dimensão está relacionada ao elemento "emissor" do modelo de comunicação Jakobson e diz respeito a quem pode determinar como, quando e em que extensão a informação pessoal do indivíduo será compartilhada no sistema. Nesta dimensão, privacidade é caracterizada de acordo com a fronteira de identidade

entre o indivíduo e outras pessoas, colocada por Palen & Dourish [2003], e o nível de privacidade está relacionado à autonomia, concedida ou não ao indivíduo, em relação ao compartilhamento de sua informação pessoal, discutida por Boyle & Greenberg [2005].

Assim, o MDP considera que informações pessoais sobre o indivíduo podem ser compartilhadas por ele próprio ou por outros usuários em uma RSO, com os possíveis valores da dimensão **fonte de informação** sendo iguais a *"indivíduo"* e *"outro usuário"*. No primeiro caso, o indivíduo pode explicitamente compartilhar informações sobre ele com outros usuários, ou mesmo executar ações que indiretamente podem caracterizá-lo, ao revelar suas opiniões, pontos de vista ou mesmo traços de sua personalidade dentro do sistema. Neste caso, o indivíduo possui autonomia para controlar a emissão da mensagem contendo informações sobre ele, o que remete a um nível mais alto de privacidade. Por outro lado, quando a **fonte de informação** é outro usuário, tal controle é concedido a este, sendo que o indivíduo não possui autonomia sobre a sua informação que é compartilhada dentro do sistema, remetendo assim a um nível mais baixo de privacidade.

Espaço de Comunicação Esta dimensão está relacionada ao elemento "canal" do modelo de comunicação de Jakobson e se refere ao local onde a informação sobre o indivíduo é compartilhada dentro do sistema. Assim como na dimensão **fonte de informação**, nesta dimensão a privacidade também é caracterizada de acordo com a fronteira de identidade entre o indivíduo e outras pessoas [Palen & Dourish, 2003], e é regulada através da autonomia [Boyle & Greenberg, 2005], que pode ou não ser concedida ao indivíduo, para controlar o acesso ao espaço onde ocorre o compartilhamento de suas informações pessoais.

Dessa forma, de acordo com o MDP, o compartilhamento de informações pessoais pode ocorrer em um dos seguintes espaços: *"espaço de perfil do indivíduo"*, *"espaço de publicação do indivíduo"*, *"espaço de outro usuário"* e *"espaço público"*. Dentre os espaços do indivíduo, o *"espaço de perfil"'* refere-se ao espaço onde são compartilhadas informações mais estáticas, como aquelas biográficas e descritivas relacionadas a elementos de identidade do indivíduo dentro do sistema, como, por exemplo, nome, data de nascimento, endereço, etc. Já o *"espaço de publicação do indivíduo"* refere-se ao local onde são compartilhadas informações mais dinâmicas, que refletem situações ou objetos que podem sofrer frequentes atualizações, e sobre as quais outros usuários costumam poder interagir. Um exemplo de espaço de publicação do indivíduo é a *"Linha do Tempo"* do Facebook, mostrada na Figura 4.4, onde o indivíduo pode compartilhar os mais variados tipos de informações, como uma atualização de status, uma foto/vídeo ou ainda um acontecimento, podendo ainda adicionar à sua publicação fotos, o que ele

está fazendo ou como está se sentindo, além de sua localização, conforme mostrado, respectivamente nos itens (a) até (f).

Figura 4.4. Compartilhamento de informação pessoal na linha do tempo do indivíduo no Facebook

O valor *"espaço de outro usuário"*, como o próprio nome indica, refere-se a um espaço que pertence a outro usuário do sistema, onde também podem ser compartilhadas informações pessoais do indivíduo. Por fim, o valor *"espaço público"* diz respeito a um espaço que não pertence especificamente a nenhum usuário, e que pode ser indistintamente acessado por todos os usuários, e em alguns casos até mesmo por pessoas fora do sistema. Um exemplo de espaço público é a página *"Questions"* no ResearchGate, mostrado na Figura 4.5, que é o local onde usuários postam suas questões de pesquisa e pode estar acessível até mesmo para pessoas que não possuem uma conta no sistema.

Considerando a autonomia concedida ao indivíduo para controlar o compartilhamento de suas informações pessoais, temos que os seus próprios espaços remetem a níveis mais altos de privacidade, em relação aos outros espaços. Assim, tanto o espaço de perfil do indivíduo, quanto o seu espaço de publicação, remetem a níveis igualmente altos de privacidade, tendo em vista que se presume que o indivíduo tenha um maior controle sobre o compartilhamento que ocorre dentro desses espaços. Por outro lado, quando o compartilhamento de informações ocorre em outros espaços, temos que o espaço de outro usuário remete a um nível de privacidade que, embora seja menor do que os níveis de privacidade remetidos pelos espaços do indivíduo, é maior do que o espaço público. Isso ocorre porque, embora o indivíduo não tenha autonomia para controlar o acesso ao espaço de outros usuários, esse controle de alguma forma ainda existe, mesmo que por parte desses últimos, enquanto que no espaço público não há

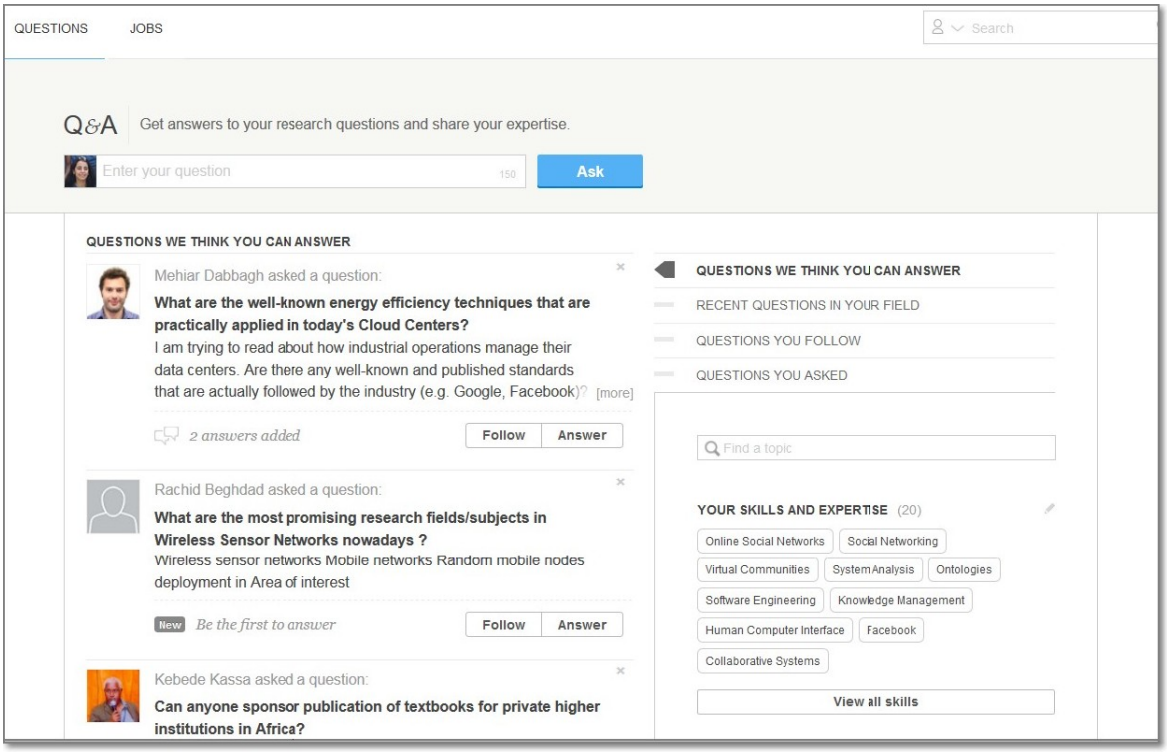


Figura 4.5. Página "Questions" no ResearchGate

nenhum tipo de controle de acesso, estando a informação aí compartilhada acessível indistintamente a todos os usuários do sistema, ou até mesmo fora desse.

Informação do Indivíduo Esta dimensão está relacionada aos elementos "mensagem" e "código" do modelo de comunicação de Jakobson, e é composta pelas subdimensões **expressão** e **conteúdo**.

A subdimensão **expressão** refere-se à forma como a informação é expressa no sistema. O MDP considera que informações podem ser expressas no formato *"predefinido"*, *"tipado"* ou *"livre"*. Informações *predefinidas* são aquelas definidas pelo sistema, em tempo de design, cabendo ao usuário apenas decidir se irá compartilhá-las ou não, ao executar determinadas ações dentro do sistema. Por exemplo, no Facebook, quando o usuário clica sobre o link "curtir" em alguma postagem, ele está compartilhando uma informação predefinida, ou seja, a sua "curtida" é compartilhada com a audiência da postagem. Isso pode ser considerado uma informação pessoal (em algum nível), devido ao fato de que, ao curtir uma postagem, o usuário pode estar indiretamente indicando sua opinião ou ponto de vista em relação ao assunto tratado na mesma, o que pode levar à inferência, por parte da audiência, de características e atributos pessoais relacionados a ele.

As informações *tipadas*, por outro lado, são aquelas que possuem o seu significado definido pelo sistema, em tempo de design, mas são fornecidas pelos usuários, em tempo de uso. Ainda no Facebook, por exemplo, informações relacionadas a local de trabalho e habilidades profissionais, compartilhadas no perfil do usuário, são informações tipadas, como mostrado Figura 4.6. Finalmente, informação *livre* é aquela em que o seu significado é definido pelo próprio usuário, em tempo de uso, a partir do seu conteúdo. No Facebook, por exemplo, quando o usuário faz uma atualização de status, ao adicionar um texto em resposta à questão *"What's on your mind?"*, como mostrado na Figura 4.7, ele está postando uma informação em formato livre, tendo em vista que a postagem pode comunicar qualquer tipo de conteúdo, como, por exemplo, emoções, opiniões e pontos de vista relacionadas a qualquer assunto, dentre outros.

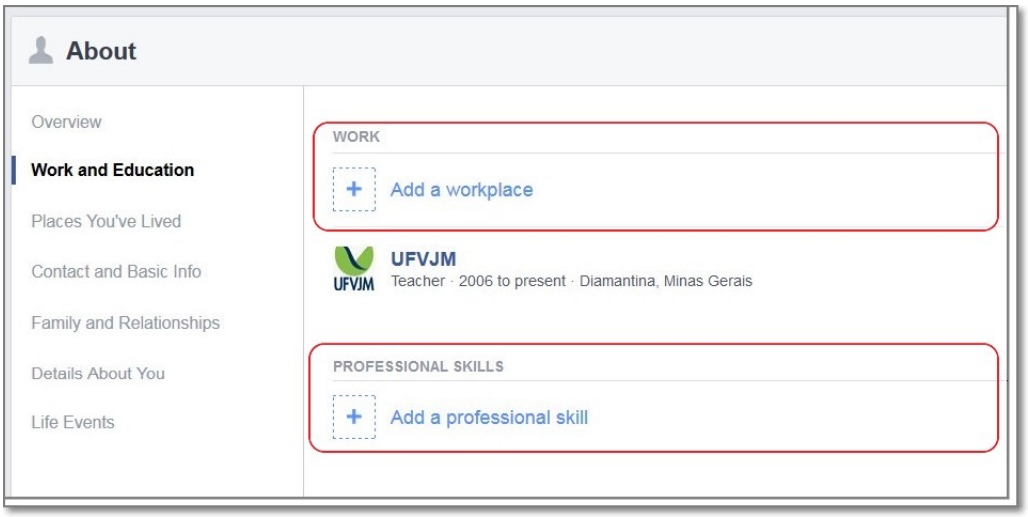


Figura 4.6. Compartilhamento de informação *tipada* no perfil do indivíduo no Facebook

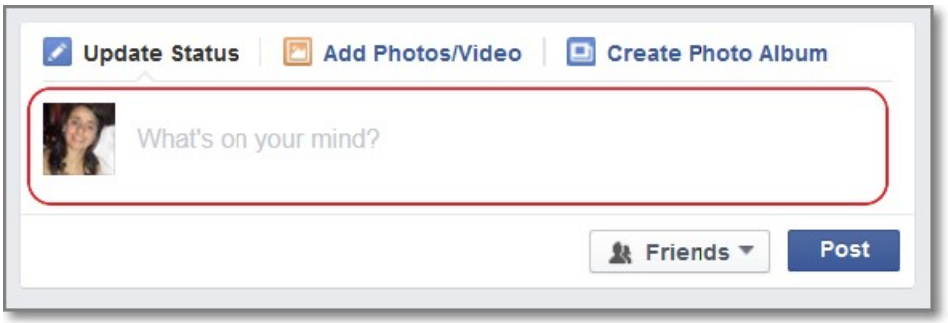


Figura 4.7. Postagem de atualização de status no Facebook

A subdimensão **conteúdo** refere-se ao teor da informação sobre o indivíduo que está sendo compartilhada, classificado de acordo com o seu *nível de pessoalidade*. De-

finimos *nível de pessoalidade* em Villela et al. [2015a], como sendo o quão pessoal uma informação é, de acordo com a forma como as pessoas a compartilham no mundo físico (das interações face-a-face) e no mundo virtual (das RSOs), levando em consideração suas preocupações com privacidade. Dessa forma, o nível de pessoalidade e, consequentemente, a subdimensão **conteúdo**, pode assumir os seguintes valores no MDP: *"pouco pessoal"*, *"levemente pessoal"*, *"pessoal"*, *"um tanto pessoal"* e *"muito pessoal"*. De acordo com o estudo feito em Villela et al. [2015a], temos que no Facebook, por exemplo, o lugar onde o indivíduo estuda ou trabalha está no nível *"pouco pessoal"*, locais visitados e estado de relacionamento estão no nível *"levemente pessoal"*, data de aniversário está no nível *"pessoal"*, endereço de email e fotos do indivíduo estão no nível *"um tanto pessoal"* e, finalmente, número de telefone e informações sobre a saúde do indivíduo estão no nível *"muito pessoal"*.

Na formação da estrutura de informação que compõe a dimensão **informação do indivíduo**, existe uma dependência intrínseca da subdimensão **conteúdo** em relação à subdimensão **expressão**. Essa dependência é caracterizada pelo fato do valor desta última poder influenciar o controle e a variação de valor da primeira da seguinte forma: se a **expressão** da informação é *"tipada"*, então o controle sobre a subdimensão **conteúdo** é do sistema, com o valor da mesma sendo definido em tempo de design. Por outro lado, se a **expressão** da informação é *"livre"*, o controle sobre a subdimensão **conteúdo** é do usuário, que é quem define o valor da mesma, em tempo de uso. Uma situação especial ocorre, porém, quando a **expressão** da informação é *"predefinida"*. Nesse caso, o valor e o controle da subdimensão **conteúdo**, ou seja, o nível de pessoalidade da informação e quem o define, dependem do contexto onde o compartilhamento da informação ocorre, e não pode ser definido a priori. Um exemplo disso é quando o indivíduo curte uma postagem de outro usuário no Facebook. Neste caso, o valor e o controle da subdimensão **conteúdo** referente à ação "curtir" do indivíduo depende da informação que ele curtiu, tendo em vista que a mesma pode estar em níveis de pessoalidade diferentes para o indivíduo e para o usuário ao qual pertence.

Dessa forma, dentro da dimensão **informação do indivíduo**, temos que a subdimensão **expressão** define "quando" (em tempo de design ou em tempo de uso) o valor da subdimensão **conteúdo** será definido e "quem" (designer ou usuário) tem o controle sobre a mesma. Assim, a expressão não está diretamente relacionada a "o que" é compartilhado, mas a "como" tal compartilhamento ocorre. Dessa forma, temos que apenas os valores para a subdimensão **conteúdo** remetem a níveis de privacidade, considerando que o compartilhamento de informações menos pessoais leva a maiores níveis de privacidade para o indivíduo, enquanto que, por outro lado, o compartilhamento de informações mais pessoais potencialmente leva a níveis decrescentes de privacidade,

uma vez que pode provocar a exposição de aspectos íntimos e privados do indivíduo.

Persistência Temporal Assim como a dimensão **informação do indivíduo**, esta dimensão também está relacionada ao elemento "mensagem" do modelo de comunicação de Jakobson e diz respeito ao período de tempo durante o qual a informação sobre o indivíduo fica acessível à sua audiência, dentro do sistema. Nesta dimensão, privacidade é caracterizada de acordo com a fronteira temporal entre passado, presente e futuro, considerada no trabalho de Palen & Dourish [2003], sendo que o nível de privacidade está relacionado ao tempo em que a informação fica disponível para acesso dentro do sistema.

De acordo com o MDP, a persistência temporal da informação pessoal do indivíduo, que é compartilhada no sistema, pode assumir os seguintes valores: *"instantânea"*, *"limitada"*, *"ilimitada em uma direção"* e *"permanente"*. O valor da dimensão **persistência temporal** é *"instantânea"* quando a informação sobre o indivíduo fica disponível no sistema por um período muito curto de tempo (tipicamente apenas para os usuários da audiência que estão acessando o sistema no momento em que a informação é compartilhada).

O valor da dimensão **persistência temporal** é *"limitada"*, por sua vez, quando a informação sobre o indivíduo fica disponível para a audiência por um período limitado (e geralmente curto) de tempo, como, por exemplo, as fotos e vídeos adicionados à história do indivíduo no aplicativo Snapchat, que fica disponível para a sua audiência por um período de vinte e quatro horas.

O valor da dimensão **persistência temporal** é *"ilimitada em uma direção"* quando a informação sobre o indivíduo é disponibilizada à sua audiência por um período ilimitado de tempo, ficando disponível a partir para o usuário a partir do momento em que ele começa a fazer parte da audiência (que é considerado o tempo presente) e prossegue em direção ao passado ou ao futuro. Isso significa, respectivamente, que o usuário tem acesso àquela informação apenas se ela tiver sido compartilhada em algum momento anterior a ele começar a fazer parte da sua audiência até o momento presente, ou que ele terá acesso apenas às informações que forem compartilhadas a partir do momento em que ele começou a fazer parte da audiência. Um exemplo para este último caso são as informações compartilhadas em grupos no aplicativo WhatsApp. Neste caso, quando novos usuários entram em um grupo, eles terão acesso apenas às informações compartilhadas a partir daquele momento.

Por fim, quando o valor da dimensão **persistência temporal** é *"permanente"*, isso indica que, uma vez que a informação sobre o indivíduo é compartilhada dentro do sistema, ela ficará sempre acessível à sua audiência, enquanto ela não for volun-

tariamente excluída pelo usuário. No Facebook, por exemplo, todas as informações pessoais que são compartilhadas possuem validade temporal permanente, uma vez que ficam acessíveis à sua audiência por um período indeterminado de tempo, só deixando de ficar acessível caso seja excluída pelo usuário.

Os valores para a dimensão **persistência temporal**, na ordem em que foram acima apresentados, remetem a níveis decrescentes de privacidade, tendo em vista que quanto mais tempo a informação fica disponível dentro do sistema, maiores são as chances delas serem acessadas, podendo despertar questões de privacidade para o indivíduo [Alarcón et al., 2005; Joinson & Paine, 2007; Palen & Dourish, 2003].

Audiência Esta dimensão está relacionada ao elemento "receptor" do modelo de comunicação de Jakobson e se refere a quem terá acesso à informação sobre o indivíduo, compartilhada no sistema. Nesta dimensão, privacidade é caracterizada de acordo com a fronteira entre público e privado, considerada no trabalho de Palen & Dourish [2003], e é regulada por meio de controles de solitude e confidencialidade, discutidos por Boyle & Greenberg [2005].

No MPD, os possíveis valores para a dimensão **audiência** são: *"indivíduo"*, *"selecionada"*, *"limitada"*, *"ilimitada"* e *"desconhecida"*. Quando a **audiência** é apenas o *"indivíduo"*, tem-se um nível máximo de privacidade por um lado, mas um nível mínimo de interação, tendo em vista que ninguém, além do próprio indivíduo, será capaz de acessar a informação e interagir a partir dela. No sentido de expandir as possibilidades de interação e, consequentemente, diminuir o nível de privacidade do indivíduo, a **audiência** é *"selecionada"* quando o usuário decide quem serão os usuários que farão parte do grupo que irá formar a audiência da informação. Por outro lado, a **audiência** é *"limitada"* quando abrange todo o conjunto de usuários do sistema, e *"ilimitada"* quando abrange, além dos usuários do sistema, outras pessoas externas ao mesmo. Por fim, temos que a **audiência** é *"desconhecida"* quando o indivíduo ao qual a informação se refere não tem conhecimento de quem poderá ter acesso à mesma. No Facebook, por exemplo, tem-se que a **audiência** é *"selecionada"* quando a informação é compartilhada com uma lista de amigos selecionados pelo usuário, ou até mesmo com todos os seus amigos. Por outro lado, quando a informação é compartilhada publicamente, tem-se uma **audiência** *"ilimitada"*, tendo em vista que a informação fica acessível neste caso até mesmo para pessoas externas ao Facebook. Finalmente, tem-se que a **audiência** é *"desconhecida"* quando a informação é compartilhada pelo indivíduo no espaço de outro usuário, uma vez que é esse outro usuário que controla quem é a audiência, a qual não é informada ao indivíduo, como mostrado na Figura 4.8.

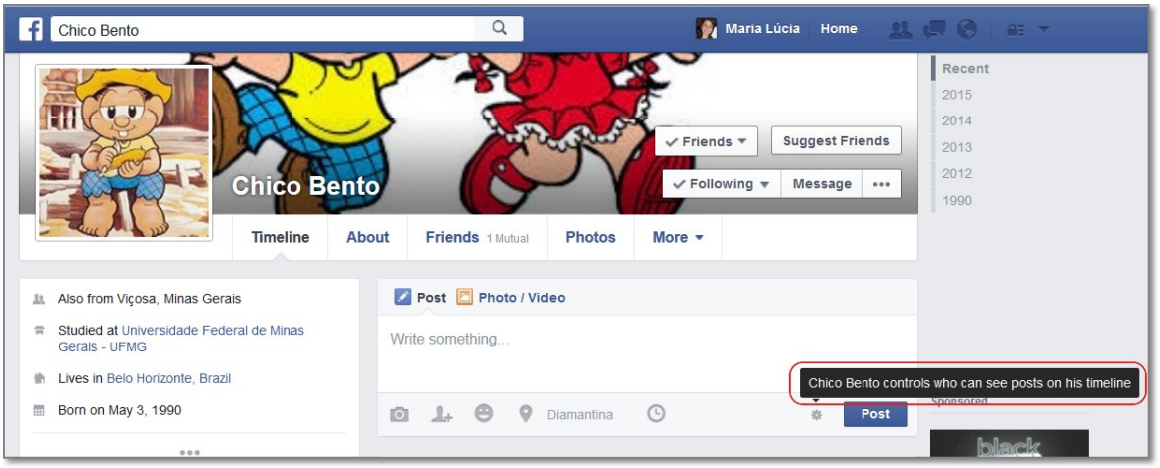


Figura 4.8. Indivíduo compartilhando informação na linha do tempo de outro usuário, com audiência desconhecida, no Facebook

4.1.1.2 Dimensões de Efeitos da Comunicação

Diferente das dimensões anteriormente apresentadas, as dimensões de efeitos da comunicação não estão diretamente relacionadas a elementos do modelo de comunicação de Jakobson. Ao invés disso, elas representam informações resultantes do processamento ou disseminação de atos comunicativos entre usuários, referentes ao compartilhamento de informações pessoais do indivíduo. Estes efeitos comunicativos podem ser *diretos* ou *inferenciais*. No primeiro caso, os efeitos são gerados a partir de um único ato comunicativo referente a uma ocorrência de compartilhamento de informação pessoal dentro do sistema. No segundo caso os efeitos são gerados (ou inferidos) a partir de um conjunto de atos comunicativos referentes a diferentes compartilhamentos.

Notificação para o Indivíduo Esta dimensão diz respeito ao sistema informar adequadamente ao indivíduo quando uma informação sobre ele é divulgada ou acessada por outros usuários e de que forma isso acontece. Assim, se o indivíduo recebe, para cada informação pessoal sua que é compartilhada, um completo relatório sobre as interações de outros usuários com a mesma, dizemos que o valor da dimensão **notificação para o indivíduo** é *"completa"*, como ocorre no Facebook, que notifica o indivíduo sempre que outros usuários interagem, de alguma forma, com a sua informação, seja curtindo, comentando ou compartilhando algo referente ao mesmo.

Caso o indivíduo seja informado apenas sobre uma parte das interações de outros usuários com sua informação, o valor da dimensão **notificação para o indivíduo** é *"parcial"*. Um exemplo de notificação parcial ocorre no ResearchGate, que notifica o indivíduo quando outros usuários seguem ou comentam uma publicação de sua autoria,

como pode ser visto na Figura 4.9, mas não o notifica quando outros usuários fazem download ou compartilham a mesma. Por fim, quando o sistema não fornece ao indivíduo nenhuma informação sobre as interações de outros usuários com sua informação que é compartilhada no mesmo, o valor da dimensão **notificação para o indivíduo** é *"ausente"*.

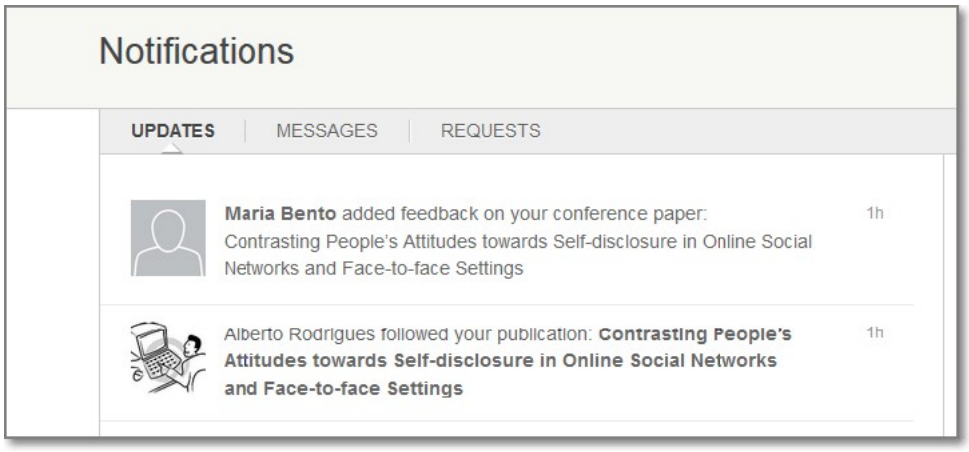


Figura 4.9. Notificações exibidas para o indivíduo quando usuários comentam e seguem suas publicações no ResearchGate

Temos que os valores para a dimensão **notificação para o indivíduo**, na ordem em que foram acima apresentados, remetem a níveis decrescentes de privacidade, tendo em vista que, embora tais valores não afetem diretamente o estado de privacidade alcançado pelo indivíduo, eles podem influenciar a forma como o mesmo gerencia a sua privacidade dentro do sistema. Isto ocorre tendo em vista que, quando o indivíduo possui uma maior consciência sobre a sua potencial exposição dentro do sistema (neste caso, relacionada a ação de outros usuários sobre sua informação), ele pode ser mais restritivo em relação às informações que ele compartilha, ou com suas configurações de privacidade [Emanuel et al., 2013].

Discurso sobre o Indivíduo Esta dimensão está relacionada ao sistema tomar a iniciativa de gerar compartilhamentos de informações do indivíduo, o que pode impactar a sua preocupação com privacidade [Hoadley et al., 2010]. Dessa forma, remetendo a níveis decrescentes de privacidade, os valores para esta dimensão podem ser: *"ausente"*, *"destaque"* e *"novo"*. O valor da dimensão **discurso sobre o indivíduo** é igual a *"ausente"* se o sistema não gera qualquer comunicação a partir de um ou mais compartilhamentos de informações pessoais do indivíduo.

Por outro lado, o valor da dimensão **discurso sobre o indivíduo** é igual a *"destaque"* quando o sistema apresenta aos usuários informações sobre o indivíduo às

quais os mesmos já possuem acesso, porém de forma destacada, trazendo-as à atenção dos usuários [Villela et al., 2015d]. Um exemplo de discurso de destaque do Facebook é o recurso *"Novidades" (Ticker)*, exibido na Figura 4.10, que mostra a outros usuários as atividades do indivíduo às quais eles já possuem acesso, mas em tempo real. Esse discurso do Facebook está no nível direto, tendo em vista que ocorre para cada instância de comunicação, referente ao compartilhamento de informação pessoal do indivíduo. Outro exemplo de discurso de destaque do Facebook, agora no nível inferencial, é a *"sugestão de amizade"*, em que são mostradas a outros usuários informações públicas disponibilizadas no perfil do indivíduo, como nome e foto de perfil, bem como os amigos em comum, conforme exibido na Figura 4.11. Esse discurso ocorre com base em informação sobre trabalho e educação do indivíduo, bem como seus amigos em comum com os usuários aos quais a sugestão é apresentada. Vale salientar que essas informações estão acessíveis no perfil dos usuários, porém, na sugestão de amizade, o Facebook extrai essas informações e as exibe diretamente na página de outros usuários, ao invés desses terem que procurar por amigos em potencial, visitando as páginas de vários usuários do sistema.

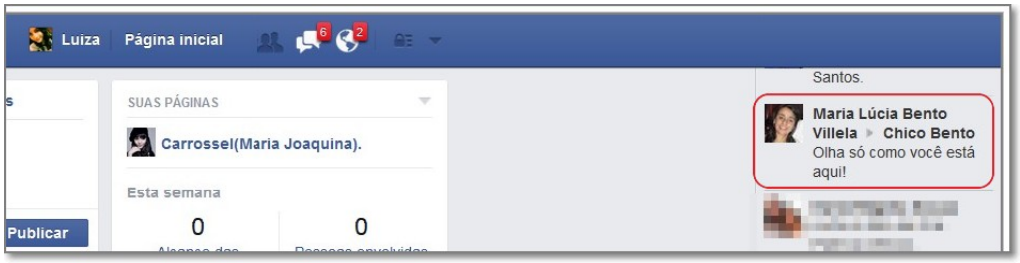


Figura 4.10. Recurso Ticker do Facebook, dando destaque à informação compartilhada sobre o indivíduo

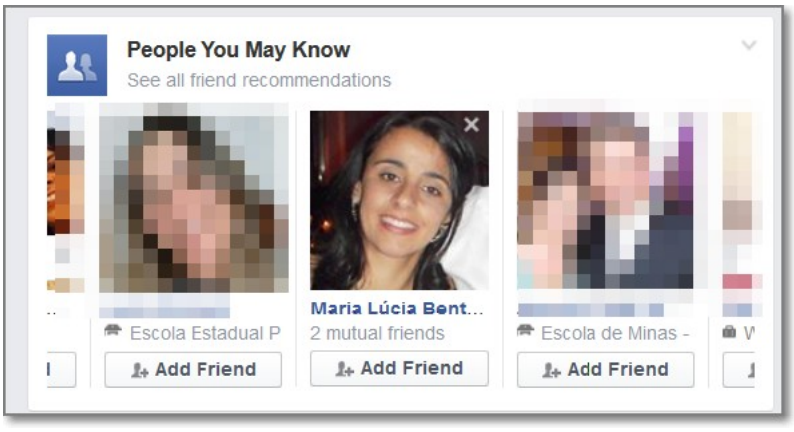


Figura 4.11. Sugestão de amizade no Facebook

Por fim, a dimensão **discurso sobre o indivíduo** recebe o valor *"novo"* caso o sistema processe uma ou mais informações pessoais do indivíduo que são compartilhadas, gerando nova informação sobre o mesmo. Um exemplo de discurso do sistema gerando uma nova informação ocorre no ResearchGate, quando calcula o *"RG Score"* do indivíduo (que consiste em uma métrica de reputação científica, calculada com base nas publicações e interações de outros pesquisadores com o conteúdo do indivíduo), e exibe tal informação em sua página, como pode ser visto na Figura 4.12. Assim como a sugestão de amizade no Facebook, essas informações no ResearchGate são geradas no nível inferencial, com base em um conjunto de comunicações referentes a compartilhamentos de informações pessoais do indivíduo.

Neste ponto, vale chamar a atenção para o fato que tanto a dimensão **notificação para o indivíduo** quanto a dimensão **discurso sobre o indivíduo** caracterizam discursos realizados pelo sistema a partir do compartilhamento de informações sobre o indivíduo. No entanto, o tema e a audiência desses discursos são claramente distintos. No primeiro caso, o discurso é feito para o indivíduo, sobre a interação de outros usuários com a sua informação. No segundo caso, o discurso é feito para outros usuários, sobre a informação do indivíduo que é compartilhada no sistema.

Disseminação da Informação Esta dimensão está relacionada à audiência ser capaz de (re)compartilhar informação pessoal do indivíduo dentro do sistema, referindo-se à possibilidade de uma informação pessoal do indivíduo se espalhar através da rede, gerando problemas de privacidade [Solove, 2008], devido ao alcance inesperado, por parte do indivíduo, de suas informações [Pereira Junior et al., 2014, 2013]. Assim como as dimensões **notificação para o indivíduo** e **discurso sobre o indivíduo**, esta dimensão também se refere ao processamento baseado nas dimensões do nível de comunicação usuário-sistema-usuário. Entretanto, diferente das dimensões anteriores, neste caso, os usuários que fazem parte da audiência da comunicação original é que são responsáveis por tal processamento, e não o sistema. Os valores que a dimensão **disseminação da informação** pode assumir são: *"ausente"*, *"limitada"* e *"ilimitada"*.

O valor da dimensão **disseminação da informação** é igual a *"ausente"* quando não é permitida à audiência da informação recompartilhá-la com outras pessoas. Um exemplo dessa situação ocorre no Facebook, quando o indivíduo compartilha informações em sua linha do tempo com uma audiência específica. Neste caso, quando algum usuário que faz parte da audiência as (re)compartilha, apenas as pessoas que fazem parte dessa audiência original são capazes de visualizar a postagem, conforme mostrado na interface da Figura 4.13.

Quando a informação compartilhada sobre o indivíduo pode ser propagada de

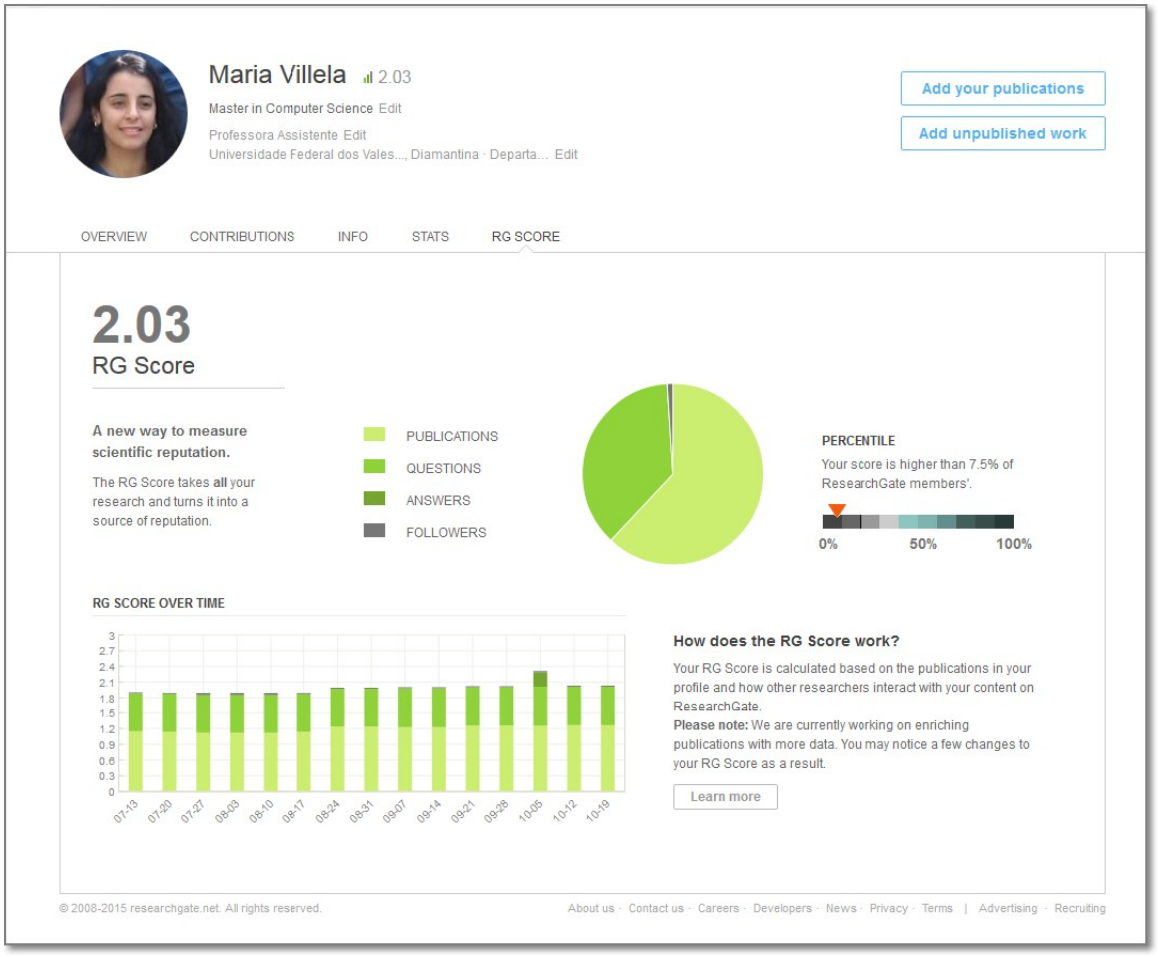


Figura 4.12. Exibição do "RGScore" na Página do Indivíduo do ResearchGate

uma maneira restrita, apenas para uma audiência adicional limitada, tem-se que o valor da dimensão **disseminação da informação** é *"limitada"*. Um exemplo dessa situação ocorre também no Facebook, quando o indivíduo compartilha uma foto em sua linha do tempo e outros usuários que pertencem à audiência da mesma marcam seus amigos na foto, expandindo a audiência para a pessoa marcada e possivelmente seus amigos, com a disseminação da informação limitada a esses.

Finalmente, o valor da dimensão **disseminação da informação** é *"ilimitada"* quando a informação sobre o indivíduo pode ser recompartilhada pela audiência sem qualquer restrição. Um exemplo desse caso ocorre no WhatsApp, quando uma pessoa recebe uma mensagem e pode recompartilhá-la com qualquer outra pessoa da sua lista de contatos ou grupo que participa.

Nesta seção, foram apresentadas as dimensões de privacidade, que permitem ao designer descrever aspectos relacionados ao compartilhamento de informação pessoal em RSOs, e que podem influenciar as experiências dos usuários no tocante à sua priva-

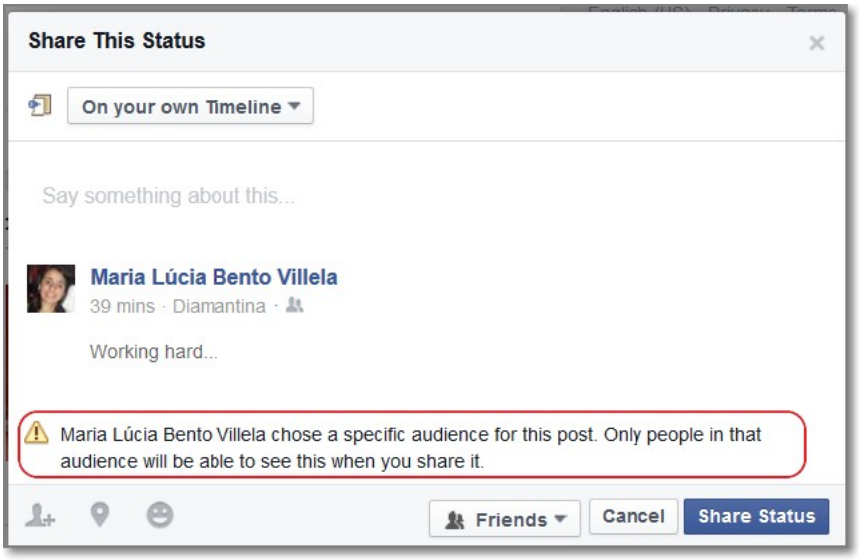


Figura 4.13. (Re)compartilhamento de postagem no Facebook

cidade, impactando, assim, a forma como interagem entre si através do sistema. Vimos que esses aspectos possibilitam ao usuário alcançar estados distintos de privacidade dentro do sistema.

4.2 Decisões de Privacidade Apoiadas no MDP

Considerando a proposta do MDP de acordo com a teoria da Engenharia Semiótica, podemos dizer que tal modelo trata questões de design relativas ao conteúdo da metacomunicação designer-usuário, relacionada ao compartilhamento de informação pessoal em RSOs. Ao fazer o projeto deste conteúdo, no momento em que está criando o seu modelo conceitual referente ao compartilhamento de informação, o designer deve tomar uma série de decisões. Não faz parte do propósito da nossa pesquisa definir um método para a aplicação do MDP, tendo em vista que o mesmo pode ser utilizado de diferentes maneiras, a critério do designer, para apoiar suas decisões. No entanto, apresentamos nesta seção uma sugestão de como o MDP pode ser utilizado no processo de design de privacidade para apoiar decisões sobre quais seriam os tipos de comunicação que representam as oportunidades de compartilhamento de informações pessoais dos usuários, e a maneira como as dimensões de privacidade do MDP são tratadas em cada um desses tipos de comunicação. Assim, ao refletir sobre os valores e controles atribuídos às dimensões de privacidade para cada tipo de comunicação identificado, o designer estará considerando como ele pode fornecer aos usuários diferentes níveis de privacidade. Essas decisões correspondem a encontrar respostas para as questões mostradas

nas subseções 4.2.1 e 4.2.2.

4.2.1 Quais são as principais oportunidades nas quais informações pessoais dos usuários podem ser compartilhadas?

De acordo com a nossa sugestão de uso do MDP, o primeiro passo a ser realizado no design do compartilhamento de informações pessoais seria definir [4] os tipos de comunicação que representam as oportunidades de compartilhamento de informação pessoal dentro do sistema, que podem despertar questões de privacidade em seus usuários. Isso permite que o designer elabore o seu modelo inicialmente de forma isolada, tomando decisões sobre valores e controles referentes às dimensões de privacidade para cada um desses tipos de comunicação. Assim, o conjunto de decisões tomadas pelo designer, considerando todos os tipos de comunicação, irá formar o modelo conceitual de privacidade referente ao compartilhamento de informação pessoal do sistema.

No Facebook, por exemplo, os tipos de comunicação, referentes ao compartilhamento de informações pessoais dentro do sistema, são os seguintes:

(1) O indivíduo compartilha informação pessoal em seu perfil;

(2) O indivíduo compartilha informação pessoal em sua linha do tempo;

(3) O indivíduo compartilha informação que potencialmente caracteriza seu ponto de vista ou opinião, ou o identifica de alguma forma, na linha do tempo de outro usuário (exemplos: curtir ou comentar postagens de outros usuários, ou confirmar sua presença em um evento);

(4) Outros usuários compartilham informação pessoal do indivíduo na linha do tempo do próprio indivíduo;

(5) Outros usuários compartilham informação pessoal do indivíduo em sua própria linha do tempo (exemplo: marcar o indivíduo em uma postagem ou foto).

Após definir os tipos de comunicação referentes às oportunidades de compartilhamento de informações pessoais dos usuários através do sistema, de acordo com a nossa

[4] Caso o MDP esteja sendo usado como ferramenta de análise de uma RSO existente, ao invés de *definir* os tipos de comunicação, seria *identificar* os tipos de comunicação existentes na RSO em questão.

sugestão de uso do MDP, o designer irá decidir[5] se haverá dimensões cujos valores serão definidos no nível de sistema, ou seja, definidos por ele mesmo, em tempo de design, e que serão fixos para todos os tipos de comunicação do sistema, e já então definir os valores para tais dimensões. No ResearchGate, por exemplo, o valor da dimensão **fonte de informação** é definido no nível de sistema como sendo *"indivíduo"*, ou seja, o sistema define (em tempo de design) que apenas o indivíduo pode ser a fonte de informação sobre si mesmo, sendo esse valor fixo para todos os tipos de comunicação.

Após definir os tipos de comunicação e as dimensões de privacidade cujos valores são fixos no sistema, o designer poderá modelar tais tipos de comunicação de acordo com as dimensões de privacidade do MDP, conforme detalhado a seguir.

4.2.2 Para cada uma das oportunidades de compartilhamento de informação pessoal identificadas, como as dimensões de privacidade serão tratadas?

Para cada um dos tipos de comunicação identificados a partir da resposta à questão apresentada na subseção anterior, o designer poderá decidir sobre os seguintes aspectos relacionados a cada uma das dimensões de privacidade do MDP cujos valores não são fixos no sistema (e que, portanto, não tiveram os seus valores definidos anteriormente):

- Em que momento o valor da dimensão será definido? Em tempo de design, ou em tempo de uso?

  (1) Caso seja em tempo de design (ou seja, o valor da dimensão é definido no nível de tipo de comunicação, mantendo-se o mesmo para todas as suas instâncias e o **controle** é do sistema), qual é o **valor** da dimensão definido pelo designer?

  (2) Caso seja em tempo de uso (ou seja, o valor da dimensão é definido no nível de instância de comunicação):

  a. Quem é o responsável por definir o valor da dimensão (ou seja, de quem é o **controle** sobre a dimensão)?

  i. Se o responsável (controle) é definido com base em um processo de decisão definido pelo designer, levando em consideração o valor de alguma outra dimensão (ou seja, existe uma **dependência de controle** para a dimensão), qual é essa outra dimensão?

[5] Caso o MDP esteja sendo usado como ferramenta de análise de uma RSO existente, esta atividade, que aí não é mais o designer decidir, mas sim identificar dimensões cujos valores são fixos no sistema, é realizada apenas ao final da modelagem de todos os tipos de comunicação do sistema.

ii. Se não, quem é o responsável por definir o valor da dimensão?

1. O indivíduo

2. Outro usuário

3. O sistema

a. O valor da dimensão é definido com base em um processo de decisão definido pelo designer, levando em consideração o valor de alguma outra dimensão (ou seja, existe uma **dependência de valor** para a dimensão)? Se sim, qual é essa outra dimensão?

b. Quais são os possíveis **valores** que a dimensão pode assumir?

Ao modelar as comunicações referentes ao compartilhamento de informações pessoais no sistema, a primeira decisão a ser tomada pelo designer é em relação ao momento em que os valores das dimensões de privacidade do MDP serão definidos, o que define o nível de flexibilidade que o sistema irá conceder ao usuário em relação a como atingir o seu estado desejado de privacidade. Assim, quando o designer atribui valores às dimensões, em tempo de design, o mesmo está definindo os níveis de privacidade que serão remetidos por tais dimensões, concedendo ao sistema o controle, total ou parcial, sobre o estado de privacidade que poderá ser atingindo pelos seus usuários. Por outro lado, quando a atribuição de valores às dimensões é feita em tempo de uso, a decisão do designer é no sentido de prover flexibilidade ao usuário para alcançar o seu estado desejado de privacidade.

Neste ponto, vale salientar que embora a opção de deixar o usuário decidir sobre os seus níveis de privacidade pareça ser melhor, uma vez que permite este tome decisões sobre o que considera apropriado no seu contexto de uso [Nissenbaum, 2004], a mesma, quando comparada à opção de designers decidirem sobre os valores para as dimensões em tempo de design, apresenta custos adicionais tanto para usuários quanto para designers. O custo adicional para os usuários está relacionado a todas as decisões que deverão tomar no sentido de alcançarem seu estado desejado de privacidade. Essas decisões podem também envolver a compreensão de todos os parâmetros disponíveis e seus efeitos potenciais no tempo [Pereira Junior et al., 2014, 2013; Prates et al., 2015]. O custo adicional para designers, por sua vez, está relacionado a decisões sobre como deveriam expressar os parâmetros, seus valores e efeitos na interface do sistema, no sentido de permitir que usuários gerenciem efetivamente a sua privacidade.

4.3 A Representação Visual do MDP

Como podemos perceber a partir das questões que guiam designers no uso do MDP, apresentadas na seção anterior, existe um número considerável de decisões a serem tomadas pelos mesmos durante o design do compartilhamento de informações pessoais em RSOs. Além disso, uma vez que o designer toma todas as decisões necessárias, pode não ser fácil para ele ter uma visão geral dos possíveis estados de privacidade definidos como consequência de suas decisões. Dessa forma, com o objetivo de facilitar que se tenha uma visão geral da decisões do designer ao fazer uso do MDP, bem como dos estados de privacidade possíveis resultantes, propomos uma representação visual para o mesmo. Tal representação descreve cada uma das dimensões de privacidade como um hexágono. A borda do hexágono representa o valor atribuído ao controle da dimensão, e o seu preenchimento representa o valor atribuído à mesma.

Para a nossa proposta de representação visual, baseamos-nos na ideia apresentada por Smith [2007], ao propor o *social software honeycomb*, um framework que contempla uma lista de elementos que fornecem uma definição funcional para software social, como ilustrado na Figura 4.14. Nessa figura, que caracteriza os blocos de construção de um sistema específico, cada hexágono corresponde a um elemento de software social, sendo que os hexágonos preenchidos com a cor cinza escuro correspondem a elementos essenciais nos quais o sistema é focado; os preenchidos com uma gradação mais clara de cinza correspondem a outros elementos que são implementados pelo sistema e os hexágonos em branco correspondem a elementos que não são explicitamente considerados no mesmo.

Figura 4.14. Representação gráfica do framework *honeycomb* [Smith, 2007]

Na representação visual do MDP, cada tipo de comunicação correspondente a uma oportunidade de compartilhamento de informação pessoal no sistema é represen-

tado como um *"honeycomb"*, formado por hexágonos que representam cada uma das dimensões de privacidade do MDP. A disposição das dimensões de privacidade no *"honeycomb"* segue a ordem em que as mesmas são mostradas na estrutura do MDP, como ilustrada na Figura 4.15. No centro do *"honeycomb"* é colocada a descrição referente ao tipo de comunicação representado pelo mesmo.

Figura 4.15. Disposição das dimensões de privacidade do MDP na representação visual de um tipo de comunicação

Para cada uma das dimensões de privacidade representadas no *"honeycomb"*, uma escala de tons de cinza está associada aos possíveis valores que a dimensão pode assumir em tempo de design. Assim, quanto mais escuro for o tom de cinza, maior é o nível de privacidade que o valor da dimensão representa, como mostrado na Tabela 4.1. Caso o valor para a dimensão seja definido em tempo de uso, o hexágono correspondente ficará sem preenchimento (equivalente à cor branca na representação visual) e o conjunto de valores que poderão ser atribuídos à mesma são listados em formato textual.

Como o MDP é qualitativo, as suas dimensões possuem diferentes gradações de valores. Assim, como mostrado na Figura 4.3, algumas dimensões vão apresentar possibilidades de valores/cores que remetem a todos os níveis de privacidade, enquanto outras vão apresentar possibilidades de valores que remetem a apenas alguns desses níveis. Nesse caso, é feito um mapeamento valor-cor, de forma que o valor que remete ao nível mais alto de privacidade dentro da dimensão é sempre mapeado no tom mais escuro de cinza, e aquele que remete ao nível mínimo de privacidade no tom mais claro, enquanto que o valor referente ao nível intermediário de privacidade será mapeado também no tom intermediário de cinza.

Neste ponto, vale salientar que a dimensão **informação do indivíduo** é representada no *"honeycomb"* apenas através de sua subdimensão **conteúdo**, tendo em vista

Tabela 4.1. Escala de cinza para os hexágonos correspondentes aos valores das dimensões do MDP

Cor/tonalidade	Descrição
	Valor da dimensão remete a um nível alto de privacidade
	Valor da dimensão remete a um nível médio-alto de privacidade
	Valor da dimensão remete a um nível médio de privacidade
	Valor da dimensão remete a um nível médio-baixo de privacidade
	Valor da dimensão remete a um nível baixo de privacidade
	Valor da dimensão definido em tempo de uso, no nível de instância de comunicação
	Valor da dimensão não aplicável ao tipo de comunicação

que são os seus valores que estão associados a níveis de privacidade dentro da dimensão. Assim, na representação visual do MDP, iremos nos referir a tal dimensão como **conteúdo da informação**.

A borda do hexágono representa o momento em que a definição de valor para a dimensão ocorre, se em tempo de uso ou em tempo de design. Neste último caso, a borda caracteriza outros aspectos específicos em relação ao escopo do valor da dimensão (nível de sistema ou nível de tipo de comunicação). Além disso, a borda também representa quem tem o controle sobre a dimensão, ou seja, quem pode definir os seus valores, como mostrado na Tabela 4.2. Assim, as dimensões cujos valores são definidos em tempo de design possuem suas bordas representadas através de linhas sólidas, com a seguinte diferenciação, relacionada ao nível em que os valores são definidos:

(a) dimensões cujos valores são definidos no nível de sistema, ou seja, seus valores são os mesmos para todos os tipos de comunicação, são representadas através bordas simples com traço sólido e espesso;

(b) dimensões cujos valores são definidos no nível de tipo de comunicação, ou seja, seus valores permanecem os mesmos para todas as instâncias de determinado tipo de comunicação, são representadas com bordas simples com traço sólido.

Já as dimensões cujos valores são definidos em tempo de uso (podendo variar para cada instância de comunicação) são representadas com bordas simples de traço

não contínuo, diferenciadas de acordo com a definição do controle sobre as mesmas, da seguinte forma:

(a) dimensões cujo controle é do sistema, ou seja, possuem seus valores definidos pelo sistema, são representadas com bordas de tracejado longo;

(b) dimensões cujo controle é do indivíduo ao qual a informação se refere, ou seja, o indivíduo define seus valores, são representadas com bordas de traços e pontos;

(c) dimensões cujo controle é de outro usuário, ou seja, outro usuário que não seja o indivíduo ao qual a informação se refere define seus valores, são representadas com bordas de tracejado curto;

(d) dimensões cujo controle também é definido em tempo de uso são representada por bordas pontilhadas.

Tabela 4.2. Bordas representado o momento em que o valor para a dimensão é definio e quem tem controle sobre ela

	Borda	Controle
Dimensão cujo valor é definido em **tempo de design** (nível de sistema ou de tipo de comunicação)		Sistema – valor fixo no sistema para todos os tipos de comunicação
		Sistema – valor fixo no tipo de comunicação
Dimensão cujo valor é definido em **tempo de uso** (nível de instância de comunicação)		Sistema
		Indivíduo
		Outro usuário
		Definido em tempo de uso

Conforme vimos anteriormente, na seção 4.2, o MDP permite também modelar a existência de dependências entre duas dimensões, seja de controle ou de valor, que ocorre caso a definição do controle sobre uma dimensão, ou do valor da mesma, dependa do valor de alguma outra dimensão. Entretanto, essas dependências ainda não estão sendo consideradas na representação visual do MDP.

A Figura 4.16 mostra a representação visual da modelagem, de acordo com as dimensões de privacidade do MDP, do seguinte tipo de comunicação do Facebook: *"o*

indivíduo compartilha informação pessoal em sua linha do tempo"[6]. Conforme podemos verificar nessa figura, a intenção é que a representação visual do MDP forneça ao designer uma visão geral dos possíveis estados de privacidade a serem alcançados pelos usuários para cada tipo de comunicação. Assim, quanto mais escuro for o *"honeycomb"*, maior é o estado de privacidade que será alcançado pelo indivíduo. As dimensões cujos valores são definidos em tempo de uso são representadas em branco, com a indicação da faixa de valores que lhes podem ser atribuídos. Portanto, se o *"honeycomb"* for predominamente branco, isso significa que a maioria das dimensões são definidas em tempo de uso. Uma representação alternativa, nesse caso, seria, ao invés de deixar as dimensões definidas em tempo de uso sem preenchimento e indicando a faixa de seus possíveis valores, criar para cada tipo de comunicação dois **"honeycombs"**: um representando os valores referentes ao nível máximo de privacidade para cada uma das dimensões e outro representando os valores referentes ao nível mínimo para cada uma das mesmas.

Figura 4.16. Representação dos níveis de privacidade da comunicação referente ao indivíduo compartilhar informação pessoal em sua linha do tempo no Facebook

Através das bordas dos hexágonos, a representação visual do MDP também permite que os designers identifiquem o quanto de flexibilidade e controle o sistema oferece aos seus usuários. As bordas permitem que o designer perceba, a partir de seu modelo, quem é o responsável por tomar decisões relativas aos valores a serem atribuídos às dimensões de privacidade: o indivíduo ou outros (sistema ou outros usuários). O primeiro caso caracteriza uma alta flexibilidade do sistema e alto controle por parte do indivíduo sobre o seu estado de privacidade a ser atingido dentro do sistema. O

[6]A modelagem de todos os tipos de comunicação do Facebook será mostrada no Capítulo 5

segundo caso, por outro lado, pode caracterizar uma alta flexibilidade do sistema, mas um baixo controle por parte do indivíduo, no caso da atribuição de valor à dimensão ocorrer em tempo de uso; ou ainda uma baixa flexibilidade e um baixo controle, no caso da atribuição de valor à dimensão ser feita pelo sistema em tempo de design.

Ampliando o escopo da análise, e considerando os tipos de comunicação referentes a todas as oportunidades de compartilhamento de informação pessoal dentro de um sistema, a visualização geral correspondente fornece ao designer uma ideia geral das diferenças nos níves de privacidade oferecidos por cada tipo de comunicação, bem como do estado de privacidade que os usuários podem alcançar no sistema. Portanto, se existe um grande número de tipos de comunicação no sistema, isso provavelmente significa uma maior complexidade no sentido de tratar questões de privacidade. Além disso, caso os tipos de comunicação se diferenciem em relação aos seus níveis de privacidade, isso pode ser uma indicação de que designers deveriam deixar claro para os usuários essas diferenças e o contexto em que elas se aplicam.

Com o objetivo de facilitar a geração e a avaliação da representação visual utilizada pelo MDP, foi desenvolvido um protótipo de uma ferramenta de visualização[7]. Nessa ferramenta, o usuário pode fazer a modelagem de cada tipo de comunicação referente a uma oportunidade de compartilhamento de informação pessoal dentro da RSO, fornecendo os valores para os atributos "controle" e "valor" de cada uma das dimensões do MDP. Assim, com base nesses valores, a ferramenta mostra a representação visual referente ao tipo de comunicação, como mostrado na Figura 4.17.

O uso da ferramenta de visualização permite que designers criem modelagens para o compartilhamento de informações pessoais em RSOs, através das dimensões do MDP, de forma mais eficiente. Assim, através da representação visual dos modelos MDP, gerada por tal ferramenta, designers possuem uma visão mais clara do impacto de suas decisões de modelagem nos estados de privacidade que podem ser alcançados pelos usuários dentro do sistema.

[7]Desenvolvido como trabalho de iniciação científica da aluna Lídia Ferreira, com a orientação da autora desta tese, do aluno de doutorado Diego Augusto Faria Barros, e das professoras Raquel Prates e Raquel Minardi. Disponível em http://homepages.dcc.ufmg.br/~lidiaferreira/mdp_beta/modeling_privacy/.

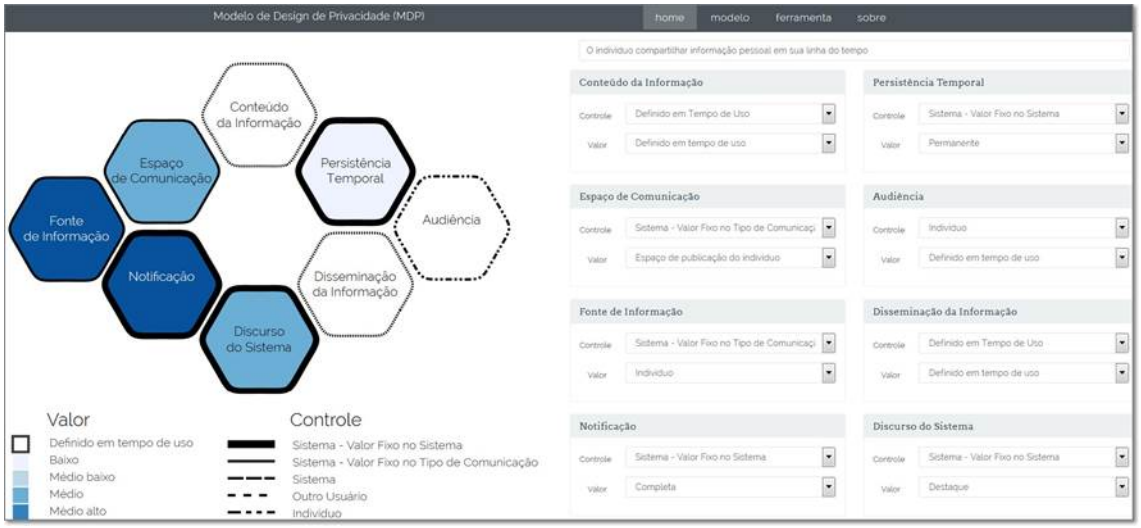


Figura 4.17. Tela do protótipo da ferramenta de visualização do MDP

Capítulo 5

Avaliação

Este capítulo apresenta e discute os principais resultados da avaliação que efetuamos do Modelo de Design de Privacidade (MDP), com o objetivo de coletar indicadores qualitativos sobre a sua expressividade. Para isso, identificamos os seguintes aspectos a serem investigados:

- **Questão de Avaliação 1 (QA1):** As dimensões de privacidade do MDP são capazes de expressar decisões de privacidade em RSOs?
- **Questão de Avaliação 2 (QA2):** O MDP é descritivo o suficiente para expressar as diferenças em aspectos de privacidade em RSOs?

A seguir, na seção 5.1, apresentamos as considerações metodológicas da avaliação da expressividade do MDP. Em seguida, na seção 5.2, mostramos como a avaliação foi executada, e, por fim, os resultados obtidos são mostrados nas seções 5.3, 5.4 e na seção 5.5.

5.1 Considerações Metodológicas

A fim de explorar as QA1 e QA2, fizemos a decisão metodológica de basear a avaliação na análise de RSOs existentes. Tal decisão foi tomada por dois motivos: o primeiro deles é que, ao fazer a modelagem de privacidade de RSOs existentes, nós garantimos que estamos considerando aspectos relevantes de privacidade que o MDP deveria ser capaz de expressar. O segundo motivo considerado foi a viabilidade da avaliação, uma vez que não seria fácil (ou mesmo viável) avaliar o MDP em um contexto real em que uma RSO estivesse sendo projetada[1].

[1]Coletar indicadores sobre o uso do MDP durante um processo real de design iria exigir ou a criação de dois modelos de privacidade paralelos (um elaborado com o uso do MDP e o outro elaborado sem

Dessa forma, a avaliação do MDP foi então planejada para ser executada em dois passos: o primeiro passo, descrito na seção 5.3, foi denominado "avaliação com especialista", e envolveu a análise de RSOs existentes, efetuada pela autora desta tese (especialista no MDP), e criação dos seus modelos MDP, com base nas decisões de seus designers. Os modelos obtidos para cada uma das RSOs analisadas produziu dados para responder a QA1. A comparação entre modelos gerados para cada RSO e a análise das diferenças entre eles nos forneceu dados para responder a QA2.

O segundo passo da avaliação, descrito na seção 5.4, foi denominado "avaliação com potenciais usuários", tendo em vista que envolveu designers de sistemas, que representam potenciais usuários do MDP. Assim, um teste com designers foi então projetado. A fim de coletar dados para responder a QA1, foi solicitado que eles descrevessem as decisões de design de privacidade, usando as dimensões do MDP, para um tipo de comunicação específico de uma RSO que havia sido analisada na avaliação pelo especialista. Para coletar dados que nos permitissem responder a QA2, foi fornecido aos designers os modelos MDP referentes a dois tipos de comunicaçao de duas das RSOs analisadas no passo anterior, e entao solicitado que eles descrevessem as diferenças que podiam perceber entre os dois sistemas.

A metodologia utilizada nesta avaliação segue o paradigma não preditivo em ciência e faz uso de métodos qualitativos interpretativos [Denzin & Lincoln, 2008]. Métodos qualitativos são apropriados para estudos como o nosso, que visam explorar extensivamente e com maior profundidade uma questão de pesquisa específica (no caso do nosso estudo, caracterizada pelas QA1 e QA2). Alcançamos isso envolvendo um grupo pequeno de participantes, especificamente no segundo passo da avaliação, buscado identificar os significados e interpretações que os mesmos atribuíram ao MDP. Dessa forma, nós fomos capazes de investigar como os participantes elaboraram e utilizaram tais significados e interpretações para modelarem o compartilhamento de informações pessoais em uma RSO, e também para compreenderem as modelagens realizadas por um especialista no MDP.

Por fim, os resultados obtidos no segundo passo da avaliação foram triangulados com os resultados obtidos no primeiro passo, buscando por consistência entre eles (como é típico em validação de pesquisa qualitativa), no sentido de gerar diferentes perspectivas sobre a expressividade do MDP. A triangulação tem como objetivo proporcionar diversidade nas condições de descoberta de conhecimento, refletindo uma

fazer uso do mesmo) para serem comparados, ou, uma vez que o modelo de privacidade do sistema fosse criado, usar o MDP para descrevê-lo e então analisar que novas considerações (se houver alguma) os designers fariam a partir do seu uso. Ambas as opções envolveriam o aumento de recursos (e assim também do custo) investidos no design do sistema sendo desenvolvido, o que poderia inviabilizar a avaliação do MDP em um contexto real de design.

compreensão aprofundada do fenômeno em questão [Cairns & Cox, 2008].

Para validar os resultados de um estudo qualitativo, a triangulação pode ser feita de diferentes maneiras, ou seja, pode-se fazer a triangulação de dados, de investigador, de teoria e de métodos. Tais triangulações consistem em fazer uso de múltiplas fontes de dados, múltiplos investigadores, múltiplas teorias e múltiplos métodos, respectivamente, para investigar o mesmo fenômeno [Cairns & Cox, 2008]. Nós fizemos a triangulação de métodos, ao comparar e contrastar os resultados obtidos nos dois passos da avaliação, acima descritos. Foram utilizadas fontes endógenas, que "referem-se ao mesmo artefato de design ou artefatos que compartilham o mesmo modelo de domínio" [de Souza et al., 2010, p.29], para validar os conhecimentos obtidos, ao fazer uso das mesmas RSOs nos dois passos da avaliação.

5.2 Execução

A primeira decisão necessária para conduzir a avaliação foi definir quais seriam as RSOs a serem analisadas. O objetivo era escolher RSOs que fossem amplamente utilizadas e que fossem voltadas para contextos distintos. A diferença entre os contextos era interessante no sentido de possibilitar que diferentes aspectos e considerações relacionados à privacidade fossem analisados, tendo em vista que o contexto é um fator determinante em decisões de privacidade [Nissenbaum, 2004]. Assim, escolhemos, para o primeiro passo da avaliação, o Facebook[2], que é uma RSO de propósito geral, o ResearchGate[3], que é uma RSO que visa conectar pesquisadores e compartilhar conhecimento científico, e o CaringBridge[4], que é uma RSO destinada a fornecer suporte emocional a pessoas que estejam passando por problemas de saúde. Para o segundo passo da avaliação, realizada com potenciais usuários do MDP, foram utilizados apenas os dois primeiros sistemas, ou seja, o Facebook e o ResearchGate.

A avaliação com especialista envolveu uma análise sistemática de cada uma das três RSOs selecionadas, inspecionando os signos presentes em suas interfaces. Inicialmente, para cada sistema, foram identificados os tipos de comunicação que representam as oportunidades para compartilhamento de informação pessoal dos seus usuários. Em seguida, para cada um desses tipos de comunicação, foram identificadas as decisões dos designers em relação às dimensões de privacidade do MDP. As análises do Facebook, ResearchGate e CaringBrige foram realizadas entre julho e outubro de 2015 e, uma vez

[2]www.facebook.com
[3]www.reseachgate.net
[4]www.caringbridge.org

que a análise de cada um desses sistemas foi concluída, a comparação entre os três foi então conduzida.

Para a avaliação com potenciais usuários do MDP, seis designers de sistemas foram convidados para participar. Como queríamos investigar a compreensão do MDP e o seu potencial para aumentar o entendimento do designer sobre privacidade relacionada ao compartilhamento de informações pessoais em RSOs, era importante que os participantes tivessem um bom nível de conhecimento de design de IHC.

A avaliação com potenciais usuários foi realizada em uma única sessão, no dia 17 de dezembro de 2015, no Departamento de Ciência da Computação da UFMG, com duração aproximada de 03 horas e meia, e consistiu de três etapas: apresentação do MDP, execução das tarefas e grupo focal. Cabe salientar que a estrutura aqui mostrada para a avaliação foi obtida após a execução de um teste piloto, realizado inicialmente, com a finalidade de verificar a exequibilidade das tarefas solicitadas durante o teste com usuários e refinar o mesmmo.

Assim, na primeira etapa, foi informado aos participantes o objetivo da avaliação, e coletado o consentimento dos mesmos, através da assinatura do termo de consentimento (veja Apêndice C – Termo de Consentimento Livre e Esclarecido). Ainda nesta etapa, os participantes responderam a um questionário (veja ApêndiceC – Questionário Pré-Teste), com questões sobre a sua experiência de uso de RSOs, bem como sua experiência em design de IHC e seu conhecimento sobre Engenharia Semiótica e suas ferramentas epistêmicas. A primeira etapa foi encerrada com uma apresentação sobre o MDP (veja Apêndice C – Apresentação do MDP), que teve duração aproximada de 30 minutos, e explicou a sua proposta geral, suas dimensões e valores, sua representação visual, e exemplos do seu uso na modelagem de uma RSO existente.

Em seguida, na segunda etapa da avaliação com potenciais usuários, cada participante recebeu material impresso contendo uma visão geral do MDP: representação gráfica (incluindo as Figuras 4.1 e 4.3) e uma breve descrição de cada dimensão, seus possíveis valores, bem como as possíveis definições para o controle, e os níveis de privacidade associados ao valores das dimensões (veja Apêndice C – Glossário do MDP). Foi então solicitado aos participantes que executassem as seguintes tarefas:

- **Tarefa 1:** os participantes deveriam definir o valor e o controle para cada dimensão do MDP para um tipo específico de comunicação do Facebook;

- **Tarefa 2:** os participantes deveriam discutir, em duplas, os modelos que criaram individualmente, identificando diferenças entre eles, e gerando (se possível) um modelo consolidado;

- **Tarefa 3:** foram apresentados aos participantes os modelos MDP referentes a dois tipos de comunicação de duas RSOs distintas e solicitado então que discutissem (também em duplas) e registrassem, com base apenas nesses modelos, as diferenças percebidas entre os dois sistemas, no que tange à privacidade relacionada ao compartilhamento de informação pessoal;
- **Tarefa 4:** os participantes foram informados que as RSOs analisadas na tarefa 3 eram voltadas para diferentes contextos (propósito geral e colaboração científica) e então solicitado que associassem cada RSO, com base em seus modelos, a um contexto específico e justificassem a sua escolha.

A execução das tarefas, durante o teste com usuários, foi dividida em duas partes: a primeira parte abrangeu as tarefas 1 e 2, descritas acima, e teve o objetivo de responder a QA1 ("As dimensões de privacidade do MDP são capazes de expressar decisões de privacidade em RSOs?"). Essa parte do teste foi realizada com base em um cenário (veja Apêndice C – Cenário), em que o participante supostamente trabalhava em uma equipe que estava fazendo a modelagem reversa do compartilhamento de informações pessoais no Facebook, a fim de identificar aspectos que pudessem despertar questões de privacidade em seus usuários. Assim, considerando que na avaliação pelo especialista os tipos de comunicação do Facebook já haviam sido identificados, na tarefa 1 solicitamos aos participantes que modelassem, usando as dimensões de privacidade do MDP, o seguinte tipo de comunicação do Facebook: *"o indivíduo compartilha informação sobre si mesmo em sua linha do tempo"*. Para isso, os participantes deveriam preencher uma tabela, fornecendo o valor e o controle[5] relacionado a cada uma das dimensões do MDP. Como todos os participantes eram usuários experientes do Facebook, eles deveriam criar o modelo com base em sua própria experiência no sistema (e não acessando o sistema e realizando uma análise do mesmo durante a avaliação). O objetivo específico dessa primeira tarefa foi verificar se os participantes conseguiam usar o MDP como ferramenta de modelagem.

Na segunda tarefa, foi solicitado que os participantes se unissem em duplas, a fim de discutirem as modelagens que cada um fez individualmente na primeira tarefa, tentando gerar um modelo consolidado. Os participantes deveriam também registrar as diferenças que porventura tivessem ocorrido na atribuição de valor e controle para cada dimensão do MDP, as razões de tais diferenças (por exemplo: diferença no entendimento do Facebook, diferença no entendimento do MDP, ou alguma outra razão)

[5]Em relação aos valores para o atributo "controle" referentes a "sistema", foi solicitado que os participantes diferenciassem apenas entre "sistema – valor definido em tempo de design" e "sistema – valor definido em tempo de uso", não sendo necessário diferenciar, no primeiro caso, se o valor era fixo no tipo de comunicação ou no sistema.

e o valor consolidado (caso a dupla tenha sido capaz de chegar ao mesmo). Além disso, caso tivessem chegado a um modelo consolidado, os participantes deveriam então registrá–lo através da representação visual, fazendo uso do protótipo da ferramenta de visualização desenvolvida para dar suporte ao uso do MDP, mencionada na seção 4.3 do Capítulo 4. O objetivo dessa segunda tarefa foi verificar se houve diferença no entendimento dos participantes sobre o MDP, refletido em diferentes modelagens realizadas pelos mesmos individualmente na primeira tarefa, bem como verificar se os participantes, em duplas, conseguiriam obter um entendimento consolidado do MDP.

A segunda parte do teste com usuários abrangeu as tarefas 3 e 4 e teve o objetivo de responder a QA2 ("O MDP é descritivo o suficiente para expressar as diferenças em aspectos de privacidade em RSOs?"). Para isso, foram apresentadas aos participantes os modelos MDP do Facebook e do ResearchGate, referentes aos seguintes tipos de comunicação: (1) "o indivíduo compartilha informação em seu perfil", e (2) "o indivíduo compartilha informação sobre si em seu espaço de publicação". Tais modelagens foram apresentadas utilizando tanto a representação textual (em uma tabela contendo cada dimensão e os valores correspondentes dos atributos "valor" e "controle") quanto a representação visual (veja Apêndice C – Tarefa 3). No entanto, não foi informado aos participantes a quais RSOs tais modelos se referiam, sendo apenas informado que eram duas RSOs distintas, referenciadas como RSO 1 (Facebook) e RSO 2 (ResearchGate). A razão para isso era que os participantes utilizassem apenas as informações transmitidas a partir das dimensões do MDP, e não seus conhecimentos ou experiências prévias sobre os sistemas, no sentido de identificar as diferenças de privacidade entre os mesmos. Assim, na tarefa 3, foi solicitado aos participantes que, mantendo as mesmas duplas formadas na tarefa anterior, discutissem e registrassem, por escrito, as diferenças de privacidade que conseguiram perceber entre a RSO 1 e a RSO 2, e suas implicações gerais no sistema, com base nos modelos MDP das mesmas. O objetivo dessa tarefa foi verificar se os participantes eram capazes de entender as diferenças de privacidade entre duas RSOs, a partir da modelagem gerada com o uso do MDP.

Ainda mantendo–se as mesmas duplas, na quarta tarefa os participantes foram apenas informados que uma das RSOs cuja modelagem lhes foi apresentada na tarefa 3 era de propósito geral e a outra era de propósito profissional, e então foi solicitado que eles identificassem, com base nos modelos MDP das mesmas, qual era referente a qual contexto, registrando por escrito o motivo pelo qual chegaram a tal conclusão. O objetivo específico dessa tarefa foi verificar se os participantes conseguiam identificar o contexto de uso das RSOs em função da forma como a privacidade é caracterizada a partir do compartilhamento de informações pessoais modelado com o uso do MDP.

A execução em duplas das tarefas 2, 3 e 4 ocorreu com o objetivo de permitir

que os participantes discutissem suas compreensões, ideias e impressões sobre o MDP, enquanto realizavam as tarefas, proporcionando–lhes um entendimento mais sólido do referido modelo, além de enriquecer as evidências empíricas coletadas a partir do seu uso. Além disso, nessas mesmas tarefas, além da expressividade do MDP, que consistiu no objetivo geral da avaliação, buscamos avaliar também a sua representação visual, ao solicitar que os participantes utilizassem o protótipo da ferramenta de visualização, na tarefa 2, e ao permitir que as representações visuais das modelagens das RSOs fossem utilizadas durante a realização das tarefas 3 e 4.

Por fim, na terceira etapa da avaliação com potenciais usuários, os participantes participaram de um grupo focal sobre o teste (veja Apêndice C – Roteiro do Grupo Focal), quando tiveram oportunidade de falar sobre suas impressões relacionadas às dimensões do MDP e ao seu uso na modelagem de privacidade de RSOs, bem como seu potencial para despertar reflexões sobre aspectos de privacidade envolvidos no compartilhamento de informações pessoais nesses sistemas. Também foram exploradas, durante o grupo focal, as opiniões dos participantes sobre a utilidade da representação visual do MDP, bem como da ferramenta de visualização que se propõe a dar suporte ao seu uso.

Os seguintes materiais foram coletados durante o teste com designers: (1) termo de consentimento assinado pelos participantes; (2) questionários pré-teste preenchido pelos participantes; (3) modelagem do tipo de comunicação específico do Facebook realizada na tarefa 1; (4) tabelas com o registro das diferenças e consensos de modelagens entre os integrantes das duplas, geradas na tarefa 2, e (5) representações visuais das modelagens consolidadas geradas com o uso da ferramenta de visualização, durante a execução da tarefa 2; (6) constatações por escrito feitas pelas duplas sobre as diferenças percebidas no que tange à privacidade dos sistemas cujas modelagens lhes foram apresentadas, na tarefa 3; (7) respostas registradas por escrito pelas duplas sobre a identificação das redes de propósito geral e profissional e suas justificativas; e, finalmente, (8) o áudio de todas as discussões de cada uma das duplas, nas tarefas 2, 3 e 4, bem como do grupo focal, que foram transcritos para que pudessem ser devidamente analisados, juntamente com todo o material gerado.

As principais evidências empíricas utilizadas nesta parte da pesquisa foram os modelos criados pelos participantes, além de seus discursos sobre os mesmos e também sobre as modelagens prontas que lhes foram apresentadas. Além disso, temos também como evidências empíricas as impressões e opiniões que os participantes expressaram, ao final do teste, durante o grupo focal.

5.3 Avaliação com Especialista

Nesta seção, apresentamos os principais resultados da modelagem reversa que realizamos do Facebook, do ResearchGate e do CaringBridge, fazendo uso das dimensões do MDP. Como mencionado na seção anterior, o primeiro passo consistiu na análise de cada uma dessas RSOs, no sentido de identificar os tipos de comunicação referentes às oportunidades de compartilhamento de informação pessoal que existem dentro delas. Assim, nas seções 5.3.1, 5.3.2 e 5.3.3, apresentaremos em detalhes a análise que efetuamos para um tipo específico de comunicação de cada uma das RSOs: Facebook, ResearchGate e CaringBridge. Para os demais tipos de comunicação desses sistemas, apresentaremos apenas a modelagem final, mostrando, para cada um deles, os valores referentes às dimensões de privacidade do MDP, tanto em formato de tabela quanto utilizando a sua representação visual. Cabe salientar que os valores nessas tabelas e visualizações representam a nossa interpretação sobre as decisões do designer, obtidas com base na análise dos signos presentes em sua metacomunicação. Os resultados completos das análises de cada um desses três sistemas encontra-se no Relatório Técnico [Villela & Prates, 2015a].

5.3.1 O compartilhamento de informações pessoais no Facebook

No Facebook[6], o indivíduo pode compartilhar informação pessoal em seu perfil e em sua linha do tempo, bem como na linha do tempo de outros usuários (por exemplo, quando ele curte ou comenta postagens de outros usuários, ou quando efetua uma postagem diretamente na linha do tempo de um amigo). Outros usuários também podem compartilhar informação pessoal sobre o indivíduo, seja postando algo na linha do tempo do indivíduo ou o marcando em uma postagem realizada em sua própria linha do tempo.

Assim, os tipos de comunicação que representam as diferentes oportunidades de compartilhamento de informação pessoal do indivíduo no Facebook são os seguintes:

(1) O indivíduo compartilha informação pessoal em seu perfil;

(2) O indivíduo compartilha informação pessoal em sua linha do tempo;

[6]Todos os termos referentes à interface do Facebook são apresentados em português nesta tese, embora tenha sido analisada a interface em inglês deste sistema, como pode ser observado nas figuras que mostram as telas do Facebook, exibidas nesta seção.

(3) O indivíduo compartilha informação que potencialmente caracteriza seu ponto de vista ou opinião, ou o identifica de alguma forma, na linha do tempo de outro usuário (exemplos: efetuar postagem, curtir ou comentar postagens de outros usuários);

(4) Outros usuários compartilham informação pessoal do indivíduo na linha do tempo do próprio indivíduo;

(5) Outros usuários compartilham informação pessoal do indivíduo em sua linha do tempo (exemplo: marcar o indivíduo em uma postagem ou foto).

A seguir, apresentaremos a explicação detalhada sobre como o tipo de comunicação (1), mostrado acima, foi modelado de acordo com as dimensões de privacidade do MDP. A nossa interpretação sobre as decisões do designer em relação a tais dimensões são apresentadas na Tabela 5.1.

Neste caso, a **fonte de informação** é o próprio *"indivíduo"* e o **espaço de comunicação** é o *"espaço de perfil do indivíduo"*, conforme especificado no próprio tipo de comunicação. Em relação à **expressão** da informação compartilhada, esta será sempre no formato *"tipada"*, sendo o seu significado e, portanto, o nível de pessoalidade referente ao seu **conteúdo**, definido pelo sistema. Assim, o nível de pessoalidade referente ao conteúdo compartilhado no perfil do indivíduo pode variar desde *pouco pessoal* até *muito pessoal*, tendo em vista que o perfil contém várias informações sobre o indivíduo, abrangendo desde o local de estudo ou trabalho, que é considerado pouco pessoal, até endereço e número de telefone, que estão no nível muito pessoal [Villela et al., 2015a]. Já a **persistência temporal** referente às informações postadas no perfil do indivíduo é *"permanente"*, tendo em vista que ficam acessíveis para a sua audiência durante todo o tempo de sua existência, ou seja, enquanto ela não for excluída pelo usuário.

A dimensão **audiência**, neste caso, possui o seu controle variando de acordo com as características da informação que está sendo compartilhada, da seguinte forma: (a) se a informação fizer parte do perfil público do usuário (como "nome", "gênero", "nome de usuário", "ID do usuário", "foto de perfil" e "foto de capa"), o Facebook já define a sua audiência, em tempo de design, como sendo *"pública"*, que remete ao valor *"ilimitada"* para a dimensão em questão do MDP; (b) caso seja outra informação que compõe o perfil do usuário, este tem o controle para definir o valor de tal dimensão, em tempo de uso. Neste caso, o valor pode variar desde um alto nível de privacidade, que corresponde à opção *"somente eu"* na interface (equivalente ao valor *"indivíduo"* para dimensão no MDP), até um nível muito baixo de privacidade, que corresponde à opção *"público"* na

Tabela 5.1. Modelagem do tipo de comunicação (1) do Facebook

		Controle	Valor*	Dependência de controle	Dependência de valor
Fonte de informação		Sistema – tempo de design	"indivíduo"	Na**	Na
Espaço de comunicação		Sistema – tempo de design	"espaço de perfil do indivíduo"	Na	Na
Informação do indivíduo	**Expressão**	Sistema – tempo de design	"tipada"	Na	Na
	Conteúdo	Sistema - tempo de uso	{"pouco pessoal", "levemente pessoal", "pessoal", "um tanto pessoal", "muito pessoal"}	Na	**Informação*** **
Persistência temporal		Sistema – tempo de design	"permanente"	Na	Na
Audiência		Definido em tempo de uso	"ilimitada" ou {"indivíduo", "selecionada", "limitada", "ilimitada"}	**Informação**	**Informação**
Notificação para o indivíduo		Sistema – tempo de design	"completa"	Na	Na
Discurso sobre o indivíduo		Sistema – tempo de design	"destaque"	Na	Na
Disseminação da informação		Sistema - tempo de uso	{"ausente", "ilimitada"}	Na	**Informação**

*Quando os valores aparecem entre chaves, indica–se que a dimensão terá seu valor definido em tempo de uso, podendo assumir qualquer valor desse conjunto.
**Não se aplica.
***Características específicas da informação compartilhada que não são representadas através de valores atribuídos à dimensão **Informação do indivíduo**.

interface (equivalente ao valor *"ilimitada"* para a dimensão no MDP), passando pela possibilidade de compartilhar com todos os *"amigos"* ou um grupo *"personalizado"* de usuários (equivalentes ao valor *"selecionado"* para dimensão do MDP), como pode ser visto na Figura 5.1.

Em relação à dimensão **notificação para o indivíduo**, seu valor é *"completa"*, tendo em vista que o Facebook notifica o indivíduo sempre que outros usuários curtem, comentam ou compartilham (neste caso especificamente para foto de perfil) as informações que ele compartilha em seu perfil, como mostrado na Figura 5.2.

O **discurso sobre o indivíduo** do Facebook, no nível direto, sobre algumas informações compartilhadas no perfil do indivíduo ocorre através dos recursos *Feed de Notícias* e *Novidades*, mostrados respectivamente nos itens (a) e (b) da Figura 5.3. O

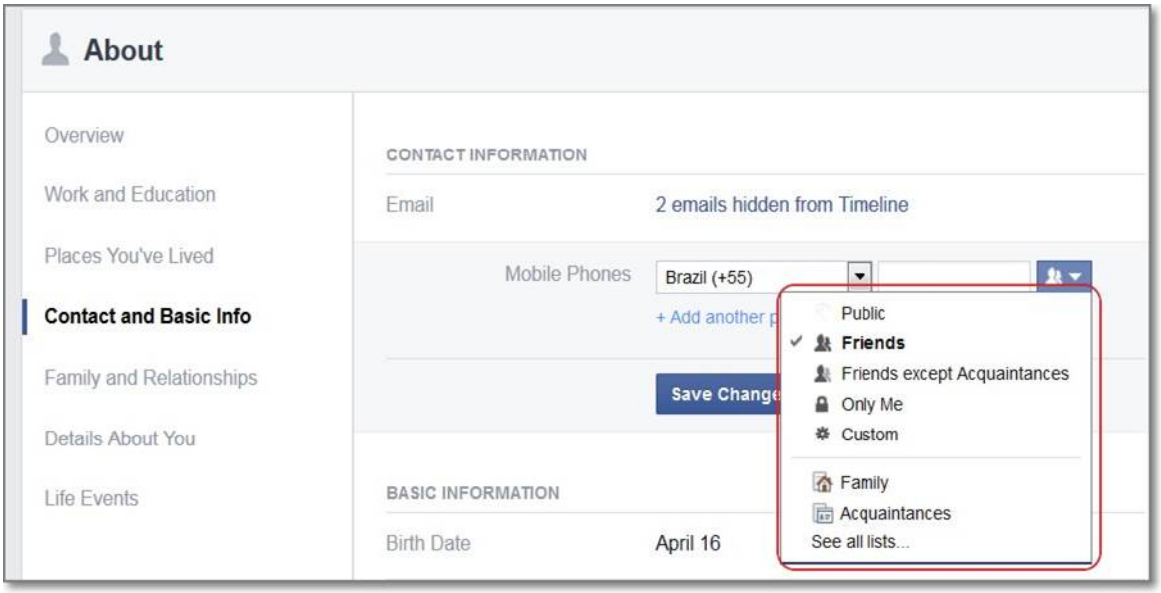


Figura 5.1. Audiência da informação divulgada no perfil do usuário no Facebook

Figura 5.2. Notificação quando outro usuário curte, comenta e compartilha informação de perfil do indivíduo no Facebook

primeiro discurso exibe ao usuário um fluxo de atualizações de seus amigos (postagens, curtidas e outros), enquanto que o segundo mostra ao usuário as atividades de seus amigos em tempo real. Esses discursos apenas destacam a informação pessoal do indivíduo, a qual seus amigos, que estão visualizando-a, já possuem acesso, como pode ser observado na página de ajuda desses recursos, mostradas na Figura 5.4 e na Figura 5.5. Assim, o valor da dimensão **discurso do sistema** neste caso é *"destaque"*.

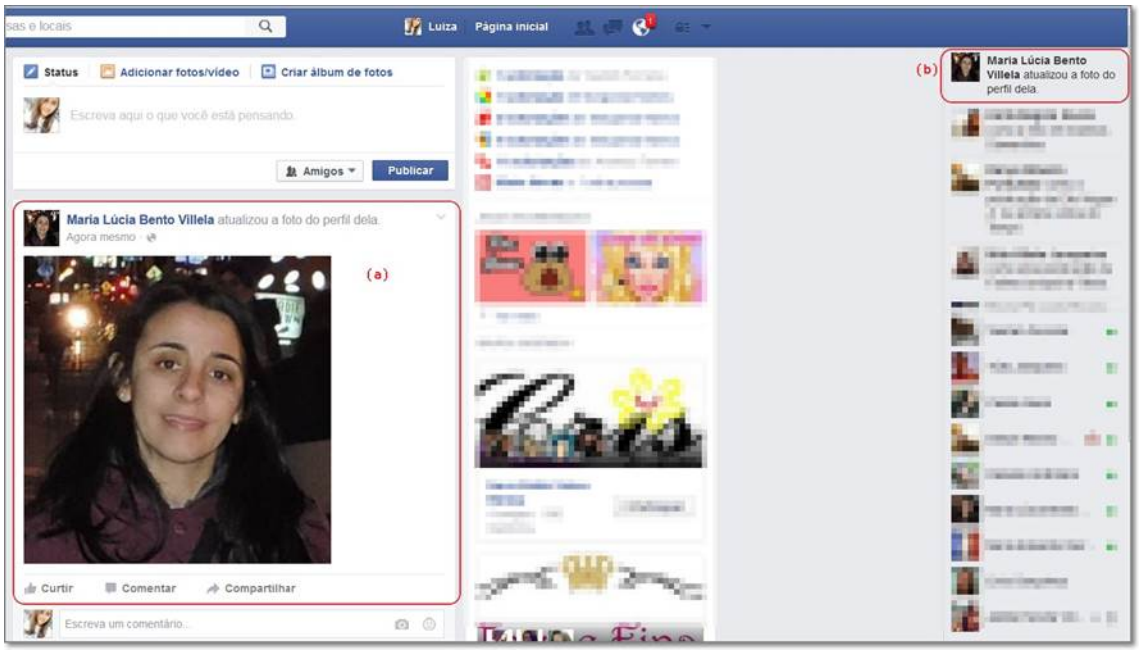


Figura 5.3. Compartilhamento de informação no perfil do indivíduo sendo mostrada no (a) *Feed de notícias* e na (b) seção *Novidades* do Facebook

Figura 5.4. Página de Ajuda sobre o *Feed de Notícias* (ou "News Feed", em inglês) do Facebook

Figura 5.5. Página de Ajuda sobre o recurso *Novidades* (ou "Ticker", em inglês) do Facebook

O Facebook também faz outro tipo de **discurso sobre o indivíduo**, a partir do compartilhamento de informações em seu perfil, que é a *sugestão de amizade*. Neste discurso, são mostradas a outros usuários informações públicas disponibilizadas no perfil do indivíduo, como nome e foto de perfil, bem como os amigos em comum, conforme exibido na Figura 5.6. Vale salientar que essas informações são acessíveis publicamente no perfil do indivíduo mas, na *sugestão de amizade*, elas são exibidas a outros usuários sem que eles tenham que procurar voluntariamente por elas, ao visitar as páginas de vários usuários em busca de amigos em potencial. A *sugestão de amizade* consiste em um discurso inferencial do Facebook, realizado com base não apenas em uma única instância de comunicação sobre o indivíduo, mas em um conjunto de comunicações referentes ao compartilhamento de informações em seu perfil, como suas informações sobre trabalho e educação, amigos em comum entre ele e o usuário ao qual a sugestão está sendo apresentada, dentre outras.

Em relação à dimensão **disseminação da informação**, o seu valor será definido em tempo de uso, dependendo da informação que está sendo compartilhada, da seguinte forma: (a) se forem informações que compõem o perfil público do usuário, como "foto de perfil" e "foto de capa", o valor da dimensão será predefinido pelo sistema como *"ilimitada"*, e o indivíduo não tem qualquer controle sobre a mesma; (b) caso sejam as demais informações que compõem o perfil do usuário no sistema, o valor da dimensão **disseminação da informação** será definido como *"ausente"*, tendo em vista que o Facebook não permite que outros usuários compartilhem as mesmas.

A representação visual do MDP referente ao tipo de comunicação (1) do Facebook é mostrada na Figura 5.7. Nesta figura, assim como em todas as demais figuras deste

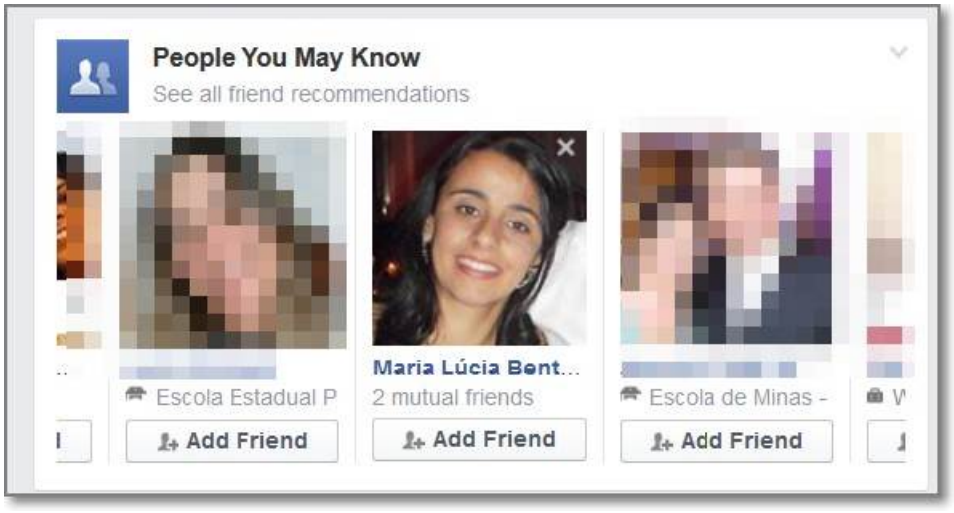


Figura 5.6. Sugestão de amizade no Facebook

capítulo que ilustram a representação visual dos tipos de comunicação nos três sistemas analisados, as dimensões cujos valores são fixos no sistema já estão representadas, apesar de somente ter sido possível identificá-las ao final do processo de modelagem de todos os tipos de comunicação do sistema.

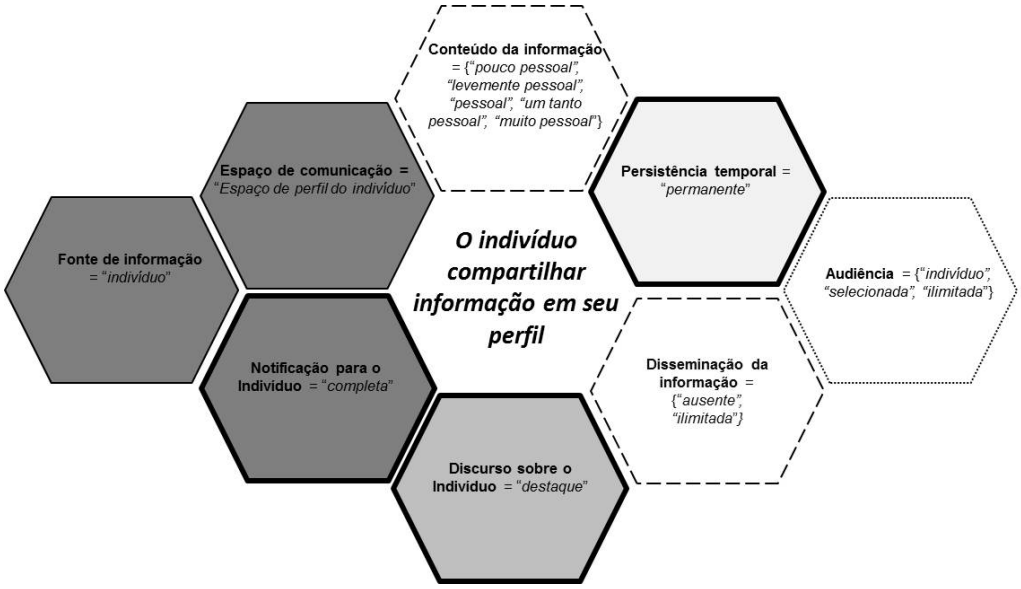


Figura 5.7. Representação visual do tipo de comunicação (1) do Facebook

As tabelas 5.2, 5.3, 5.4 e 5.5 apresentam a nossa interpretação sobre as decisões do designer em relação às dimensões de privacidade do MDP para os tipos de comunicação (2), (3), (4) e (5) do Facebook, respectivamente. As figuras 5.8, 5.9, 5.10 e 5.11 mostram as representações visuais de suas modelagens MDP.

Tabela 5.2. Modelagem do tipo de comunicação (2) do Facebook

		Controle	Valor*	Dependência de controle	Dependência de valor
Fonte de informação		Sistema – tempo de design	*"indivíduo"*	Na**	Na
Espaço de comunicação		Sistema – tempo de design	*"espaço de publicação do indivíduo"*	Na	Na
Informação do indivíduo	**Expressão**	Indivíduo	{*"tipada", "livre"*}	Na	Na
	Conteúdo	Definido em tempo de uso	{*"pouco pessoal", "levemente pessoal", "pessoal", "um tanto pessoal", "muito pessoal"*}	**Expressão**	Na
Persistência temporal		Sistema – tempo de design	*"permanente"*	Na	Na
Audiência		Indivíduo	{*"indivíduo", "selecionada", "ilimitada"*}	Na	Na
Notificação para o indivíduo		Sistema – tempo de design	*"completa"*	Na	Na
Discurso sobre o indivíduo		Sistema – tempo de design	*"destaque"*	Na	Na
Disseminação da informação		Definido em tempo de uso	{*"ausente", "limitada", "ilimitada"*}	**Tipo da disseminação da informação*** **	**Audiência**

*Quando os valores aparecem entre chaves, indica–se que a dimensão terá seu valor definido em tempo de uso, podendo assumir qualquer valor desse conjunto.

**Não se aplica.

***Características específicas do tipo da interação.

Figura 5.8. Representação visual do tipo de comunicação (2) do Facebook

Tabela 5.3. Modelagem do tipo de comunicação (3) do Facebook

		Controle	Valor*	Dependência de controle	Dependência de valor
Fonte de informação		Sistema – tempo de design	*"indivíduo"*	Na**	Na
Espaço de comunicação		Sistema – tempo de design	*"espaço de outro usuário"*	Na	Na
Informação do indivíduo	**Expressão**	Indivíduo	{*"tipada", "predefinida", "livre"*}	Na	Na
	Conteúdo	Definido em tempo de uso	{*"pouco pessoal", "levemente pessoal", "pessoal", "um tanto pessoal", "muito pessoal", "dependente do contexto"*}	**Expressão**	Na
Persistência temporal		Sistema – tempo de design	*"permanente"*	Na	Na
Audiência		Sistema – tempo de design	*"desconhecida"*	Na	Na
Notificação para o indivíduo		Sistema – tempo de design	*"completa"*	Na	Na
Discurso sobre o indivíduo		Sistema – tempo de design	*"destaque"*	Na	Na
Disseminação da informação		Definido em tempo de uso	{*"ausente", "limitada", "ilimitada"*}	**Tipo da disseminação da informação*** **	**Audiência**

*Quando os valores aparecem entre chaves, indica–se que a dimensão terá seu valor definido em tempo de uso, podendo assumir qualquer valor desse conjunto.

**Não se aplica.

***Características específicas do tipo da interação.

Figura 5.9. Representação visual do tipo de comunicação (3) do Facebook

Tabela 5.4. Modelagem do tipo de comunicação (4) do Facebook

		Controle	Valor*	Dependência de controle	Dependência de valor
Fonte de informação		Sistema – tempo de design	*"outro usuário"*	Na**	Na
Espaço de comunicação		Sistema – tempo de design	*"espaço de publicação do indivíduo"*	Na	Na
Informação do indivíduo	**Expressão**	Outro usuário	{*"tipada", "livre"*}	Na	Na
	Conteúdo	Definido em tempo de uso	{*"pouco pessoal", "levemente pessoal", "pessoal", "um tanto pessoal", "muito pessoal", "dependente do contexto"*}	**Expressão**	Na
Persistência temporal		Sistema – tempo de design	*"permanente"*	Na	Na
Audiência		Indivíduo	{*"indivíduo", "selecionada", "limitada", ilimitada"*}	Na	Na
Notificação para o indivíduo		Sistema – tempo de design	*"completa"*	Na	Na
Discurso sobre o indivíduo		Sistema – tempo de design	*"destaque"*	Na	Na
Disseminação da informação		Definido em tempo de uso	{*"ausente", "limitada", "ilimitada"*}	**Tipo da disseminação da informação*** **	**Audiência**

*Quando os valores aparecem entre chaves, indica–se que a dimensão terá seu valor definido em tempo de uso, podendo assumir qualquer valor desse conjunto.

**Não se aplica.

***Características específicas do tipo da interação.

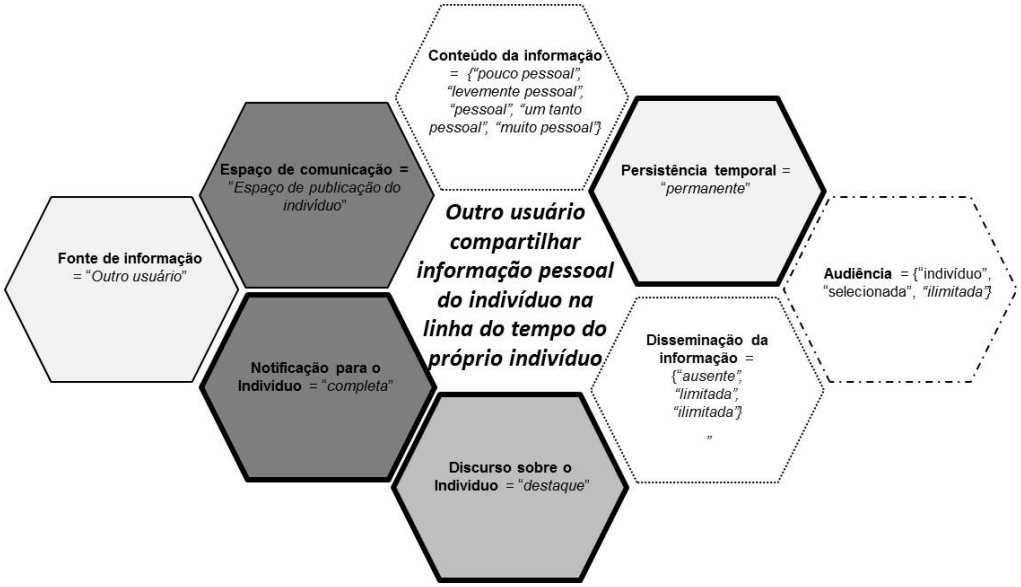


Figura 5.10. Representação visual do tipo de comunicação (4) do Facebook

Tabela 5.5. Modelagem do tipo de comunicação (5) do Facebook

		Controle	Valor*	Dependência de controle	Dependência de valor
Fonte de informação		Sistema – tempo de design	*"outro usuário"*	Na**	Na
Espaço de comunicação		Sistema – tempo de design	*"espaço de outro usuário"*	Na	Na
Informação do indivíduo	**Expressão**	Sistema – tempo de design	*"predefinida"*	Na	Na
	Conteúdo	Outro usuário	{*"pouco pessoal", "levemente pessoal", "pessoal", "um tanto pessoal", "muito pessoal", "dependente do contexto"*}	**Expressão**	Na
Persistência temporal		Sistema – tempo de design	*"permanente"*	Na	Na
Audiência		Sistema – tempo de design	*"desconhecida"*	Na	Na
Notificação para o indivíduo		Sistema – tempo de design	*"completa"*	Na	Na
Discurso sobre o indivíduo		Sistema – tempo de design	*"destaque"*	Na	Na
Disseminação da informação		Definido em tempo de uso	{*"ausente", "limitada", "ilimitada"*}	**Tipo da disseminação da informação*** **	**Audiência**

*Quando os valores aparecem entre chaves, indica–se que a dimensão terá seu valor definido em tempo de uso, podendo assumir qualquer valor desse conjunto.

**Não se aplica.

***Características específicas do tipo da interação.

Figura 5.11. Representação visual do tipo de comunicação (5) do Facebook

Considerando os valores atribuídos às dimensões de privacidade do MDP na modelagem do compartilhamento de informações pessoais no Facebook, podemos identificar alguns pontos interessantes relacionados a aspectos de privacidade no sistema. Primeiramente, observamos que os valores das dimensões **persistência temporal**, **notificação** e **discurso do sistema** foram definidos em tempo de design, no nível de sistema (ou seja, seus valores fixos para todos os tipos de comunicação). O valor da dimensão **persistência temporal** é igual a *"permanente"*, tendo em vista que toda informação pessoal compartilhada no Facebook fica sempre acessível para a sua audiência, enquanto ela não for voluntariamente excluída pelo usuário. Dessa forma, dado que quanto mais tempo a informação sobre o indivíduo fica disponível no sistema, maiores são as chances dela ser acessada (devida ou indevidamente), remetendo à fronteira temporal de privacidade colocada por Palen & Dourish [2003], a persistência da informação no Facebook está relacionada a um baixo nível de privacidade para o indivíduo.

Em relação à dimensão **notificação**, o seu valor é igual a *"completa"*, tendo em vista que o Facebook sempre notifica o indivíduo sobre atividades de outros usuários que o envolvem, como, por exemplo, quando outro usuário o marca em suas postagens ou compartilha o seu conteúdo. Dessa forma, a notificação no Facebook está relacionada a um alto nível de privacidade, dado que, ao ter uma maior consciência da sua potencial exposição online, o indivíduo pode ser mais criterioso com suas configurações de privacidade, ou até mesmo com as informações que ele compartilha no sistema, conforme mostrado no estudo de Emanuel et al. [2013].

O valor da dimensão **discurso do sistema** é *"destaque"* para todos os tipos de comunicação no Facebook. Entretanto, embora os usuários já tenham acesso, de outras formas, à informação que lhes é destacada em seu *Feed de Notícias* e na seção *Novidades*, a emissão desse discurso pode afetar a privacidade do indivíduo que possui a sua informação em destaque através desses recursos. Enquanto o primeiro recurso pode não ser considerado um problema, tendo em vista que quando o indivíduo compartilha uma informação no sistema, ele pretende de fato alcançar a audiência que definiu para a mesma, o segundo, por sua vez, pode não ser percebido da mesma forma. Este discurso do Facebook transmite a outros usuários informações sobre as atividades do indivíduo dentro do sistema em tempo real. Assim, mesmo que os usuários já tenham acesso a tais informações, como mencionado anteriormente, eles teriam que explicitamente procurar por elas, ao invés de tê-las apresentadas a eles. Uma analogia aos usuários procurando dentro do sistema pelas informações que são mostradas através do recurso *Novidades* seria como se estivessem procurando uma "agulha em um palheiro", sendo que este recurso então muda isso, e "aponta a agulha" para os usuários. O fato do indivíduo não ter qualquer controle sobre tal recurso pode lhe trazer problemas de privacidade, como aqueles relatados em Xavier et al. [2014] e Villela et al. [2015d].

Em relação às dimensões do MDP cujos valores variam entre os tipos de comunicação no Facebook, primeiramente, em relação à dimensão **fonte de informação**, vimos que ela pode assumir os valores *"indivíduo"* e *"outro usuário"*. O fato de outros usuários poderem compartilhar informação pessoal do indivíduo tira deste o controle em relação a o que é compartilhado sobre ele dentro do sistema. Neste caso, mesmo que o indivíduo escolha não compartilhar alguma informação pessoal sua, caso outro usuário a compartilhe, seus amigos poderão ter acesso à mesma, apesar da intenção do indivíduo de não compartilhá-la. Assim, percebemos que, quando o indivíduo é a fonte de informação, ele possui um maior controle sobre a sua privacidade. Por outro lado, quando outros usuários são a fonte de informação sobre o indivíduo, questões de privacidade podem surgir, o que remete à fronteira de identidade relacionada à privacidade, colocada por Palen & Dourish [2003], que descreve a tensão que existe entre o indivíduo e os outros, na busca por sua privacidade. No sentido de minimizar o surgimento de questões desse tipo, o Facebook oferece alguma flexibilidade ao indivíduo, ao permiti-lo alterar suas configurações para impedir que outros usuários postem em sua linha do tempo. No entanto, o indivíduo ainda não tem nenhum controle sobre o que outros usuários falam sobre ele em seus próprios espaços de comunicação, o que pode também lhe trazer problemas de privacidade.

Em relação à dimensão **espaço de comunicação**, vimos que o compartilhamento de informação pessoal pode ocorrer no perfil e na linha do tempo do indivíduo, bem

como na linha do tempo de outros usuários. No primeiro caso, o indivíduo pode alcançar um maior nível de privacidade, tendo em vista que ele possui um maior controle sobre o conteúdo que é postado por ele e sobre quem pode acessar o seu espaço, ao definir, neste caso, quem pode ser a fonte de informação e quem é a audiência do conteúdo ali compartilhado. Por outro lado, quando a informação pessoal do indivíduo é compartilhada na linha do tempo de outro usuário, o indivíduo possui um menor nível de privacidade, tendo em vista que esse outro usuário tem o controle sobre quem terá acesso ao espaço de comunicação. Neste caso, mesmo que o indivíduo seja a fonte de informação, ele não terá conhecimento sobre quem será a audiência da mesma. Além disso, o indivíduo pode até mesmo não estar consciente da possibilidade de atributos pessoais sobre ele serem inferidos a partir da informação que ele compartilha na linha do tempo de outros usuários e que poderiam impactar a sua privacidade [Kosinski et al., 2013]. Por exemplo, quando o indivíduo curte uma postagem de um amigo com algum conteúdo político, ele pode estar indiretamente compartilhando com a audiência daquela postagem (definida pelo amigo que a compartilhou) o seu posicionamento político.

O **conteúdo da informação** pode ser classificado em diferentes níveis de pessoalidade no Facebook. No caso de informações cuja **expressão** é *"tipada"*, elas podem ser classificadas em qualquer um dos níveis de pessoalidade identificados em nosso estudo empírico realizado anteriormente à proposta do MDP, mostrados na seção 3.1 do Capítulo 3 (por exemplo, "telefone" e "informações sobre saúde" estão no nível *muito pessoal*, "email" e "fotos do indivíduo" estão no nível *um tanto pessoal*, "data de aniversário" está no nível *pessoal*, "status de relacionamento" e "lugares visitados" estão no nível *levemente pessoal*, e "local de trabalho" e "local de estudo" estão no nível *pouco pessoal*). No caso de informação cuja **expressão** é *"livre"*, cabe à fonte da informação decidir sobre seu nível de pessoalidade, no momento em que a mesma é compartilhada. No caso de informação cuja **expressão** é *"predefinida"*, o nível de pessoalidade da mesma depende do contexto, e também pode estar em qualquer dos níveis de pessoalidade acima mencionados. Como a preocupação do indivíduo em relação a compartilhar suas informações no Facebook diminuem à medida que o nível de pessoalidade da informação também diminui [Villela et al., 2015a,c], temos que a decisão do usuário em relação a compartilhar ou não um informação pode ser afetada pelo nível de pessoalidade da mesma.

A **audiência** no Facebook, na maior parte das vezes, é controlada pelo dono do espaço onde ocorre o compartilhamento da informação, podendo variar a partir de um nível alto de privacidade (apenas o *"indivíduo"*) até um nível muito baixo (*"público"*), passando pela possibilidade de contemplar um grupo *"selecionado"* de pessoas (amigos

ou algum subconjunto desses). No caso do indivíduo compartilhar uma informação no espaço de outro usuário, a audiência, que é definida por este último, será *"desconhecida"* para o primeiro, tendo em vista que o Facebook não informa ao mesmo quem terá acesso à informação. Especificamente no caso do indivíduo ser referenciado em uma postagem de outro usuário, ele terá o controle para definir se deseja que a informação também seja compartilhada em sua própria linha do tempo (tendo assim o controle sobre a audiência), mas continuará não tendo controle e nem conhecimento sobre a audiência para a qual a informação foi originalmente compartilhada. Neste caso, mesmo que o indivíduo exclua a referência que a postagem faz a ele, isso não terá nenhum impacto sobre a audiência original da informação. Outro aspecto que merece ser ressaltado é que, apesar do Facebook permitir que o usuário controle, na maior parte das vezes, a audiência para a informação que ele compartilha em seu espaço, através de configurações de privacidade associada a cada informação compartilhada, ainda assim várias questões de privacidade podem surgir. Isso ocorre devido ao fato dos usuários não compreenderem completamente essas configurações ou seus impactos [Pereira Junior et al., 2014; Netter et al., 2013].

Finalmente, em relação à dimensão **disseminação da informação**, quando outros usuários compartilham uma postagem contendo informações sobre o indivíduo no Facebook, apenas pessoas que fazem parte da audiência original da mesma terão acesso ao compartilhamento. Uma exceção ocorre no compartilhamento de fotos do indivíduo. Neste caso, usuários que fazem parte da audiência da foto podem marcar amigos nela, expandindo assim o acesso à foto a pessoas marcadas e possivelmente seus amigos. Isso pode trazer questões de privacidade para o indivíduo, tendo em vista que ele pode não ser capaz de antecipar todas as interações que estão disponíveis a outros usuários sobre a sua informação, e a extensão futura das mesmas [Pereira Junior et al., 2014; Prates et al., 2015].

5.3.2 O compartilhamento de informações pessoais no ResearchGate

Como o contexto do ResearchGate[7] é a colaboração científica, consideramos como informações pessoais neste sistema aquelas relacionadas a características e produções científicas e acadêmicas do indivíduo, tais como habilidades e conhecimentos, experiência de pesquisa, experiência docente, educação, prêmios e realizações, dentre outras.

[7]Todos os termos referentes à interface do ResearchGate são apresentados em português nesta tese, embora a interface do sistema seja em inglês, como pode ser percebido nas figuras que mostram as telas do ResearchGate, exibidas nesta seção.

Também consideramos como informações pessoais publicações e trabalhos não publicados de autoria do indivíduo, que ele pode compartilhar no sistema, bem como as questões que ele posta e suas respostas a questões de outros usuários, dentro de discussões sobre tópicos de pesquisa que podem ocorrer dentro do sistema.

No ResearchGate, apenas o indivíduo pode compartilhar informações sobre si mesmo. Assim, apesar dele poder adicionar publicações em coautoria com outros usuários, tal publicação apenas será vinculada ao perfil desses outros usuários caso estes a adicionem manualmente (ou seja, não é permitido que um usuário adicione informação explicitamente vinculada ao perfil de outros usuários). Dessa forma, identificamos os seguintes tipos de comunicação, referentes às diferentes oportunidades de compartilhamento de informação pessoal no ResearchGate:

(1) O indivíduo compartilha informação pessoal em seu perfil;

(2) O indivíduo compartilha uma publicação de sua autoria;

(3) O indivíduo revisa ou comenta uma publicação de outro usuário;

(4) O indivíduo compartilha uma questão ou uma resposta a uma questão;

(5) O indivíduo interage com uma questão postada por outro usuário (curte ou segue).

Como fizemos na seção anterior, a seguir descrevemos em detalhes apenas a modelagem do tipo de comunicação (1), mostrado acima, de acordo com as dimensões de privacidade do MDP. A nossa intrepretação sobre as decisões do designer em relação a tais dimensões são apresentadas na Tabela 5.6.

Neste caso, a **fonte de informação** é o próprio *"indivíduo"* e o **espaço de comunicação** é o *"espaço de perfil do indivíduo"*, mostrado na Figura 5.12, conforme especificado no próprio tipo de comunicação. Em relação à **expressão** da informação compartilhada, esta será sempre *"tipada"*, sendo o seu significado e, portanto, o nível de pessoalidade referente ao seu **conteúdo**, definido pelo sistema. O ResearchGate agrupa as informações que o usuário pode compartilhar em seu perfil em três categorias: (a) **informações de contato**, compostas por "endereço", "website", "telefone", "contatos em outras redes sociais" e "aniversário", que se encontram nos níveis "muito pessoal" e "pessoal", de acordo com Villela et al. [2015a]; (b) **informações de pesquisa**, como "habilidades e conhecimentos", "experiência de pesquisa", "experiência docente" e "educação", que são classificadas no nível "levemente pessoal"; e (c) **informações básicas**, compostas por "posição", "titulação" e "instituição", que são classicadas no nível "pouco pessoal". A **persistência temporal** dessas informações é *"permanente"*, tendo em

Tabela 5.6. Modelagem do tipo de comunicação (1) do ResearchGate

		Controle	Valor*	Dependência de controle	Dependência de valor
Fonte de informação		Sistema – tempo de design	*"indivíduo"*	Na**	Na
Espaço de comunicação		Sistema – tempo de design	*"espaço de perfil do indivíduo"*	Na	Na
Informação do indivíduo	**Expressão**	Sistema – tempo de design	*"tipada"*	Na	Na
	Conteúdo	Sistema - tempo de uso	{*"pouco pessoal", "levemente pessoal", "muito pessoal"*}	Na	**Informação*** **
Persistência temporal		Sistema – tempo de design	*"permanente"*	Na	Na
Audiência		Definido em tempo de uso	{*"selecionada", "limitada", "ilimitada"*}	**Informação**	**Informação**
Notificação para o indivíduo		Na	Na	Na	Na
Discurso sobre o indivíduo		Sistema – tempo de design	*"ausente"*	Na	Na
Disseminação da informação		Sistema – tempo de design	*"ausente"*	Na	Na

*Quando os valores aparecem entre chaves, indica–se que a dimensão terá seu valor definido em tempo de uso, podendo assumir qualquer valor desse conjunto.
**Não se aplica.
***Características específicas da informação compartilhada que não são representadas através de valores atribuídos à dimensão **Informação do indivíduo**.

vista que ficam acessíveis para a sua audiência durante todo o tempo de sua existência, ou seja, enquanto ela não for excluída pelo usuário.

No ResearchGate, a audiência é definida para cada uma das três categorias de informação mostradas anteriormente, e não para cada unidade de informação compartilhada, como acontece no Facebook. O controle e o valor da dimensão **audiência**, neste caso, variam de acordo com dessas categorias, da seguinte forma: (a) **informações básicas** possuem a sua audiência predefinida como *"todos"* na interface do sistema (equivalente ao valor *"ilimitada"* no MDP); (b) **informações de pesquisa** possuem sua audiência definida pelo indivíduo, podendo variar de *"seguidores mútuos"* (equivalente ao valor *"selecionada"* no MDP) até *"qualquer pessoa"* (equivalente ao valor *"ilimitada"* no MDP), passando pela possibilidade de compartilhar com todos os usuá-

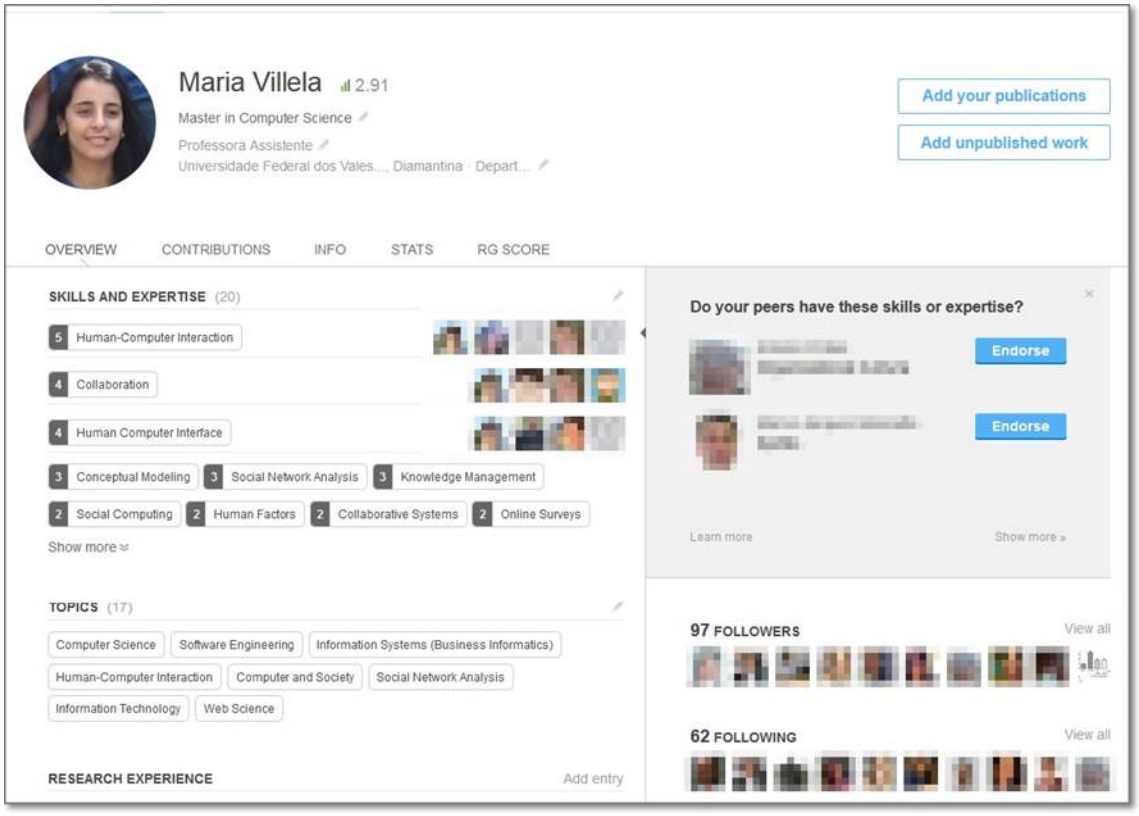


Figura 5.12. Parte da página perfil do usuário no ResearchGate

rios do sistema ("membros do ResearchGate"), que é equivalente ao valor *"limitada"* no MDP; e, por fim, (c) **informações de contato** possuem sua audiência predefinida como *"seguidores mútuos"* (equivalente ao valor *"selecionada"* no MDP). A Figura 5.13 mostra as configurações de privacidade relacionadas à audiência no ResearchGate, para a informação de perfil do indivíduo.

Como o ResearchGate não permite que outros usuários interajam sobre a informação que o indivíduo compartilha em seu perfil, não existe a possibilidade de atribuição de valor para a dimensão **notificação para o indivíduo**, sendo a mesma não aplicável, neste caso. Já o valor da dimensão **disseminação da informação** é *"ausente"*, uma vez que não é possível que outros usuários (re)compartilhem uma informação que o indivíduo compartilha em seu perfil.

Em relação à dimensão **discurso sobre o indivíduo**, apesar do seu valor ser *"ausente"* para cada instância de comunicação, o ResearchGate faz um discurso de *"destaque"* sobre o indivíduo no nível inferencial, que é a *"sugestão para seguir pesquisadores"*. Neste caso, são mostradas, na *Home Feed* de outros usuários, informações públicas disponibilizadas no perfil do indivíduo, como nome e foto de perfil, bem como a relação do indivíduo com o usuário, conforme exibido na Figura 5.14. Esse discurso

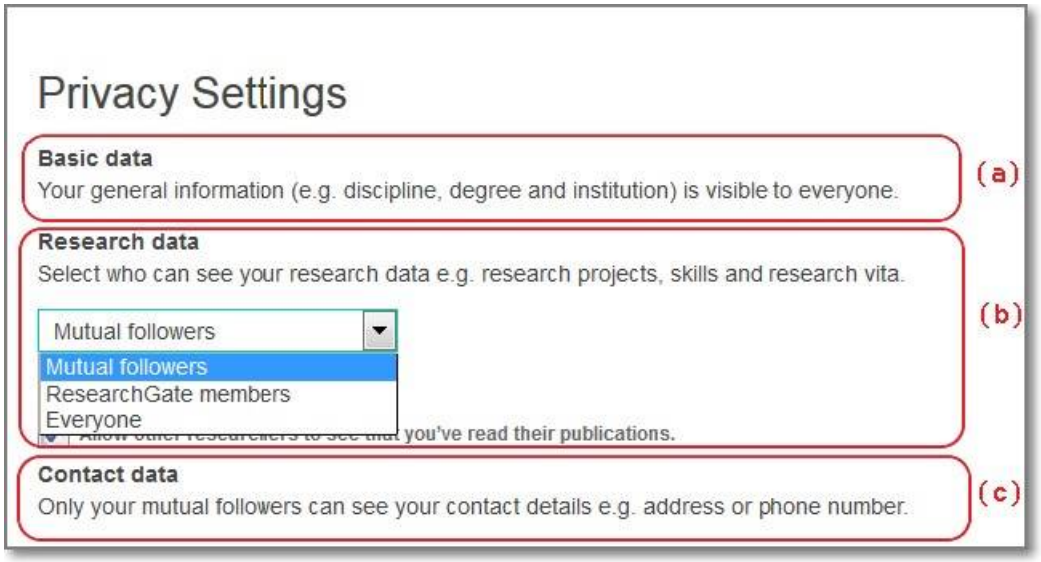


Figura 5.13. Configurações de privacidade no ResearchGate

do ResearchGate é realizado com base em um conjunto de comunicações, referentes ao compartilhamento de informações do indivíduo em seu perfil, citações, local de trabalho, redes de contatos, dentre outras.

Por fim, o valor da dimensão **disseminação da informação** é *"ausente"* para informação compartilhada no perfil do indivíduo e este não possui qualquer controle sobre a mesma.

A representação visual da modelagem do tipo de comunicação (1) do ResearchGate, através das dimensões do MDP, é mostrada na Figura 5.15.

As tabelas 5.7, 5.8, 5.9 e 5.10 apresentam a nossa interpretação sobre as decisões do designer em relação às dimensões de privacidade do MDP para os tipos de comunicação (2), (3), (4) e (5) do ResearchGate, respectivamente. As figuras 5.16, 5.17, 5.18[8] e5.19 mostram as representações visuais de suas modelagens MDP.

[8]Note que a representação, neste caso, é composta por duas *"beehives"*, tendo em vista que o indivíduo compartilhar uma questão ou resposta a uma questão gera, na realidade, dois compartilhamentos de informação em espaços de comunicação distintos no sistema, com diferentes controles sobre a dimensão **audiência**.

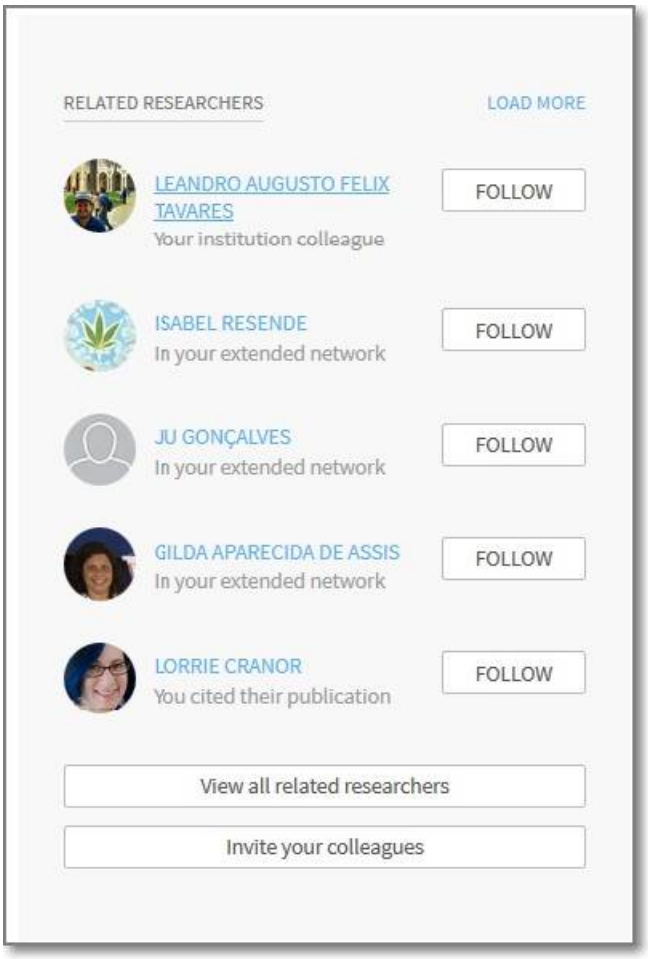


Figura 5.14. Sugestão para seguir pesquisadores no ResearchGate

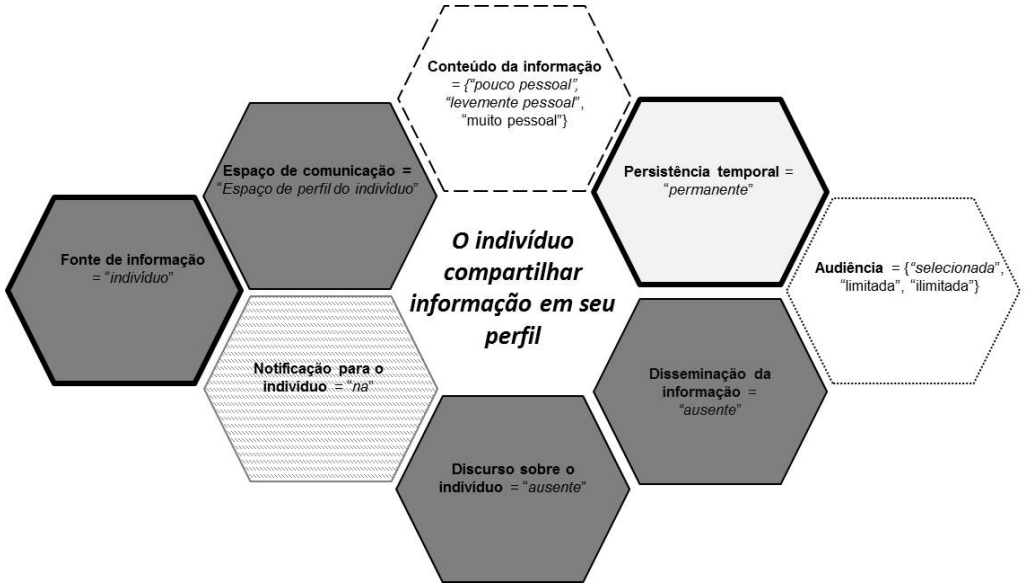


Figura 5.15. Representação visual do tipo de comunicação (1) do ResearchGate

Tabela 5.7. Modelagem do tipo de comunicação (2) do ResearchGate

		Controle	Valor	Dependência de controle	Dependência de valor
Fonte de informação		Sistema – tempo de design	*"indivíduo"*	Na*	Na
Espaço de comunicação		Sistema – tempo de design	*"espaço de publicação do indivíduo" e "espaço público"*	Na	Na
Informação do indivíduo	**Expressão**	Sistema – tempo de design	*"tipada"*	Na	Na
	Conteúdo	Sistema – tempo de design	*"pouco pessoal"*	Na	Na
Persistência temporal		Sistema – tempo de design	*"permanente"*	Na	Na
Audiência		Sistema – tempo de design	*"ilimitada"*	Na	Na
Notificação para o indivíduo		Sistema – tempo de design	*"parcial"*	Na	Na
Discurso sobre o indivíduo		Sistema – tempo de design	*"destaque"*	Na	Na
Disseminação da informação		Sistema – tempo de design	*"ilimitada"*	Na	Na

*Não se aplica.

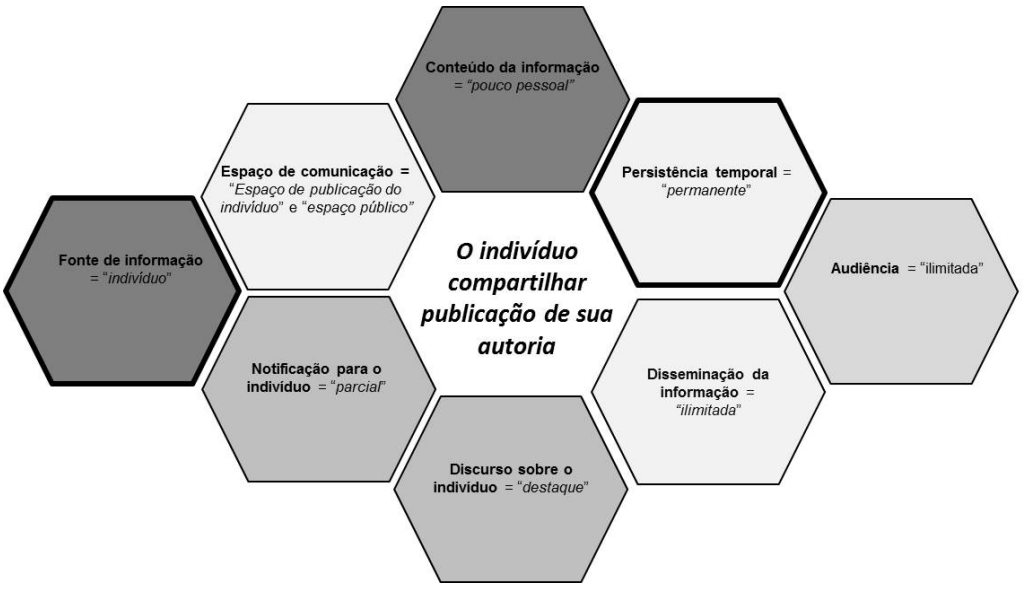


Figura 5.16. Representação visual do tipo de comunicação (2) do ResearchGate

Tabela 5.8. Modelagem do tipo de comunicação (3) do ResearchGate

		Controle	Valor	Dependência de controle	Dependência de valor
Fonte de informação		Sistema – tempo de design	*"indivíduo"*	Na*	Na
Espaço de comunicação		Sistema – tempo de design	*"espaço de outro usuário" e "espaço público"*	Na	Na
Informação do indivíduo	**Expressão**	Sistema – tempo de design	*"tipada"*	Na	Na
	Conteúdo	Sistema – tempo de design	*"pouco pessoal"*	Na	Na
Persistência temporal		Sistema – tempo de design	*"permanente"*	Na	Na
Audiência		Sistema – tempo de design	*"ilimitada"*	Na	Na
Notificação para o indivíduo		Sistema – tempo de design	*"ausente"*	Na	Na
Discurso sobre o indivíduo		Sistema – tempo de design	*"destaque"*	Na	Na
Disseminação da informação		Sistema – tempo de design	*"ausente"*	Na	Na

*Não se aplica.

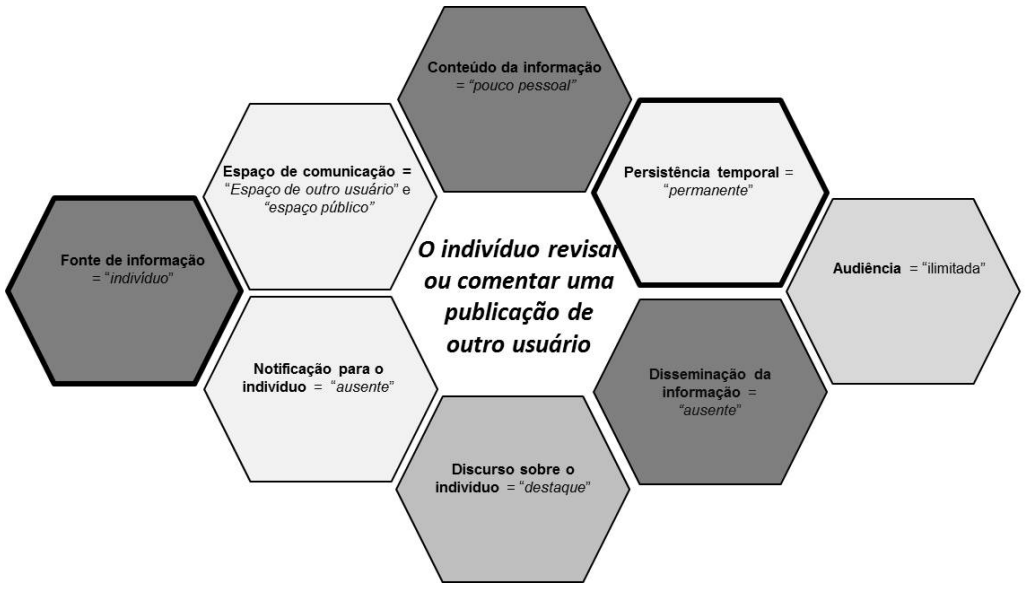


Figura 5.17. Representação visual do tipo de comunicação (3) do ResearchGate

Tabela 5.9. Modelagem do tipo de comunicação (4) do ResearchGate

		Controle	Valor*	Dependência de controle	Dependência de valor
Fonte de informação		Sistema – tempo de design	*"indivíduo"*	Na**	Na
Espaço de comunicação		Sistema – tempo de design	*"espaço de publicação do indivíduo" e "espaço público"*	Na	Na
Informação do indivíduo	**Expressão**	Sistema – tempo de design	*"tipada"*	Na	Na
	Conteúdo	Sistema – tempo de design	*"pouco pessoal"*	Na	Na
Persistência temporal		Sistema – tempo de design	*"permanente"*	Na	Na
Audiência	**Espaço de publicação do indivíduo**	Indivíduo	*{"limitada", "Ilimitada"}*	Na	Na
	Espaço público	Sistema – tempo de design	*"ilimitada"*	Na	Na
Notificação para o indivíduo		Sistema – tempo de design	*"parcial"*	Na	Na
Discurso sobre o indivíduo		Sistema – tempo de design	*"destaque"*	Na	Na
Disseminação da informação		Sistema – tempo de design	*"ilimitada"*	Na	Na

*Quando os valores aparecem entre chaves, indica–se que a dimensão terá seu valor definido em tempo de uso, podendo assumir qualquer valor desse conjunto.

**Não se aplica.

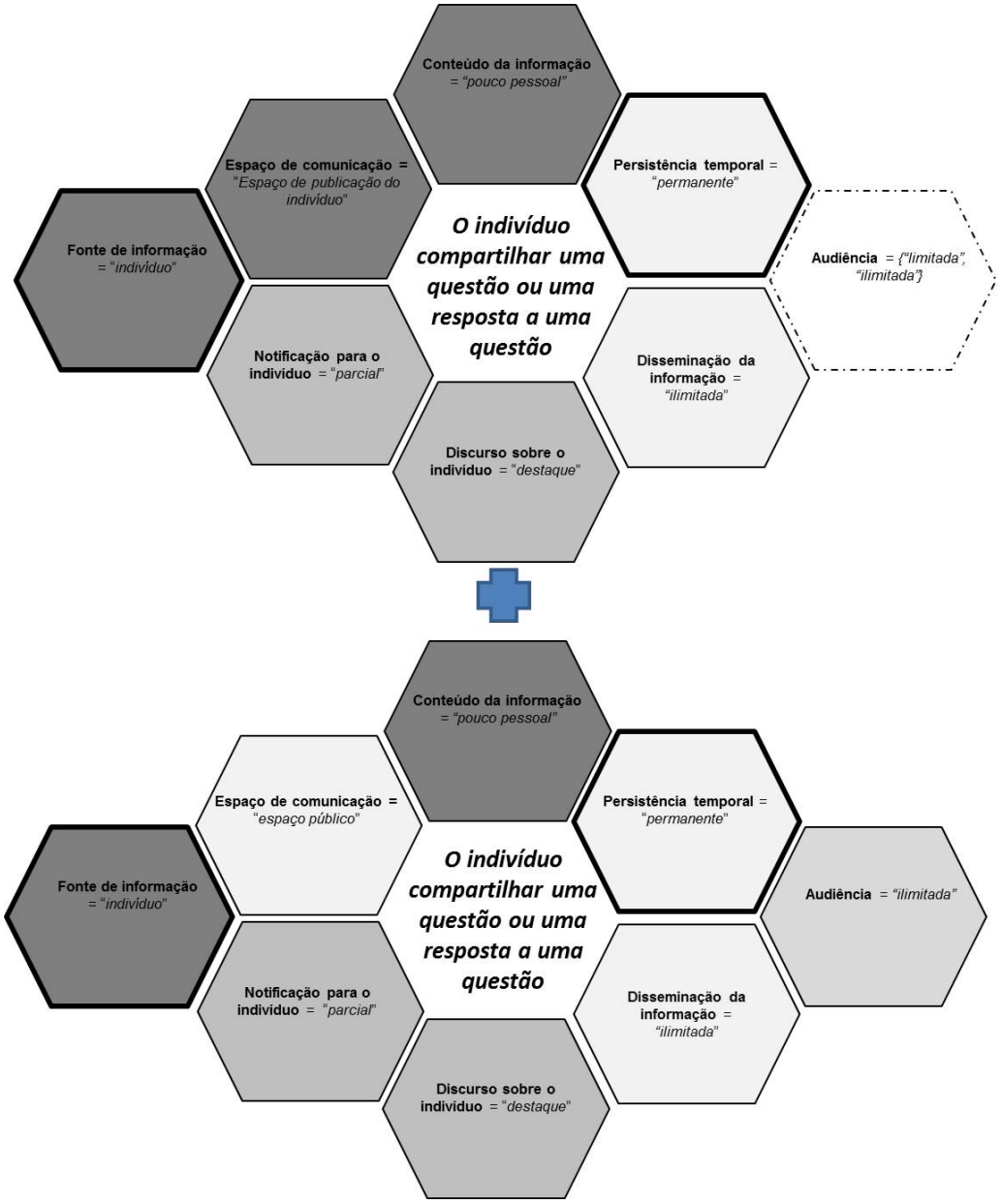


Figura 5.18. Representação visual do tipo de comunicação (4) do ResearchGate

Tabela 5.10. Modelagem do tipo de comunicação (5) do ResearchGate

		Controle	Valor	Dependência de controle	Dependência de valor
Fonte de informação		Sistema – tempo de design	*"indivíduo"*	Na*	Na
Espaço de comunicação		Sistema – tempo de design	*"espaço público"*	Na	Na
Informação do indivíduo	**Expressão**	Sistema – tempo de design	*"predefinida"*	Na	Na
	Conteúdo	Sistema – tempo de design	*"pouco pessoal"*	Na	Na
Persistência temporal		Sistema – tempo de design	*"permanente"*	Na	Na
Audiência		Sistema – tempo de design	*"desconhecida"*	Na	Na
Notificação para o indivíduo		Na	Na	Na	Na
Discurso sobre o indivíduo		Sistema – tempo de design	*"destaque"*	Na	Na
Disseminação da informação		Sistema – tempo de design	*"ausente"*	Na	Na

*Não se aplica.

Figura 5.19. Representação visual do tipo de comunicação (5) do ResearchGate

Tendo mostrado os valores das dimensões do MDP em cada um dos tipos de comunicação do ResearchGate, vale chamar a atenção para um aspecto importante

desse sistema, relacionado à dimensão **discurso sobre o indivíduo**. O ResearchGate faz dois discursos desse tipo, que são as *estatísticas de publicações e de visualização de perfil* e o *RG Score* (métrica de reputação científica, calculada com base nas publicações e interações de outros pesquisadores do ResearchGate com o conteúdo do indivíduo), e os exibe na página do indivíduo, como pode ser visto nas Figuras 5.20 e 5.21. Esses discursos estão no nível inferencial, ocorrendo com base não apenas em uma instância de comunicação, mas em um conjunto de comunicações, que são inclusive de tipos diferentes, como o compartilhamento de informações de perfil, de publicações e de questões, que configuram os tipos de comunicação (1), (2) e (4), respectivamenente.

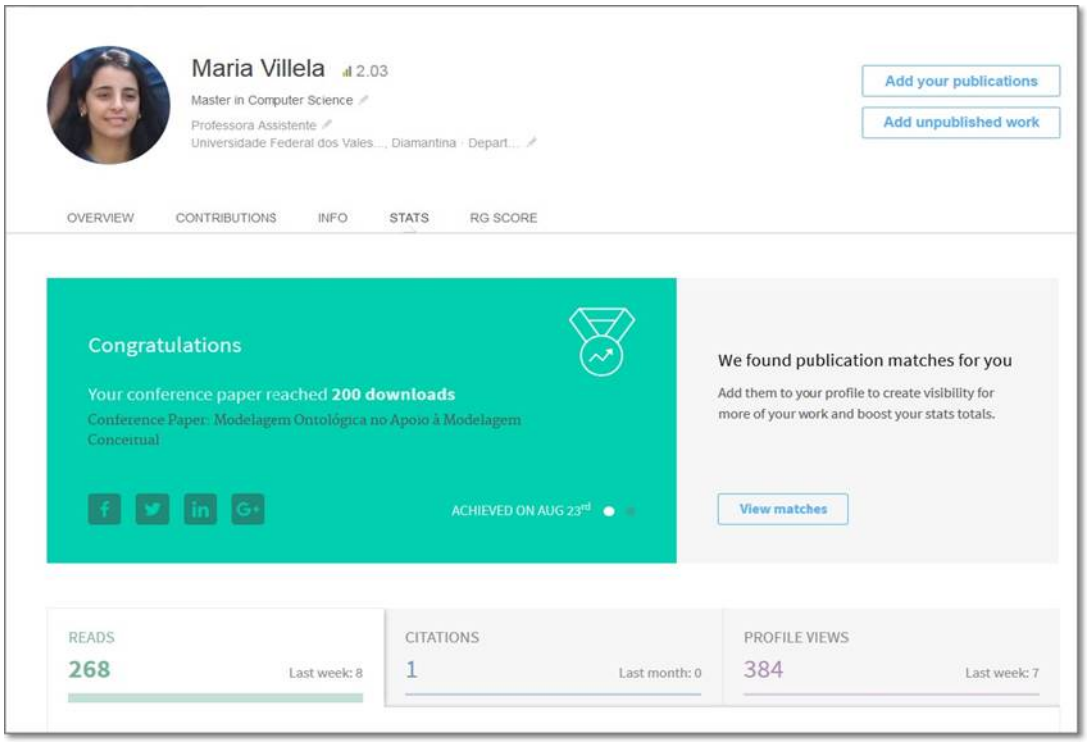


Figura 5.20. Exibição de estatísticas (guia "Stats") na página do indivíduo no ResearchGate

Nossa análise do ResearchGate baseada no MDP nos indicou alguns pontos interessantes relacionados às dimensões de privacidade. Primeiramente, apenas o indivíduo pode ser a **fonte de informação** sobre ele no sistema, o que lhe concede um maior controle sobre o seu nível de privacidade, no sentido de permitir que ele tenha o controle sobre a informação que está sendo compartilhada, bem como sobre o espaço onde a comunicação ocorre. Por outro lado, o valor da dimensão **persistência temporal** é definida em tempo de design, sendo igual a *"permanente"*, e fixo para todos os tipos de comunicação, tendo em vista que toda informação compartilhada no ResearchGate fica

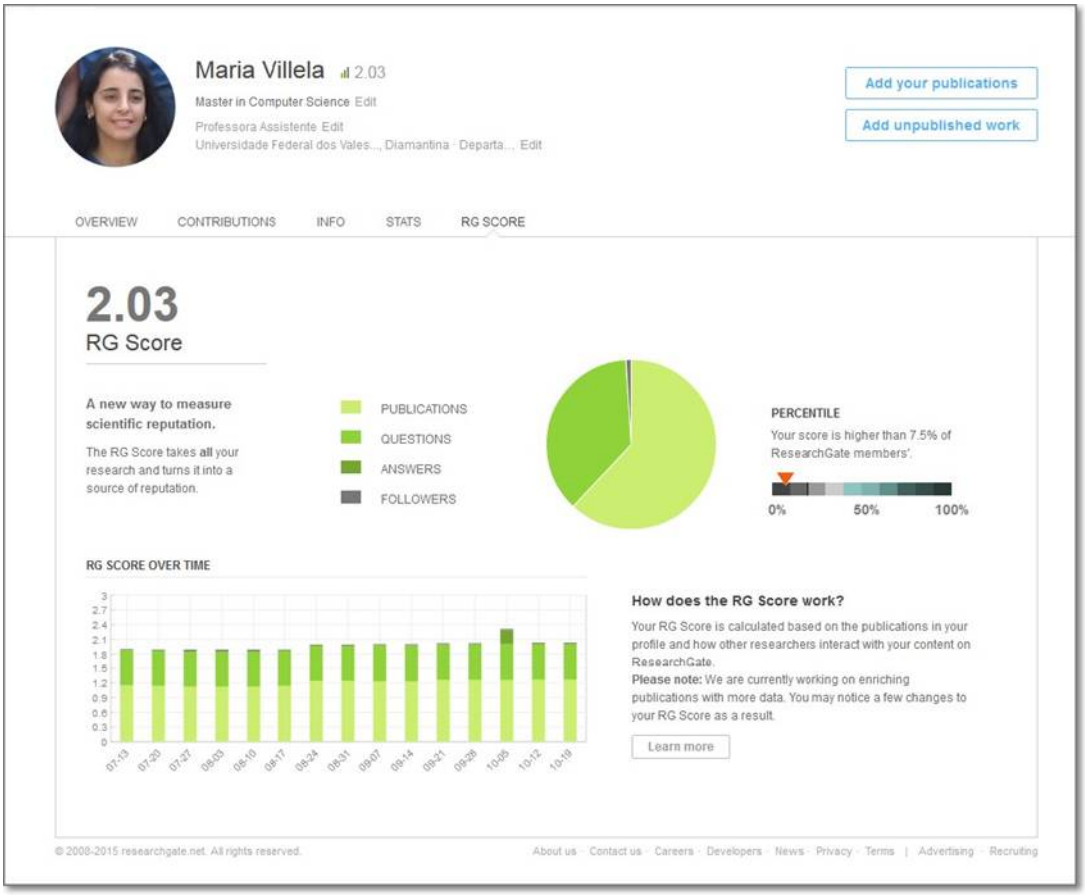


Figura 5.21. Exibição de métrica de reputação científica (guia "RG Score") na página do indivíduo no ResearchGate

acessível para a sua audiência durante todo o tempo de sua existência, o que remete a um nível baixo de privacidade.

As demais dimensões de privacidade do MDP possuem seus valores variando entre os tipos de comunicação. Primeiramente, em relação à dimensão **espaço de comunicação**, todas as informações pessoais estão sempre disponíveis em um espaço público, com exceção das informações de perfil do indivíduo (tipo de comunicação 1). Além de serem compartilhadas em um espaço público, as publicações do indivíduo (tipo de comunicação 2), bem como suas questões e respostas a questão de outros usuários (tipo de comunicação 4), são compartilhadas também em seu espaço de publicação, e suas revisões e comentários sobre publicações de outros usuários (tipo de comunicação 3) são compartilhadas também no espaço de publicação destes últimos. O controle sobre a dimensão **audiência** é do sistema na maior parte das vezes, que define a mesma, em tempo de design, como *"ilimitada"*, independente do espaço onde a informação é compartilhada, o que remete a um nível baixo de privacidade. Um nível mais alto de pri-

vacidade relacionado à dimensão **audiência** ocorre apenas no caso em que informações de contato são compartilhadas no perfil do usuário, quando a mesma é predefinida no sistema como sendo *"selecionada"* (caracterizada pelo valor *"mutual followers"*). Ainda no perfil do usuário, para as informações de pesquisa, é fornecido ao mesmo o controle sobre a audiência, podendo definir, em tempo de uso, se a mesma será *"selecionada"*, *"limitada"* ou *"ilimitada"*, caracterizadas respectivamente pelos valores *"seguidores mútuos"*, *"usuários do ResearchGate"* e *"qualquer pessoa"*. O usuário também possui o controle sobre a audiência no caso do compartilhamento de questões e respostas, que são vinculadas à sua página como contribuições, podendo defini-la como *"limitada"* ou *"ilimitada"*, caracterizada respectivamente pelos valores *"usuários do ResearchGate"* e *"qualquer pessoa"*.

Percebemos que a ampla audiência para as informações compartilhadas no ResearchGate é contrabalanceada pelo nível de pessoalidade referente ao seu **conteúdo**. Primeiramente, tal nível de pessoalidade é definido em tempo de design, tendo em vista que a **expressão** de todas as informações compartilhadas é *"tipada"* (com exceção do caso em que o indivíduo curte ou segue uma questão postada por outro usuário, em que a expressão é *"predefinida"*). Assim, com exceção das informações de contato e dados de pesquisa que o indivíduo compartilha em seu perfil, que remetem respectivamente ao nível *"muito pessoal"* e *"levemente pessoal"*, os demais conteúdos compartilhados no sistema estão todos no nível *"pouco pessoal"*, tendo em vista que são informações referentes à formação, discussão ou produtividade científica do indivíduo.

Em relação às dimensões relacionadas aos efeitos da comunicação, temos, primeiramente, que o ResearchGate não permite que outros usuários interajam sobre a informação compartilhada no perfil do indivíduo, nem sobre a interação do indivíduo com uma questão postada por outro usuário. Assim, nesses casos, não há sobre o quê o sistema notificar o indivíduo e a dimensão **notificação para o indivíduo** não é aplicável. Em outros casos, tal notificação é *"ausente"*, quando outros usuários respondem a um comentário que o indivíduo faz sobre uma publicação, ou *"parcial"*, quando outros usuários interagem sobre uma publicação ou questão compartilhada pelo indivíduo.

No caso da dimensão **discurso sobre o indivíduo**, o ResearhGate não faz nenhum discurso sobre a informação que o indivíduo compartilha em seu perfil. Entretanto, para publicações e questões/respostas compartilhadas pelo indivíduo, bem como suas interações sobre publicações e questões postadas por outros usuários, o ResearchGate gera um discurso que é apresentado no *Live Feed* dos usuários que seguem o indivíduo. Esse discurso apenas fornece a esses usuários *"destaque"* à informação sobre o indivíduo, à qual eles já possuem acesso. Por outro lado, considerando o escopo de um conjunto de comunicações, referentes a diferentes compartilhamentos de informações

(de perfil, publicações e questões), o ResearchGate faz discursos que geram *"novas"* informações sobre o indivíduo, que são as estatísticas de visualização de perfil e o RG Score. O fato do ResearchGate gerar um discurso com novas informações sobre o indivíduo está relacionado a um nível mais baixo de privacidade, tendo em vista a falta de controle por parte deste em relação à informação sobre ele que é gerada pelo sistema. No entanto, tal fato é contrabalanceado pelo nível de pessoalidade dessas informações, que são pouco pessoais e remetem, portanto, a um nível mais alto de privacidade.

A **disseminação de informação** no ResearchGate é *"ilimitada"* na maior parte dos casos, tendo em vista que a maior parte das informações compartilhadas pelo indivíduo pode ser recompartilhada por qualquer usuário com os seus seguidores. A exceção ocorre apenas no caso das informações de perfil do indivíduo e de seus comentários em publicações de outros usuários, que não podem ser recompartilhados.

Em geral, como podemos perceber, os valores das dimensões relacionadas aos efeitos da comunicação remetem a níveis mais baixos de privacidade. Porém, esses valores, como no caso das dimensões **audiência** e **persistência temporal**, são contrabalanceados pelo **conteúdo da informação**, tendo em vista que a maior parte da informação que é amplamente compartilhada é classificada como *"pouco pessoal"*, e provavelmente não despertaria questões de privacidade para os usuários.

5.3.3 O compartilhamento de informações pessoais no CaringBridge

O CaringBridge[9] é uma rede social cujo foco é permitir que pessoas que estejam passando por problemas sérios de saúde obtenham apoio e encorajamento para lidarem com a situação. Dessa forma, consideramos em nossa análise como sendo informações pessoais aquelas voltadas para a condição de saúde do indivíduo. Essas informações são compartilhadas com outras pessoas em sites criados pelo usuário, onde são registradas atualizações sobre o estado de saúde, além de fotos e vídeos do indivíduo[10], permitindo que sua família e amigos o ofereçam o apoio necessário (psicológico, emocional ou até mesmo financeiro). O usuário tem o controle sobre a privacidade dessas informações no sistema, podendo fazê-las públicas ou privadas, e apenas o indivíduo pode compartilhar informação sobre ele mesmo.

[9]Todos os termos referentes à interface do CaringBridge são apresentados em português nesta tese, embora a interface do sistema seja em inglês, como pode ser percebido nas figuras que mostram as telas do CaringBridge, exibidas nesta seção.

[10]Embora o usuário não seja necessariamente o indivíduo ao qual a informação se refere, tendo em vista que ele pode criar o site no CaringBridge para um amigo ou alguém da família que esteja enfrentando um problema sério de saúde, consideraremos nesta análise o usuário como sendo o próprio indivíduo, dado que ele pode ser considerado o representante deste dentro do sistema.

Dessa forma, identificamos os seguintes tipos de comunicação, referentes às diferentes oportunidades de compartilhamento de informação pessoal do indivíduo no CaringBride:

(1) O indivíduo compartilha informação pessoal em seu perfil;

(2) O indivíduo compartilha informação em seu website;

(3) O indivíduo interage com um website de outro usuário (visita, assina o livro de visitas, aceita uma tarefa, comenta ou curte atualizações realizadas no mesmo).

Como apresentamos nas seções anteriores, a seguir descrevemos em detalhes a modelagem referente do tipo de comunicação (1), mostrado acima, de acordo com as dimensões de privacidade do MDP. A nossa interpretação sobre as decisões do designer em relação a tais dimensões são apresentadas na Tabela 5.11.

Tabela 5.11. Modelagem do tipo de comunicação (1) do CaringBridge

		Controle	Valor*	Dependência de controle	Dependência de valor
Fonte de informação		Sistema – tempo de design	*"indivíduo"*	Na**	Na
Espaço de comunicação		Sistema – tempo de design	*"espaço de perfil do indivíduo"*	Na	Na
Informação do indivíduo	**Expressão**	Sistema – tempo de design	*"tipada"*	Na	Na
	Conteúdo	Sistema – tempo de design	*"um tanto pessoal"*	Na	Na
Persistência temporal		Sistema – tempo de design	*"permanente"*	Na	Na
Audiência		Indivíduo	{*"indivíduo"*, *"limitada"*}	Na	Na
Notificação para o indivíduo		Na	Na	Na	Na
Discurso sobre o indivíduo		Sistema – tempo de design	*"ausente"*	Na	Na
Disseminação da informação		Sistema – tempo de design	*"ausente"*	Na	Na

*Quando os valores aparecem entre chaves, indica–se que a dimensão terá seu valor definido em tempo de uso, podendo assumir qualquer valor desse conjunto.
**Não se aplica.

Neste caso, a **fonte de informação** é o próprio *"indivíduo"* e o **espaço de comunicação** é o *"espaço de perfil do indivíduo"*, conforme especificado no próprio tipo de comunicação. Em relação à **expressão** da informação compartilhada, esta será sempre *"tipada"*, sendo o seu significado e, portanto, o **conteúdo** referente ao seu nível de pessoalidade, definido pelo sistema, em tempo de design. Como pode ser visto na Figura 5.22, todas as informações compartilhadas no perfil do indivíduo no CaringBridge são classificadas como *"pessoais"*, como *cidade*, *estado*, uma *frase sobre a pessoa* e *sites que ela visita*. O CaringBridge trata o compartilhamento de informações de maneira agrupada. Assim, a unidade de privacidade vale para todas as informações do perfil, e não para cada informação específica. A **persistência temporal** dessas informações é *"permanente"*, tendo em vista que ficam acessíveis para a sua audiência durante todo o tempo de sua existência, ou seja, enquanto ela não for excluída pelo usuário.

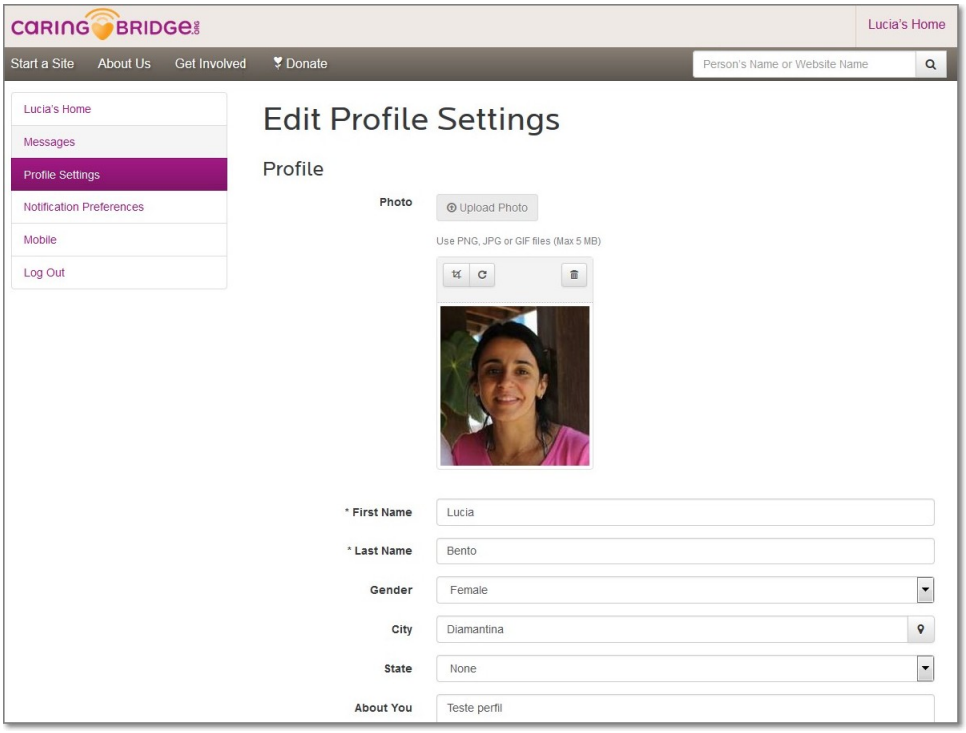


Figura 5.22. Compartilhando informações no perfil do CaringBridge

Dado o objetivo do sistema de estimular a apoio emocional (e financeiro) a pessoas que enfrentam problemas de saúde, a audiência para informação de perfil do usuário é controlada por ele próprio (Figura 5.23), que pode escolher entre ter um perfil público (ou seja, informações referentes à sua cidade e estado, bem como sites que ele possui ou visita são visíveis a todos os usuários do sistema) ou privado (com apenas sua foto

e nome visíveis a todos os usuários do sistema), com a dimensão **audiência** remetendo aos valores *"limitada"* e *"indivíduo"*, respectivamente.

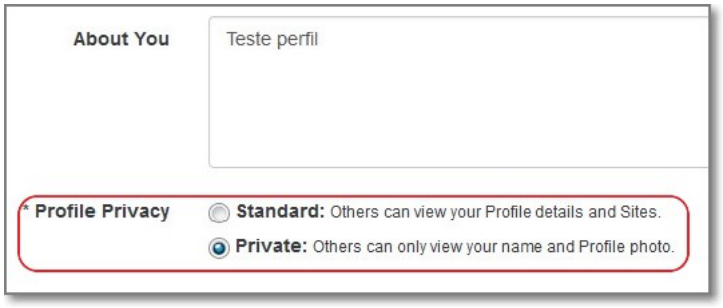


Figura 5.23. Configuração de privacidade do perfil no CaringBridge

Como o CaringBridge não permite que outros usuários interajam sobre a informação que o indivíduo compartilha em seu perfil, não existe a possibilidade de atribuição de um valor para a dimensão **notificação para o indivíduo**. O CaringBridge também não faz nenhum discurso relacionado às informações que o indivíduo compartilha em seu perfil e nem permite que essas informações sejam disseminadas por outros usuários. Assim, o valor para ambas as dimensões **discurso sobre o indivíduo** e **disseminação da informação** é *"ausente"*.

A representação visual da modelagem do tipo de comunicação (1) do CaringBridge, através das dimensões do MDP, é mostrada na Figura 5.24.

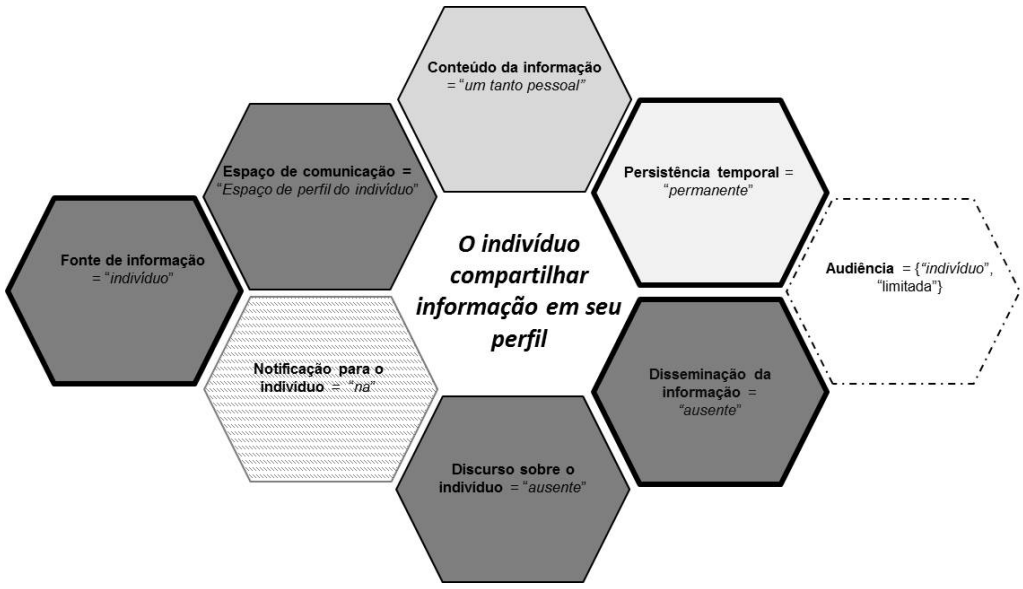


Figura 5.24. Representação visual do tipo de comunicação (1) do CaringBridge

Para o tipo de comunicação (2)(*"o indivíduo compartilha informação em seu web-*

site"), a nossa interpretação sobre as decisões do designer em relação às dimensões de privacidade do MDP são apresentadas na Tabela 5.12. A representação visual da modelagem deste tipo de comunicação é mostrada na Figura 5.25.

Tabela 5.12. Modelagem do tipo de comunicação (2) do CaringBridge

		Controle	Valor*	Dependência de controle	Dependência de valor
Fonte de informação		Sistema – tempo de design	*"indivíduo"*	Na**	Na
Espaço de comunicação		Sistema – tempo de design	*"espaço de publicação do indivíduo"*	Na	Na
Informação do indivíduo	**Expressão**	Sistema – tempo de design	*"tipada"*	Na	Na
	Conteúdo	Sistema – tempo de design	*"muito pessoal"*	Na	Na
Persistência temporal		Sistema – tempo de design	*"permanente"*	Na	Na
Audiência		Indivíduo	{*"selecionada"*, *"limitada"*, *"ilimitada"*}	Na	Na
Notificação para o indivíduo		Sistema – tempo de design	*"ausente"*	Na	Na
Discurso sobre o indivíduo		Sistema – tempo de design	*"destaque"*	Na	Na
Disseminação da informação		Sistema – tempo de design	*"ausente"*	Na	Na

*Quando os valores aparecem entre chaves, indica–se que a dimensão terá seu valor definido em tempo de uso, podendo assumir qualquer valor desse conjunto.
**Não se aplica.

A Tabela 5.13 apresenta a nossa interpretação sobre as decisões do designer em relação às dimensões de privacidade do MDP para o tipo de comunicação (3) (*"o indivíduo interage com o website de outro usuário"*). A representação visual da modelagem deste tipo de comunicação é mostrada na Figura 5.26.

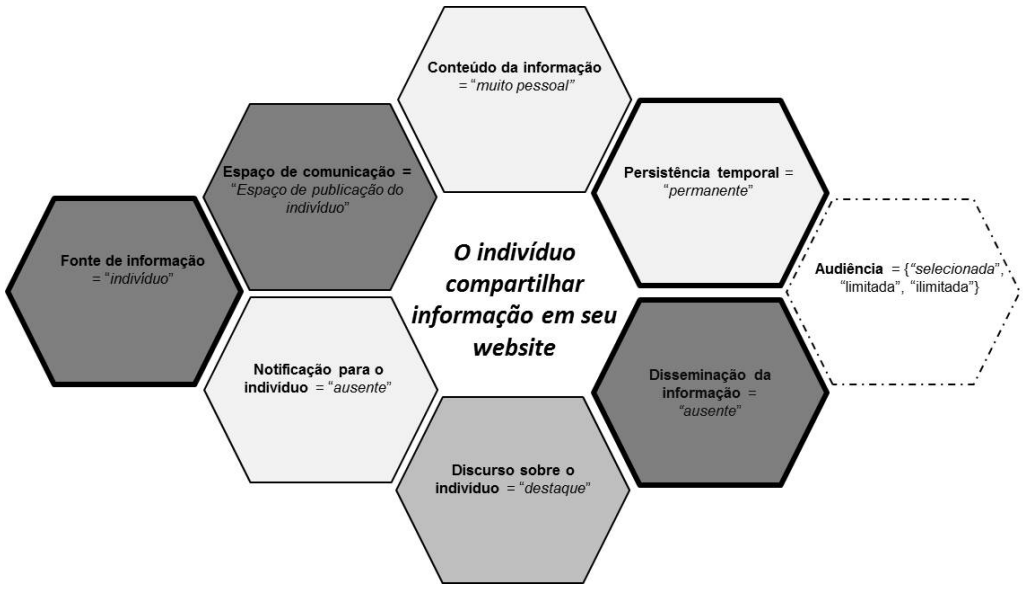


Figura 5.25. Representação visual do tipo de comunicação (2) do CaringBridge

Tabela 5.13. Modelagem do tipo de comunicação (3) do CaringBridge

		Controle	Valor*	Dependência de controle	Dependência de valor
Fonte de informação		Sistema – tempo de design	*"indivíduo"*	Na**	Na
Espaço de comunicação		Sistema – tempo de design	*"espaço de outro usuário"*	Na	Na
Informação do indivíduo	**Expressão**	Indivíduo	{*"tipada", "predefinida"*}	Na	Na
	Conteúdo	Definido em tempo de uso	{*"pouco pessoal", "levemente pessoal", "pessoal", "um tanto pessoal", "muito pessoal"*}	Expressão	Na
Persistência temporal		Sistema – tempo de design	*"permanente"*	Na	Na
Audiência		Sistema – tempo de design	*"desconhecida"*	Na	Na
Notificação para o indivíduo		Sistema – tempo de design	*"ausente"*	Na	Na
Discurso sobre o indivíduo		Sistema – tempo de design	*"ausente"*	Na	Na
Disseminação da informação		Sistema – tempo de design	*"ausente"*	Na	Na

*Quando os valores aparecem entre chaves, indica–se que a dimensão terá seu valor definido em tempo de uso, podendo assumir qualquer valor desse conjunto.
**Não se aplica.

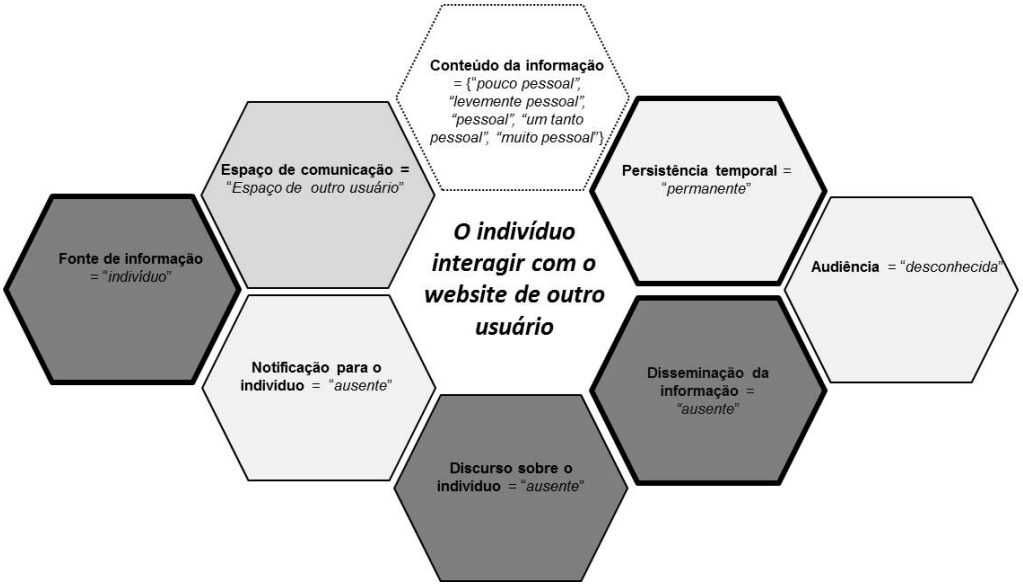


Figura 5.26. Representação visual do tipo de comunicação (3) do CaringBridge

A partir da nossa análise do CaringBridge com base nas dimensões de privacidade do MDP, identificamos alguns aspectos interessantes relacionados à privacidade nesse sistema. Em primeiro lugar, apenas o indivíduo (representando a pessoa que está enfrentando um problema grave de saúde) pode ser a **fonte de informação** sobre ele no sistema. Isso lhe concede um maior controle sobre o seu nível de privacidade, no sentido de permitir que ele tenha o controle sobre a informação que está sendo compartilhada, bem como sobre o espaço onde a comunicação ocorre.

Além da dimensão **fonte de informação**, as dimensões **persistência temporal** e **disseminação da informação** também possuem seus valores definidos pelos designers do CaringBridge e fixos para todos os tipos de comunicação. Assim, o valor da dimensão **persistência temporal** é igual a *"permanente"*, tendo em vista que toda informação pessoal compartilhada no CaringBridge fica acessível para a sua audiência durante todo o tempo de sua existência, enquanto ela não for voluntariamente excluída pelo usuário, o que remete a um nível mais baixo de privacidade. Por outro lado, remetendo a um nível mais alto de privacidade, a dimensão **disseminação da informação** tem o seu valor igual a *"ausente"*, uma vez que o CaringBridge não permite que as informações compartilhadas pelo indivíduo sejam disseminadas, em nenhuma situação, por outros usuários, o que remete a um nível mais alto de privacidade.

Em relação às dimensões do MDP cujos valores variam entre os tipos de comunicação no CaringBridge, primeiramente, no que tange à dimensão **espaço de comunicação**, vimos que o compartilhamento de informação sobre o indivíduo pode ocorrer tanto em seu perfil ou website, como no website de outro usuário. Quando o indivíduo

compartilha em seu próprio espaço, temos que ele pode alcançar um nível maior de privacidade, tendo em vista que ele possui o controle sobre quem será a **audiência** da informação. Nesse caso, a audiência pode variar desde apenas o *"indivíduo"* até um público *"limitado"* a todos os usuários do sistema (para informações de perfil), ou desde apenas um grupo *"selecionado"* de pessoas (convidadas pelo indivíduo) até um público *"ilimitado"*, que abrange pessoas que não são usuárias do sistema (para websites). Por outro lado, quando o indivíduo compartilha informação no website de outro usuário, é este que controla a **audiência**, que é *"desconhecida"* do indivíduo, o que portanto remete a um nível mais baixo de privacidade.

Em relação ao **conteúdo** da informação compartilhada no CaringBridge, temos que o seu nível de pessoalidade é definido em tempo de design, tendo em vista que a **expressão** de todas as informações compartilhadas no CaringBridge é *"tipada"* (com exceção do caso em que o indivíduo visita, curte atualizações ou aceita uma tarefa em um website de outro usuário, em que a expressão é *"predefinida"*). Assim, no caso do compartilhamento de informações pelo indivíduo em seu espaço, as informações de perfil (que abrangem a cidade e o estado onde o indivíduo reside e websites que ele visita) são classificadas no nível *"um tanto pessoal"* e as informações compartilhadas em seu website, que estão relacionadas ao seu estado de saúde, estão no nível *"muito pessoal"*. Por outro lado, quando o compartilhamento ocorre em um website de outro usuário, as informações sobre o indivíduo que estão sendo compartilhadas, nesse caso, dizem respeito à sua interação com as informações de outra pessoa (como assinar o livro de visitas, aceitar tarefas a serem realizadas, curtir e comentar atualizações). Nos três primeiros casos, o **conteúdo** da informação pode ser classificado como *"pouco pessoal"*, tendo em vista que não está relacionado de forma direta ao indivíduo (apesar de consistir em interações sobre informações muito pessoais, mas de outra pessoa). No entanto, no caso de comentários, o indivíduo define o nível de pessoalidade relacionado ao conteúdo, tendo em vista que, como é um campo de texto livre na interface, ele pode expor a sua relação com o dono do website, situações que passaram juntos, sentimentos, dentre outros tipos de informações, cujo conteúdo pode remeter a níveis mais altos de pessoalidade.

Em relação às dimensões relacionadas aos efeitos da comunicação que podem ter os seus valores variando entre os tipos de comunicação, temos, primeiramente, que o CaringBridge não notifica o indivíduo quando outros usuários curtem comentários que ele faz no website de outras pessoas, ou quando outros usuários interagem com as informações que ele disponibiliza em seu website. Assim, nesses casos, o valor da dimensão **notificação para o indivíduo** é *"ausente"*. Já para informações que o indivíduo compartilha em seu perfil, o CaringBridge não permite que outros usuários sequer in-

terajam sobre elas, sendo, nesse caso, a dimensão **notificação para o indivíduo** não aplicável. Para a dimensão **discurso dsobre o indivíduo,** o CaringBridge não faz nenhum discurso sobre a informação que o indivíduo compartilha em seu perfil e nem sobre as suas interações no website de outros usuários, sendo, nesses casos, o seu valor igual a *"ausente"*. Para o compartilhamento de informações no website do indivíduo, o **discurso sobre o indivíduo** é caracterizado pelo fato do CaringBridge chamar a atenção dos usuários que visitam o website sobre a atualização da informação ocorrida ali, sendo então esse discurso apenas de *"destaque"*. Assim, temos que as dimensões de efeitos da comunicação remetem, de um modo geral, a níveis mais altos de privacidade, tendo vista que, apesar do CaringBridge não notificar o indivíduo sobre ações que outros usuários executam sobre a sua informação (caso essas sejam possíveis), o seu discurso sobre as informações compartilhadas pelo indivíduo é ausente ou apenas de destaque, e a disseminação da informação do indivíduo não é permitida.

Assim, percebemos que o fato dos efeitos da comunicação remeterem a níveis mais altos de privacidade apresenta-se como uma compensação ao compartilhamento de informações muitos pessoais que ocorre no sistema. Tal compensação é importante, no sentido de possibilitar que o indivíduo alcance seu estado maiores de privacidade.

5.3.4 Usando o MDP para diferenciar RSOs sob o ponto de vista de privacidade

A partir das modelagens reversas do Facebook, do ResearchGate e do CaringBridge (mostradas nas subseções 5.3.1, 5.3.2 e 5.3.3, respectivamente), de acordo com as dimensões de privacidade do MDP, conseguimos identificar alguns aspectos que diferenciam esses três sistemas, no que concerne à privacidade relacionada ao compartilhamento de informações pessoais. A Tabela 5.14 mostra uma comparação dessas três RSOs, a partir dos resultados obtidos com a criação de seus modelos MDP.

Primeiramente, observamos que em todos os três sistemas analisados a informação sobre o indivíduo pode ser compartilhada tanto em seus **espaços de comunicação** (perfil e publicação), como no espaço de outro usuário, o que remete a níveis alto e baixo de privacidade, respectivamente. Além disso, a **persistência temporal** das informações compartilhadas nos três sistemas é permanente, o que remete a um nível baixo de privacidade.

Dessa forma, focando no que diferencia esses sistemas em relação ao estado de privacidade que oferecem aos seus usuários, observamos inicialmente a quantidade de oportunidades de compartilhamento de informação pessoal, e percebemos que no Facebook e no ResearchGate o número delas é maior, em comparação ao CaringBridge.

Tabela 5.14. Comparação das modelagens MDP das RSOs Facebook, ResearchGate e CaringBridge

Característica / Dimensão \ RSO	Facebook	ResearchGate	CaringBridge
Número de oportunidades de compartilhamento de informação pessoal	Maior	Maior	Menor
Fonte de informação	*Indivíduo* e *outro usuário*	Apenas o *indivíduo*	Apenas o *indivíduo*
Espaço de comunicação	*Espaço do indivíduo* e *espaço de outro usuário*	*Espaço do indivíduo* e *espaço de outro usuário*	*Espaço do indivíduo* e *espaço de outro usuário*
Conteúdo da informação	Definido na maior parte das vezes em **tempo de uso**	Definido na maior parte das vezes em **tempo de design**, como *"pouco pessoal"*	Definido na maior parte das vezes em **tempo de design**, como *"muito pessoal"*
Persistência temporal	*Permanente*	*Permanente*	*Permanente*
Audiência	Definida na maior parte das vezes em **tempo de uso**	Definido na maior parte das vezes em **tempo de design**, como *"ilimitada"*	Definida na maior parte das vezes em **tempo de uso**
Notificação para o indivíduo	*Completa*	*Parcial* ou *ausente*	*Ausente*
Discurso sobre o indivíduo	*Destaque,* nos níveis direto e inferencial	*Ausente* ou *destaque*, no nível direto *Destaque e Novo,* no nível inferencial	*Ausente* ou *destaque,* no nível direto
Disseminação da informação	Definido em **tempo de uso**, de acordo com o valor da dimensão **audiência** e com características da **informação** compartilhada	*Ilimitada*, na maior parte das vezes	*Ausente*

Assim, presume-se que as oportunidades de surgimento de questões de privacidade nos dois primeiros sistemas também tendem a ser maiores, ou os aspectos de privacidade nesses tendem a ser mais complexos. No entanto, antes de tirar qualquer conclusão em relação à complexidade das questões de privacidade nesses sistemas, é preciso olhar minuciosamente para como o compartilhamento de informações em cada um deles é caracterizado, de acordo com as dimensões de privacidade do MDP.

No Facebook, temos que, além do próprio indivíduo, outros usuários também podem ser a **fonte de informação** sobre o mesmo, enquanto que no ResearchGate e no CaringBridge apenas o indivíduo pode ser a **fonte de informação**. Como consequência, existe uma possibilidade maior do indivíduo alcançar um estado indesejado de privacidade no Facebook, quando comparado a esses outros dois sistemas. Isso ocorre porque, quando outro usuário é a fonte de informação, o indivíduo possui pouco

ou nenhum controle sobre a informação que vai ser compartilhada sobre ele, que pode se enquadrar em qualquer nível de pessoalidade e, consequentemente, remeter a níveis altos ou baixos de privacidade. Por exemplo, um estado indesejado de privacidade pode ocorrer para o indivíduo quando outros usuários compartilham uma informação muito pessoal sua, para uma audiência que ele não pode controlar, ou pode nem mesmo conhecer (quando o compartilhamento ocorre na linha do tempo de outro usuário).

Além disso, no Facebook, observamos que o **conteúdo da informação** e a **audiência** são definidos, na maior parte das vezes, em tempo de uso. O usuário, nesse caso, pode escolher se deseja definir uma audiência padrão para o seu espaço de comunicação, ou definir uma audiência diferente para cado ato comunicativo, ou seja, para cada instância de compartilhamento de informação pessoal. Em ambos os casos, o usuário pode atingir um estado indesejado de privacidade, caso ele inadvertidamente compartilhe uma informação muito pessoal com uma audiência mais ampla do que a pretendida.

No ResearchGate, diferente do Facebook, o **conteúdo da informação** e a sua **audiência** são definidos em tempo de design (com exceção das informações compartilhadas no perfil do indivíduo). Assim, os valores dessas dimensões estão relacionados ao tipo de comunicação, e não a uma instância específica da comunicação referente ao compartilhamento de informação pessoal. Tal fato tira o controle que o usuário possui em relação ao seu estado de privacidade no ResearchGate. Porém, como as informações compartilhadas são predominantemente *pouco pessoais* e o indivíduo é a única **fonte de informação**, as possibilidades deste alcançar um estado indesejado de privacidade são reduzidas, mesmo que a audiência seja predefinida como *"ilimitada"*. Além disso, o foco em informação profissional e uma ampla audiência estão em linha com o propósito do ResearchGate, que é permitir o compartilhamento e acesso à produção, ao conhecimento e à experiência científica[11].

Já no CaringBridge, diferente do Facebook e do ResearchGate, o **conteúdo da informação** é sempre definido em tempo de design, e a **audiência** é definida na maior parte das vezes pelo usuário, em tempo de uso. Dessa forma, o usuário tem controle parcial sobre a sua privacidade. O **conteúdo da informação** é, na maior parte das vezes, *muito* ou *um tanto pessoal*, o que remete a níveis baixos de privacidade. No entanto, apenas o indivíduo pode ser a **fonte de informação**, indicando que ele tem sempre o controle sobre o que vai ser compartilhado sobre ele dentro do sistema, além de poder controlar, na maior parte das vezes, a audiência para as informações que compartilhar. Neste caso, o indivíduo pode escolher uma audiência que abrange,

[11]Conforme colocado em https://www.researchgate.net/about (acesso em janeiro de 2016).

no caso de informação de perfil, apenas ele ou todos os usuários do sistema. No caso do compartilhamento de informações no website, o indivíduo pode selecionar uma audiência que abrange desde pessoas específicas convidadas por ele, passando por todos os usuários do sistema, até pessoas que nem mesmo sejam usuárias, remetendo, neste caso, a níveis baixos de privacidade. Essa situação específica, em que se tem conteúdo muito pessoal compartilhado com uma audiência ilimitada, pode resultar em um estado indesejado de privacidade para o indivíduo. No entanto, tal fato pode ser atenuado devido ao propósito do CaringBridge de angariar apoio, seja no campo psicológico, emocional ou até mesmo financeiro, para pessoas que estão enfrentando problemas graves de saúde[12].

Assim, no Facebook, quando comparado aos demais sistemas, os usuários possuem uma controle maior e mais fino sobre a privacidade da informação que eles compartilham em seu próprio espaço. Entretanto, o fato de outros usuários poderem ser a fonte de informação, além de se poder compartilhar informações muito pessoais e o indivíduo não conhecer a audiência quando o compartilhamento ocorre no espaço de outros usuários, cria oportunidades para o não atingimento do seu estado de privacidade desejado.

Vale ressaltar que no ResearchGate as informações mais pessoais são compartilhadas apenas no *espaço de perfil do indivíduo*. Para essas informações, a **audiência** não é tão ampla quanto para as publicações e questões e respostas que são compartilhadas. Embora o sistema possua o controle sobre a audiência da informação de contato do indivíduo, esta é "equilibrada", uma vez que tal informação apenas pode ser acessada por seguidores mútuos (usuários que seguem e são seguidos pelo indivíduo), ou seja, o indivíduo tem acesso às mesmas informações sobre as pessoas que têm acesso às suas informações. Já no CaringBridge, o indivíduo possui controle sobre a **audiência**, sempre que está postando no seu espaço, situação em que a expectativa é que esteja postando informações sobre sua saúde, que são *"muito pessoais"*. Quando o indivíduo compartilha informações no espaço de outro usuário, então ele não possui controle sobre a audiência, que inclusive é desconhecida para ele. No entanto, tal informação potencialmente seria menos pessoal, uma vez que está relacionada ao estado de saúde de outra pessoa e, portanto, não deveria levar o indivíduo a atingir um estado indesejado de privacidade.

Considerando as dimensões de efeitos da comunicação, observamos que o Facebook permite que os seus usuários tenham uma maior consciência sobre as ações de outros usuários em cima da sua informação, ou seja, a **notificação para o indivíduo**

[12]Conforme colocado em http://www.caringbridge.org/about-us (acesso em janeiro de 2016).

é *"completa"* para todos os tipos de comunicação. Por outro lado, no ResearchGate essa notificação é no máximo *"parcial"* e no CaringBridge *"ausente"*. No entanto, pode-se argumentar que o ResearchGate exige menos esse tipo de conscientização por parte de seus usuários, tendo em vista que ele permite que outros usuários interajam apenas sobre a informação pública do indivíduo, e nunca sobre informações mais pessoais, que são compartilhadas em seu perfil. Já no CaringBridge, outros usuários podem executar ações também sobre informações privadas do indivíduo e o sistema não notifica o indivíduo sobre tais interações, o que remete a um nível mais baixo de privacidade. No entanto, tais ações são realizadas sempre no espaço do indivíduo, o que, a rigor, indica que ele as veria sempre que acessar o seu espaço. Por outro lado, no Facebook e no ResearchGate, as ações de outros usuários sobre a informação do indivíduo podem ocorrer em outros espaços, que não sejam o dele próprio.

Em todos os sistemas, o discurso direto sobre o compartilhamento de informações do indivíduo é limitado a *"destaque"*. Porém, o Facebook e o ResearchGate ainda fazem discursos inferenciais sobre o indivíduo, que são as sugestões de amizade e de seguir pesquisador, respectivamente. Além disso, o ResearchGate ainda possui discursos inferenciais que geram novas informações sobre o indivíduo, que são as estatísticas de publicações e visualizações de perfil e o *RG Score*. No entanto, como a informação no ResearchGate tende a ser menos pessoal, os destaques, e até mesmo o novo discurso, estão relacionados a informações menos pessoais do que aquelas normalmente compartilhadas no Facebook e no CaringBridge. Finalmente, considerando a **disseminação da informação**, o seu valor depende da **audiência** de cada instância de informação compartilhada no Facebook, enquanto que no CaringBridge ela é *"ausente"*, e no ResearchGate é *"ilimitada"* para a maior parte dos compartilhamentos, exceto para o informações de perfil e comentários do indivíduo sobre publicação de outros usuários.

Assim, em resumo, podemos dizer que o Facebook oferece aos usuários, de uma forma geral, um maior controle do compartilhamento e uma maior percepção dos efeitos da comunicação resultantes mesmo, quando comparado aos outros dois sistemas. Isso faz sentido, primeiramente porque a informação aí compartilhada é potencialmente mais sensível, no que tange à privacidade, quando comparada à informação compartilhada no ResearchGate. Além disso, quando comparado ao Facebook, o CaringBeidge limita mais os efeitos comunicativos e o compartilhamento de informação por outros usuários, fatores que potencialmente poderiam facilitar que o indivíduo alcance estados indesejados de privacidade. O ResearchGate, de forma consistente com o CaringBridge, não permite que ocorram efeitos da comunicação relativos ao compartilhamento de informações mais pessoais, mas facilita o compartilhamento de outras informações que tendem a ser públicas e menos pessoais.

5.4 Avaliação com Potenciais Usuários

Conforme já mencionado, a avaliação envolveu seis participantes, todos com conhecimento em Engenharia Semiótica e na maior parte de suas ferramentas epistêmicas, através de estudo, uso ou pesquisa envolvendo as mesmas. Apenas um participante declarou não ter experiência prática em design de IHC, apesar de já ter utilizado e até mesmo desenvolvido pesquisa envolvendo algumas ferramentas epistêmicas da Engenharia Semiótica. Além disso, todos os participantes eram usuários frequentes de RSOs, acessando esses sistemas, na maior parte das vezes, mais de uma vez por dia, com exceção de um participante que acessa esse tipo de sistema menos de uma vez por semana. Todos os participantes já haviam também alterado suas configurações de privacidade nesses sistemas, pelo menos para estabelecer uma configuração padrão para o compartilhamento de suas informações.

Nesta seção, apresentamos os resultados gerados a partir do teste realizado com designers, no sentido de responder às questões QA1 e QA2. Assim, na subseção 5.4.1, mostramos os resultados relacionados aos modelos gerados pelos participantes, bem como ao seu entendimento e uso do MDP, no sentido de identificar o quão similar ou diferente foram os modelos gerados, e também se qualquer valor ou controle inesperados foram associados a alguma dimensão. Na subseção 5.4.2, apresentamos os resultados relacionados a como foi o entendimento, por parte dos participantes, das diferenças entre o Facebook e o ResearchGate, no que tange a aspectos de privacidade, a partir dos modelos MDP dos mesmos. Na subseção 5.4.3, apresentamos os principais argumentos relacionados à percepção dos participantes sobre os custos e benefícios do MDP. Por fim, extrapolando QA1 e QA2, fizemos uma avaliação da representação visual do MDP, e mostramos, na subseção 5.4.4, os resultados referentes ao uso que os participantes fizeram da mesma, tanto para fazerem a modelagem reversa de um tipo específico de comunicação, na tarefa 2, quanto para analisarem os modelos MDP que lhes foram apresentados, nas tarefas 3 e 4.

5.4.1 Entendimento e uso do MDP

Os indicadores referentes aos resultados mostrados nesta subseção foram obtidos a partir da execução pelos participantes das tarefas 1 e 2, detalhadas na seção 5.2. A análise dos dados empíricos coletados durante a realização dessas tarefas ocorreu em três passos: primeiramente, analisamos a modelagem realizada por cada participante na tarefa 1; em seguida, analisamos as modelagens consolidadas geradas pelas duplas, realizada na tarefa 2; e, por fim, analisamos os discursos das duplas referentes à discussão que

tiveram a fim de chegar aos modelos consolidados, bem como os discursos de todos os participantes durante a realização do grupo focal.

Todos os participantes foram capazes de gerar o modelo MDP completo para o tipo de comunicação solicitado, ou seja, atribuíram a cada uma das dimensões valores para os atributos *valor* e *controle*. Ao analisar os modelos gerados, observamos que não houve muitas discrepâncias entre os valores atribuídos às dimensões, e quando houve, as mesmas tenderam a ser resolvidas através das discussões entre os participantes (durante a realização da tarefa 2). Por outro lado, os participantes não compreenderam claramente o significado do atributo *controle*, tendo ocorrido diferenças nos valores atribuídos ao mesmo.

Para as dimensões **fonte de informação**, **espaço de comunicação**, **conteúdo da informação**, **persistência temporal** e **discurso sobre o indivíduo**, todos os participantes atribuíram os mesmos valores, que eram consistentes com as decisões de design do Facebook. Para as outras quatro dimensões – **expressão da informação**, **audiência**, **notificação** e **disseminação da informação** – houve diferenças entre os modelos. Ao analisar tais diferenças, percebemos que existiram diferentes razões que deram origem às mesmas.

Para a dimensão **expressão da informação**, apenas um participante atribuiu um valor diferente dos demais. Porém, para a dimensão **disseminação da informação**, quatro participantes atribuíram o mesmo valor e dois participantes atribuíram valores diferentes dos demais e entre si. Para a dimensão **audiência**, três participantes atribuíram o mesmo valor e os outros três atribuíram valores diferentes dos demais e entre si. Em todos esses três casos, através da discussão em duplas (realizada na tarefa 2), os participantes chegaram a um consenso sobre os valores, embora os modelos consolidados das duplas tenham diferido no que tange aos valores para essas dimensões. No entanto, todos esses valores se encaixavam em um intervalo de valores que tais dimensões poderiam assumir, ou, em outras palavras, os modelos estavam incompletos, uma vez que não representavam todos os valores possíveis, mas apenas um subconjunto deles.

No caso da dimensão **notificação para o indivíduo**, quatro participantes atribuíram a ela o mesmo valor e os outros dois participantes atribuíram valores diferentes. Neste caso, mesmo após a discussão em duplas, todos os modelos consolidados apresentaram valores distintos para tal dimensão. Porém, diferente do que ocorreu com as outras dimensões, ao analisarmos a discussão das duplas, percebemos que tal distinção de valores foi causada por uma percepção distinta dos participantes em relação ao funcionamento do Facebook no que tange à notificação. Assim, a dupla P1–P5 entendeu corretamente que o Facebook sempre notifica o indivíduo sobre interações de outros

usuários com a sua informação. A dupla P2–P4 mostrou inicialmente ter o mesmo entendimento de P1–P5, no sentido de considerar que o Facebook, como configuração padrão, sempre notifica o indivíduo nesses casos. Porém, tal dupla acredita que é permitido ao indivíduo definir situações específicas sobre as quais não deseja ser notificado. A dupla formada por P3–P6, por outro lado, após longa discussão, chegou à conclusão de que o indivíduo pode escolher se deseja receber uma **notificação** *"completa"* ou *"parcial"*, ou até mesmo não receber nenhuma notificação sobre a interação de outros usuários sobre a sua informação compartilhada dentro do Facebook.

Apesar das diferenças entre as modelagens, todas as três duplas foram capazes de expressar corretamente no MDP seus entendimentos acerca das dimensões de privacidade do Facebook (mesmo que alguns participantes não tenham entendido o funcionamento correto do mesmo). Em outras palavras, o uso que os participantes fizeram do MDP foi correto, considerando que o objetivo não era avaliar o entendimento que possuiam do Facebook. Além disso, não lhes foi concedida a oportunidade de inspecionarem o sistema durante a avaliação.

A atribuição de valores ao atributo *controle* mostrou-se muito mais difícil para os participantes. No grupo focal, alguns dos participantes referiram-se explicitamente a essa dificuldade, como pode ser visto nas falas de P2 e P6:

P2: *"Particularmente, eu acho a parte mais difícil [...], essa parte do controle, ela é um pouco abstrata. Não sei se é em virtude dessa nomenclatura, mas eu particularmente não sei que horas é o sistema e que horas sou eu que estou definindo as coisas...se é em tempo de design."*

P6: *"A gente teve um pouco de dificuldade...por exemplo, no controle, pra entender o que é controle."*

Essas dificuldades foram claramente percebidas a partir das discussões e dos modelos criados pelos participantes. Aparentemente, as principais dificuldades estavam relacionadas ao entendimento sobre: (1) o momento em que o valor era atribuído à dimensão, ou seja, se o valor era atribuído em tempo de design ou em tempo de uso, especificamente no caso em que o controle era do sistema; (2) a independência entre os atributos *controle* e *valor*. Um exemplo da dificuldade relacionada ao momento em que o valor era atribuído à dimensão pôde ser percebida no modelo criado por P1 durante a execução da tarefa 1, em que o usuário tinha que fazer a modelagem do tipo de comunicação *"o indivíduo compartilha informação sobre si mesmo em sua linha do tempo"*. Neste caso, P1 atribuiu o valor *"livre"* para a subdimensão **expressão** e determinou que o seu valor é definido pelo usuário, em tempo de uso. Entretanto, quando o designer deixa o valor da dimensão para ser definido em tempo de uso, significa que o usuário, ou mesmo o sistema, pode escolher entre diferentes valores. Assim, determinar que uma

dimensão será definida em tempo de uso implica que haverá um conjunto de valores possíveis que ela poderá assumir. No entanto, apesar de P1 ter definido que o valor da subdimensão **expressão** seria definido em tempo de uso, ele determinou um único valor para ela, o que é inconsistente, de acordo com as definições do MDP. Possivelmente, parece que houve um problema no entendimento das subdimensões **expressão** e **conteúdo** da informação por parte de P1, que provavelmente associou erroneamente o fato do **conteúdo** ser definido pelo usuário, em tempo de uso, ao controle sobre a subdimensão **expressão**.

Em relação à independência entre os atributos *controle* e *valor*, a discussão entre P3 e P6 sobre a dimensão **notificação para o indivíduo** ilustra que eles compreenderam incorretamente tais atributos como sendo dependentes entre si. Esses participantes acreditavam que no Facebook os usuários poderiam configurar quais tipos de notificações eles desejariam receber e quais não[13]. Neste caso, os participantes pensaram que não poderia ser dado o controle ao usuário para definir o valor para tal dimensão, a partir de um conjunto de valores que incluía o valor *"completa"*, uma vez que este que significa que o sistema *sempre* notifica o usuário sobre ações de outros usuários sobre a sua informação. Após uma longa discussão, os participantes foram capazes de compreender corretamente a relação entre *controle* e *valor*, e representaram seu entendimento do Facebook (que era, por sinal, incorreto) definindo o *controle* sobre a dimensão **notificação para o indivíduo** como sendo do usuário e o seu *valor* variando dentre três possíveis valores: *"completa"*, *"parcial"* e *"ausente"*, significando que o usuário poderia escolher, em tempo de uso, qual dos valores seria atribuído a tal dimensão.

Considerando que os participantes estavam usando o MDP pela primeira vez, era esperado que ocorressem dúvidas e dificuldades na sua compreensão. Assim, os resultados mostram que realmente eles tiveram algumas dúvidas no entendimento das dimensões e dos possíveis valores que as mesmas poderiam assumir. Entretanto, apesar de tais dificuldades, os participantes foram capazes de representar com sucesso as decisões de design de privacidade do Facebook (ou o seu próprio entendimento delas) através das dimensões do MDP. Por outro lado, o *controle* sobre as dimensões se mostrou como sendo a maior desafio para os participantes. Porém, tal dificuldade pode ter sido devido à situação do teste, considerando que o *controle* foi apenas brevemente explicado a estes. Assim, talvez uma explicação mais detalhada sobre tal atributo poderia ter sido suficiente para esclarecer as dúvidas dos potenciais usuários. Além disso, o fato de que quando o controle sobre a dimensão é do sistema ainda ser necessário

[13]De fato, no Facebook, os usuários podem configurar se desejam receber notificação através de e-mail ou não, mas o sistema **sempre** notifica o indivíduo quando outros usuários comentam, curtem ou compartilham alguma postagem sua.

representar duas situações distintas – controle é do sistema porque foi definindo em tempo de design pelo designer, ou será definido em tempo de uso pelo sistema a partir de algum processamento – aparentemente dificultou ainda mais a sua compreensão por parte dos participantes.

5.4.2 O Uso do MDP para caracterizar RSOs distintas com relação à privacidade

Os indicadores referentes aos resultados mostrados nesta subseção foram obtidos a partir da execução pelos participantes das tarefas 3 e 4, detalhadas na seção 5.2. A análise dos dados empíricos, coletados durante a realização dessas tarefas, ocorreu em três passos. Primeiramente, analisamos o registro por escrito que cada dupla fez sobre as diferenças de privacidade que identificaram a partir das modelagens das duas RSOs, e suas implicações na privacidade do sistema como um todo. Em seguida, verificamos se as duplas conseguiram identificar corretamente qual era a RSO de propósito geral e qual era a de propósito profissional e analisamos suas justificativas. Por fim, analisamos os discursos que as duplas tiveram durante a realização das tarefas referentes a esta parte do teste, bem como os discursos de todos os participantes durante a realização do grupo focal.

Ao analisarem os modelos MDP das RSO 1 e RSO 2, duas das três duplas o fizeram por tipo de comunicação, ou seja, compararam os tipos de comunicação equivalentes dos dois sistemas. A terceira dupla, formada por P1–P5, entendeu incorretamente a tarefa referente à comparação entre os dois sistemas e trabalhou por um tempo executando a tarefa errada[14]. No entanto, quando o erro foi identificado e a dupla compreendeu o que deveria ser feito, restava pouco tempo para concluir a tarefa.

Assim, a dupla P1–P5 fez uma análise mais geral sobre as diferenças entre as duas RSOs, apontando que a RSO 1 (Facebook) era mais flexível do que a RSO 2 (ResearchGate), uma vez que permitia que um número maior de dimensões fossem definidas em tempo de uso. A dupla concluiu que tal flexibilidade é importante no sentido de permitir que os usuários atinjam níveis mais altos de privacidade, como ilustrado por P5 em suas considerações:

P5: *"Na RSO 1, a pessoa tem um maior nível de privacidade do que na RSO 2 [...], por causa da concentração de cores mais escuras [na representação visual] e também da pessoa ter uma maior liberdade para definir [...]. Agora, na RSO 2, tem só duas dimensões que a pessoa tem liberdade para definir [o valor]. Então isso diminui*

[14] A dupla entendeu que deveria comparar entre si os dois tipos de comunicação da mesma RSO (e não das duas RSOs).

um pouco a privacidade. Ela não tem muita liberdade [...]. Isso reforça que o indivíduo tem maior controle sobre a privacidade na RSO 1 do que na RSO 2."

As demais duplas (P2–P4 e P3–P6) fizeram a análise dos dois sistemas comparando os valores e controles de cada uma das dimensões, para cada um dos dois tipos de comunicação na RSO 1 e na RSO 2. Assim, a partir das diferenças encontradas, elas analisaram a privacidade para cada um dos tipos de comunicação (e não para a RSO como um todo). As conclusões das duas duplas são consistentes entre si, como mostrado a seguir.

Para o primeiro tipo de comunicação (*"o indivíduo compartilha informação em seu perfil"*), foi constatado que os usuários estão mais sujeitos a terem a sua privacidade violada na RSO 1 (Facebook) do que na RSO 2 (ResearchGate), uma vez que a RSO 2 apresenta um controle mais adequado de privacidade. A justificativa para tal conclusão foi baseada nas dimensões do MDP. As duplas comentaram que na RSO 2 o valor da dimensão **discurso sobre o indivíduo** é *"ausente"*, enquanto que na RSO 1 seu valor é *"destaque"*, que remete a um nível menor de privacidade. Além disso, na RSO 2, a dimensão **disseminação da informação** tem o seu valor definido como *"ausente"*, enquanto que na RSO 1 seu valor é definido em tempo de uso, o que pode levar o indivíduo a um estado de privacidade menor, caso valores mais permissivos sejam atribuídos a tal dimensão.

Para o segundo tipo de comunicação (*"o indivíduo compartilha informação sobre ele em seu espaço"*), as duplas concluíram que o controle de privacidade na RSO 1 (Facebook) era mais adequado do que na RSO 2 (ResearchGate). A justificativa foi porque na RSO 1 o usuário possui uma maior liberdade para escolher o que quer compartilhar e com quem, além de poder definir, de algum modo, como será a disseminação dessa informação dentro do sistema. Na RSO 2, por outro lado, a **audiência** e a **disseminação da informação** são sempre *"ilimitadas"*, remetendo a níveis mais baixos de privacidade, embora o **conteúdo** da informação seja *"pouco pessoal"*. A fala de P6 ilustra esse ponto de vista: *"É interessante que quanto mais poder você oferece ao usuário, eu acho que teoricamente é melhor né?! Ele escolhe o que vai fazer...é igual na vida, você que escolhe o que vai compartilhar"*. A dupla P2–P4 também considerou em sua explicação que os valores das dimensões **espaço de comunicação** e **notificação para o indivíduo** estão associados a níveis mais altos de privacidade na RSO 1, quando comparados aos valores das mesmas dimensões na RSO 2.

Quando foi solicitado aos participantes para associarem cada uma das RSOs a um contexto (geral x profissional), as duplas P2–P4 e P3–P6 indicaram que a RSO 1 (Facebook) era a de propósito geral e a RSO 2 (ResearchGate) era a de propósito profissional. Elas explicaram que a flexibilidade oferecida aos usuários para escolherem

o **conteúdo** a ser compartilhado e a sua **audiência** foi um fator determinante para identificarem que a RSO 1 era de propósito geral. Elas também argumentaram que faz sentido a RSO 2 estar associada a um contexto profissional, tendo em vista que informações sobre trabalho são menos pessoais e podem ter uma audiência pré-definida. A dupla P3–P6 acrescentou em sua justificativa para a RSO 2 ser de propósito profissional o fato de permitir apenas o compartilhamento de informações pouco pessoais no espaço de publicação do indivíduo e, de acordo com o que constataram a partir de suas discussões, informações de trabalho são consideradas pouco pessoais. A discussão de P6 com P3 ilustra este ponto:

P6: *"[o que caracteriza essas duas redes] acho que é a sensibilidade da informação: na rede social [de propósito geral], você pode sair publicando o que você quiser, e na rede profissional, não. Eu acho que esse conteúdo "pouco pessoal" ajuda a decidir [...]. No meu ponto de vista, se tem um propósito específico, você vai institucionalizar mais a comunicação para atingir aquele público, se é de propósito geral, você vai oferecer um monte de opções para o usuário."*

Embora a dupla P1–P5 também tenha identificado que a RSO 1 oferece mais controle aos usuários sobre o compartilhamento de informações do que a RSO 2, ela associou a mesma a um contexto profissional. A explicação que tal dupla deu para a sua constatação foi a seguinte: *"Observou-se que quando se tem um espaço de comunicação público [referindo-se à RSO 2], este se refere a um espaço para discussões mais gerais. Além disso, a privacidade e o controle em uma rede profissional deve ser maior do que em uma rede geral"*. Por essa justificativa, parece que a dupla P1–P5 estava provalemente pensando em um tipo mais específico de rede profissional, em que poderiam ser compartilhadas informações proprietárias ou informações que não deveriam (ainda) ser amplamente compartilhadas. Assim, como não foi falado aos participantes o contexto específico da rede de propósito profissional, o cenário considerado pela dupla P1–P5 pode ser considerado plausível.

Os resultados apresentados nesta seção mostram que, embora os participantes não tivessem qualquer outra informação sobre as RSOs analisadas, além dos seus modelos MDP, eles foram capazes de descrever seus modelos de privacidade e identificar diferenças relevantes entre elas. Os argumentos apresentados para explicar suas conclusões descrevem suas considerações sobre como o significado das dimensões, seus valores e controle impactam na privacidade geral do sistema. Quando informados sobre os contextos a que as RSOs se referiam, conforme foi mostrado, duas duplas foram capazes de associar corretamente as RSOs a seus contextos, com base apenas em seus modelos de privacidade, e a outra dupla (P1-P5), embora não tenha feito a associação esperada, fez considerações que poderiam se aplicar a um contexto plausível.

5.4.3 Custos e benefícios do MDP

Apesar das dificuldades experimentadas pelos participantes durante a realização das tarefas, em seus discursos durante o grupo focal eles comentaram sobre a utilidade do MDP na análise e modelagem de privacidade de RSOs. P2 destacou que, ao estruturar o espaço de design, o MDP facilita que o analista pense em diferentes aspectos de privacidade no sentido de alcançar uma visão geral da privacidade relacionada ao compartilhamento de informação pessoal no sistema:

P2: *"Acho que o ponto positivo [do MDP] é que ele te ajuda a ter uma visão geral de como a coisa funciona, a partir de aspectos separadamente [...]. E no fim você monta a análise da privacidade de uma forma geral, o que simplifica bastante [a análise]. Porque se você começar, no início, já pensando no todo, parece que você não sai do lugar. Eu acho que, nesse ponto, o modelo é um apoio interessante."*

Embora os participantes tenham mencionado o *controle* como uma das maiores fontes de dúvidas, eles reconheceram que ele é relevante no entendimento e na descrição de decisões de privacidade. Sobre esse tópico, P5 comentou:

P5: *"O fato de que a gente pode visualizar sobre o que o usuário tem o controle, que ele pode configurar a privacidade, nos permite entender o mínimo de controle que o usuário tem sobre o sistema, sobre sua própria privacidade, e o que o sistema está configurando para ele."*

Durante as discussões, no grupo focal, os participantes extrapolaram o contexto de análise em que eles utilizaram o MDP, e falaram sobre seu suporte a designers. P3, por exemplo, vislumbrou como seria o uso do MDP em tempo de design: *"Se você está desenvolvendo [...], você consegue pensar no cenário para o sistema que você vai desenvolver, e usar o modelo já pra prever situações [...], porque é muito difícil, quando você está desenvolvendo, pensar em possibilidades"*. Complementando o raciocínio de P3, P6 destaca a capacidade do MDP mostrar os possíveis valores que cada um desses elementos podem assumir, contribuindo na composição do estado de privacidade alcançado pelo indivíduo em uma RSO: *"o modelo te ajuda mostrando todas as possibilidades, né?! [...] Aí eu escolho qual eu vou adotar para aquele sistema, para aquela funcionalidade, e aí sim fica muito melhor, porque você sabe o que você está fazendo e não escolhe qualquer valor"*.

Os participantes também evidenciaram o valor do MDP durante o design de RSOs, no sentido de despertar reflexões sobre aspectos que não pensariam sem o seu uso, como pode ser evidenciado no discurso de P2:

P2: *"Levanta uma relação causa efeito [...]: 'isso aqui ser publicado em espaço público tem impacto aonde? Essa informação vai ficar ali pra vida inteira' [...], esse*

tipo de coisa. Então ele [o MDP] ajuda a levantar vários aspectos que, as vezes o cara não iria pensar na hora que ele tá projetando."

Os participantes também levantaram a questão do custo do MDP, como pode ser visto no comentário de P3: *"[...] a questão do custo, como todo modelo, é alto...você tem que modelar cada uma das comunicações, pra você poder ver..."*. Entretanto, P6 mostra a sua opinião no sentido de acreditar que o benefício trazido pelo uso do MDP no projeto de RSOs justifica o seu custo: *"Eu acho, assim, se vai ser projetado um software social [...], que quem vai fazer esse sistema tem que pagar esse custo [...] de projetar a privacidade"*.

Finalmente, P2 mencionou que acreditava que a aplicação imediata do MDP seria mais como uma ferramenta analítica do que para suportar o design: *"Se você pegar a nossa realidade, quem vai projetar uma rede social do zero? É mais difícil. Então, a aplicação do modelo hoje, que a gente vê, é em análise...assim, a aplicação imediata...é lógico que pode surgir, mas a aplicação imediata é em análise"*. Porém, outros participantes argumentaram que alguns tipos de projetos, como os de softwares comunitários, poderiam também ser considerados como redes sociais, e que atualmente a maioria das aplicações que estão sendo desenvolvidas são colaborativas, necessitando, portanto, de que se projete um modelo de privacidade.

5.4.4 A representação visual como apoio ao entendimento e uso do MDP

Os indicadores referentes aos resultados mostrados nesta subseção foram obtidos a partir do uso do protótipo da ferramenta de visualização do MDP, durante a realização da tarefa 2, bem como da representação visual dos modelos MDP do Facebook e do ResearchGate, nas tarefas 3 e 4. Analisamos então os discursos que as duplas tiveram durante a realização dessas tarefas, bem como os discursos de todos os participantes durante a realização do grupo focal.

Os participantes destacaram que o uso da representação visual os ajudou a entender melhor a modelagem que fizeram com o MDP e os seus efeitos, bem como a ter uma visão mais clara das relações entre as dimensões dentro do modelo. P4, por exemplo, apontou: *"Olhando a colmeia [fazendo referência ao conjunto de hexágonos que representam as dimensões de privacidade do MDP], a gente conseguiu enxergar as relações entre os elementos 'tá vendo esse aqui: tá falando isso e isso [referindo-se às dimensões e seus valores], tem a ver com esse outro aqui, que tem a ver com aquele outro. Isso aqui [referindo-se ao valor de uma dimensão] talvez não tá batendo"'*. P3 também destacou a importância da representação visual no entendimento do MDP: *"O*

fato de ter uma representação visual, assim, ajudou bastante. Ela organiza um monte de informação de um jeito muito mais fácil. Tá tudo ali...você olha e já sabe"'.

Ao comparar as modelagens MDP das duas RSOs, nas tarefas 3 e 4, apesar de terem acesso também à representação tabular de tais modelagens, os participantes utilizaram a representação visual das mesmas. P6, por exemplo, ao iniciar a discussão sobre a comparação das duas RSOs com P3, expressou a sua preferência pela representação visual em relação à representação tabular das modelagens: *"Eu acho que essa tabela é irrelevante [...]. O desenho [referindo-se à representação visual] é muito bom [...]. Gostei, resolve o problema"*. P4, durante as discussões no grupo focal, também afirmou ter usado apenas a representação visual nesta parte da avaliação: *"Especificamente, sobre a tarefa de comparar os dois sistemas, a gente nem olhou as tabelas"*. P1 justificou o porquê de ter preferido utilizar a representação visual para comparar as duas RSOs: *"Pela questão das cores, o realce...você vê lá uma cor mais forte, questão da privacidade...na sua cara [...]. Se você pega o texto [se referindo ao texto na tabela], precisa ler. Já na [representação] visual, eu bato o olho e consigo identificar"*.

O uso de tonalidades diferentes de cores para representar os níveis de privacidade remetidos pelos valores das dimensões foi apontado pelos participantes como sendo de grande importância para o entendimento dos níveis de privacidade dos sistemas e, consequentemente, para diferenciá-los no que tange à privacidade. P6, por exemplo, ilustra isso em sua fala: *"Você vê um modelo todo preto, você já sabe que o nível de privacidade é alto, mas quando você vê um modelo todo claro, sabe que o nível de privacidade é baixo [...]. Foi muito útil ter as cores para tentar ver a diferença entre os modelos"*. P1, por sua vez, associou as cores com o baixo nível de controle concedido ao usuário: *"onde está mais escuro, eu já consigo entender que o usuário não tem tanta liberdade"*.

Entretanto, o uso da cor branca (ou ausência de preenchimento do hexágono correspondente à dimensão de privacidade), para representar que o valor da dimensão será definido em tempo de uso, foi apontado como sendo um problema pelos participantes. Nesse caso, o usuário pode incorretamente associar o "branco" (ou ausência de cor) ao nível mais baixo de privacidade, devido à sua proximidade com o tom mais claro de cinza, utilizado na representação visual do MDP para denotar tal nível. P6, por exemplo, expôs essa dificuldade da seguinte forma: *"Agora, tem aquela questão das cores [...], por exemplo, branco que significa quando [o valor] não é especificado, mas o branco, teoricamente, seria o nível mais baixo de privacidade. Então isso aí, a questão de significado ficou pobre, né?! Tinha que ser uma outra cor"* .

Os participantes também fizeram críticas diretamente ao protótipo da ferramenta de visualização, utilizada por eles na execução da tarefa 2, apontando algumas incon-

sistências na forma como os elementos do MDP eram apresentados na interface da ferramenta e fora dela. Além disso, os participantes fizeram sugestões de aspectos a serem incorporados na ferramenta, que foram considerados como trabalhos futuros. Uma das sugestões foi a incorporação de um sistema de ajuda, com a explicação sobre as dimensões de privacidade e os possíveis valores para seus atributos *valor* e *controle*. Além disso, P6 sugeriu estender o protótipo para fornecer feedback sobre aspectos no sistema que seriam críticos em relação à privacidade do indivíduo, com base nos valores atribuídos às dimensões do MDP, como destacado em seu discurso: *"Quando você usa [o MDP] pra análise [...], o feedback da ferramenta sobre os pontos que você precisa dar atenção, seria, no meu ponto de vista, fundamental. Aquele esquema lá, de audiência ilimitada e conteúdo muito pessoal, por exemplo, isso precisa ser destacado [...]. Então eu acho que seria fundamental, como ferramenta de análise, ter um feedback"*. Em outras palavras, a sugestão de P6 seria que se acrescentasse ao MDP um componente semântico que pudesse alertar o projetista para decisões que poderiam expor o usuário a estados de baixo nível de privacidade, e potencialmente, mais indesejáveis.

Dessa forma, percebemos que a representação visual se mostra como um importante suporte ao uso e entendimento do MDP, no sentido de melhorar a percepção dos designers sobre os efeitos das suas modelagens na forma como a privacidade relacionada ao compartilhamento de informações pessoais é tratada no sistema. Assim, vale a pena investir para que o protótipo possa se tornar uma ferramenta robusta para apoiar melhor o designer no uso do MDP.

5.5 Revisitando as Questões de Avaliação 1 e 2

Após termos apresentado os resultados da avaliação com especialista e da avaliação com potenciais usuários do MDP, nesta seção discutimos os indicadores que esses resultados geraram para as questões de avaliação QA1 e QA2, colocadas no início deste Capítulo.

Para responder a QA1 (*As dimensões de privacidade do MDP são capazes expressar decisões de privacidade em RSOs?*), nós a dividimos em dois aspectos: (a) Todas as oportunidades de compartilhamento de informação pessoal nas RSOs podem ser expressas através do MDP? Ou existe alguma decisão de design que não pode ser expressa através do mesmo? (b) Ao expressar decisões de privacidade através do MDP, existem quaisquer dimensões ou valores que são redundantes ou desnecessários? Em outras palavras, existem dimensões e/ou valores que não deveriam estar no MDP?

Assim, no sentido de obter resposta para a QA1, levamos em consideração a avaliação com especialista, em que efetuamos a modelagem reversa de privacidade

do Facebook, do ResearchGate e do CaringBridge, bem como a modelagem de um tipo específico de comunicação do Facebook, de acordo com as dimensões do MDP, realizada pelos potenciais usuários do mesmo. Na primeira avaliação, foram modelados cinco tipos de comunicação para o Facebook e para o ResearchGate, e três tipos para o CaringBridge. Em todos eles, fomos capazes de descrever todos os aspectos relacionados a decisões de privacidade para tais oportunidades de compartilhamento de informação pessoal. Além disso, ao contrastar as análises feitas para os três sistemas, percebemos que o modelo MDP dos mesmos foi capaz de representar as diferenças nas decisões de design de cada um deles, o que consiste em um indicador do poder expressivo do MDP.

Percebemos a partir dos modelos MDP (e sua descrição detalhada), que todas as dimensões foram necessárias para descrever de forma completa os aspectos envolvidos nas decisões de privacidade. Além disso, não há dimensões redundantes, ou seja, que descrevem os mesmos aspectos de privacidade. Como, na avaliação com especialista, fomos nós mesmos, que propomos o MDP, que realizamos a análise das RSOs fazendo uso do mesmo, a avaliação com potenciais usuários adicionou valor aos nossos resultados, ao mostrar que outras pessoas também podem usar o MDP para expressar decisões de privacidade. Nesta avaliação, os participantes fizeram a modelagem reversa de apenas um tipo de comunicação do Facebook fazendo uso do MDP, e a análise de suas modelagens mostra que para cinco (de um total de nove) dimensões do MDP, todos os participantes atribuíram os mesmos valores, a fim de expressar decisões de design de privacidade do Facebook. Esses foram os mesmos valores que atribuímos quando fizemos a análise do Facebook.

Por outro lado, considerando as outras quatro dimensões às quais os participantes atribuíram valores distintos, em uma delas (**notificação para o indivíduo**) tal diferença foi resultante de um entendimento incorreto sobre o funcionamento do Facebook. A dupla de participantes que entendeu tal funcionamento corretamente atribuiu à dimensão o mesmo valor que nós atribuímos em nossa análise.

As outras três dimensões (**expressão**, **audiência** e **disseminação da informação**) tinham seus valores definidos em tempo de uso, o que significa que elas podem assumir uma faixa de valores, e a principal diferença ocorreu porque os participantes atribuíram um conjunto incompleto de valores a tais dimensões, em relação ao conjunto que atribuímos, quando analisamos o sistema. A análise do discurso dos participantes mostrou que eles tiveram algumas dúvidas relacionadas a essas dimensões e seus possíveis valores, além de terem dificuldade em compreender o atributo *controle* das dimensões. Entretanto, as dúvidas eram relacionadas ao significado das dimensões e seus valores, e não foram indicativas de outras decisões que não pudessem ser expressas pelo MDP. De fato, essas dúvidas eram indicativas do custo de aprendizagem do MDP

e não de seu poder expressivo.

Na análise que fizemos do Facebook, observamos que algumas dimensões que tinham seus valores definidos em tempo de execução apresentavam dependências com outras dimensões, como, por exemplo, o valor da dimensão **disseminação da informação** pode depender do valor da dimensão **audiência**. Assim, embora essas dependências não possam ser devidamente expressas no MDP, isso não significa que novas dimensões ou valores deveriam ser incluídos no mesmo. Ao invés disso, tal fato indica que provavelmente seria válido investigar outro nível de abstração que pudesse ser adicionado ao MDP, a fim de que tais dependências possam ser representadas.

A análise da QA2 (*O MDP é descritivo o suficiente para expressar as diferenças em aspectos de privacidade em RSOs?*) foi executada com base em ambas as análises, a que realizamos, na avaliação com especialista, e a realizada com potenciais usuários do MDP, a fim de distinguir os sistemas em relação a aspectos de privacidade relacionados ao compartilhamento de informação pessoal.

A comparação que fizemos das RSOs que analisamos, na avaliação com especialista, foi capaz de apontar maiores diferenças nas decisões de design relacionadas à privacidade, com base nas dimensões do MDP e seus valores. Para muitas dessas decisões, fomos capazes de fazer considerações sobre a sua adequação ao objetivo geral do sistema e ao o seu contexto de aplicação. A comparação realizada pelos potenciais usuários, por outro lado, forneceu resultados especialmente interessantes. Embora os participantes não soubessem quais eram as RSOs modeladas, além de terem examinado apenas dois dos cinco tipos de comunicação desses sistemas, eles foram capazes de apontar os principais aspectos de privacidade em cada um deles, que foram consistentes com os resultados mais detalhados que obtivemos a partir de nossa análise.

Dessa forma, tais resultados são indicadores positivos de como um modelo MDP pode ser descritivo em relação a uma RSO, e como ele pode apoiar a comparação e discussão de diferentes decisões de design relacionadas à privacidade.

Por fim, temos que ambos os passos da avaliação (avaliação com especialista e avaliação com potenciais usuários), apresentados neste Capítulo, ilustram a expressividade do MDP, ao mostrar que ele pode ser utilizado tanto para descrever diferentes decisões de design, em RSOs voltadas para diferentes contextos, quanto para analisar essas diferenças.

Capítulo 6

Discussão

Neste capítulo, discutimos os principais aspectos relacionados à proposta do MDP de apoiar designers em suas decisões sobre privacidade em RSOs. Assim, incialmente, na seção 6.1, apresentamos algumas constatações que fizemos sobre tal modelo, bem como algumas limitações do mesmo. Em seguida, na seção 6.2, discutimos os resultados da avaliação que realizamos do MDP em um contexto de análise e apresentamos algumas considerações e limitações relacionadas à sua avaliação em um contexto real de uso. Encerramos o capítulo comparando o MDP com outras propostas de apoio ao design de privacidade em sistemas de informação com foco em interações sociais entre seus usuários, na seção 6.3.

6.1 Constatações e Limites do MDP

A partir da avaliação que fizemos do MDP como ferramenta de análise de RSOs, percebemos alguns aspectos interessantes em relação à sua estrutura, como o papel e a importância diferenciada das suas dimensões na composição do estado de privacidade alcançado pelos seus usuários, mostrados na subseção 6.1.1, e também em relação à sua utilização na análise da privacidade desses sistemas, discutidos na subseção 6.1.2. As limitações do MDP são discutidas nas seções 6.1.3 e 6.1.4.

6.1.1 O papel das dimensões do MDP no estado de privacidade do indivíduo

A partir da análise de diferentes RSOs com o uso do MDP, mostrada no Capítulo 5, podemos observar que as suas dimensões de privacidade apresentam importâncias distintas na caracterização do estado de privacidade de seus usuários.

Inicialmente, vimos que as dimensões **fonte de informação**, **conteúdo da informação** e **audiência** desempenham um papel diferenciado na caracterização da privacidade relacionada ao compartilhamento de informação pessoal em RSOs, em comparação às outras dimensões do MDP. Quando o MDP foi utilizado para diferenciar o Facebook, o ResearchGate e o CaringBridge, sob o ponto de vista de privacidade, conforme mostrado no Capítulo 5, na seção 5.3.4, essas foram as primeiras dimensões que se destacaram. Também na avaliação com potenciais usuários, foi chamada a atenção para essas dimensões[1], na diferenciação da privacidade no Facebook e no ResearchGate, conforme mostrado na seção 5.4.2.

Ao refletirmos sobre isso, percebemos que tal constatação é consistente com nosso pensamento relacionado à forma como ocorre o compartilhamento de informações pessoais dentro de uma RSO, levando-se em consideração a possibilidade do surgimento de problemas de privacidade para seus usuários. Neste caso, o que primeiro vem à nossa mente é a seguinte pergunta: "*quem* está compartilhando *o que* com *quem*?", o que remete às dimensões **fonte de informação** (relacionada ao primeiro *"quem"* da pergunta), **informação do indivíduo**, neste caso caracterizada pela subdimensão **conteúdo** (relacionada ao pronome interrogativo *"que"*), e **audiência** (relacionada ao segundo *"quem"* da questão). Dessa forma, podemos considerar essas três dimensões como sendo fundamentais na determinação do estado de privacidade do usuário em RSOs.

Tendo em vista a importância dessas dimensões na composição do estado de privacidade alcançado pelo indivíduo, percebemos que a combinação de valores assumidos simultaneamente pelas mesmas pode resultar em estados de privacidade que remetem a diferentes graus de exposição do indivíduo. A Tabela 6.1 mostra os estados de privacidade obtidos a partir da combinação de valores atribuídos em tempo de design a essas dimensões. Consideramos nessa tabela os valores extremos para as dimensões **conteúdo** e **audiência**, relacionados aos níveis mais alto e mais baixo de privacidade, uma vez que são eles que podem levar mais claramente a um maior grau de exposição do indivíduo. Para a dimensão **audiência**, consideramos também a possibilidade do valor poder ser definido pelo próprio indivíduo, em tempo de uso.

Conforme podemos verificar na Tabela 6.1, quando o próprio *"indivíduo"* é a **fonte de informação**, um **alto grau de exposição** irá ocorrer apenas quando ele compartilha uma informação cujo **conteúdo** seja *"muito pessoal"* (o que remete a um

[1]Diferente da análise que realizamos desses sistemas, nesse caso, como foram apresentadas aos participantes da avaliação apenas modelagens em que a **fonte de informação** era o próprio indivíduo, não foi dado destaque a esta dimensão na caracterização da privacidade oferecida pelos sistemas aos seus usuários.

Tabela 6.1. Níveis de exposição a partir das dimensões "Fonte de Informação", "Conteúdo" e "Audiência" do MDP

Dimensões de privacidade do MDP						**Grau de exposição do indivíduo**
Fonte de Informação		**Conteúdo**		**Audiência**		
Valor	**Nível de privacidade**	**Valor**	**Nível de privacidade**	**Valor**	**Nível de privacidade**	
Indivíduo	Alto	***Muito pessoal***	Baixo	***Indivíduo/selecionada***	Alto	Baixo grau de exposição
				Ilimitada/desconhecida	Baixo	**Alto grau de exposição**
				Definida pelo indivíduo	nd*	Baixo ou alto grau de exposição
		Pouco pessoal	Alto	***Indivíduo/selecionada***	Alto	Baixo grau de exposição**
				Ilimitada/desconhecida	Baixo	Baixo grau de exposição
				Definida pelo indivíduo	nd	Baixo ou alto grau de exposição
Outro usuário	Baixo	***Muito pessoal***	Baixo	***Indivíduo/selecionada***	Alto	**Alto grau de exposição**
				Ilimitada/desconhecida	Baixo	
				Definida pelo indivíduo	nd	Baixo ou alto grau de exposição
		Pouco pessoal	Alto	***Indivíduo/selecionada***	Alto	Baixo ou alto grau de exposição
				Ilimitada/desconhecida	Baixo	
				Definida pelo indivíduo	nd	

* não definido

** desejado sob o ponto de vista de privacidade, mas não sob o ponto de vista de possibilidades de interação

nível baixo de privacidade), com uma **audiência** *"ilimitada"* ou *"desconhecida"* (o que remete também a um nível baixo de privacidade). No caso do *"indivíduo"* compartilhar uma informação *"muito pessoal"*, um **baixo grau de exposição** será atingido quando o valor da dimensão **audiência** for igual a *"indivíduo"* ou *"selecionada"* (o que remete a um alto nível de privacidade).

Por outro lado, quando o *"indivíduo"* compartilha uma informação *"pouco pessoal"* (o que remete a um nível alto de privacidade), não se espera que ocorram questões de privacidade, mesmo caso a audiência seja *"ilimitada"* ou *"desconhecida"* (o que remete a um nível baixo de privacidade), e muito menos caso a audiência seja apenas o *"indivíduo"* ou *"selecionada"*. No entanto, neste último caso, as possibilidades de interação também ficam mais limitadas, o que pode ir contra o objetivo de RSOs de permitir a interação entre pessoas, através do compartilhamento de informações.

Assim, podemos dizer que, no caso do *"indivíduo"* ser a **fonte de informação**, as dimensões **conteúdo** e **audiência** tendem a ser conflitantes, ou seja, normalmente uma se contrapõe à outra, e pode não ser desejável que se tenha níveis igualmente baixos ou altos para ambas dimensões, simultaneamente. Assim, se o **contéudo** é *"muito pessoal"* (nível de privacidade baixo), pode-se desejar uma **audiência** que seja um *"indivíduo"* ou *"selecionada"* (nível de privacidade alto). Por outro lado, se o **contéudo** for *"pouco pessoal"* (nível de privacidade alto), pode-se desejar uma **audiência** mais ampla, como *"limitada"* ou *"ilimitada"* (nível de privacidade baixo).

Por fim, quando a **fonte de informação** é *"outro usuário"*, aumenta a possibilidade do compartilhamento de informação resultar em um estado indesejado de privacidade para o indivíduo, caracterizado por um alto grau de exposição do mesmo. Tal situação fica mais evidente no caso em que o **conteúdo** da informação compar-

tilhada é *"muito pessoal"*, o que remete a um baixo nível de privacidade. Neste caso, mesmo que o valor da dimensão **audiência** remeta a níveis mais altos de privacidade, questões de privacidade podem ocorrer pelo fato do indivíduo não ter o controle sobre a informação que é compartilhada sobre ele.

Embora as dimensões **fonte de informação**, **conteúdo da informação** e **audiência** sejam fundamentais na determinação do estado de privacidade do indivíduo, as demais dimensões do MDP também possuem papel relevante nesse sentido. Por exemplo, se a informação do indivíduo possui um **conteúdo** *"muito pessoal"*, a **persistência temporal** da mesma também terá impacto em sua privacidade. Assim, mesmo que a informação seja compartilhada com uma **audiência** mais ampla, se for por um período de **tempo** mais curto (*"instantâneo"* ou *"limitado"*), pode ser que se propicie ao indivíduo um estado de privacidade mais desejável do que se o compartilhamento fosse com uma **audiência** *"selecionada"*, mas ficasse disponível no sistema por um período indeterminado de tempo. As dimensões de efeitos da comunicação também podem alterar o estado de privacidade do indivíduo. Por exemplo, se a **disseminação da informação** puder ampliar a audiência original da informação compartilhada, ela pode levar o indivíduo, que a princípio estaria em um estado de privacidade com baixo grau de exposição, para um estado com alto grau de exposição. Além disso, se o sistema gerar novos **discursos** sobre o indivíduo, isso pode, por si só, gerar estados de privacidade indesejados para mesmo. Assim, percebemos que apenas as dimensões **fonte de informação**, **conteúdo da informação** e **audiência**, apesar de serem fundamentais, não definem o estado de privacidade do indivíduo, tendo em vista a importância das demais dimensões na composição do mesmo.

No entanto, a existência dessas dimensões fundamentais cria oportunidade para que se tenha um melhor compromisso entre a expressividade dos modelos criados com o MDP e o custo de utilização deste. Apesar de todas as dimensões serem importantes para a composição do estado de privacidade do indivíduo, pode-se desejar diminuir o custo de utilização do MDP, ao permitir que o designer leve em consideração em sua modelagem apenas algumas dimensões do MDP e as dimensões fundamentais seriam as primeiras a serem definidas. Nesse caso, obviamente a expressividade do modelo criado não será a mesma do que caso fossem definidos os valores para todas as dimensões do MDP. Porém o custo de modelagem é menor, o que pode ser útil em alguns contextos, em que o designer queira simplificar o uso do MDP.

Outro aspecto que identificamos foi que as demais dimensões, que não são as fundamentais, podem apresentar diferentes pesos ao impactarem o estado de privacidade do indivíduo. Assim, pode ocorrer que uma dimensão cujo valor remeta a um nível maior de privacidade tenha um impacto mais negativo no estado de privacidade do

indivíduo do que outra dimensão que remeta a um nível mais baixo de privacidade. Um exemplo disso pode ser percebido com as dimensões **discurso sobre o indivíduo** e **notificação para o indivíduo**. Neste caso, pode haver uma situação de modelagem em que a dimensão **discurso sobre o indivíduo** recebe o valor *"destaque"* (que remete a um nível médio de privacidade), e a dimensão **notificação para o indivíduo** recebe o valor *"ausente"* (que remete ao nível mais baixo de privacidade). Porém, o impacto negativo da primeira dimensão no estado de privacidade do indivíduo pode ser maior, no sentido do sistema dar destaque à informação compartilhada sobre ele para a sua audiência, do que o impacto do indivíduo não ser notificado sobre o que outras pessoas fazem com a sua informação que é compartilhada no sistema.

6.1.2 Níveis de análise da privacidade através do MDP

Vimos, a partir das análises que fizemos do Facebook, do ResearchGate e do CaringBridge, mostradas no Capítulo 5, que a modelagem MDP dos tipos de comunicação referentes às oportunidades de compartilhamento de informações pessoais nos possibilita fazer uma análise da privacidade geral do mesmo. Percebemos que, para que essa análise seja completa, faz-se necessário que ela ocorra nos níveis de *intracomunicação* e de *intercomunicação*. A análise *intracomunicação* consiste em olhar os valores de todas as dimensões dentro de cada tipo de comunicação e analisar o impacto desses valores na privacidade dos usuários. Além disso, essa análise é importante para verificar como as dimensões se relacionam em cada tipo de comunicação. Por exemplo, no ResearchGate, quando o valor da dimensão **conteúdo da informação** remete a um nível baixo de privacidade, ou seja, quando uma informação *"muito pessoal"* é compartilhada (quando o indivíduo compartilha determinadas informações em seu perfil), para compensar, o valor da dimensão **audiência** remete a um nível mais alto de privacidade, recebendo o valor *"selecionada"*, e a **disseminação da informação** é *"ausente"*. Assim, a partir da análise *intracomunicação*, fica evidente esse equilíbrio nos níveis de privacidade entre essas dimensões, bem como o seu impacto positivo no sentido dos usuários alcançarem graus menores de exposição.

Já a análise *intercomunicação* não olha cada dimensão separadamente, mas analisa os diferntes tipos de comunicação e o contexto referentes ao compartilhamento de informações pessoais no sistema. A partir dessa análise, iremos identificar a variação de níveis de privacidade entre os tipos de comunicação, o que pode trazer informações importantes sobre os estados de privacidade que podem ser atingidos pelos usuários. Por exemplo, com a análise *intercomunicação*, é possível perceber que no ResearchGate a informação muito pessoal é mais "restrita", enquanto que a menos pessoal é bastante

disseminada. No CaringBridge, por outro lado, a análise intercomunicação nos mostra que, como a informação compartilhada é geralmente muito pessoal, obtém-se um nível mais alto de privacidade ao permitir que a audiência seja mais restrita e ao oferecer poucas oportunidades para que efeitos da comunicação ocorram. Já no Facebook, embora seja oferecido uma maior flexibilidade e controle ao indivíduo quando ele é a fonte de informação, o sistema abre espaço para problemas de privacidade ao permitir que outros usuários também sejam fonte de informação sobre o indivíduo.

Assim, temos que as análises *intracomunicação* e *intercomunicação* possuem focos distintos e complementares, e devem ser realizadas em conjunto, no sentido de identificar o impacto das decisões de design nos estados de privacidade oferecidos aos usuários de RSOs.

6.1.3 Limites representacionais do MDP

Ao utilizar o MDP para modelar os tipos de comunicação referentes ao compartilhamento de informações pessoais em RSOs, algumas limitações foram observadas em seu poder de representação, que se subdividem em duas categorias: (a) limitações dentro do nível de abstração tratado atualmente pelo MDP; e (b) limitações relacionadas à necessidade de criação de outro nível de abstração para representar aspectos importantes a serem considerados na privacidade.

Quanto às limitações existentes dentro do nível de abstração tratado pelo MDP, percebemos que o mesmo se mostra limitado, no que diz respeito ao seu poder de representação, quando o tipo de comunicação modelado contempla um conjunto de informações, ao invés de uma única estrutura de informação. A modelagem MDP não explicita essa situação, não permitindo distinguir quando a informação compartilhada se refere a uma única estrutura de informação, como é o caso do Facebook, ou a um conjunto de estruturas de informação, como é o caso do compartilhamento de informações de perfil no ResearchGate, em que, por exemplo, *"informações de contato"* engloba endereço, telefone, contatos em outras redes sociais e data de aniversário. Assim, seria interessante investigar uma forma de representar, na modelagem do tipo de comunicação, a situação em que a informação compartilhada refere-se a várias estruturas de informação.

As demais limitações desse tipo identificadas estão relacionadas principalmente à sua representação visual. A primeira delas é que esta representação "perde", de algum modo, a estrutura do modelo de comunicação de Jakobson [1960], que estrutura as dimensões de comunicação usuário-sistema-usuário, mostrada na Figura 4.1. Embora exista uma tentativa de manter um índice de tal modelo na representação visual, atra-

vés do posicionamento dos hexágonos que representam as dimensões do MDP dentro do *beehive*, as informações referentes à estrutura de comunicação subjacente ao compartilhamento de informação são perdidas. Isso nos faz refletir sobre a necessidade de se fazer uma análise mais minuciosa sobre a real importância do modelo de Jakobson como estrutura subjacente ao MDP. Isso pode ser feito ao analisar qual seria o custo desta "perda" da referência ao modelo de Jakobson para o designer, quando o mesmo faz uso da representação visual. Caso este custo seja alto, deve-se reconsiderar então a sua representação visual, de modo que a mesma possa transmitir informações sobre tal modelo.

Outra limitação relacionada à representação visual do MDP é a modelagem de dependências entre dimensões, seja de controle ou de valor, que ocorre respectivamente quando o controle sobre uma dimensão, ou o valor da mesma, depende de algum aspecto ou valor de outra dimensão. Embora essas dependências possam ser registradas na representação tabular utilizada pelo MDP (mostrada no Capítulo 5 - Seção 5.3), as mesmas ainda não estão sendo consideradas em sua representação visual, apesar de serem importantes para explicar o porquê da definição de valores, ou até mesmo do controle, para certas dimensões ocorrer em tempo de uso. Assim, no sentido de superar essa limitação do MDP, a dependência poderia ser explicitada em sua representação visual através da utilização de símbolos diferenciados de acordo com o tipo de dependência (de valor ou de controle) que representam, que poderiam indicar a conexão entre duas dimensões, caso o valor ou controle de uma dimensão dependa do valor de outra dimensão. Além disso, na representação tabular, é registrada apenas a ocorrência da dependência, não sendo considerada nenhuma informação adicional sobre a mesma. Assim, um ponto a ser investigado é se apenas o registro da ocorrência da dependência é suficiente, ou se deveria ser possível também definir alguma sintaxe mais elaborada para representá-la.

Outro limite na representação visual do MDP, detectado na sua avaliação com potenciais usuários (conforme mostrado no Capítulo 5 - Seção 5.4.4), está relacionado à forma como as dimensões cujos valores são definidos em tempo de uso são representadas atualmente. O uso da cor branca (ou ausência de preenchimento) para denotar tal situação não deixa explícito visualmente a faixa de valores que a dimensão pode assumir, remetendo aos níveis mínimos e máximos de privacidade que podem ser oferecidos pelo sistema, através da mesma, em tempo de uso. Além disso, o fato da ausência de coloração ser representada (no papel ou no protótipo da ferramenta de visualização desenvolvida para dar suporte ao uso do MDP) pela cor branca, que está próxima do tom mais claro de cinza que é utilizado para representar o nível mais baixo de privacidade, pode confundir o usuário no momento em que está fazendo a análise da privacidade do

sistema, com base na representação visual das modelagens dos seus tipos de comunicação. Assim, seria interessante investigar a melhor forma de representar a dimensão cuja definição de valor só vai acontecer em tempo de uso. Algumas sugestões que poderiam ser analisadas seriam (a) utilizar algum tipo de textura e manter a indicação textual do intervalo de valores que pode ser assuido; (b) representar dentro da dimensão a variação das cores que ela poderia assumir (de forma bidimensional ou tridimensional). Dessa forma, o usuário teria acesso a uma informação visual sobre os níveis mínimo e máximo de privacidade que podem ser atingidos por tais dimensões em tempo de uso, o que impactaria na coloração geral do *beehive* correspondente ao tipo de comunicação representado, no sentido de ilustrar o nível geral de privacidade considerado no mesmo.

Um aspecto que o MDP não considera é o relacionamento existente entre os usuários, em seus papeis de emissor e receptor da informação que é compartilhada, e o seu impacto no compartilhamento. Tendo em vista que o tipo desse relacionamento pode determinar a possibilidade ou não da ocorrência de determinados compartilhamentos, podemos dizer que, neste caso, há uma dependência, no sentido de que o compartilhamento só acontece caso exista um relacionamento específico entre o emissor e o receptor da informação. Um exemplo disso seria o caso de o compartilhamento de um determinado tipo de informação só ser possível dentro do sistema, caso o receptor da informação, ou seja, a audiência da mesma, compartilhe o mesmo tipo de informação para o emissor, que, nesse caso, agora é a audiência (ou seja, há necessidade de um relacionamento de reciprocidade entre os usuários). Tal fato pode implicar em negociação entre essas partes envolvidas na comunicação referente ao compartilhamento, o que vai ao encontro da ideia de privacidade como consequência de um processo de negociação entre pessoas [Petronio, 2002]. Assim, seria interessante investigar em mais profundidade o que se perde em não se possibilitar a representação destes relacionamentos e se seria viável que fosse definido um outro nível de abstração que trataria de aspectos de relacionamento entre as dimensões.

O MDP também mostra-se limitado ao não ser capaz de representar os efeitos inferenciais da comunicação, ou seja, aqueles efeitos gerados (ou inferidos) a partir de um conjunto de informações pessoais compartilhadas sobre o indivíduo, representadas a partir de um mesmo tipo de comunicação ou não, como por exemplo a recomendação de amizade no Facebook e o RG Score no ResearchGate. Isso ocorre porque o MDP é capaz apenas de representar os valores das dimensões de efeitos da comunicação no nível direto, ou seja, o nível relacionado a uma única instância de comunicação. Assim, percebemos a necessidade de investigar se deveríamos criar outro nível de abstração para o MDP, que nos permitisse representar aspectos relacionados a mais de uma ocorrência (ou instância) de compartilhamento de informação pessoal no sistema. Além

de permitir a representação dos efeitos inferenciais da comunicação, esse novo nível de abstração também poderia tratar outros aspectos que ocorrem no nível intercomunicação (que envolve mais de um tipo de comunicação), como é o caso do controle, que pode ser concedido ao indivíduo, no sentido de permitir ou não a ocorrência de um determinado tipo de comunicação dentro do sistema. Um exemplo desse controle no nível intercomunicação ocorre no Facebook, tendo em vista que o indivíduo, ao alterar suas configurações, pode não permitir que outros usuários compartilhem informação em sua linha do tempo. Nesse caso, o indivíduo tem o controle no sentido de impedir que ocorra o tipo de comunicação referente a *"outro usuário compartilhar informação pessoal do indivíduo na linha do tempo do próprio indivíduo"*, o que pode impactar o seu estado de privacidade dentro do sistema.

Essas limitações do MDP aqui mostradas nos indicam pontos a serem investigados, no sentido de ampliar o seu poder de representação. Tal ampliação permite que sejam considerados, além dos aspectos que o MDP atualmente trata, outros elementos que também são importantes na determinação do estado de privacidade dos usuários de RSOs.

6.1.4 Aspectos não Considerados no MDP

Conforme mostramos no Capítulo 4, o MDP tem o propósito de apoiar designers em suas decisões sobre privacidade relacionada ao compartilhamento de informações em RSOs. No entanto, um ponto importante a observar é que o MDP foi elaborado com o modelo de RSOs existentes nos dias atuais em mente. Assim, não podemos garantir a sua aplicabilidade para novos modelos de RSOs que serão desenvolvidos no futuro.

Outro ponto que vale ressaltar é que não foi considerado no MDP o tipo de mídia compartilhada como sendo um fator impactante no nível de privacidade do usuário. No entanto, tal diferenciação pode ser importante, uma vez que que o compartilhamento de um vídeo, por exemplo, pode ter um impacto maior na privacidade do indivíduo do que o compartilhamento de um texto. Assim, seria interessante investigar o impacto de se considerar o tipo de mídia no MDP. Uma possibilidade para isso seria uma redefinição da dimensão **expressão** da informação, no sentido de que a mesma esteja relacionada ao tipo de mídia compartilhada, tendo em vista que no MDP essa dimensão não tem seus valores remetendo a níveis de privacidade, e sim associados ao controle da **conteúdo** da informação, conforme mostrado no Capítulo 4 - Seção 4.1.

Estes pontos indicam novas questões a serem investigadas sobre o MDP, no sentido de ampliar o escopo de aspectos de privacidade relacionados ao compartilhamento de informações pessoais em RSOs considerados no mesmo.

6.2 Considerações sobre a Avaliação do MDP

Embora o foco do MDP seja o apoio ao design de RSOs, nós apresentamos nesta tese a sua avaliação inicial, dentro de um contexto de análise.

Através de tal avaliação, mostramos a utilidade do MDP como uma ferramenta analítica e entendemos que apoiar a avaliação de privacidade em RSOs é, por si só, uma relevante contribuição [Boyle & Greenberg, 2005]. Embora ainda não tenhamos avaliado o MDP em um contexto de design, sua avaliação inicial gerou indicadores de seu potencial como uma ferramenta epistêmica.

A análise que fizemos das três RSOs - Facebook, ResearchGate e CaringBridge - e a comparação entre elas (mostradas no Capítulo 5 - seção 5.3), nos permitiu fazer discussões sobre como decisões de privacidade poderiam ser apropriadas ou não para o contexto dos sistemas. Por exemplo, o fato do ResearchGate ser voltado para o contexto profissional leva ao compartilhamento de informação pessoal relacionada a questões profissionais (que não é considerada como sendo muito pessoal), e isso justifica a decisão de design de se ter as informações compartilhadas na maior parte das vezes publicamente, além de oferecer aos usuários um menor controle de privacidade e menos notificações sobre ações que outros usuários executam sobre suas informações.

Outros aspectos que foram identificados na avaliação também poderiam levantar discussões interessantes relacionadas ao (re)design. Por exemplo, em todos os sistemas que analisamos, a persistência temporal da informação compartilhada é *"permanente"*. Em um contexto de (re)design, seria interessante discutir se isso é realmente a melhor decisão, ou que outras opções poderiam ser consideradas. Se olharmos para o caso do ResearchGate, por exemplo, faz sentido termos algumas informações profissionais (tais como formação e publicações) disponíveis permanentemente no sistema, desde que a história profissional do usuário é um sinal importante do seu papel como pesquisador e de sua vida profissional. Por outro lado, talvez não fosse necessário ter disponíveis por um longo período de tempo dentro do sistema as questões e respostas que o usuário compartilha. Após alguns anos, uma discussão pode não mais ser interessante, embora algumas pessoas possam argumentar que discussões que levam a decisões e mudanças devem ser armazenadas de forma permanente no sistema. De qualquer forma, simplesmente o fato do MDP ter despertado reflexões e discussões desse tipo pode ser considerado um indicador de sua utilidade no processo de (re)design.

Embora a nossa discussão tenha focado em decisões de privacidade, ela poderia também levar a aspectos de interação que afetam diretamente o usuário final. Por exemplo, o fato do Facebook permitir que o usuário controle a audiência para cada postagem que ele realiza (ou seja, para cada instância de um tipo de comunicação) pode

ser levantado e discutido. Por um lado, isso fornece flexibilidade ao usuário final, além de um controle mais fino de sua privacidade. Por outro lado, isso pode tornar o controle de privacidade uma tarefa excessivamente complexa para o usuário, tendo em vista o custo associado ao mesmo ter que interagir com configurações específicas de privacidade do Facebook. Nesse caso, estados indesejados de privacidade podem ser atingidos, caso ocorram rupturas durante a interação do indivíduo com o sistema e, por qualquer razão, ele não seja capaz de definir adequadamente a audiência pretendida para a informação. Além disso, tal controle traz implicações também para a interface, que deve deixar claro para seus usuários os níveis de privacidade remetidos pelas dimensões que compõem o tipo de comunicação referente à postagem que está sendo realizada, bem como a possibilidade de alterá-los. Algumas dessas questões de interface não são novas, e já foram identificadas e discutidas previamente [Liu et al., 2011; Netter et al., 2013; Pereira Junior et al., 2014]. Entretanto, o fato do MDP gerar questões que levam a tais discussões é um indicador de que seu uso permitiria que estas fossem feitas antes que o sistema fosse lançado e estivesse em uso.

Um aspecto que deveria ser considerado em relação a usar modelos de design são seus custos e benefícios. Na avaliação com potenciais usuários, nós coletamos alguns indicadores iniciais nessa direção. Assim, as dúvidas sobre as dimensões e seus valores, percebidas durante o uso do MDP pelos participantes, são um indicador do custo envolvido em seu uso. No entanto, o tempo investido na aprendizagem do MDP em tal avaliação foi de apenas cerca de 30 minutos e, caso tivesse sido maior, talvez as dúvidas dos participantes fossem reduzidas. Assim, seria necessário um estudo mais aprofundado para se identificar o tempo necessário para o aprendizado consolidado do MDP, além dos pré-requisitos necessários para facilitar o seu aprendizado, como o nível de conhecimento de IHC e Engenharia Semiótica.

Uma ferramenta para apoiar os usuários do MDP na criação de seus modelos de privacidade é um ponto importante a ser considerado no sentido de atenuar os custos com a aprendizagem e uso do MDP. Na avaliação, os participantes utilizaram um protótipo de tal ferramenta, ainda bastante simplificado, que permite aos usuários definirem o valor e o controle para cada dimensão e, com base nisso, gera então a representação visual do modelo. Nosso objetivo é melhorar esse protótipo, de forma que ele se transforme em uma ferramenta mais robusta e completa para apoiar efetivamente a modelagem MDP. Um ponto a ser considerado seria também a oportunidade de utilizar a própria ferramenta para auxiliar no aprendizado do modelo. Para isso, deveria se oferecer na ferramenta um sistema de ajuda nos moldes do proposto por Silveira et al. [2004], que pudesse ser utilizado pelos usuários para entenderem melhor ou tirarem dúvidas sobre as dimensões e seus valores.

Os participantes também levantaram espontaneamente, durante suas discussões no grupo focal, o tópico relacionado aos custos e benefícios do MDP. Além do tempo investido na aprendizagem do mesmo, eles mencionaram o fato do designer ter que descrever cada tipo de comunicação como estando associado ao custo de utilização do MDP. No entanto, eles próprios concluíram que os benefícios trazidos pelo seu uso compensam seus custos, dada a relevância de questões de privacidade em RSOs e a necessidade de considerá-la amplamente nesses sistemas. De acordo com os participantes, o MDP pode ser uma ferramenta útil a ser utilizada nos processos de design e avaliação de RSOs, estruturando o espaço de design de privacidade, apoiando assim o avaliador ou o designer, ao permitir que esses pensem em diferentes aspectos que impactam as decisões de privacidade nesses sistemas.

Neste ponto, vale chamar atenção para um aspecto que precisa ser considerado no sentido de ampliar a avaliação do MDP como ferramenta epistêmica. Como identificamos em nossas avaliações que o MDP ajuda o analista a pensar sobre privacidade relativa ao compartilhamento de informações pessoais em RSOs, consequentemente isso nos fornece um indício de sua influência na metacomunicação designer-usuário, transmitida através da interface. No entanto, não avaliamos tal influência, no sentido do identificar como o MDP altera tal metacomunicação, ou mesmo a visão do projetista do seu papel como emissor desta metacomunicação.

Conforme já mencionamos, os custos e benefícios do MDP, apontados na avaliação com potenciais usuários, são indicadores iniciais e precisam ser mais amplamente explorados e considerados em avaliações futuras. Além disso, todos os participantes da avaliação são de alguma forma envolvidos com pesquisa em Engenharia Semiótica, o que poderia tê-los inclinado a ter uma visão positiva sobre ferramentas epistêmicas.

Embora a avaliação inicial do MDP tenha trazido indicadores interessantes sobre o seu uso e inclusive sobre como ele poderia gerar reflexões para o redesign, ainda não foi feita uma avaliação sobre sua utilização no processo de design, que é seu principal propósito. Dessa forma, no futuro, é necessário avaliar o MDP em um contexto real de design, o que por sua vez representa uma série de desafios. Inicialmente, seria necessário que tivéssemos acesso a designers que trabalham com o desenvolvimento de sistemas em que a privacidade relacionada ao compartilhamento de informação pessoal seja um aspecto crítico a ser considerado, de forma que o uso do MDP se justifique para eles. Além disso, seria necessário que esses designers tivessem disponibilidade e interesse em participarem da avaliação do MDP como voluntários, ao fazerem uso do mesmo em seu contexto real de trabalho, como ferramenta para auxiliá-los no processo de design. Como isso possivelmente implicaria em um tempo maior de projeto, seria necessário também que a empresa responsável pelo mesmo estivesse disposta a fazer

este investimento.

Uma vez tendo acesso a esses designers, outro desafio é identificar qual seria a melhor forma de coletar indicadores sobre os benefícios trazidos pelo uso do MDP. A princípio, percebemos que apenas designers utilizarem diretamente o MDP em seus projetos não gera indicadores reais sobre seus benefícios, uma vez que, nesse caso, não há como comparar projetos feitos sem e com o uso do MDP, a fim de se identificar as vantagens trazidas pelo mesmo.

Uma alternativa no sentido de obter melhores resultados sobre o efeito do uso do MDP no design de RSOs seria a avaliação contar com duas equipes de designers, efetuando simultaneamente o design do mesmo sistema, sendo uma equipe fazendo uso do MDP como ferramenta de apoio, e a outra equipe não. Assim, ao final, poderíamos comparar os projetos de ambas as equipes e verificar se a equipe que fez uso do MDP produziu um melhor projeto de privacidade do sistema. Nesse caso, como a comparação envolveria produtos de trabalho de diferentes pessoas (membros das duas equipes), teríamos que lidar com diferentes variáveis que poderiam influenciar os resultados, como, por exemplo, o nível de conhecimento dos designers sobre o domínio do problema, bem como suas habilidades técnicas de design.

Assim, a alternativa que parece ser mais viável seria, considerando uma única equipe de designers, solicitar que inicialmente estes façam o design do compartilhamento de informações pessoais da RSO que estão projetando, sem fazerem uso e sem sequer terem conhecimento do MDP. Em seguida, os designers teriam acesso ao material sobre o MDP, bem como a explicações sobre o mesmo, para então fazerem o design do mesmo sistema, agora fazendo uso do MDP. Dessa forma, ao fazer a comparação das modelagens criadas pelos mesmos designers, em ambas as situações, seria verificado o que mudou no design a partir do uso do MDP. Dessa forma, seria verificado se o seu uso ampliou o entendimento dos designers sobre o problema relacionado à privacidade no compartilhamento de informação pessoal, permitindo um design que aborde de maneira mais eficaz esse aspecto de privacidade. Nesse caso, apresenta-se como um desafio também encontrar uma forma adequada de controlar as diferenças que interferem nos resultados nas duas situações, de forma a coletar indicadores sobre o real benefício do uso do MDP. Assim, um estudo mais aprofundado precisa ser feito, no sentido de estabelecer parâmetros de comparação nesses casos, a fim de efetuar uma avaliação que retorne resultados confiáveis sobre o impacto do uso do MDP no design de privacidade relacionada ao compartilhamento de informação pessoal em RSOs.

6.3 O MDP e outros estudos relacionados ao design de privacidade

O MDP, através de suas dimensões que estruturam o espaço de design do compartilhamento de informação pessoal em RSOs, abrange elementos apresentados pelos diferentes *frameworks* teóricos que se propõem a tratar e discutir aspectos de privacidade desses sistemas [Skinner et al., 2006; Palen & Dourish, 2003; Boyle & Greenberg, 2005; Barkhuus, 2012].

Primeiramente, temos que o MDP contempla as dimensões *tempo*, *assunto* e *espaço*, consideradas na taxonomia de privacidade apresentada por Skinner et al. [2006], através de suas dimensões **persistência temporal**, **informação do indivíduo** e **espaço de comunicação**, respectivamente.

Quando consideramos a privacidade nas RSOs, onde o indivíduo mantém relações sociais e possui a sua própria identidade, caracterizada pelas informações que ele ali compartilha, não só este é o responsável por controlar os seus limites de acesso, mas também o sistema desempenha o papel de agente, ao definir e impactar esses limites [Palen & Dourish, 2003]. Nesse sentido, o MDP permite que o designer reflita, dentre outros aspectos, sobre os limites de *identidade*, *divulgação* e *temporalidade*, considerados centrais por Palen & Dourish para o gerenciamento de privacidade nos ambientes sociais online, levando em consideração os controles de *solitude*, *autonomia* e *confidencialidade*, que descrevem tal gerenciamento, descritos por Boyle & Greenberg [2005].

Assim, ao refletir sobre as dimensões **fonte de comunicação** e **espaço de comunicação**, o designer está levando em consideração o limite de *identidade*, tendo em vista que os valores possíveis para essas dimensões remetem ao limite entre o *"indivíduo"* e *"outras pessoas"*. Além disso, o nível de privacidade associado a tais dimensões está associado à *autonomia* do indivíduo escolher como suas informações serão compartilhadas no sistema. O designer está refletindo sobre o limite de *divulgação* quando toma decisões em relação à dimensão **audiência**, cujos possíveis valores ilustram o limite entre o *"privado"* e o *"público"*. O controle sobre tal dimensão remete aos conceitos de *solitude* e *confidencialidade*, colocados por Boyle & Greenberg [2005], relacionados, respectivamente, ao controle dos níveis desejados de interação social por parte do indivíduo e ao controle do acesso de outras pessoas à sua informação. Por fim, quando decide sobre a dimensão **persistência temporal**, que tem seus valores refletindo a tensão entre passado, presente e futuro, o designer reflete sobre o limite de *temporalidade*. Nesse caso, as decisões do designer impactam os controles de *solitude*, *confidencialidade* e *autonomia* referentes ao indivíduo ao qual a informação compartilhada no sistema se

refere.

Além desses limites, o MDP permite que o designer reflita sobre outros aspectos, também importantes na caracterização do estado de privacidade a ser alcançado pelos usuários de RSOs. Alguns desses aspectos nos foram apontados nos estudos empíricos que realizamos em etapa anterior ao desenvolvimento do MDP [Xavier et al., 2014; Villela et al., 2015a,c,d]. Vimos, por exemplo, que o **conteúdo** da informação compartilhada, que reflete o seu nível de pessoalidade, tem papel importante na privacidade do indivíduo.

Nossos estudos prévios também nos indicaram que aspectos relacionados a ações de terceiros sobre as informações pessoais do indivíduo em RSOs, como é o caso da possibilidade da **fonte de informação** ser *"outro usuário"* e também a possibilidade de outros usuários **disseminarem** a informação do indivíduo dentro do sistema, podem gerar problemas de privacidade para os usuários. Identificamos também com esses estudos que o **discurso** que o sistema faz sobre o compartilhamento de informação do indivíduo, como é o caso do *Feed de notícias* e do recurso *Novidades* no Facebook, pode trazer experiências negativas relacionadas à sua privacidade. Assim, as preocupações dos usuários em relação à **disseminação da informação** e ao **discurso sobre o indivíduo** realizado pelo sistema, identificadas em nossos estudos, nos chamou atenção para a importância de consideramos as dimensões de mesmo nome do MDP.

Nossos estudos prévios também nos mostraram que as pessoas consideram muito alto o custo de configurarem adequadamente sua privacidade em RSOs [Xavier et al., 2014; Villela et al., 2015d]. Levando em consideração tal custo, no MDP atribuímos ao designer a decisão sobre o quanto de controle deve ser fornecido ao indivíduo, no sentido de permitir que ele gerencie a sua privacidade, ao possibilitar que ele defina os valores das dimensões em tempo de uso. Assim, o designer deve tomar a decisão sobre quais dimensões o usuário deverá ter o controle apoiando-se em uma reflexão sobre os custos e benefícios que ela pode trazer aos usuários. Consideramos que o *contexto*, que não é diretamente tratato no MDP, irá embasar as decisões do designer, nessa situação. No entanto, é interessante investigar outros referenciais teóricos a fim de verificar a possibilidade de considerar o *contexto* diretamente no MDP, ao incluir no mesmo elementos que tratem as normas de adequação social e fluxo de informação, que regem o compartilhamento de informação em SiCo's [Barkhuus, 2012].

Por fim, a proposta do MDP de ajudar os designers a refletirem sobre níveis de privacidade relacionados ao compartilhamento de informações pessoais em RSOs, além de permitir que estes registrem a lógica de design de seus modelos de privacidade, faz com que o mesmo seja uma ferramenta que tem um propósito único e diferenciado, em relação a outras ferramentas propostas para apoiar designers em suas decisões de

privacidade [Lipford et al., 2009; Lederer et al., 2004; Romero et al., 2012; Epstein et al., 2015], descritas no Capítulo 3.

Capítulo 7

Considerações Finais

O gerenciamento de privacidade relacionada ao compartilhamento de informação pessoal tem se tornado uma preocupação crescente no design de RSOs. Usuários frequentemente são confrontados com questões relacionadas ao alcance indesejado ou inesperado de suas informações pessoais nesses ambientes. Uma abordagem comum para tratar tais questões tem sido principalmente relacionada a aumentar a flexibilidade que os sistemas oferecem a seus usuários para lidarem com aspectos específicos de privacidade [Pang & Zhang, 2015; Fong et al., 2009; Lederer et al., 2003; Tierney & Subramanian, 2014]. Entretanto, tal flexibilidade impacta os custos referentes às decisões do usuário ao definir configurações de privacidade, e também às decisões dos designers sobre como expressar os elementos na interface do sistema a fim de permitir que os usuários gerenciem efetivamente a sua privacidade. Assim, designers deveriam decidir sobre o que oferecer aos usuários no sistema, de modo que eles possam alcançar seu estado desejado de privacidade, buscando por um equilíbrio entre o custo e os benefícios de tal estratégia. Pesquisadores têm apontado a necessidade de apoiar designers em suas decisões sobre privacidade em tempo de design [Cavoukian, 2006; Bélanger & Crossler, 2011].

Esta necessidade está em linha com a perspectiva que a Engenharia Semiótica [de Souza, 2005] assume sobre o processo de design. Como tal teoria entende um sistema como uma metacomunicação entre designers e usuários, ela chama atenção para apoiar designers na geração de sua mensagem. Para isso, ela propõe que designers deveriam utilizar ferramentas epistêmicas que os apoiem na reflexão sobre aspectos relevantes do sistema, ajudando-os a tomarem decisões sobre o mesmo e analisarem as implicações de tais decisões para o sistema e seus usuários.

Nesta tese, nós propomos o Modelo de Design de Privacidade como uma ferramenta epistêmica, que visa fornecer ao designer um melhor entendimento sobre aspec-

tos que impactam a privacidade em RSOs. Fazemos isso ao estruturar o espaço de design do compartilhamento de informação pessoal através de dimensões de privacidade e possibilitando o registro da lógica do projeto. Nossos resultados mostram que o MDP é capaz de expressar decisões relevantes de design referentes à privacidade em RSOs, bem como distinguir entre diferentes modelos de privacidade. A avaliação que procedemos mostra que o MDP pode ser utilizado como uma ferramenta analítica para avaliar a privacidade em RSOs, embora também tenha gerado indicadores positivos de como ele poderia apoiar a reflexão dos designers durante o processo de (re)design. Isso demonstra a contribuição do nosso trabalho para a pesquisa em privacidade, ao propor um modelo novo, que apoia o design e a avaliação de privacidade em RSOs, com foco no compartilhamento de informação pessoal.

A nossa pesquisa contribui então para as áreas de IHC e Sistemas Colaborativos. Além disso, em IHC, o nosso estudo contribui também para a pesquisa em Engenharia Semiótica, tendo em vista que propõe uma nova ferramenta epistêmica baseada nesta teoria. Apesar de já ter sido proposta uma ferramenta epistêmica para a modelagem da comunicação entre usuários em SiCo's baseada na Engenharia Semiótica - a Manas, com o MDP nós temos um foco distinto e mais específico, que é a comunicação que caracteriza o compartilhamento de informações pessoais e no seu impacto na privacidade. Além disso, os dados coletados sobre o MDP serão úteis na discussão sobre a relevância da aplicação da estrutura do espaço de design da Engenharia Semiótica na geração da metamensagem relativa à comunicação usuário-sistema-usuário, e o papel de suas ferramentas epistêmicas no design de sistemas.

Ainda em IHC, o nosso modelo também contribui com a pesquisa em *"End User Programming"*, uma vez que ele pode apoiar a reflexão, e mesmo o design de interação de aspectos de configuração de privacidade em RSOs.

7.1 Trabalhos Futuros

Este trabalho é um primeiro passo na direção da construção de um ambiente de apoio ao processo de design de privacidade relacionada ao compartilhamento de informações pessoais em RSOs. Para isso, alguns trabalhos futuros são propostos, a curto, médio e longo prazo.

Inicialmente, a curto prazo, vamos investigar a necessidade de rever a terminologia utilizada para dimensões e valores, analisando algumas dificuldades que surgiram na avaliação com os potenciais usuários.

No sentido de efetuar uma consolidação adicional dos resultados que obtivemos

como o uso do MDP, é importante realizar uma avaliação mais ampla do mesmo. Para isso, a ideia, a curto prazo, é executar novas avaliações analíticas de outras RSOs, de contextos e propósitos distintos. Nós também pretendemos fazer avaliações que envolvam o uso do MDP por outras pessoas não diretamente envolvidas com sua proposta, como ferramenta analítica e epistêmica. A nossa expectativa é que seja mais fácil encontrar pessoas que poderiam aplicar o MDP na avaliação de RSOs, uma vez que existe um grande número de sistemas desse tipo e muitas pessoas (tanto na área acadêmica quanto na indústria) poderiam se interessar em avaliá-los ou compará-los. No processo de design, pretendemos avaliar o uso do MDP em uma situação acadêmica, em que estudantes de pós-graduação poderiam desenvolver um protótipo de uma RSO. Entretanto, a longo prazo, o ideal é avaliar o MDP em um contexto real de desenvolvimento, embora tal avaliação dependa de se encontrar uma empresa interessada em colaborar com este esforço, o que pode, por si só, mostrar-se um desafio.

É relevante também, a médio prazo, investigar sobre a possibilidade e o benefício de se propor outros níveis de abstração para o MDP, que permitiriam modelar aspectos importantes de privacidade, que não são modelados no nível de abstração tratado atualmente pelo mesmo. Um exemplo seria a criação de um nível sintático que permitisse a definição de elementos relacionados a mais de uma ocorrência de compartilhamento de informação pessoal no sistema, ou a mais de um tipo de comunicação referente a tal compartilhamento, possibilitando uma reflexão mais estruturada sobre privacidade, no nível intercomunicação.

A médio prazo, também pretendemos transformar o protótipo da ferramenta de visualização, desenvolvido para apoiar o uso e avaliação do MDP (mostrado no Capítulo 4 - Seção 4.3), em uma ferramenta robusta e completa, que possa ajudar designers a aprenderem e aplicarem o MDP no (re)projeto de RSOs. Vale salientar que alguns dos resultados que obtivemos na avaliação do MDP irão contribuir para a melhoria da ferramenta, como, por exemplo, a emissão de mensagem de advertência quando seus usuários determinam que o valor de uma dimensão será definido em tempo de uso, mas indicam apenas uma opção de valor, ao invés de uma faixa de valores, que é o esperado nesse caso.

Outro ponto a ser considerado na ferramenta de visualização do MDP, a longo prazo, seria a inclusão do componente semântico que alerte o designer para o caso em que valores atribuídos às dimensões do MDP possam levar o usuário a um alto grau de exposição, indicando possivelmente um estado indesejado de privacidade, aos moldes do que é feito em outras ferramentas epistêmicas da Engenharia Semiótica, como p Marq-G* e a Manas. Além disso, para que a ferramenta seja utilizada como apoio ao aprendizado do MDP, é importante que seja incluída na mesma um sistema

de ajuda, que possa auxiliar seus usuários no entendimento das dimensões do MDP e seus valores. A geração dessa ferramenta, que facilite a utilização e até mesmo apoie o aprendizado do MDP, será importante para que possamos conduzir as avaliações previstas e necessárias do MDP.

Por fim, pode ser interessante avaliar o MDP no que tange à sua capacidade de transceder o seu propósito de ser uma ferramenta de apoio ao design de RSOs. Nesse sentido, pode-se considerar fazer uma investigação sobre a sua utilidade como ferramenta de análise de privacidade de redes sociais existentes no mundo físico, ou mesmo da possibilidade do mesmo ser utilizado pelos próprios usuários finais de RSOs, para fazerem uma avaliação sobre os níveis de privacidade oferecidos por esses sistemas.

Referências Bibliográficas

Ackerman, M. (2000). The intellectual challenge of cscw: The gap between social requirements and technical feasibility. *Human-Computer Interaction*, 15(2):179--203.

Acquisti, A.; Brandimarte, L. & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221):509--514.

Alarcón, R. A.; Guerreiro, L. A. & Pino, J. A. (2005). Temporal blurring: a privacy model for oms users. Em *User Modeling 2005*, pp. 417--422. Springer Berlin Heidelberg.

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*. Brooks/Cole Pub. Co., Inc., Monterry, CA.

Baranauskas, M.; de Souza, C. & Pereira, R. (2015). *I GranDIHC-BR - Grand Research Challenges for Human-Computer Interaction in Brazil*. ISBN: 9788576692966. Human-Computer Interaction Special Committee (CEIHC) of the Brazilian Computer Society (SBC).

Barbosa, C. (2002). Metacom-g*: especificação da comunicação entre membros de um grupo. Dissertação de mestrado, Dissertação de mestrado. Departamento de Ciência da Computação, PUC-Rio, Brasil.

Barbosa, C. M. d. A. (2006). *Manas: uma ferramenta epistêmica de apoio ao projeto da comunicação em sistemas colaborativos*. Tese de doutorado, Departamento de Informática, PUC-Rio.

Barbosa, S. D. J. & de Paula, M. G. (2003). Designing and evaluating interaction as conversation: A modeling language based on semiotic engineering. Em *Interactive Systems. Design, Specification, and Verification*, pp. 16--33. Springer.

Barkhuus, L. (2012). The mismeasurement of privacy. Em *Proceedings of CHI*, pp. 367--376, New York, New York, USA. ACM.

Besmer, A. & Lipford, H. R. (2010). Moving beyond untagging: photo privacy in a tagged world. Em *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 1563--1572. ACM.

Bevan, J.; Cummings, M.; Kubiniec, A.; Mogannam, M.; Price, M. & Todd, R. (2015). How are important life events disclosed on facebook? relationships with likehood of sharing and privacy. *Cyberpsychology, behavior and social networking*, 18(1):8--11.

Bélanger, F. & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4):1017--1041.

boyd, d. (2007). Why youth heart social network sites: The role of networked publics in teenage social life. *MacArthur foundation series on digital learning - Youth, identity, and digital media volume*, pp. 119--142.

boyd, d. m. & Ellison, N. B. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1):210--230.

Boyle, M. & Greenberg, S. (2005). The language of privacy : Learning from video media space analysis and design. *ACM Transactions on Computer-Human Interaction*, 12(2):328--370.

Bruns, G.; Fong, P. W.; Siahaan, I. & Huth, M. (2012). Relationship-based access control: its expression and enforcement through hybrid logic. Em *Proceedings of the second ACM Conference on Data and Application Security and Privacy (CODASPY)*, pp. 117--124. ACM.

Cairns, P. & Cox, A. L. (2008). *Research methods for human-computer interaction*, volume 12. Cambridge University Press New York (NY).

Carminati, B.; Ferrari, E.; Heatherly, R.; Kantarcioglu, M. & Thuraisingham, B. (2009a). A semantic web based framework for social network access control. Em *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies (SACMAT)*, pp. 177--186. ACM.

Carminati, B.; Ferrari, E. & Perego, A. (2009b). Enforcing access control in web-based social networks. *ACM Transactions on Information and System Security (TISSEC)*, 13(1):6.

Cavoukian, A. (2006). Privacy by design the 7 foundational principles implementation and mapping of fair information practices. *Information and Privacy Commissioner of Ontario, Canada.*

Cheng, Y.; Park, J. & Sandhu, R. (2012). Relationship-based access control for online social networks: Beyond user-to-user relationships. Em *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*, pp. 646--655. IEEE.

de Souza, C. S. (2005). *The semiotic engineering of human computer interaction*. MIT Press, Cambridge, MA.

de Souza, C. S.; Leitão, C. F.; Prates, R. O.; Bim, S. A. & da Silva, E. J. (2010). Can inspection methods generate valid new knowledge in hci? the case of semiotic inspection. *International Journal of Human-Computer Studies*, 68(1-2):22--40.

de Souza, C. S.; Leitão, C. F., C. F.; Prates, R. O. & da Silva, E. J. (2006). The semiotic inspection method. *Proceedings of VII Brazilian symposium on Human factors in computing systems - IHC '06*, p. 148.

de Souza, L. G. & Barbosa, S. D. J. (2014). Estendendo a molic para apoiar o design de sistemas colaborativos. Em *Companion Proceedings of the 13th Brazilian Symposium on Human Factors in Computing Systems*, pp. 25--28. Sociedade Brasileira de Computação.

de Souza, L. G. & Barbosa, S. D. J. (2015). Extending molic for collaborative systems design. Em *Human-Computer Interaction: Design and Evaluation*, pp. 271--282. Springer.

Debatin, B.; Lovejoy, J. P.; Horn, A.-K. & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1):83--108.

DeCew, J. W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press.

Denzin, N. K. & Lincoln, Y. S. (2008). *Collecting and interpreting qualitative materials*, volume 3. Sage.

Downs, J. S.; Holbrook, M. B.; Sheng, S. & Cranor, L. F. (2010). Are your participants gaming the system? Em *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*, p. 2399, New York, New York, USA. ACM Press.

Eco, U. (1976). *A theory of semiotics*, volume 217. Indiana University Press.

Eco, U. (1986). *Semiotics and the Philosophy of Language*, volume 398. Indiana University Press.

Ellis, C. A.; Gibbs, S. J. & Rein, G. (1991). Groupware: Some issues and experiences. *Commun. ACM*, 34(1):39--58.

Emanuel, L.; Bevan, C. & Hodges, D. (2013). What does your profile really say about you?: privacy warning systems and self-disclosure in online social network spaces. Em *CHI'13 Extended Abstracts on Human Factors in Computing Systems*, pp. 799--804. ACM.

Epstein, D. A.; Jacobson, B. H.; Bales, E.; McDonald, D. W. & Munson, S. A. (2015). From nobody cares to way to go!: A design framework for social sharing in personal informatics. Em *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, pp. 1622--1636. ACM.

Fong, P. W. (2011). Relationship-based access control: protection model and policy language. Em *Proceedings of the first ACM conference on Data and Application Security and Privacy (CODASPY)*, pp. 191--202. ACM.

Fong, P. W.; Anwar, M. & Zhao, Z. (2009). A privacy preservation model for facebook-style social network systems. Em *Computer Security–ESORICS 2009*, pp. 303--320. Springer.

Fong, P. W. & Siahaan, I. (2011). Relationship-based access control policies and their policy languages. Em *Proceedings of the 16th ACM symposium on Access control models and technologies*, pp. 51--60. ACM.

Gao, B. & Berendt, B. (2013). Circles, posts and privacy in egocentric social networks: An exploratory visualization approach. Em *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, ASONAM '13, pp. 792--796, New York, NY, USA. ACM.

Golbeck, J.; Robles, C.; Edmondson, M. & Turner, K. (2011). Predicting personality from twitter. Em *Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom)*, pp. 149--156. IEEE.

Gross, R. & Acquisti, A. (2005). Information revelation and privacy in online social networks. Em *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pp. 71--80. ACM.

Grudin, J. & Poltrock, S. (2016). Computer supported cooperative work. Em Soegaard, M. & Dan, R. F., editores, *The Encyclopedia of Human-Computer Interaction*, capítulo 27. Interaction Design Foundation, 2 edição.

Hargittai, E. et al. (2010). Facebook privacy settings: Who cares? *First Monday*, 15(8).

Hoadley, C. M.; Xu, H.; Lee, J. J. & Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the facebook news feed privacy outcry. *Electronic Commerce Research and Applications*, 9(1):50--60.

Jakobson, R. (1960). Linguistics and poetics. Em A.Sebeok, T., editor, *Style in language*, pp. 350--377. The MIT Press, Cambridge, MA.

Jakobsson, M. (2009). Experimenting on mechanical turk: 5 how tos. *ITWorld*.

Joinson, A. N. & Paine, C. B. (2007). Self-disclosure, privacy and the internet. *The Oxford handbook of Internet psychology*, pp. 235--250.

Joinson, A. N.; Reips, U.-D.; Buchanan, T. & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction*, 25(1):1--24.

Kisilevich, S.; Ang, C. S. & Last, M. (2011). Large-scale analysis of self-disclosure patterns among online social networks users: a russian context. *Knowledge and Information Systems*, 32(3):609--628.

Kosinski, M.; Stillwell, D. & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, 110(15):5802--5805.

Lederer, S.; Hong, J. I.; Dey, A. K. & Landay, J. A. (2004). Personal privacy through understanding and action: five pitfalls for designers. *Personal and Ubiquitous Computing*, 8(6):440--454.

Lederer, S.; Mankoff, J.; Dey, A. K. & Beckmann, C. (2003). Managing personal information disclosure in ubiquitous computing environments. Relatório técnico, Computer Science Division, University of California.

Lewis, K.; Kaufman, J. & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication*, 14(1):79--100.

Lipford, H. R.; Hull, G.; Latulipe, C.; Besmer, A. & Watson, J. (2009). Visible flows: Contextual integrity and the design of privacy mechanisms on social network sites. Em *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, volume 4, pp. 985--989.

Liu, Y.; Gummadi, K. P. & Mislove, A. (2011). Analyzing facebook privacy settings: User expectations vs . reality. Em *Proceedings of the 2011 ACM SIGCOMM Internet Measurement Conference (IMC)*, pp. 61--70. ACM.

MacQueen, J. B. (1967). Some methods for classification and analysis of multivariate observations. Em *Proceedings of 5th Berkeley Symposium on Mathematical Statistics and Probability*, pp. 281--297. University of California Press.

Malandrino, D.; Petta, A.; Scarano, V.; Serra, L.; Spinelli, R. & Krishnamurthy, B. (2013). Privacy awareness about information leakage: Who knows what about me? Em *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society*, WPES '13, pp. 279--284, New York, NY, USA. ACM.

Marshall, C. C. & Shipman, F. M. (2013). Experiences surveying the crowd: Reflections on methods, participation, and reliability. Em *Proceedings of the 5th Annual ACM Web Science Conference*, pp. 234--243. ACM.

Mazzia, A.; LeFevre, K. & Adar, E. (2012). The pviz comprehension tool for social network privacy settings. Em *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pp. 13:1--13:12, New York, NY, USA. ACM.

Netter, M.; Riesner, M.; Weber, M. & Pernul, G. (2013). Privacy settings in online social networks–preferences, perception, and reality. Em *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, pp. 3219--3228. IEEE.

Nicolaci-da Costa, A. A. M.; Leitão, C. F. & Romão-Dias, D. (2004). Como conhecer usuários através do método de explicitação do discurso subjacente (meds). Em *Proceedings of VI Simpósio Brasileiro de Fatores Humanos em Sistemas Computacionais*, pp. 47--56.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(30):119--158.

Palen, L. & Dourish, P. (2003). Unpacking "privacy"for a networked world. Em *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 129--136, New York, New York, USA. ACM.

Pang, J. & Zhang, Y. (2015). A new access control scheme for facebook-style social networks. *Computers & Security*, 54:44–59.

Paul, T.; Stopczynski, M.; Puscher, D.; Volkamer, M. & Strufe, T. (2012). C4ps: Colors for privacy settings. Em *Proceedings of the 21st International Conference Companion on World Wide Web*, WWW '12 Companion, pp. 585--586, New York, NY, USA. ACM.

Peirce, C. S. (1998). *The essential Peirce: selected philosophical writings*, volume 2. Indiana University Press.

Pereira Junior, M.; Xavier, S. & Prates, R. O. (2013). Antecipando possíveis implicações de privacidade na postagem de fotos no facebook. Em *Proceedings of the 12th Brazilian Symposium on Human Factors in Computing Systems*, IHC '13, pp. 62--71, Porto Alegre, Brazil, Brazil. Brazilian Computer Society.

Pereira Junior, M.; Xavier, S. & Prates, R. O. (2014). Investigating the use of a simulator to support users in anticipating impact of privacy settings in facebook. Em *Proceedings of the 18th ACM International Conference on Supporting Group Work*, pp. 63--72. ACM.

Perrin, A. (2015). Social media usage: 2005-2015. Relatório técnico October, Pew Research Center.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Suny Press.

Pontes, T.; Magno, G.; Vasconcelos, M.; Gupta, A.; Almeida, J.; Kumaraguru, P. & Almeida, V. (2012). Beware of what you share: Inferring home location in social networks. Em *Data Mining Workshops (ICDMW), 2012 IEEE 12th International Conference on*, pp. 571--578. IEEE.

Prates, R. O. (1998). *A Engenharia Semiótica de Linguagens de Interfaces Multi-Usuário*. Tese de doutorado, Departamento de Informática, PUC-Rio.

Prates, R. O.; Rosson, M. B. & de Souza, C. S. (2015). Interaction anticipation: Communicating impacts of groupware configuration settings to users. Em *End-User Development*, pp. 192--197. Springer International Publishing.

Romero, N. A.; Markopoulos, P. & Greenberg, S. (2012). Grounding privacy in mediated communication. *Computer Supported Cooperative Work (CSCW)*, 22(1):1--32.

Rubel, A. & Biava, R. (2014). A framework for analyzing and comparing privacy states. *Journal of the Association for Information Science and Technology*, 65(12):2422--2431.

Salgado, L. C. d. C. (2011). *Cultural Viewpoint Metaphors to Explore and Communicate Cultural Perspectives in Cross-cultural HCI Design*. Tese de doutorado, Pontificia Universidade Católica do Rio de Janeiro.

Schön, D. A. (1983). *The reflective practitioner: How professionals think in action*, volume 5126. Basic books.

Silva, B. S. (2005). *MoLIC Segunda Edição: revisão de uma linguagem para modelagem da interação humano-computador*. Tese de doutorado, Departamento de Informática, PUC-RJ.

Silveira, M. S.; Barbosa, S. D. J. & Souza, C. S. d. (2004). Designing online help systems for reflective users. *Journal of the Brazilian Computer Society*, 9(3):25--38.

Skinner, G.; Han, S. & Chang, E. (2006). An information privacy taxonomy for collaborative environments. *Information Management & Computer Security*, 14(4):382--394.

Smith, G. (2007). Social software building blocks. Disponível em http://nform.com/ideas/social-software-building-blocks/. Acesso: Fevereiro de 2016.

Solove, D. J. (2008). Understanding privacy. *GWU Legal Studies Research Paper*, 420(May).

Stutzman, F. & Hartzog, W. (2012). Boundary regulation in social media. Em *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work*, CSCW '12, pp. 769--778, New York, NY, USA. ACM.

Tausczik, Y. R. & Pennebaker, J. W. (2010). The psychological meaning of words: Liwc and computerized text analysis methods. *Journal of language and social psychology*, 29(1):24--54.

Tierney, M. & Subramanian, L. (2014). Realizing privacy by definition in social networks. Em *Proceedings of 5th Asia-Pacific Workshop on Systems*, pp. 1--7.

Villela, M. L.; Xavier, S. I.; Prates, R. O.; Prates, M. O.; Shipman, F.; Prates, A. A. & Cardoso, A. A. (2015a). Contrasting people's attitudes towards self-disclosure in online social networks and face-to-face settings. Em *Proceedings of 21th International Conference on Collaboration and Technology (CRIWG 2015)*, pp. 232--247.

Villela, M. L. B. & Prates, R. O. (2015a). Análise do facebook, researchgate e caringbridge de acordo com as dimensões do mdp. Relatório técnico, DCC/UFMG.

Villela, M. L. B. & Prates, R. O. (2015b). Supporting designer in modeling privacy for social network sites. Em *Proceedings of XIV Brazilian Symposium on Human Factors in Computer Systems (IHC 2015)*, pp. 113--122, Salvador - BA. Sociedade Brasileira de Computação.

Villela, M. L. B. & Prates, R. O. (2016). Privacy design model for social network sites. *Artigo submetido ao Journal of Visual Languages and Computing.*

Villela, M. L. B.; Xavier, S. & Prates, R. O. (2015b). Identifying collaboration strategies in scientific collaboration networks. Em *Proceedings of 17th International Conference on Human-Computer Interaction (HCII 2015)*, pp. 253--264.

Villela, M. L. B.; Xavier, S.; Prates, R. O.; Prates, M. O.; Shipman, F. M. & Prates, A. A. P. (2015c). Investigating brazilian and american users' perceptions of content "personalness"and the impact on their attitudes towards information sharing. Relatório técnico RT.DCC.001/2015, DCC/UFMG.

Villela, M. L. B.; Xavier, S. I. R.; Prates, R. O.; Prates, M. O.; Prates, A. A. & Cardoso, A. A. (2015d). An exploratory qualitative study on people's attitudes towards offline and online social networks: A case study at a brazilian university. *Journal on Interactive Systems*, 6(1):4--17.

Wang, Y. & Zhou, M. X. (2015). Veilme : An interactive visualization tool for privacy configuration of using personality traits. Em *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 817--826. ACM.

Westin, A. F. (1967). Privacy and freedom. *Washington and Lee Law Review*, 25(1):166.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, 59(2):431--453.

Xavier, S.; Villela, M. L. B.; Prates, R. O.; Prates, A. A. P.; Cardoso, A. & Prates, M. O. (2014). Migrando das redes sociais offline para as redes sociais online: O que houve com a privacidade? Em *Proceedings of the XIII Brazilian Simposium on Human Factors in Computing Systems (IHC 2014)*, pp. 265--274, Foz do Iguaçu - PR. Sociedade Brasileira de Computação.

Xavier, S. I. d. R. (2014). Privacidade em redes sociais: Uma análise da experiência dos usuários. Dissertação de mestrado, Departamento de Ciência da Computação, UFMG.

Yarkoni, T. (2010). Personality in 100,000 words: A large-scale analysis of personality and word use among bloggers. *Journal of research in personality*, 44(3):363--373.

Apêndice A

Roteiro da Entrevista e Questionário

Neste Apêndice, incluímos o roteiro da Entrevista e o Questionário (versões em português e em inglês) que conduzimos com o objetivo de contrastar privacidade online e off-line.

Roteiro de Entrevista sobre Percepção de Privacidade Offline e Online

DADOS PESSOAIS: Nome | Idade | Formação | Profissão | Sexo	
Blocos	**Principais Itens**
I. Sobre percepção de Privacidade em geral **(off-line e online)**	1. Falar sobre o **significado** do termo "Privacidade". a. Se o termo "Privacidade" tiver relação com a **manutenção do sigilo das suas informações pessoais**, o que seria "informações pessoais". b. Que tipos de informações você considera pessoal: Dados, relações familiares, eventos na família, sentimentos, etc
	2. Você se **preocupa** com sua **privacidade**? a. **Tipo** de **preocupação**. b. **Atitudes** tomadas.
	3. No nosso dia-a-dia as pessoas, muitas vezes, interferem no nosso mundo pessoal através de **perguntas ou conselhos**. Isto te incomoda? Por quê? Em que situações? Como reage?
	4. Quem você considera que seriam as pessoas mais **próximas**, com quem você mais compartilha suas informações pessoais? Que **tipo de informações** seriam? a. E em segundo lugar...terceiro lugar, e assim por diante (tentar extrair os grupos de pessoas que o entrevistado considera relevante).
II. Privacidade online x offline	5. Caso o entrevistado estiver referindo-se apenas a um lado do significado do termo (físico ou virtual), perguntar sobre o lado não mencionado.
	6. Explorar as **diferenças entre privacidade online e off-line**. Por exemplo, estas duas faces estão relacionadas? Qual é a mais importante?
	7. **Experiência negativa** com perda de privacidade em alguma situação real ou virtual (ou alguém próximo). Em caso positivo, descreva a experiência.
III. Sobre a experiência do respondente com Redes Sociais Online	8. **Redes sociais** online utilizadas. Com que **frequência**.
	9. **Conhece pessoalmente** todos os seus amigos? a. Quais critérios para aceitar as pessoas como amigos. b. Aproximadamente, quantos amigos tem?
	10. Que **tipos de informações** você costuma divulgar via rede social? Para quem?
	11. Já leu a política de privacidade das redes que usa (inteira ou partes). a. Em caso afirmativo, que **pontos destaca**. Por quê?
	12. Acha que em geral as pessoas se **preocupam** com as **políticas de uso e privacidade**?
	13. Já **alterou as configurações de privacidade** da sua rede social. (Mostrar tela do Facebook) a. Em caso afirmativo, lembra **o que alterou**. Por que achou importante alterar. b. Faz uso de **listas** no Facebook? Com que objetivo?

	14. Já **restringiu/bloqueou acesso** a alguma informação que você postou? a. Em caso afirmativo, por quê?
	15. Já restringiu quem tem acesso a você no ***chat*** do Facebook? Motivo.
	16. Problemas de privacidade em alguma rede social online. Qual(is)?
	17. As redes sociais mudaram a forma como você se preocupa com privacidade? Como?
IV. Sobre Privacidade e Sociedade	18. A imprensa e as pessoas, nos dias de hoje, criticam a **hiperexposição involuntária** das pessoas nas redes sociais online. Acha que isso de fato acontece? a. Conhece alguém **vítima** dessa hiperexposição?
	19. Acha que privacidade **é um direito essencial** (que você não abre mão)? Por quê?
	20. Já **questionou** o motivo de **pedirem determinada informação**, ao fazer uma conta ou cadastro?
	21. Relação entre **Privacidade e Confiança** (usar exemplo dos dados de conta bancária na Noruega)
	22. Acha que o tema "**Privacidade**" é importante para ser **pensado** pelas **autoridades políticas do país**. Por quê? a. Especificamente sobre **internet**, acha que o **Governo deveria interferir** através de regulamentações legais para garantir a privacidade (dos dados) de seus usuários. b. Em caso afirmativo, que tipo de regulamentação?
	23. **Comentários** adicionais sobre o tema.

Conteúdo do Questionário (em português)

Seção 1 de 5 – Perfil

Este grupo de questões permitirá a identificação do perfil dos respondentes, que será útil para posterior análise das respostas das próximas seções do questionário, permitindo correlação de variáveis de perfil dos usuários com as questões de pesquisa.

1. Qual é o seu relacionamento com a UFMG?

a. Tipo: Marcação múltipla (checkbox)

b. Opções:

i. Professor
ii. Aluno
iii. Funcionário
iv. Ex-aluno
v. Outros

c. Comportamento especial: Se a pessoa marcar "Outros" ou "Ex-aluno" sem ter marcado as outras opções, mostrar o botão "Enviar" e a seguinte mensagem: "Essa pesquisa tem como perfil de interesse apenas professores, alunos e funcionários da UFMG. Agradecemos a sua boa vontade e disponibilidade.".

d. Justificativa: Como não há como o sistema garantir que apenas professores e alunos responderão o questionário, acho que é importante colocarmos uma pergunta para garantir que apenas eles irão responder.

2. Sexo

a. Tipo: Marcação única (Radio)

b. Opções:

i. Feminino
ii. Masculino

c. Justificativa: Fator que pode influenciar o comportamento do respondente

3. Qual o seu ano de nascimento?

a. Tipo: Lista de opções (Combobox)

b. Opções:

i. 1940
ii. 1941
iii. ...
iv. 2003

c. Justificativa: A idade pode influenciar o comportamento do respondente

4. **Qual é o seu último nível de formação concluído?**

   a. Tipo: Marcação única (Radio)

   b. Opções
      i. Ensino fundamental
      ii. Ensino Médio
      iii. Graduação
      iv. Mestrado
      v. Doutorado

   c. Justificativa: Fator que pode influenciar o comportamento já que de acordo com o nível de instrução a pessoa poderia estar melhor informada ou até entender melhor o que está a sua volta

5. **Você estuda, é formado ou atua na área Tecnologia da Informação (TI)?**

   a. Tipo: Marcação única (Radio)

   b. Opções
      i. Sim
      ii. Não

   c. Justificativa: ser da área de TI pode influenciar a preocupação da pessoa com privacidade e o comportamento relacionado a mesma nas redes sociais.

6. **Qual é seu estado civil?**

   a. Tipo: Marcação única (radio)

   b. Opções
      i. Solteiro(a)
      ii. Casado(a) ou União estável
      iii. Separado(a)/Desquitado(a)/Divorciado(a)
      iv. Víuvo(a)

   c. Justificativa: Pois isso pode influenciar ou estar relacionado com a sua preocupação com privacidade.

Seção 2 de 5 – Experiência de uso de redes sociais

Este grupo de questões permitirá identificar se o respondente faz uso de plataformas de redes sociais e se a preocupação com a privacidade é um motivo determinante para o encerramento de uma conta em uma dessas plataformas. O objetivo é verificar, também, se o usuário é experiente ou não nas redes sociais e se já enfrentou problemas de privacidade em alguma delas.

7. **Há quanto tempo você utiliza redes sociais?**

   a. Tipo: Marcação única (radio)

   b. Opções
      i. Nunca utilizei
      ii. Menos de 6 meses
      iii. 6 meses a 1 ano
      iv. Mais de 1 ano e menos de 3 anos
      v. Mais de 3 anos

   c. Comportamento especial: Se a pessoa marcar “Nunca utilizei”, mostrar apenas a pergunta abaixo e o botão enviar. O restante continua escondido.

d. Justificativa: Como precisamos saber se a pessoa é ou não usuário das redes sociais, já aproveitamos e perguntamos a quanto tempo utiliza. O tempo pode ser um fator que influencie sua percepção de privacidade e o quanto conhece sobre as possibilidades que as redes sociais oferecem para gerenciamento de privacidade.

8. Por que você não criou conta em uma rede social? (Exibir apenas se a pessoa disse que nunca utilizou redes sociais na questão 7)

a. Tipo: Marcação única (Radio) por linha

b. Opções

	Muito importante	Importante	Pouco importante	Sem importância	Não tenho opinião
É perigoso para a minha segurança	O	O	O	O	O
É muita exposição	O	O	O	O	O
Acho que é muito complicado/ Não saberia configurar	O	O	O	O	O
Não sei o que empresa responsável pela rede social faz com os dados dos usuários	O	O	O	O	O
Considero que toma muito tempo	O	O	O	O	O
Não tenho interesse	O	O	O	O	O

c. Justificativa: essa questão pode indiretamente levantar preocupação das pessoas acerca de sua privacidade, ao perguntar o motivo de nunca ter criado uma conta em uma rede social.

9. Assinale, abaixo, as redes sociais que você já utilizou ou utiliza (Exibir apenas se a pessoa marcou qualquer opção, com exceção da "i", na pergunta 7):

a. Tipo: Marcação múltipla (Checkbox)

b. Opções:
   i. Facebook
   ii. Foursquare
   iii. Google +
   iv. Instagram
   v. Myspace
   vi. Orkut
   vii. Tumblr
   viii. Twitter
   ix. Academia.edu
   x. LinkedIn
   xi. ResearchGate
   xii. Badoo
   xiii. Outra(s)

c. Justificativa: É interessante saber quantas redes sociais a pessoa utiliza, pois se uma pessoa possui conta em muitas redes sociais, possivelmente sua preocupação com privacidade não é tão grande assim. Mas talvez essa pergunta possa ser retirada se precisar diminuir o questionário, pois a resposta dela em si não nos permite tirar nenhuma conclusão e nem afirmar que a pessoa se preocupa ou não se preocupa. Pode talvez ser útil para a comparação cultural entre os países.

10. **Você já encerrou sua conta em alguma rede social?**
    a. Tipo: Marcação única (radio)
    b. Opções
        i. Sim
        ii. Não
    c. Justificativa: essa questão tem propósito similar ao da pergunta 8, que pode indiretamente levantar o problema da privacidade
    d. Comportamento especial: se a pessoa responder “sim” a esta questão, mostrar a questão a seguir.

11. **Por qual motivo você já encerrou a sua conta em alguma rede social? (Exibir esta questão apenas se a pessoa marcou “sim” na pergunta anterior)**
    a. Tipo: Marcação múltipla (Checkbox)]
    b. Opções:
        i. Abandono da rede por amigos / migração para outras redes
        ii. Falta de uso
        iii. Perda de interesse
        iv. Dificuldade de utilizar o sistema
        v. Problemas relacionados à privacidade
        vi. Outros. Especifique:
    c. Justificativa: essa questão tem propósito similar ao da pergunta 8, que pode indiretamente levantar o problema da privacidade, ao perguntar o motivo de saída de alguma rede social.

12. **Há quanto tempo você possui conta no Facebook?**
    a. Tipo: Marcação única
    b. Opções
        i. Não tenho conta no Facebook
        ii. Menos de 6 meses
        iii. 6 meses a 1 ano
        iv. Mais de 1 ano a 3 anos
        v. Mais de 3 anos
    c. Comportamento especial: Se a pessoa marcar “Não tenho conta no Facebook” o formulário encerra aqui. Se marcar qualquer uma das outras, mostra as outras questões do formulário.
    d. Justificativa: Saber se a pessoa possui conta no Facebook e qual a sua experiência com ele. Assim saberemos se ela já teve mais tempo para conhecer os recursos e se familiarizar com a interface.

Seção 3 de 5 – Privacidade em Geral

Este grupo de questões tem como objetivo identificar a percepção de privacidade em geral dos respondentes, que será útil para correlação dessas variáveis com aquelas relacionadas à privacidade no mundo virtual, buscando compreender melhor as mudanças acarretadas pelos recursos da vida moderna na forma como as pessoas entendem o conceito de privacidade.

13. Para você, a privacidade <u>no mundo físico</u> está associada a que? (Escolha todas as opções que se aplicam):

a. Tipo: Marcação múltipla (Checkbox)

b. Opções
   i. Proteger os dados de criminosos e ameaças a minha segurança
   ii. Poder escolher as informações que eu vou compartilhar e com quem
   iii. Ter o meu espaço e ninguém ter acesso a ele sem minha permissão
   iv. Não sei responder.
   v. Outros. Qual? _____

c. Justificativa: Essa questão tem como objetivo identificar a que aspectos os respondentes relacionam o conceito de privacidade. As opções de respostas foram obtidas a partir das respostas da pergunta sobre o significado do conceito de privacidade feita na entrevista.

d. Justificativa das opções
   i. Saber se a pessoa associa a segurança
   ii. Saber se a pessoa associa com a restrição de informações (não associada a segurança)
   iii. Saber se a pessoa associa com a ideia de ter o seu espaço
   iv. Saber se a pessoa teve dificuldade para responder a questão

14. Classifique cada uma das informações abaixo de acordo com o quanto você a considera pessoal, em uma escala de quatro pontos, variando de "muito pessoal" a "não é pessoal (sendo que o primeiro ponto significa um nível mais alto de preocupação em relação a com quem você compartilharia tal informação, e o último ponto significa uma menor preocupação em relação a restringir quem teria acesso à mesma):

a. Tipo: Marcação única (Radio) por linha

b. Opções

	Muito pessoal	**Meio pessoal**	**Pouco pessoal**	**Não é pessoal**
Local onde trabalha ou já trabalhou				
Local onde estuda ou estudou				
Estado civil / Relacionamento				
Relações de parentesco (por exemplo, quem são as pessoas da sua família)				
Data do seu aniversário				
Endereço de e-mail				
Telefone				
Endereço residencial				
Opinião sobre crenças/religião				
Opiniões políticas				
Estado de saúde				
Fotos suas				
Fotos de sua família				
Locais que frequenta				
Emoções negativas				
Emoções positivas				
Problemas de relacionamento				
Conquistas pessoais (por exemplo, um prêmio recebido, uma viagem realizada, um novo emprego, etc).				

c. Justificativa: Essa pergunta é para saber, ao fazer o cruzamento com as respostas da questão 15, com quem as pessoas compartilham as informações que disseram ser pessoais aqui e o quanto essas informações são consideradas pessoais pelos participantes. É importante saber o "grau de pessoalidade" das informações para verificar a teoria que havia sido levantada nas entrevistas, de que haveria um grau de variação, entre as informações pessoais, e aquelas consideradas "muito pessoais" não são colocadas nas redes sociais. Além disso, esse grau de pessoalidade das informações pode ser útil para mostrar possíveis diferenças culturais.

15. <u>No mundo físico</u>, marque, dentre os grupos de pessoas abaixo, aqueles com os quais você se sente confortável para compartilhar as seguintes informações (para cada informação, escolha todos os grupos que se aplicam):

a. Tipo: Marcação Múltipla (checkbox) por linha

b. Opções:

	Uma ou mais pessoas do Núcleo familiar (pais, companheiro (a), filhos, irmãos)	**Parentes em geral**	**Amigos íntimos**	**Amigos**	**Colegas de estudo ou trabalho**	**Conhecidos**	**Qualquer pessoa**	**Ninguém**
Local onde trabalha ou já trabalhou								
Local onde estuda ou estudou								
Estado civil / Relacionamento								
Relações de parentesco (por exemplo, quem são as pessoas da sua família)								
Data do seu aniversário								
Endereço de e-mail								
Telefone								
Endereço residencial								
Opinião sobre crenças/religião								
Opiniões políticas								
Estado de saúde								
Fotos suas								
Fotos de sua família								
Locais que frequenta								
Emoções negativas								
Emoções positivas								
Problemas de relacionamento								

Conquistas pessoais (por exemplo, um prêmio recebido, uma viagem realizada, um novo emprego, etc).								

c. Justificativa: Esse quadro possibilitará uma comparação posterior com a pergunta que possui o quadro no qual é pedido para o respondente marcar para as mesmas informações, se as compartilha no Facebook ou não, e com quem.

Seção 4 de 5 – Questões relacionadas a Privacidade no Facebook

Este conjunto de questões, que somente será exibido se o respondente marcar qualquer opção na questão 12, com exceção da "i", têm como objetivo levantar informações sobre como os usuários lidam com questões relacionadas à privacidade no Facebook.

16. Para você, a privacidade no mundo virtual está associada a que? (Escolha todas as opções que se aplicam):

a. Tipo: Marcação múltipla (Checkbox)

b. Opções
   i. Proteger os dados de criminosos e ameaças a minha segurança
   ii. Poder escolher as informações que eu vou divulgar e com quem
   iii. Poder escolher quem tem acesso à diferentes partes do meu perfil (mural, álbuns, ...)
   iv. Não sei responder.
   v. Outros. Qual? _____

c. Justificativa: Essa questão tem como objetivo identificar a que aspectos os respondentes relacionam o conceito de privacidade no mundo virtual. As opções de respostas foram obtidas a partir das respostas da pergunta sobre o significado do conceito de privacidade feita na entrevista.

d. Justificativa das opções
   i. Saber se a pessoa associa a segurança
   ii. Saber se a pessoa associa com a restrição de informações (não associada a segurança)
   iii. Saber se a pessoa associa com a ideia de ter o seu espaço
   iv. Saber se a pessoa teve dificuldade para responder a questão

17. Com qual frequência você acessa o Facebook?

a. Marcação única (Radio)

b. Opções
   i. Sempre conectado (via dispositivo móvel)
   ii. Várias vezes por dia
   iii. Pelo menos uma vez por dia
   iv. Pelo menos quatro vezes por semana
   v. Pelo menos uma vez por semana
   vi. Pelo menos uma vez por mês
   vii. Menos de uma vez por mês

c. Justificativa: informação importante para saber a experiência que o usuário tem com o Facebook. Pode ser que quanto menos ele usa provavelmente menos ele compartilha

18. Você possui mais de um perfil no Facebook?

a. Tipo: Marcação única (radio)

b. Opções
   i. Sim
   ii. Não

c. Justificativa: esta questão permite identificar se a pessoa tem algum perfil falso, o qual pode representar tentativa de preservar identidade e privacidade do espaço das relações concretas, mas também facilitar a invasão da privacidade alheia no ciberespaço.

d. Comportamento especial: Se marcou "Sim", mostra a próxima questão

19. Qual o principal motivo pelo qual você tem outro perfil?

a. Tipo: Marcação única (radio)

b. Opções
   i. Observar/Interagir com outras pessoas sem ser identificado.
   ii. Separar meus contatos pessoais e profissionais
   iii. Testar como as pessoas estão vendo meu perfil ou testar recursos do Facebook e entender como funcionam
   iv. Outros. Quais? _____

c. Justificativa: A questão anterior sem uma questão sobre qual o motivo de ter uma outra conta não nos permite tirar nenhuma conclusão ou fazer maiores afirmativas. Com o conjunto das duas questões isso se torna possível.

20. Você utiliza as redes sociais para ...

a. Tipo: Marcação única (Radio) por linha

b. Opções

	Principalmente	Às vezes	Pouco	Nunca
Compartilhar minhas informações pessoais	O	O	O	O
Compartilhar informações úteis/interessantes	O	O	O	O
Acompanhar as atualizações dos contatos	O	O	O	O
Manter-se atualizado sobre assuntos em geral	O	O	O	O
Encontrar novos amigos	O	O	O	O
Refazer contatos	O	O	O	O
Conversar	O	O	O	O
Participar de grupos	O	O	O	O

c. Justificativa: O motivo da pessoa utilizar a rede social pode estar diretamente relacionado com como ela vê a questão de privacidade nesse ambiente. Então, se ela vê ali apenas como um lugar de diversão (como disse uma das entrevistadas), ela talvez não ache adequado ficar compartilhando ali coisas negativas, e ache até ruim ou excesso de exposição se vê outras pessoas fazendo isso. Porém, se ela vê ali como um lugar de desabafo, então pode acabar se expondo.

21. Você considera que a partir do momento em que você criou uma conta no Facebook, você abriu mão de parte da sua privacidade?

a. Tipo: Marcação única (Radio)

b. Opções
   i. Sim
   ii. Não

c. Justificativa: esta questão é importante para identificar se o respondente considera que abriu mão de um direito seu ao entrar no Facebook.

22. Você tem aproximadamente quantos amigos no Facebook?

a. Tipo: Marcação única (Radio)

b. Opções
   i. 0 a 50
   ii. 51 a 100
   iii. 101 a 200
   iv. 201 a 500
   v. 501 a 700
   vi. 701 a 1000
   vii. Mais de 1000

c. Justificativa: esta questão objetiva *identificar o tamanho da rede de amizades do respondente, tendo em vista que quanto maior tal rede, acredita-se que mais susceptível estará o mesmo a ter suas informações pessoais acessadas por terceiros, bem como maior será a quantidade de informações de terceiros que o respondente poderá ter acesso.* Um número exagerado de amigos pode ser um indicativo da falta de preocupação em relação à preservação da privacidade dos dados postados pelo respondente. Por outro lado, um número pequeno de amigos pode indicar que a pessoa é exigente em relação à preservação de sua privacidade.

23. Entre os seus amigos no Facebook, quantos deles você conhece pessoalmente ? Marque a opção que melhor descreve:

a. Tipo: Marcação única (Radio)

b. Opções
   i. Todos.
   ii. A grande maioria (80% ou mais)
   iii. A maioria (50% ou mais)
   iv. A minoria (menos de 50%)
   v. Poucos (20% ou menos)
   vi. Nenhum

c. Justificativa: Queremos descobrir o quanto as pessoas se preocupam em selecionar os seus amigos. Com essa questão, é possível ver a quantidade de pessoas desconhecidas que o participante aceita como amigo.

24. Marque quem, entre as pessoas abaixo, você possui adicionado como amigo no Facebook:

a. Tipo: Marcação múltipla (Checkbox)

b. Opções

i. Núcleo familiar (pais, companheiro(a), filhos, irmãos)
ii. Parentes
iii. Amigos íntimos
iv. Amigos
v. Colegas de estudo ou trabalho
vi. Conhecidos
vii. Pessoas que você não conhece pessoalmente

c. Justificativa:

i. Não adianta falar que a pessoa não está restringindo adequadamente no Facebook para a sua família se a sua família não tem conta ou não é seu contato no Facebook. Portanto, é importante saber quem ele tem como amigo no Facebook.

ii. Além disso, no momento da correlação entre os dois quadros de compartilhamento, se a pessoa marcar que "Comparitlha com todos os seus amigos", se não soubermos quem são seus amigos, isso não irá significar muita coisa. Além disso, é preciso saber quem são seus amigos para decidir se a equivalência dos níveis será feita entre "Amigos não íntimos" (off-line) e "Amigos"(contatos do Facebook), ou entre "Pessoas que conhece apenas de vista.." e "Amigos" (contatos do Facebook).

25. Classifique os recursos disponíveis no Facebook de acordo com o seu grau de utilização:

a. Tipo: Marcação única (Radio) por linha

b. Opções:

	Sempre (pelo menos uma vez por dia)	**Várias vezes** (pelo menos uma vez por semana)	**Ás vezes** (pelo menos uma vez por mês)	**Poucas vezes** (menos de uma vez por mês)	**Nunca** (nunca usei ou faz mais de um ano)
Postar em sua própria linha do tempo					
Postar Fotos / Vídeos em que você aparece					
Marcar pessoas em fotos					
Compartilhamento de conteúdo postado por terceiros					
Curtir postagens ou fotos de terceiros					
Comentar postagens ou fotos de terceiros					
Aplicativos ou					

jogos					
Mensagens/Chat					
Criar ou participar de eventos					
Localização (Check-in)					

c. Justificativa: esta questão objetiva identificar se os recursos do Facebook utilizados pelo usuário estão relacionados de alguma forma com questões relativas à violação de privacidade, como o compartilhamento de informações pessoais. O uso dos recursos pode apontar indícios de que uso mais privativo (como as conversas privadas no chat) ou público (como publicação em mural).

26. Quais das seguintes ações relacionadas à privacidade você já executou no Facebook?

a. Tipo: Marcação única (Radio) por linha

b. Opções

	Já usei	**Não usei, apesar de ter conhecimento da existência desse recurso**	**Não sabia desse recurso**
• Restringir quem pode ver minhas publicações • Restringir quem pode entrar em contato comigo • Restringir quem pode me procurar no Facebook usando meu endereço de email ou número de telefone • Desativar a exibição de um link da minha linha do tempo por mecanismos de busca • Restringir quem pode publicar em minha linha do tempo • Analisar publicações nas quais meus amigos me marcam antes de serem exibidas na minha linha do tempo • Restringir quem pode ver publicações nas quais fui marcado em minha linha do tempo? • Restringir quem pode ver o que outras pessoas postam em minha linha do tempo. • Adicionar amigos à lista de restritos, de forma que eles poderão ver somente as minhas informações e postagens que são públicas. • Desafazer amizades • Bloquear pessoas			

c. Justificativa: Gostaríamos de saber se a pessoa se preocupou com privacidade a ponto de explorar a página específica para configurações de privacidade do Facebook e alterar essas configurações. Como são muitas, escolhemos algumas configurações a fim de saber se a pessoa já chegou a realiza-las.

27. Geralmente, as suas postagens do Facebook ficam visíveis para quem?

a. Tipo: Marcação única (radio)

b. Opções:

i. Amigos
ii. Amigos de amigos
iii. Amigos exceto conhecidos
iv. Para listas criadas automaticamente pelo Facebook (ex. família, colegas de trabalho)
v. Personalizado (pessoas específicas ou lista criada por você)
vi. Público
vii. Não sei

c. Justificativa: Em nenhum momento nas entrevistas procuramos saber qual é o comportamento padrão do usuário. Esse comportamento padrão pode ser interessante até mesmo para comparações culturais. Será que o comportamento padrão da maioria dos americanos é diferente do que a maioria dos brasileiros?

28. Você coloca algum tipo de informação falsa sobre você no Facebook?

a. Tipo: Marcação única (radio)

b. Opções:

i. Sim
ii. Não

29. Marque com quem você se sente confortável para compartilhar as seguintes informações no Facebook:

a. Tipo: Marcação única (radio) por linha

b. Opções:

	Não compartilha	**Amigos**	**Amigos e Amigos de amigos**	**Público**	**Personalizado (pessoas específicas ou listas)**	**Grupo (comunidade)**
Local onde trabalha ou já trabalhou						
Local onde estuda ou estudou						
Estado civil / Relacionamento						
Relações de parentesco (por exemplo, quem são as pessoas da sua família)						
Data do seu aniversário						
Endereço de e-mail						
Telefone						
Endereço residencial						
Opinião sobre crenças/religião						
Opiniões políticas						
Estado de saúde						
Fotos suas						
Fotos de sua família						
Locais que frequenta						

Emoções negativas						
Emoções positivas						
Problemas de relacionamento						
Conquistas pessoais (por exemplo, um prêmio recebido, uma viagem realizada, um novo emprego, etc).						

c. Justificativa: Comparar o que a pessoa disse que compartilha no meio off-line na questão 15 ("**Marque com quem você se sente confortável para compartilhar as seguintes informações")** com o que ela compartilha ou é capaz de compartilhar no Facebook. Porém, as colunas de lá são diferentes das desse quadro. A comparação será da seguinte forma:

   i. Se o participante escolheu "Público" nesse quadro, será verificado se ele marcou "Qualquer pessoa" no outro.

      1. Caso tenha marcado, seus níveis estão compatíveis
      2. Caso contrário, online ele está mais exposto do que off-line

   ii. Se o participante escolheu "Amigo" nesse quadro, será verificada a pergunta 40 sobre quem são os seus amigos no Facebook (amigos íntimos, não íntimos, pessoas q conhece de vista,...)

      1. Se na questão 18 marcou "Ninguém" então
         a. Está mais exposto online do que off-line
      2. Se na questão 18 marcou "Everybody" então
         a. Se marcou Pessoas que não conhece na 29
            i. Está compatível
         b. Senão
            i. Está mais exposto off-line
      3. Será comparado se todos os papéis da pergunta 29 foram marcados no quadro off-line
         a. Se os papéis da pergunta 29 são exatamente os mesmos com os quais a pessoa compartilha a informação off-line, então os níveis estão compatíveis
         b. Se o conjunto de papéis da pergunta 29 contém os papéis do quadro off-line, porém os off-line compartilha com menos pessoas, então online ele está mais exposto do que off-line
         c. Se o conjunto de papéis da pergunta 29 é contido pelos papéis do quadro off-line, e se off-line então ele compartilha com mais pessoas, então online ele está **menos** exposto do que off-line
         d. Se o conjunto de papéis da pergunta 29 divergir dos papéis do quadro off-line, não havendo a relação de contém ou contido, pode-se concluir que o comportamento do usuário no mundo virtual não está consistente com o seu comportamento no mundo físico.

   iii. Se o participante escolheu "Não compartilharia" neste quadro, será verificado se no quadro off-line ele marcou "Ninguém".

      1. Caso tenha marcado, seus níveis estão compatíveis

2. Caso contrário, ele está se expondo menos online do que off-line.

iv. Se o participante escolheu "Amigos de amigos" neste quadro será verificado se marcou "Qualquer pessoa" no quadro off-line (pois não é possível ter controle de quem seus contatos aceitam como contato)

1. Se marcou, então seus níveis estão compatíveis
2. Caso contrário, ele está se expondo mais online do que off-line

v. Se o participante escolheu "Personalizado" neste quadro será verificado se marcou qualquer opções diferente de "qualquer pessoa" ou "ninguém" no quadro off-line

1. Caso positivo, seus níveis estão compatíveis
2. Caso contrário:
    a. se marcou "qualquer pessoa" no quadro off-line, ele está se expondo **mais** no mundo off-line
    b. Se marcou "ninguém" no quadro off-line, ele está se expondo **menos** no mundo off-line.

vi. Não será feita uma equivalência para "Grupo" no Facebook e o mundo offline, pois existem tipos diferentes de grupos dentro do Facebook (abertos e restritos) e não é possível saber quais são as pessoas que estão lá.

30. Considere a seguinte situação: Você esqueceu seu Facebook aberto, e uma pessoa que você conhece mas não tem muito contato, ao usar o mesmo computador que você estava usando, acaba vendo informações do seu Facebook (linha do tempo, fotos, ...). Você se sentiria incomodado?

a. Tipo: Marcação única (radio)

b. Opções
    i. Muito incomodado
    ii. Um pouco incomodado
    iii. Não me incomodaria

c. Justificativa: As pessoas estão ou não compartilhando sua privacidade nas redes sociais? Essa pergunta seria para ajudar a responder a essa pergunta. Se a pessoa não se incomoda, talvez ela não esteja colocando nada ali tão privativo assim. Essa pergunta é complementar a pergunta que a pessoa fala quais são as informações pessoais pra ela e a pergunta na qual ela fala o que compartilha no Facebook. Ela tem o intuito apenas de **confirmar** a resposta das outras questões e detectar contradições.

As três próximas questões objetivam identificar se o usuário já teve problemas relacionados à privacidade no Facebook e, em caso positivo, e se, após o ocorrido, este continuou utilizando a sua conta, porém mostrando maior preocupação com questões relacionadas à privacidade, através da alteração de sua forma de uso.

31. Que tipo de problema relacionado à privacidade você teve no Facebook?

a. Tipo: Marcação múltipla (Checkbox)

b. Opções:
    iv. Acesso indevido à minha conta no Facebook (por exemplo: roubo de senha)
    v. Ser marcado em fotos indesejáveis
    vi. Ser contatado por pessoa indesejável
    vii. Ser mencionado em postagens/comentários inconvenientes de terceiros
    viii. Receber comentários inconvenientes em algo que postei
    ix. Acesso a minhas informações por uma audiência indesejada dentro do Facebook
    x. Difusão indevida de minhas informações para um público externo ao Facebook

xi. Ter o meu comportamento dentro do Facebook monitorado
xii. Nunca tive problema
xiii. Outros. Quais? ____

c. Comportamento especial: só mostra a próxima questão se o respondente marcou uma opção diferente de "Nunca tive problema" nesta questão.

32. Você alterou a forma de uso dos recursos do Facebook após o problema que teve com privacidade?

a. Tipo: Marcação única (radio)

b. Opções:
   i. Sim.
   ii. Não

c. Justificativa: essa questão tem o propósito de investigar se a pessoa alterou a forma como utiliza os recursos do Facebook após ter problema com privacidade em sua conta, ou seja, se ela tomou alguma atitude depois do problema ter acontecido.

33. Já leu a política de privacidade do Facebook?

a. Tipo: Marcação única (radio)

b. Opções
   i. Não li
   ii. Comecei a ler, mas acabei desistindo
   iii. Li apenas as partes que me interessavam
   iv. Li a maior parte da política
   v. Li ela inteira

c. Justificativa: Essa questão é importante para contraste cultural. Ambos os países se preocupam com a política de privacidade? Ou um se preocupa e o outro não? Essa questão ainda é útil para mostrar o tanto que as pessoas se preocupam com privacidade e até que ponto estão dispostas a se esforçar para garanti-la.

34. Na barra lateral direita do Facebook é possível acompanhar as atividades dos seus amigos, por exemplo, se um amigo curtiu ou comentou uma postagem. Como você se sentiria ao saber que alguém esta usando esse recurso para acompanhar o que você esta fazendo?

a. Tipo: Marcação única (radio)

b. Opções
   a. Não me incomodaria.
   b. Sentiria um pouco incomodado
   c. Sentiria muito incomodado
   d. Dependendo de quem fosse, sentiria incomodado
   e. Nenhuma das opções.

c. Justificativa:

   a. Essa questão permite ver se a pessoa se sentiria incomodada ao ser monitorada por alguém na internet.

   b. Além disso, também possibilita saber como as pessoas vêem esse recurso oferecido pelo Facebook (e o Facebook não permite desabilita-lo).

Seção 5 de 5 – Privacidade online (mundo virtual) versus Privacidade off-line (mundo real)

35. Abaixo são apresentadas algumas perguntas relacionadas à privacidade de suas informações. Marque se você considera que a característica está mais associada ao mundo virtual, ao mundo físico, igualmente associada a ambos ou a nenhum dos dois.

a. Tipo: Marcação única (Radio) por linha

b. Opções:

Sobre suas informações	Principalmente no mundo online	Principalmente no mundo físico	Igualmente em ambos	Em nenhum dos dois
Em qual mundo você tem mais controle sobre elas?				
Onde há mais chances delas serem disseminadas/divulgadas por outras pessoas sem sua autorização?				
Em qual mundo você tem maior preocupação com a segurança das suas informações?				
Em qual deles há mais chances de suas informações poderem atingir um destino inesperado ou desconhecido?				
Onde é necessário mais cuidado com o que você divulga sobre sua vida?				
Onde é necessário mais cuidado em relação a quem você divulga suas informações?				
Em qual deles é mais comum ser feito o mau uso de suas informações?				

c. Justificativa: Esse quadro tem como objetivo entender se o respondente diferencia e como ele diferencia ou percebe privacidade online de privacidade off-line.

36. A partir do momento em que você começou a utilizar redes sociais, marque como a sua preocupação com privacidade mudou (ou não) nos mundos físico e virtual:

a. Tipo: Marcação única (Radio) por linha

b. Opções:

	Aumentou	Não mudou	Diminuiu
Mundo físico			
Mundo virtual			

c. Justificativa: Essa pergunta é importante se a preocupação das pessoas com privacidade mudou a partir do momento em que começaram a utilizar redes sociais.

37. Considere o seguinte trecho:

"Desde que o Facebook foi lançado, há dez anos, em 4 de fevereiro, de 2004, tornou-se possível conectar a quase todas as pessoas no mundo, instantaneamente. Essas conexões levaram a coisas incríveis, seja o amor entre duas pessoas ou um movimento que mobiliza milhões. [...]" (Trecho extraído e traduzido livremente do site http://www.facebookstories.com/10)

§ Em relação a esse trecho, pode-se afirmar:

a) Fala sobre privacidade no Facebook
b) Fala sobre a criação das grandes empresas Facebook e Google
c) Fala sobre a criação do Facebook e como ele ajudou a conectar pessoas
d) Fala sobre como utilizar a linha do tempo do Facebook

Referências bibliográficas

Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2010. **Research Methods in Human-Computer Interaction**. Wiley Publishing.

Kumaraguru, P., and Sachdeva, N. **Privacy in India: Attitudes and Awareness V 2.0**. Tech. rep., PreCog-TR-12-001, PreCog@IIIT-Delhi, 2012. http://precog.iiitd.edu.in/research/privacyindia/

Paul Cairns and Anna L. Cox. 2008. **Research Methods for Human-Computer Interaction (1st ed.)**. Cambridge University Press, New York, NY, USA.

Conteúdo do Questionário (em inglês)

Section 1 of 5 – Respondent's Profile

This group of questions intend to identify the respondents' profile, which will be useful for further analysis of the responses in the following sections of the questionnaire, allowing correlation of variables of user profiles with the research questions.

1. **What is your nationality?**
   a. Type: Multiple Choice (Select One)
   b. Options:
      i. American
      ii. Other (please specify)_____

2. **(Conditional) How long have you been in U.S.? (answer this question only if you chose "Other" in question above)**
   a. Type: Multiple Choice (Select One)
   b. Options:
      i. Less than two years
      ii. Two to five years
      iii. More than five years to ten years
      iv. More than ten years

3. **Do you have a current relationship with an American university?**
   a. Type: Multiple Choice (Select One)
   b. Options:
      i. Yes. Please specify the University: _____
      ii. No.

4. **(Conditional) What is your relationship with this university? (answer this question only if you chose "Yes" in question above)**
   a. Type: Multiple Choice (Select One)
   b. Options:
      i. Faculty
      ii. Student
      iii. Staff
      iv. Former student
      v. Others
   c. Reason: This question is specific to the version of the general survey to be applied through Mechanical Turk – this question aims to filter respondents belonging to any American academic community (Faculties and Students) in order to contrast with data from the survey with a Brazilian academic community (UFMG).

5. **What is your gender?**
    a. Type: Multiple Choice (Select One)
    b. Options:
        i. Female
        ii. Male
    c. Reason: This feature might influence respondent's behavior and beliefs about privacy.

6. **In which year were you born?**
    a. Type: Drop Down Menu
    b. Options:
        i. 1940
        ii. 1941
        iii. ...
        iv. 2003
    c. Reason: Age might influence respondent's behavior and beliefs about privacy. The reason we chose ask the birth year rather than age is here: http://www.rockresearch.co.nz/blog/2008/09/16/how-old-are-you-how-to-ask-the-age-question-in-surveys

7. **What is the highest level of education you have completed?**
    a. Type: Multiple Choice (Select One)
    b. Options:
        i. High school or equivalent
        ii. Vocational or equivalent
        iii. Some college
        iv. Bachelor degree
        v. Master degree
        vi. Doctoral degree
        vii. Professional degree (MD, JD, etc...)
    c. Reason: Feature that might influence respondent's behavior considering that people might be better informed and concerned about privacy when they have higher level of education.

8. **Are you a student, have you graduated in or work in the field of Information Technology (IT)?**
    a. Type: Multiple Choice (Select One)
    b. Options:
        i. Yes
        ii. No
    c. Reason: This feature might influence participant's privacy concerns and behaviour.

9. **What is your marital status?**
    a. Type: Multiple Choice (Select One)
    b. Options:
        i. Single
        ii. Married
        iii. Separated / Divorced
        iv. Widower
    c. Reason: This feature might influence respondent's behavior and beliefs about privacy.

Section 2 of 5 – The Use Experience of Social Network

This group of questions will help to identify if respondents online social networks and if the concern about privacy is a decisive reason for closing an account in one of these systems. The goal in this section is also to verify if respondent is experienced in social networks, if he/she have already faced privacy issues in some of these networks and if he/she is currently a Facebook user.

10. How long have you been using social networks?

a. Type: Multiple Choice (Select One)

b. Options:

i. Never used
ii. Less than 6 months
iii. From 6 months to 1 year
iv. More than 1 to 3 years
v. More than 3 years

b. Special behavior: If person choose "never used", show only the question below and the “send” button.

c. Reason: As we need to know if the respondent is an user of online social networks, we took advantage of it and asked him how long he use these networks. Time of use can be a factor that influences user’s perception of privacy and what he knows about the resources that social networks provide for privacy management.

11. (Conditional) Why didn’t you create an account in an online social network? (show this question only if the person said he never used social networks in question10)

a. Type: Multi-point Scales (Matrix Single Select)

b. Options:

	Very important	Important	Somewhat important	Not important	I have no opinion
I think it’s dangerous for my safety.	O	O	O	O	O
I think it’s a lot of exposure	O	O	O	O	O
I think it’s very complicated to configure	O	O	O	O	O
I´m unsure about what the company behind online social network could do with the users’ data	O	O	O	O	O
It takes up a lot of time	O	O	O	O	O
I’m not interested.	O	O	O	O	O

c. Reason: This question might indirectly raise people’s concern about privacy issues, asking them why they never created an account on an online social network.

12. **(Conditional) What social networks have you ever used or do you currently use? (Choose all that apply) (Show this question only if person chose any option except the "i" in question 10)**
    a. Type**:** Multiple Choice (Select Many)
    b. Options:
        i. Facebook
        ii. Foursquare
        iii. Google +
        iv. Instagram
        v. Myspace
        vi. Orkut
        vii. Tumblr
        viii. Twitter
        ix. Academia.edu
        x. LinkedIn
        xi. ResearchGate
        xii. Badoo
        xiii. Other
    c. Reason: It is interesting to know how many social networks the person uses, because if a person has several social networking accounts, possibly he doesn't care very much about his privacy. Perhaps this question can be removed if we will need to reduce the questionnaire because this answer does not allow us to draw any conclusion nor claim that the person cares or does not care. It might be useful for comparison between American and Brazilian cultures.

13. **(Conditional) Have you ever deactivated your account on an online social network? (Show this question only if the person chose any option except the "i" in question 10)**
    a. Type: Multiple Choice (Select One)
    b. Options:
        i. Yes
        ii. No
    c. Special behavior: If person choose "Yes", show the question below.
    d. Reason: this question, as question 8, might indirectly raise people's concern about privacy.

14. **(Conditional) Why did you deactivate your account on any social network? (Show this question only if the respondent chose "yes" in question above)**
    a. Type**:** Multiple Choice (Select Many)
    b. Options:
        i. Friends left the network / migrated to other networks
        ii. Lack of use
        iii. Lack of interest
        iv. Difficulty in using the system
        v. Problems related to privacy
        vi. Others (please specify) _____
    c. Reason: this question, as question 8, might indirectly raise people's concern about privacy issues, asking them why they left some social network.
    d.

15. **(Conditional) How long have you been using the Facebook? (Show this question only if the person chose option "i" in question 12)**

    a. Type: Multiple Choice (Select One)

    b. Options:

        i. I don't have a Facebook account.
        ii. Less than 6 months
        iii. From 6 months to 1 year
        iv. More than 1 to 3 years
        v. More than 3 years

    c. Special behavior: If the person chooses "I don't have a Facebook account" the questionnaire will be closed. If the respondent chooses any of the other options, the remainder of the questionnaire will be showed.

    d. Reason: this question aims to know if the respondent has a Facebook account and how is his experience about it in order to figure out if he had time to try its privacy resources and get familiarized to its interface. If the respondent is currently a Facebook user, he will be directed to the next set of questions which are specifics about privacy. Although Facebook had appeared as an option in question 12, the respondent there can select it whether it has previously used it but doesn't use it anymore.

Section 3 of 5 – Privacy in General

This group of questions aims to identify the respondents' perception about privacy in general. The answers in this section will be useful for correlation with other answers related to privacy in the virtual world, looking for a better understanding about the changes brought by the resources of modern life in how people understand the privacy concept.

16. **In your opinion, what is privacy in the <u>physical world</u> associated to? (Choose all that apply):**

    a. Type**:** Multiple Choice (Select Many)

    b. Options:

        i. Protect data from criminal attacks and threats to my safety
        ii. Be able to choose the information that I'm going to share and with whom
        iii. Have my own space and no one has access to it without my permission
        iv. I don't know.
        v. Others (please specify) _____

    b. Reason: this question aims to identify to what aspects respondents relate the privacy concept in the physical world. The answers options were obtained from the responses of question about the meaning of the concept of privacy during the interviews.

    Reason for the answers options:

        i. It aims to know if person associates privacy to safety
        ii. It aims to know if person associates privacy to information restrictions (not related to safety)
        iii. It aims to know if person associates privacy to the idea of having his own space.
        iv. It aims to know if person had some difficulty to answer this question.

17. **Rate the following information according to how personal you consider it, on a four-points scale, ranging from "very personal" to "it's not personal (the first point means a greater concern regarding with whom you share such information and the last point means less concern to restrict who would access to information):**

    a. Type: Multi-point Scales (Matrix Single Select)

    b. Options:

	Very personal	**Personal**	**Somewhat personal**	**Not personal**
Where do you work or worked in the past				
Where do you study or have studied				
Marital status / Relationship status				
Birthday				
Email address				
Phone number				
Address				
Religion / thoughts about beliefs				
Political views				
Health and history				
Photos of you				
Photos of your family				
Places you visit				
Your bad emotions				
Your good emotions				
Relationship issues				
Personal achievements (e.g. an award received, a trip, a new job etc.)				

    c. Reason: This question aims to find out how much information is considered personal by respondents in order to contrast with the question 15 and to know with whom the information marked as personal here is shared. This is for verifying the theory raised during the interviews, that there would be a degree of variation between personal information and those considered "very personal" are not placed on the social networks. Furthermore, this degree of personhood of the information can be helpful to show possible cultural differences between Brazil and the USA.

18. **<u>In the physical world</u>, among groups of people below, choose those with whom you feel comfortable to share the following information (For each information, choose all that apply):**

    a. Type: Check box / Multi-select (Matrix multi-Select)

    b. Options:

	Family (parents, spouse, siblings, children)	**Relatives**	**Closest friends**	**Friends**	**Work/School colleagues**	**Acquaintances**	**Everybody**	**Nobody**
Where do you work or worked in the past								
Where do you study or have studied								
Marital status / Relationship								

status								
Birthday								
Email address								
Phone number								
Address								
Religion / thoughts about beliefs								
Political views								
Health and history								
Photos of you								
Photos of your family								
Places you visit								
Your bad emotions								
Your good emotions								
Relationship issues								
Personal achievements (e.g. an award received, a trip, a new job etc.)								

c. Reason: This frame will allow a comparison with the question 29 that has a frame where the respondent is asked to choose if he shares the same information on Facebook and with whom.

Section 4 of 5 –Privacy on Facebook

This group of questions aims to identify information on how users deal with issues related to privacy on Facebook.

19. In your opinion, what is privacy in the virtual world associated to? (Choose all that apply):

a. Type**:** Multiple Choice (Select Many)

b. Options:

i. Protect data from criminal attacks and threats to my safety
ii. Be able to choose the information that I'm going to share and with whom
iii. Be able to choose who has access to different parts of my profile (mural, albums, ...)
iv. I don't know.
v. Others (please specify) _____

c. Reason: this question aims to identify to what aspects respondents relate the privacy concept in the virtual world. The answers options were obtained from the responses of question about the meaning of the concept of privacy during the interviews.

Reason for the answers options:

i. It aims to know if person associates privacy to safety
ii. It aims to know if person associates privacy to information restrictions (not related to safety)
iii. It aims to know if person associates privacy to the idea of having his own space related to his profile on Facebook.
iv. It aims to know if person had some difficulty to answer this question.

20. How often do you access your Facebook?

a. Type: Multiple Choice (Select One)

b. Options:

i. Always connected (via mobile)
ii. Several times a day
iii. At least once a day
iv. At least four times a week
v. At least once a week
vi. At least once a month
vii. Less than once a month

c. Reason: this question is important to know the users experience on Facebook. It might be user shares less information if he does not access Facebook very often.

21. Do you have more than one Facebook profile?

a. Type: Multiple Choice (Select One)

b. Options:

i. Yes
ii. No

c. Special behavior: if respondent choose "Yes", show the next question.

d. Reason: This question allows identifying if the respondent has any extra profile, which may represent an attempt to preserve identity and privacy of his space of concrete relations, but also facilitate the invasion of another's privacy in cyberspace.

22. (Conditional) What is the main reason why you have an extra profile? (Choose all that apply) (Show this question only if the respondent chose "yes" in question above)

a. Type**:** Multiple Choice (Select Many)

b. Options:

i. To observe/interact with other people without being identified.
ii. To separate my personal and professional contacts
iii. To test how people are seeing my Facebook profile or to test Facebook features and understand how they work
i. Others (please specify) _____

c. Reason: The previous question without a question on the reason to have another account does not allow us to draw any conclusions.

23. Do you use Facebook to ...

a. Type: Multi-point Scales (Matrix Single Select)

b. Options:

	Often	Sometimes	Rarely	Never
Share my personal information	O	O	O	O
Share useful/interesting information	O	O	O	O
Follow updates from contacts	O	O	O	O
Keep updated on issues in general	O	O	O	O
Find new friends	O	O	O	O

Update contacts	O	O	O	O
Talk	O	O	O	O
Join to groups	O	O	O	O

c. Reason: the reason for the people use Facebook can be directly related to how they see the issue of privacy in this environment.

24. Do you consider that by creating a Facebook account you are giving up part of your privacy?

a. Type: Multiple Choice (Select One)

b. Options:

i. Yes
ii. No

c. Reason: This question is important to identify if the respondent thinks that he/she gave up part of his/her privacy rights with the creation of a Facebook account.

25. How many friends do you have on Facebook?

a. Type: Multiple Choice (Select One)

b. Options:

i. 0 to 50
ii. 51 to 100
iii. 101 to 200
iv. 201 to 500
v. 501 to 700
vi. 701 to 1000
vii. More than 1000

c. Reason: This question aims to identify how large the respondent's friendship network is, given that a larger network, it is believed that it will be more likely to have his personal information accessed by others and the greater the amount of other people's information the respondent may have access to. An excessive number of friends may be indicative of a lack of concern regarding the privacy preservation of the data posted by the respondent. On the other hand, a small number of friends may indicate that the person is demanding regarding the preservation of his privacy.

26. Among your friends on Facebook, how many do you know personally?

a. Type: Multiple Choice (Select One)

b. Options:

i. Everyone.
ii. The vast majority (80% or more)
iii. The majority (50% or more)
iv. The minority (less than 50%)
v. Few (20% less)
vi. Nobody

c. Reason: We want to find out how great is the people's concern to select their friends on Facebook. With this question it is possible to quantify the amount of unknown people that the participant has as friend on Facebook.

27. Choose below which people you have added as a friend on Facebook (Choose all that apply):

a. Type**:** Multiple Choice (Select Many)

b. Options:

i. Family (parents, spouse, children, siblings)
ii. Relatives
iii. Closest friends
iv. Friends
v. Colleagues (work or study)
vi. Acquaintance
vii. People you do not know personally

c. Reason:

i. It is important to know who the respondent has as friends on Facebook in order to verify if he is properly restricting their information there.

ii. Furthermore, when the correlation between the two sharing frame, if the person said that share his information with all his friends, we need to know who his friends are on Facebook.

28. Classify the resources available on Facebook according to how much you use them:

a. Type: Multi-point Scales (Matrix Single Select)

b. Options:

	Always (at least once a day)	**Often** (at least once a week)	**Sometimes** (at least once a month)	**Rarely** (less than once a month)	**Never** (never used or used in more than one year)
Post photos to your timeline					
Post Photo / Video where you appear					
Tag people in photos					
Share content (from other people)					
Like other people photos or posts					
Post comments to other people's photos or posts					
Use Apps or games					
Send Messages / Chat					
Create or participate in events					
Use location service (check-in)					

c. Reason: this question aims to identify whether Facebook's resources used by respondent are related in some way with issues of privacy violation, such as sharing personal information. Resource use can

indicate a more private use (as private conversations in chat) or a more public use (as publications in timeline).

29. Which of the following actions related to privacy settings have you ever executed on Facebook?

a. Type: Multi-point Scales (Matrix Single Select)

b. Options:

	I have already used	**I have not used, despite being aware of the existence of this setting**	**I was unaware of this setting**
Restrict who can see my posts			
Restrict who can contact me			
Restrict who can look me up using my email address or phone number			
Turn off the setting to other search engines to link to my timeline			
Restrict who can post in my timeline			
Review posts friends tag me in before they appear on my timeline			
Restrict who can see posts I've been tagged in on my timeline			
Restrict who can see what other people post on my timeline			
Add friends to my restricted list so that they can only see the information and posts that I make public.			
Undo friendship			
Block users			

c. Reason: We wonder if the person worried about privacy to the point of exploring the specific page to Facebook's privacy settings and modify these settings. We chose some these settings in order to know if the person has already modified them.

30. Usually, your posts on Facebook are visible to whom?

a. Type: Multiple Choice (Select One)

b. Options:

i. Friends
ii. Friends of friends
iii. Friends except Acquaintaces
iv. Lists created automatically by Facebook (e.g. Close friends, Family etc.)
v. Custom (lists you have created or specific people)
vi. Everyone (Public)
vii. I don't know

c. Reason: The default behavior of users may be of interest to cultural comparisons and to check their privacy concerns when they post content on Facebook.

31. Do you share some fictitious information about you on Facebook?

a. Type: Multiple Choice (Select One)

b. Options:

i. Yes
ii. No

32. Choose with whom you would feel comfortable to share the following information on Facebook:

a. Type: Multi-point Scales (Matrix Single Select)

b. Options:

	Don't share	**Friends**	**Friends and Friends of friends**	**Public**	**Custom (specific people or lists)**	**Groups**
Where you work or worked in the past						
Where you study or have studied						
Marital status / Relationship status						
Birthday						
Email address						
Phone number						
Address						
Religion / thoughts about beliefs						
Political views						
Health and history						
Photos of you						
Photos of your family						
Places you visit						
Your bad emotions						
Your good emotions						
Relationship issues						
Personal achievements (e.g. an award received, a trip, a new job etc.)						

c. Reason: Compare what the respondent said he shares the offline world in question 15 ("**Choose with whom do you feel comfortable to share the following information with in the physical world** ") with what he shares or might share on Facebook. However, the column in each table is not the same. The comparison is as follows:

i. If the respondent chose "Public" in this table, it will be verified if he chose "Everybody" on question 15.

1. If so, his levels are compatible
2. Otherwise, he is more exposed online than offline

ii. If the respondent chose "Friends" in this table, it will be verified who are his friends on Facebook (question 24 – Choose who among the people below you have added as a friend on Facebook – Family, Relatives, Close friends, less close friends, colleagues etc.)

    1. It will be compared if all the roles in question 24 were marked in table of question 15 (offline world)

        a. If roles in question 24 are exactly the same with whom the respondent shares information offline, then the levels are compatible (online and offline)

        b. If the set of roles marked in question 24 contains the roles of the off-line table in question 15, but in offline world the respondent shares with less people, then he is more exposed online than offline

        c. If the set of roles marked in question 24 is contained by roles of the off-line table in question 15, and in the world offline the respondent share information with a large number of people, then he is more exposed offline than online.

        d. If the set of roles marked in question 24 differ from the offline table in question 15, without a contain or contained relationship, it can be concluded that the behavior of the user in the virtual world (online) is not consistent with his behavior in the physical world (offline).

iii. If the respondent chose "not share" in this table, it will be verified in offline world if he marked "Nobody" in table of question 15

    1. If so, his levels are compatible

    2. Otherwise, he is more exposed offline than online

iv. If the respondent chose "Friends and friends of friends" in this table, it will be verified in offline world if he marked "Everybody" in table of question 15 (because the respondent cannot control who are the friends of his friends)

    1. If so, his levels are compatible

    2. Otherwise, he is more exposed online than offline

v. If the respondent chose "Custom" in this table, it will be verified in offline world if he marked any option other than "Everybody" or “Nobody” in table of question 15

    1. If so, his levels are compatible

    2. Otherwise:

        a. If the respondent chose “Everybody” in table of question 15, he is more exposed offline than online

        b. If the respondent chose “Nobody” in table of question 15, he is more exposed online than offline.

vi. It is not possible to make equivalence for "Group" on Facebook and offline world because there are different types of groups within Facebook (open and restricted) and it is not possible to know what are the people who are there.

vii. If the participant chose “Nobody” in off-line world (question 15), it will be verified if he chose any options other than “No share” on Facebook

    1. If so, the respondent is more exposed online than offline.

viii. If the participant chose “Everybody” in off-line world, it will be verified if he chose any options other than “Public” on Facebook

    1. If so, the respondent is more exposed offline than online..

33. Consider the following situation: You forgot to logout of your Facebook account, and a person with whom you do not have much contact comes later, uses the same computer and sees information from your Facebook (timeline, photos, …). Would you feel uncomfortable?

    a. Type: Multiple Choice (Select One)

    b. Options:
        i. Yes. Quite uncomfortable.
        ii. Yes. A little uncomfortable.
        iii. I would not bother.

    c. Reason: People are sharing their privacy on Facebook or not? This question is to help answer it. If the person does not mind, he/she might not be putting any information there so private. This question is complementary to question about personal information and that question about what they share on Facebook. It is intended only to confirm the response of other questions and detect inconsistencies.

The next two questions aim to identify if the user had issues related to privacy on Facebook and, after the fact, if he continued using his account, but with greater concern about privacy, by changing its manner of use.

34. **What kind of privacy-related issue have you had on Facebook?**

    a. Type**:** Multiple Choice (Select Many)
    b. Options:

        i. Unauthorized access to my Facebook account (eg, password theft)
        ii. Be tagged in undesirable photos
        iii. Be contacted by unwanted person
        iv. Be mentioned in inconvenient posts / comments from other people
        v. Receive inconvenient commented on something I posted
        vi. Access to my information by an unwanted audience within Facebook
        vii. Improper dissemination of my information to a Facebook's outside audience
        viii. Someone monitoring my behavior on Facebook
        ix. I never had issues related to privacy on Facebook
        x. Others (please specify)_____

    c. Special behavior: if respondent choose any option except "I never had issues related to privacy on Facebook", show the next question.

35. **(Conditional) Have you changed the way that you use Facebook resources after you have had privacy issues? (Show this question only if the respondent chose any option except "I never had issues related to privacy on Facebook" in question above)**

    a. Type: Multiple Choice (Select One)

    b. Options:

        i. Yes
        ii. No

    c. Reason: This question aims to investigate whether the person changed the way she uses Facebook resources after having problem with privacy on her account, or if she took any action after the problem has happened.

36. **Have you ever read Facebook's privacy policy?**
    a. Type: Multiple Choice (Select One)
    b. Options:
        i. No, never.
        ii. I began to read, but I gave up.
        iii. I just read the parts that interest me
        iv. I have read most of it.
        v. Yes. I read it all.
    c. Reason: This question is important for cultural contrast. Are both countries concerned about the privacy policy?

37. **On the Facebook's right sidebar you can track the activities of your friends, for example, if a friend liked or commented on a post. How would you feel to know that someone is using this feature to keep track of what you are doing on Facebook?**
    a. Type: Multiple Choice (Select One)
    b. Options:
        i. I would not bother.
        ii. I would feel a little uncomfortable
        iii. I would feel very uncomfortable
        iv. Depending on who it was, I would feel uncomfortable
        v. None of the above
    c. Reason: This question will verify if the person would feel uncomfortable to be monitored by someone on Facebook. Moreover, it also allows to know how people view this feature offered by Facebook (and Facebook does not allow disable it).

Section 5 of 5 – Online Privacy online (virtual world) versus Off-line Privacy (real world)

38. **Some questions related to privacy of your information are showed below. Choose if you think that the feature is more associated to the online world, to the physical world, equally associated to both worlds or to neither.**
    a. Type: Multi-point Scales (Matrix Single Select)
    b. Options:

Taking into account your information	**In the online world mainly**	**In the physical world mainly**	**Equally on both**	**In neither**
In what world do you have more control over it?				
In what world are there greater possibilities of it being distributed by other people without your permission?				
In what world are you more worried about your information's safety?				
In what world are there greater possibilities of it arriving at an unexpected or unknown destination?				
In what world is more attention needed on what you disclose about your life?				
In what world is more attention needed on who you tell your information?				
In what world is the misuse of your information easier?				

c. Reason: This question aims to understand whether the respondent differentiates and how he differentiates online privacy and offline privacy.

39. From when you started using social networks, select how your privacy concern has changed (or not) in both physical and virtual worlds:

a. Type: Multi-point Scales (Matrix Single Select)

b. Options:

	Increased	Not changed	Decreased
Physical world			
Virtual world			

c. Reason: This question aims to know whether people's privacy concern changed when they started using social networks.

40. Consider the following excerpt

"Since Facebook launched 10 years ago on February 4, 2004, it has become possible to connect to almost anyone in the world, instantly. These connections have led to incredible things, whether it's love between two people or a movement that mobilizes millions [...]" (Excerpt extracted from the website http://www.facebookstories.com/10)

Relative to that excerpt, it can be stated that (select one):

i. It talks about privacy on the Facebook
ii. It talks about the creation of Facebook and Google
iii. It talks about the creation of Facebook and how it helped to connect people
iv. It talks about using the Facebook timeline

References

Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2010. **Research Methods in Human-Computer Interaction**. Wiley Publishing.

Kumaraguru, P., and Sachdeva, N. **Privacy in India: Attitudes and Awareness V 2.0**. Tech. rep., PreCog-TR-12-001, PreCog@IIIT-Delhi, 2012. http://precog.iiitd.edu.in/research/privacyindia/

Paul Cairns and Anna L. Cox. 2008. **Research Methods for Human-Computer Interaction (1st ed.)**. Cambridge University Press, New York, NY, USA.

Apêndice B

Guia Prático sobre o MDP

Este guia consiste na explicação sobre as dimensões de privacidade do MDP, seus atributos e possíveis valores, que estão representados nas Tabelas B.1, B.2 e B.3, respectivamente. Os significados dos níveis de privacidade associados aos possíveis valores de cada dimensão são mostrados na Tabela B.4.

Tabela B.1. Descrição das dimensões do PDM

Categoria	**Dimensão**		**Explicação**
Comunicação usuário-sistema-usuário	**Fonte de Informação**		Refere-se a **quem é o responsável pelo compartilhamento** de informações sobre o indivíduo dentro do sistema, ou seja, **quem** pode determinar como, quando e em que extensão tal informação será compartilhada.
	Espaço de Comunicação		Refere-se ao **local** onde a informação sobre o indivíduo será compartilhada no sistema.
	Informação do Indivíduo		Refere-se à **informação sobre o indivíduo** que será compartilhada no sistema. Esta dimensão é composta por uma ou mais estruturas de informação, que se subdividem nas subdimensões "Expressão" e "Conteúdo", descritas nas próximas duas linhas.
	Estrutura da Informação	*Expressão*	*Refere-se à **forma** como a informação compartilhada sobre o indivíduo é **expressa** dentro do sistema.*
		Conteúdo	*Refere-se ao **nível de pessoalidade** atribuído à informação sobre o indivíduo, que é compartilhada dentro do sistema.*
	Persistência Temporal		Refere-se ao **período de tempo** em que a informação sobre o indivíduo fica disponível para a sua audiência dentro do sistema.
	Audiência		Refere-se **quem terá acesso à informação** sobre o indivíduo dentro do sistema.
Efeitos da Comunicação	**Notificação**		Diz respeito ao sistema **informar adequadamente ao indivíduo** quando informação sobre ele é divulgada ou acessada por outros usuários e de que forma.
	Discurso do Sistema		Está relacionada ao sistema **informar a outros usuários** sobre a ocorrência do compartilhamento de informação do indivíduo.

continua na próxima página

continuação da página anterior		
Categoria	**Dimensão**	**Explicação**
	Disseminação da Informação	Está relacionada à **audiência ser capaz de recompartilhar** informação pessoal sobre o indivíduo com outros usuários dentro do sistema.

Tabela B.2. Descrição dos atributos das dimensões do MDP

Atributo	**Descrição**
Valor	Valor que a dimensão de privacidade pode assumir.
Controle	Quem é o responsável por determinar o valor da dimensão.
Dependência de Controle	Dimensão ou outro aspecto que determina de quem é o controle sobre a dimensão em questão.
Dependência de Valor	Dimensão ou outro aspecto que determina o valor da dimensão em questão.

Tabela B.3. Possíveis valores dos atributos das dimensões do MDP

Dimensão	**Atributo**	**Possíveis valores (domínio)**	**Descrição**
Todas	**Controle**	**Sistema - tempo de design**	O valor da dimensão é definido pelo designer, em tempo de design.
		Sistema - tempo de uso	O valor da dimensão é definido pelo designer, mas em tempo de uso, tendo em vista que depende do valor de alguma outra dimensão ou de outro aspecto relacionado ao compartilhamento.
		Indivíduo	O indivíduo é responsável por definir o valor da dimensão de privacidade, em tempo de uso.
		Outro usuário	Outro usuário é responsável por definir o valor da dimensão de privacidade, em tempo de uso.
		Definido em tempo de uso	Quem será o responsável por definir o valor da dimensão de privacidade será definido em tempo de uso, dependendo do valor de alguma outra dimensão ou de outro aspecto relacionado ao compartilhamento.
Todas	**Dependência de Controle**	**<nome dimensão >**	O valor de <nome dimensão> determina de quem é o controle sobre a dimensão.
		Informação	Características específicas da informação compartilhada, que não são representadas através de valores atribuídos à dimensão **Informação do indivíduo**, determinam de quem é o controle sobre a dimensão.
		Tipo da disseminação da informação	Características específicas sobre o tipo da interação que provoca a disseminação da informação, que não são representadas por nenhuma dimensão do MDP, determinam de quem é o controle sobre a dimensão (valor específico para a dimensão **Disseminação da Informação**) .

continua na próxima página

continuação da página anterior

Dimensão		Atributo	Possíveis valores (domínio)	Descrição
			na	Não aplicável (não há dependência de controle para a dimensão, ou seja, o controle sobre a dimensão não é definido pelo valor de outra dimensão)
Todas		**Dependência de Valor**	**<nome dimensão>**	O valor de <nome dimensão> determina o valor da dimensão.
			Informação	Características específicas da informação compartilhada, que não são representadas através de valores atribuídos à dimensão **Informação do indivíduo**, determinam o valor da dimensão.
			na	Não aplicável (não há dependência de valor para a dimensão, ou seja, o valor da dimensão não é definido a partir do valor de outra dimensão)
Fonte de Informação		**Valor**	**Indivíduo**	O próprio indivíduo compartilha informações sobre ele no sistema, seja explicitamente ou através de suas ações.
			Outro usuário	Outro usuário compartilha informações pessoais do indivíduo dentro do sistema.
Espaço de Comunicação		**Valor**	**Espaço de perfil do indivíduo**	Espaço onde são compartilhadas informações mais estáticas, como aquelas biográficas e descritivas relacionadas a elementos de identidade do indivíduo dentro do sistema, como, por exemplo, nome, data de nascimento, endereço, etc.
			Espaço de publicação do indivíduo	Espaço controlado pelo indivíduo destinado a compartilhar informações que são mais dinâmicas, que refletem situações ou objetos que podem ser sofrer frequentes atualizações, e sobre as quais outros usuários podem interagir.
			Espaço de outro usuário	Espaço pertencente a outro usuário.
			Espaço público	Espaço público, que não pertence a nenhum usuário e pode ser acessado amplamente por todos os usuários do sistema.
Informação do Indivíduo	**Expressão**	**Valor**	**Predefinida**	Mensagem pré-definidas pelo sistema em que os usuários apenas decidem se desejam enviá-las ou não (ex.: curtir ou confirmar a presença e um evento, no Facebook).
			Tipada	Mensagem cujo significado é definido pelo sistema, mas cujo valor é definido pelo usuário (ex.: nome e data de nascimento, no Facebook).
			Livre	Mensagem cujo significado da informação é definido pelo seu conteúdo (ex.: comentário no Facebook pode ser usado para dizer algo positivo, negativo ou mesmo algo que não está relacionado ao que o comentário se refere) .
	Conteúdo	**Valor**	**Pouco pessoal**	Informação pouco pessoal, de acordo com classificação realizada por usuários em Villela et al. [2015a], como, por exemplo, o local onde o indivíduo trabalha ou estuda.
			Levemente pessoal	Informação levemente pessoal, de acordo com classificação realizada por usuários em Villela et al. [2015a], como, por exemplo, opiniões políticas, lugares visitados, estado de relacionamento e conquistas pessoais do indivíduo.

continua na próxima página

continuação da página anterior

Dimensão	Atributo	Possíveis valores (domínio)	Descrição
		Pessoal	Informação pessoal, de acordo com classificação realizada por usuários em Villela et al. [2015a], como, por exemplo, emoções positivas, aniversário e religião/crenças do indivíduo.
		Um tanto pessoal	Informação um tanto pessoal, de acordo com classificação realizada por usuários em Villela et al. [2015a], como fotos de família, endereço de e-mail, fotos e emoções negativas do indivíduo.
		Muito pessoal	Informação muito pessoal, de acordo com classificação realizada por usuários em Villela et al. [2015a], como, por exemplo, problemas de relacionamento, endereço e telefone e informações relacionadas ao estado e saúde do indivíduo.
Persistência Temporal	**Valor**	**Instantânea**	Informação pessoal do indivíduo é disponibilizada no sistema apenas por um período muito curto de tempo (tipicamente em tempo real, apenas para os usuários que estão logados no sistema no momento em que a informação é compartilhada)
		Limitada	Informação pessoal do indivíduo é disponibilizada no sistema por um período limitado de tempo (geralmente curto).
		Ilimitada em uma direção	Informação pessoal do indivíduo é disponibilizada no sistema por um período ilimitado de tempo, iniciando a partir do presente em direção ao passado ou ao futuro. Considerando como presente o momento em que o usuário torna-se parte da audiência da informação, este valor indica que o usuário tem acesso a toda informação compartilhada com a audiência da qual ele faz parte (em qualquer momento anterior ao momento presente) ou o usuário tem acesso apenas às informações compartilhadas com a audiência da qual ele faz parte a partir do momento em que ele começa a fazer parte da mesma (exemplo: grupos no WhatsApp).
		Permanente	Uma vez que a informação é compartilhada no sistema, ela será sempre acessível para a sua audiência.
Audiência	**Valor**	**Indivíduo**	Apenas o próprio indivíduo possui acesso à informação, indicando um nível máximo de privacidade, por um lado, mas, por outro lado, um nível mínimo de interação, dado que ninguém, além do indivíduo, terá acesso à informação.
		Selecionada	O usuário decide quem serão os usuários que farão parte do grupo que irá formar a audiência da informação.
		Limitada	Abrange todo o conjunto de usuários do sistema.
		Ilimitada	Abrange todos os usuários do sistema, além de outras pessoas que não são usuárias do mesmo.

continua na próxima página

continuação da página anterior

Dimensão	Atributo	Possíveis valores (domínio)	Descrição
		Desconhecida	O indivíduo não sabe quem fará parte da audiência de sua informação.
Notificação	**Valor**	**Completa**	O sistema sempre notifica o indivíduo quando outros usuários interagem de alguma forma com a sua informação, como, por exemplo, no Facebook, quando outros usuários curtem, comentam ou compartilham a mesma.
		Parcial	O sistema notifica o indivíduo apenas sobre uma parte das interações de outros usuários com a sua informação.
		Ausente	O sistema não fornece ao indivíduo nenhuma notificação sobre a interação de outros usuários com a sua informação.
Discurso do Sistema	**Valor**	**Ausente**	O sistema não gera nenhuma comunicação sobre o compartilhamento de uma informação do indivíduo.
		Destaque	O sistema apresenta informação do indivíduo a outros usuários à qual estes já possuem acesso, porém dá destaque à mesma.
		Novo	O sistema processa informação do indivíduo, gerando informação nova sobre o mesmo.
Disseminação da Informação	**Valor**	**Ausente**	Não é permitida à audiência da informação do indivíduo recompartilhá-la com outras pessoas.
		Limitada	Informação sobre o indivíduo pode ser compartilhada por sua audiência, porém de uma maneira restrita, apenas para uma audiência adicional limitada.
		Ilimitada	Informação sobre o indivíduo pode ser compartilhada pela sua audiência, sem nenhuma restrição.

Tabela B.4. Níveis de privacidade relacionados às dimensões do MDP

Dimensão		**Significado do Nível de Privacidade**	**Possíveis valores (domínio)**	**Nível de Privacidade**
Fonte de Informação		Relacionado à autonomia, concedida ou não ao indivíduo, em relação ao compartilhamento de sua informação pessoal, discutida por Boyle & Greenberg [2005]	**Indivíduo**	Alto
			Outro usuário	Baixo
Espaço de Comunicação		Relacionado à autonomia, concedida ou não ao indivíduo, para controlar o acesso ao espaço onde ocorre o compartilhamento de informações.	**Espaço de perfil do indivíduo**	Alto
			Espaço de publicação do indivíduo	Alto
			Espaço de outro usuário	Médio-baixo
			Espaço público	Baixo
Informação do Indivíduo	**Expressão**	Os valores dessa dimensão não estão associados a nenhum nível de privacidade.	**Predefinida**	Não aplicável
			Tipada	
			Livre	
	Conteúdo	Relacionado ao **nível de pessoalidade** da informação. Assim, quanto mais pessoal for a informação, o compartilhamento da mesma dentro do sistema leva a um menor nível de privacidade.	**Pouco pessoal**	Alto
			Levemente pessoal	Médio-alto
			Pessoal	Médio
			Um tanto pessoal	Médio-baixo
			Muito pessoal	Baixo
Persistência Temporal		Relacionado ao **tempo** em que a informação fica disponibilizada à sua audiência, dentro do sistema. Assim, quanto mais tempo a informação fica disponível, maior a chance dela ser acessada dentro do sistema, levando a um menor nível de privacidade.	**Instantânea**	Alto
			Limitada	Médio-alto
			Ilimitada em uma direção	Médio-baixo
			Permanente	Baixo
Audiência		Relacionado à quantidade de **pessoas** que vão ter acesso à informação compartilhada. Assim, quanto mais ampla (e desconhecida) é a audiência, menor o nível de privacidade.	**Indivíduo**	Alto
			Selecionada	Médio-alto
			Limitada	Médio
			Ilimitada	Médio-baixo
			Desconhecida	Baixo
Notificação		Relacionado à **consciência** que o indivíduo possui sobre o que está sendo dito ou acessado por outros usuários sobre ele. Assim, quanto maior é tal consciência por parte do indivíduo, maior é a chance dele ser mais restritivo em relação às informações que ele compartilham ou com suas configurações de privacidade.	**Completa**	Alto
			Parcial	Médio
			Ausente	Baixo
Discurso do sistema		Relacionado ao **compartilhamento** que o sistema faz de informações sobre o indivíduo. Assim, quanto mais amplo tal compartilhamento, no que tange ao escopo das informações compartilhadas, menor é o nível de privacidade.	**Ausente**	Alto
			Destaque	Médio
			Novo	Baixo

continua na próxima página

continuação da página anterior

Dimensão	**Significado do Nível de Privacidade**	**Possíveis valores (domínio)**	**Nível de Privacidade**
Disseminação da Informação	Relacionado ao **controle** que o indivíduo tem sobre a sua informação, em relação ao momento em que ela foi inicialmente compartilhada. Assim, quanto menor for tal controle, menor é o nível de privacidade.	**Ausente**	Alto
		Limitada	Médio
		Ilimitada	Baixo

Apêndice C

Material Utilizado na Avaliação com Potenciais Usuários do MDP

Neste Apêndice, incluímos o material utilizado na avaliação com potenciais usuários do MDP, como o Termo de Consentimento Livre e Esclarecido, o questionário pré-teste, a apresentação que fizemos para os participantes sobre o MDP, bem como o seu glossário, o cenário e material utilizado durante a execução das tarefas e, por fim, o roteiro do grupo focal que conduzimos com os participantes, ao final da avaliação.

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Eu, Maria Lúcia Bento Villela, orientada pela Profa. Dra. Raquel Oliveira Prates, desenvolvi como parte da minha pesquisa de doutorado o Modelo de Design de Privacidade (MDP), que consiste em uma ferramenta epistêmica, fundamentada na Engenharia Semiótica, que tem como objetivo apoiar o designer na modelagem do compartilhamento de informações pessoais em Redes Sociais Online (RSOs), com foco na privacidade dos seus usuários. Com isso, esperamos que os designers de RSOs, ao utilizarem o MDP, possam refletir sobre o impacto de suas decisões nos níveis de privacidade proporcionados aos usuários dentro do sistema.

Diante disso, você está sendo convidado pelo Núcleo de Pesquisa em Engenharia Semiótica e Interação (PENSI), o grupo de pesquisa em IHC do Departamento de Ciência da Computação da UFMG, para participar do presente estudo, que tem como objetivo avaliar o uso do MDP na análise do compartilhamento de informação pessoal em RSOs, com foco em aspectos de privacidade relativos ao mesmo. Além disso, este estudo também possui como objeto avaliar a capacidade do MDP gerar descrições de RSOs que permitem diferencia-las entre si, de acordo com considerações específicas de privacidade.

Neste contexto, gostaria de solicitar que você manifeste o seu consentimento para participar deste estudo, realizando as seguintes atividades:

- Responder um questionário sobre a sua experiência em design de IHC, sua experiência de uso de RSOs e seu conhecimento sobre Engenharia Semiótica e suas ferramentas epistêmicas;
- Ouvir uma explicação sobre a proposta geral do MDP, sua estrutura e exemplos;
- Realizar tarefas de modelagem usando o MDP e participar de discussões com outro participante sobre o uso do mesmo;
- Participar de uma breve entrevista pós-teste, para que você possa relatar suas experiências na execução da tarefa e com o uso do MDP.

O estudo completo terá duração aproximada de três horas, incluindo todas as atividades descritas acima. É importante você saber que:

1. Os dados coletados durante o estudo serão utilizados **estritamente** no contexto acadêmico e de pesquisa.
2. A equipe envolvida neste estudo tem o compromisso de publicar os resultados de suas pesquisas em fóruns acadêmicos. Entretanto, a publicação é baseada em nosso

respeito à **privacidade** e **anonimato** dos participantes. Assim, a sua identidade e a sua participação nesta pesquisa serão mantidas em sigilo e os dados divulgados pela pesquisa não conterão nomes ou quaisquer outras informações que permitam identificá-lo(a).

3. O consentimento para participar deste estudo é uma **escolha livre** de sua parte, realizada a partir do esclarecimento de todas as suas dúvidas e questões sobre a pesquisa.
4. Você **pode interromper a sua participação** neste estudo a qualquer momento, sem sofrer nenhuma penalidade. Neste caso, todos os seus dados e resultados parciais serão descartados.
5. Eu, Maria Lúcia Bento Villela, responsável pela condução do presente estudo, estou **disponível** para contato pelo telefone *(38) 99160-5558* e pelo e-mail *mvillela@dcc.ufmg.br*.

De posse das informações acima apresentadas, gostaria que você se pronunciasse sobre a sua decisão:

( ) Dou o meu consentimento para participar do presente estudo.
( ) Não dou o meu consentimento para participar do presente estudo.

Belo Horizonte, ____ de dezembro de 2015.

Nome do participante: _____

Assinatura do participante: _____

Nome da pesquisadora: Maria Lúcia Bento Villela

Assinatura da pesquisadora: _____

QUESTIONÁRIO PRÉ-TESTE

(1) Por favor, preencha o questionário abaixo. Suas repostas irão nos ajudar a analisar as informações que serão coletadas durante o estudo.
(2) Se necessário, utilize o verso das páginas para completar suas respostas.

Data: _____ Identificador_____

1. <u>DADOS PESSOAIS:</u>

Nome: _____ Sexo (M ou F):___ Idade: _____

Formação: _____ Profissão: _____

2. **<u>EXPERIÊNCIA DE USO DE REDES SOCIAIS ONLINE</u>** (Por favor, preencha os campos com a opção que melhor representa a sua resposta a cada pergunta)

2.1. Você utiliza alguma rede social online (RSO), como Facebook Google + ou afins?

a) ( ) Sim. Qual(is)?_____
b) ( ) Não

2.2. Caso sua resposta à questão anterior tenha sido sim, com qual frequência você usa RSOs?

a) ( ) Mais de uma vez por dia
b) ( ) Uma vez por dia
c) ( ) 6 a 5 vezes por semana
d) ( ) 4 a 3 vezes por semana
e) ( ) 2 vezes por semana
f) ( ) 1 vez por semana
g) ( ) Menos de 1 vez por semana

2.3. Ainda caso sua resposta à questão 2.1 tenha sido sim, com que frequência você costuma alterar as suas configurações de privacidade nesses sistemas?

a) ( ) sempre que compartilho alguma informação
b) ( ) às vezes, em algumas situações específicas
c) ( ) alterei para estabelecer uma configuração padrão de privacidade
d) ( ) nunca alterei

3. **CONHECIMENTO SOBRE IHC**

3.1. Você possui conhecimento sobre IHC?

a) ( ) Sim
b) ( ) Não

3.2. Se você marcou "sim" na pergunta anterior, como e em qual período você adquiriu ou tem adquirido conhecimento em IHC? (você pode escolher mais de uma opção)

a) ( ) Graduação, ano(s)_____
b) ( ) Mestrado, ano(s)_____
c) ( ) Doutorado, ano(s)_____
d) ( ) Estudo por conta própria, ano(s)_____
a) ( ) Desenvolvimento de aplicação, ano(s)_____

4. **EXPERIÊNCIA DE DESIGN DE IHC**

4.1. Você já projetou ou desenvolveu interfaces de usuário?

a) ( ) Sim
b) ( ) Não

4.2. Se você marcou "sim" na pergunta anterior, para que tipo de sistema você projetou interfaces de usuário (você pode escolher mais de uma opção)

a) ( ) Sistema monousuário
b) ( ) Sistema colaborativo

4.3. Se você marcou "sim" na pergunta 4.1, de que forma você obteve o conhecimento em design de IHC que você utilizou em seu projeto? (você pode escolher mais de uma opção)

a) ( ) Projeto desenvolvido em disciplina de graduação ou pós-graduação
b) ( ) Projeto desenvolvido em pesquisa
c) ( ) Projeto desenvolvido no mercado de trabalho

5. **<u>CONHECIMENTO SOBRE ENGENHARIA SEMIÓTICA E SUAS FERRAMENTAS EPISTÊMICAS</u>**

5.1. Você possui conhecimento em Engenharia Semiótica?

a) ( ) Sim
b) ( ) Não

5.2. Se você marcou "sim" na pergunta anterior, como e em qual período você adquiriu ou tem adquirido conhecimento em Engenharia Semiótica? (você pode escolher mais de uma opção)

a) ( ) Graduação, ano(s)_____
b) ( ) Mestrado, ano(s)_____
c) ( ) Doutorado, ano(s)_____
d) ( ) Estudo por conta própria, ano(s)_____

5.3. Em relação às ferramentas epistêmicas da Engenharia Semiótica, listadas na tabela abaixo, para cada uma delas, marque um "x" na coluna correspondente.

Obs.: Caso você conheça a ferramenta, especifique o tipo de contato que teve com a mesma (pode especificar mais de um): se foi através de estudo, de uso ou se trabalhou em pesquisa sobre a ferramenta, marcando um "x" nas colunas "Já estudei", "Já utilizei" e "Já pesquisei", respectivamente.

Ferramenta Epistêmica	**Não conheço**	**Conheço**		
		Já estudei	**Já utilizei**	**Já pesquisei**
MOLIC				
Arquitetura de Sistemas de Ajuda				
MANAS				
Metáforas e princípios de SiCos				
CVM (Cultural Viewpoint Metaphors)				
MIS				
MAC				
MISI				

Modelo de Design de Privacidade (MDP)

Uma ferramenta epistêmica para apoio ao projeto do compartilhamento de informações pessoais em Redes Sociais Online, com foco em privacidade

UFMG PENSi Winweb UFVJM

REDES SOCIAIS ONLINE (RSOs)

- Apesar dos **benefícios** associados à **popularidade** das Redes Sociais Online (RSOs)
  - Aumenta a preocupação com **privacidade** relacionada ao **compartilhamento de informação** nesses sistemas
  - Estudos mostram que os **modelos atuais de configuração de privacidade** oferecem **proteção inadequada** aos usuários.

Disparidade entre **configuração de privacidade desejada e real**

OBJETIVO

Proporcionar aos **designers** uma melhor **compreensão** de como a **privacidade** pode ser **tratada** em RSOs.

Criar um **modelo descritivo** para ajudar o **designer** a **refletir** sobre como **comunicar** a ideia de **privacidade** em RSOs.

Ferramenta Epistêmica

Deve **aumentar** o **entendimento do designer** sobre **privacidade** relacionada ao compartilhamento de informações pessoais

O MODELO DE DESIGN DE PRIVACIDADE (MDP)

- Caracteriza **privacidade** em RSOs em relação ao **compartilhamento de informações pessoais**

Inclui **discursos** e **atividades** que expressam **opiniões e pontos de vista do indivíduo**

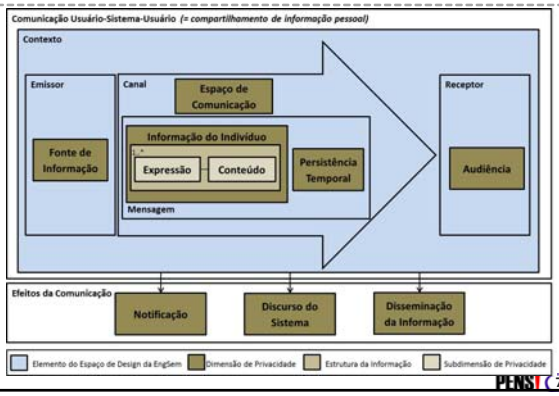
O MODELO DE DESIGN DE PRIVACIDADE (MDP)

- Estruturado por meio de **dimensões de privacidade**
  - Baseadas no **espaço de design** da **Engenharia Semiótica**

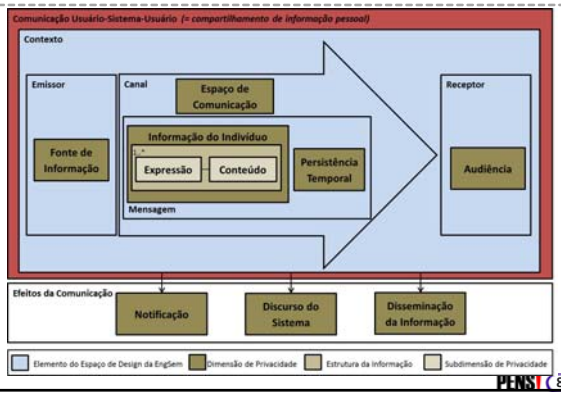
O MODELO DE DESIGN DE PRIVACIDADE (MDP)

- **Dimensões de privacidade**
  - Representam **aspectos**, sobre os quais designers devem **pensar**, que podem influenciar a **privacidade** dos usuários

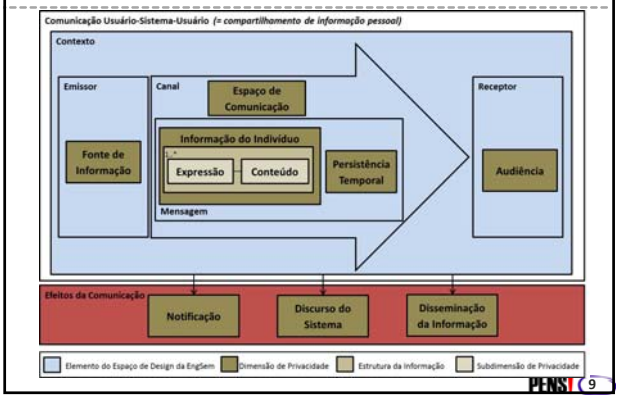
O MODELO DE DESIGN DE PRIVACIDADE (MDP)



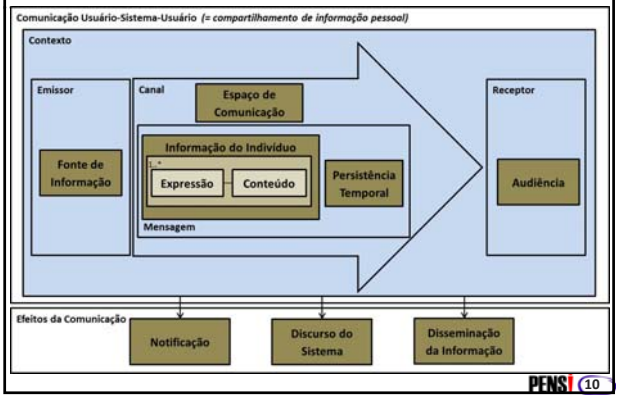
O MODELO DE DESIGN DE PRIVACIDADE (MDP)



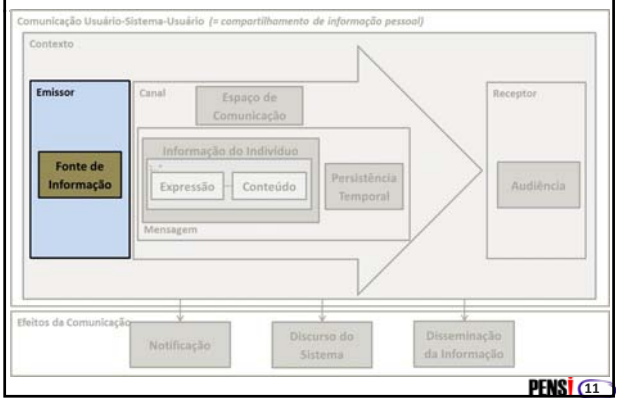
O MODELO DE DESIGN DE PRIVACIDADE (MDP)



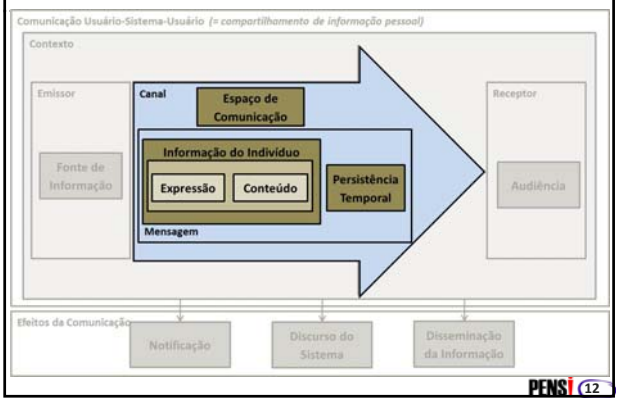
O MODELO DE DESIGN DE PRIVACIDADE (MDP)



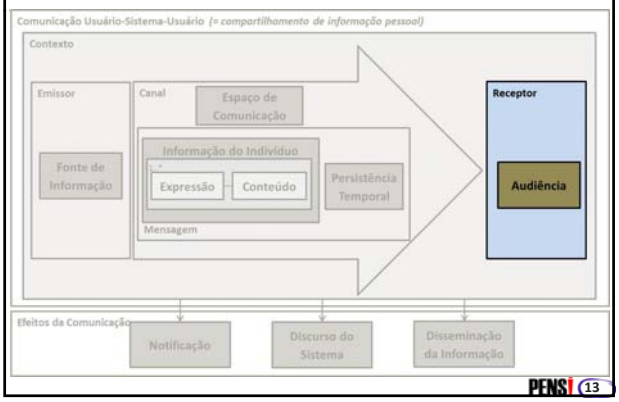
O MODELO DE DESIGN DE PRIVACIDADE (MDP)



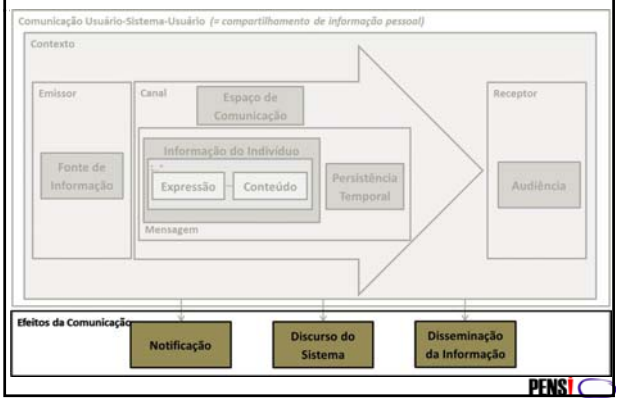
O MODELO DE DESIGN DE PRIVACIDADE (MDP)



O MODELO DE DESIGN DE PRIVACIDADE (MDP)



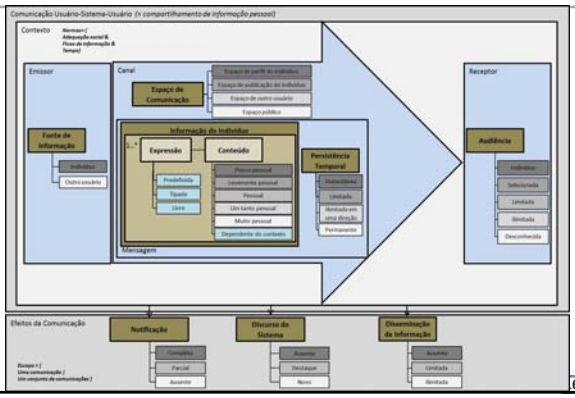
O MODELO DE DESIGN DE PRIVACIDADE (MDP)



O MODELO DE DESIGN DE PRIVACIDADE (MDP)

- **Dimensões de privacidade**
  - Pares **"atributo-valor"**
    - Representando **níveis distintos de privacidade**

O MODELO DE DESIGN DE PRIVACIDADE (MDP)



O MODELO DE DESIGN DE PRIVACIDADE (MDP)

- **Controle sobre as dimensões de privacidade**
  - Para cada uma das dimensões de privacidade, o designer deve **decidir**:
    - **Quem** define o seu valor?
      - O sistema
        - » Quando? Em tempo de design ou tem tempo de uso
      - O indivíduo ao qual a informação se refere – em tempo de uso
      - Outro usuário – em tempo de uso

O DESIGN DO COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS COM O MDP

1. Definir os **tipos de comunicação** que representam as oportunidades de compartilhamento de informação pessoal do indivíduo através do sistema
   - Exemplo CaringBridge

O DESIGN DO COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS COM O MDP

1. Definir os **tipos de com**
   representam as opo
   compartilhamento d
   indivíduo através do
   - Exemplo CaringBridge

RSO cujo foco é permitir que pessoas que estejam passando por problemas sérios de saúde obtenham apoio e encorajamento para lidarem com a situação

O DESIGN DO COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS COM O MDP

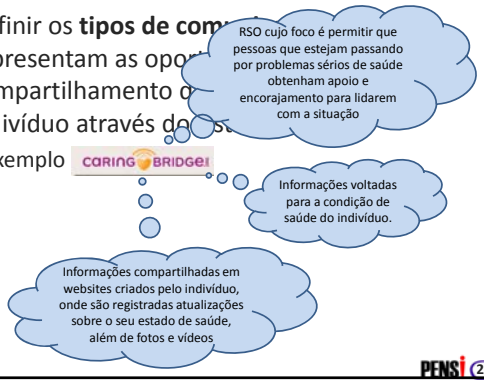
1. Definir os **tipos de com**
   representam as opo
   compartilhamento d
   indivíduo através do
   - Exemplo CaringBridge

RSO cujo foco é permitir que pessoas que estejam passando por problemas sérios de saúde obtenham apoio e encorajamento para lidarem com a situação

Informações voltadas para a condição de saúde do indivíduo.

O DESIGN DO COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS COM O MDP

1. Definir os **tipos de com** representam as opo compartilhamento d indivíduo através do s
   – Exemplo CARING BRIDGE!



O DESIGN DO COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS COM O MDP

1. Definir os **tipos de comunicação** que representam as oportunidades de compartilhamento de informação pessoal do indivíduo através do sistema
   – Exemplo CARING BRIDGE!
   - Tipos de comunicação:
     1. O indivíduo compartilhar informação em seu perfil;
     2. O indivíduo compartilhar informação em seu website;
     3. O indivíduo interagir com um website de outro usuário (visitar, assinar o "guestbook", aceitar uma tarefa, comentar ou curtir atualizações realizadas no mesmo).

O DESIGN DO COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS COM O MDP

2. Para cada um dos tipos de comunicação, **definir** como será o **valor** e o **controle** referente a cada uma das dimensões de privacidade
   – Qual é o **valor** da dimensão ou **intervalo de valores** que ela poderá assumir?
   – Quem é o responsável por definir o valor da dimensão, ou seja, de quem é o **controle**?
     - O **sistema** (em **tempo de design** - valor fixo no sistema ou no tipo de comunicação)
     - O **sistema** (em **tempo de uso**)
     - O **indivíduo** ao qual a informação se referente (em **tempo de uso**)
     - **Outro usuário** (em **tempo de uso**)

VISUALIZAÇÃO DOS NÍVEIS DE PRIVACIDADE

- Cada tipo de comunicação é representado como um "*honeycomb* ", com os hexágonos que o compõem representando as dimensões de privacidade.
  – Permitir que o designer visualize os níveis de privacidade através de gradações crescentes de cores associadas aos valores atribuídos às dimensões

VISUALIZAÇÃO DOS NÍVEIS DE PRIVACIDADE

- **Legenda para as cores de preenchimento dos hexágonos correspondentes aos valores das dimensões de privacidade do MDP**

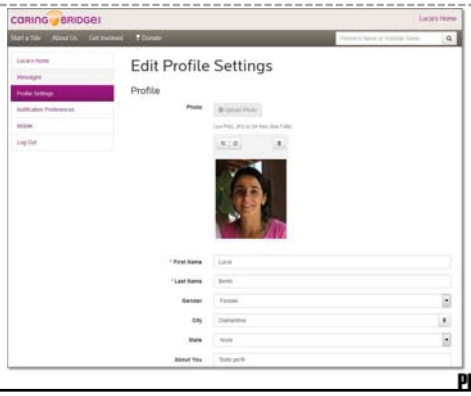
Cor/tonalidade	Nível de privacidade
	Alto
	Médio-alto
	Médio
	Médio-baixo
	Baixo
	Definido em tempo de uso
	Não aplicável

VISUALIZAÇÃO DOS NÍVEIS DE PRIVACIDADE

- **Legenda para o controle representado pelas bordas dos hexágonos correspondentes às dimensões de privacidade do MDP**

	Borda	Controle
Dimensão cujo valor é definido em tempo de design (nível de sistema ou de tipo de comunicação)		Sistema – valor fixo no sistema (valor definido em tempo de design)
		Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)
Dimensão cujo valor é definido em tempo de uso (nível de instância de comunicação)		Sistema (valor definido em tempo de uso)
		Outro usuário
		Indivíduo
		Definido em tempo de uso

EXEMPLO CARINGBRIDGE: "O indivíduo compartilhar informações sem seu perfil"



EXEMPLO RESEARCHGATE: "O indivíduo compartilhar informações sem seu perfil"

- **Fonte de informação**, nesse caso, é o próprio "*indivíduo*";
- **Espaço de comunicação** é o "*espaço de perfil do indivíduo*"
- **Expressão da informação** compartilhada, esta será sempre no formato "*tipada*"
  - *Assim,* o seu significado e, portanto, o seu nível de pessoalidade, é definido pelo sistema em tempo de design.
- **Conteúdo da informação** é "*um tanto pessoal*", (Villela et al., 2015)
  - Cidade, estado, frase sobre o indivíduo e websites que ele visita

EXEMPLO RESEARCHGATE: "O indivíduo compartilhar informações sem seu perfil"

- A **persistência temporal** dessas informações é *"permanente"*
  - Ficam acessíveis para a sua audiência durante todo o tempo de sua existência, ou seja, enquanto ela não for excluída pelo usuário

EXEMPLO RESEARCHGATE: "O indivíduo compartilhar informações sem seu perfil"

- A **audiência** para informação de perfil é controlada pelo próprio indivíduo
  - Pode escolher entre ter um perfil público ou privado
  - Remetendo aos valores *"limitada"* e *"indivíduo"*, para a dimensão **audiência** respectivamente .

EXEMPLO CARINGBRIDGE: "O indivíduo compartilhar informações sem seu perfil"

- A dimensão **notificação** é não aplicável
  - O CaringBridge não permite que outros usuários interajam sobre a informação que o indivíduo compartilha em seu perfil
    - Assim, **não existe a possiblidade de atribuição de um valor** para a dimensão **notificação**.

EXEMPLO CARINGBRIDGE: "O indivíduo compartilhar informações sem seu perfil"

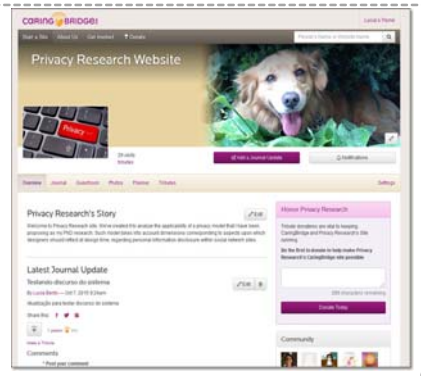
- Os valores para ambas as dimensões **discurso do sistema** e **disseminação da informação** é *"ausente"*.
  - O CaringBridge não faz nenhum discurso relacionado às informações que o indivíduo compartilha em seu perfil e nem permite que essas informações sejam disseminadas por outros usuários.

EXEMPLO CARINGBRIDGE: “O indivíduo compartilhar informações sem seu perfil”

Dimensão \ Atributo		Valor	Controle
Fonte de informação		*“Indivíduo”*	Sistema – valor definido em tempo de design
Espaço de comunicação		*“Espaço de perfil do indivíduo”*	Sistema – valor definido em tempo de design
Informação	**Expressão**	*“Tipada”*	Sistema – valor definido em tempo de design
	Conteúdo	*“Um tanto pessoal”*	Sistema – valor definido em tempo de design
Persistência temporal		*“Permanente”*	Sistema – valor definido em tempo de design
Audiência		*{“indivíduo”, “limitada”}*	Indivíduo
Notificação			Não aplicável
Discurso do sistema		*“Ausente”*	Sistema – valor definido em tempo de design
Disseminação da informação		*“Ausente”*	Sistema – valor definido em tempo de design

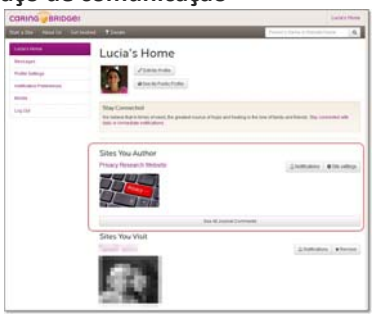
EXEMPLO CARINGBRIDGE: “O indivíduo compartilhar informações sem seu perfil”

EXEMPLO CARINGBRIDGE: “O indivíduo compartilhar suas informações em seu website”



EXEMPLO CARINGBRIDGE: “O indivíduo compartilhar suas informações em seu website”

- **Espaço de comunicação**



Perfil do indivíduo no CaringBridge

EXEMPLO CARINGBRIDGE: “O indivíduo compartilhar suas informações em seu website”

- **Expressão e Conteúdo da Informação**

Adicionando uma atualização de jornal - Website

EXEMPLO CARINGBRIDGE: “O indivíduo compartilhar suas informações em seu website”

- **Expressão e Conteúdo da Informação**

Adicionando uma foto - Website

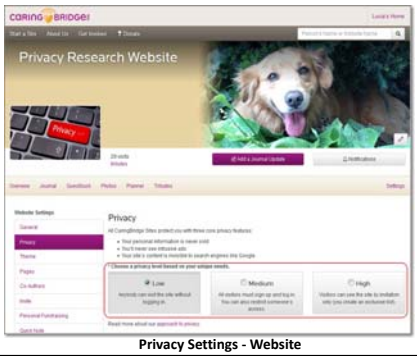
EXEMPLO CARINGBRIDGE: “O indivíduo compartilhar suas informações em seu website”

- **Expressão e Conteúdo da Informação**

Planejando uma tarefa - Website

EXEMPLO CARINGBRIDGE: “O indivíduo compartilhar suas informações em seu website”

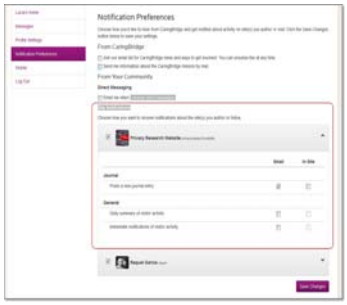
- **Audiência**



Privacy Settings - Website

EXEMPLO CARINGBRIDGE: “O indivíduo compartilhar suas informações em seu website”

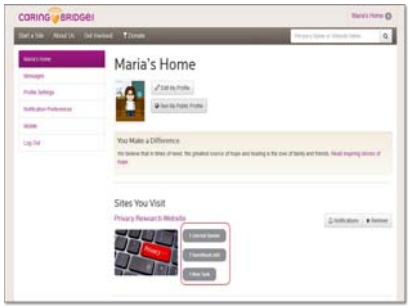
- **Notificação**



Preferências de Notificações para websites

EXEMPLO CARINGBRIDGE: “O indivíduo compartilhar suas informações em seu website”

- **Discurso do Sistema**

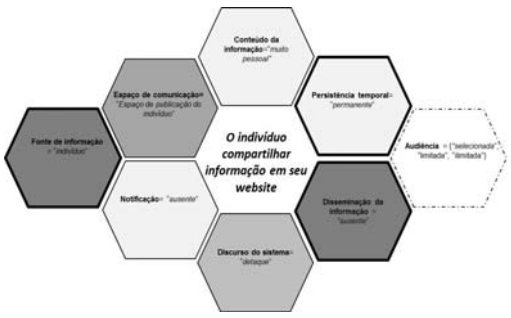


Discurso do sistema sobre atualizações realizadas em site que o usuário visita

EXEMPLO CARINGBRIDGE: “O indivíduo compartilhar suas informações em seu website”

Dimensão \ Atributo		Valor	Controle
Fonte de informação		*“Indivíduo”*	Sistema – valor definido em tempo de design
Espaço de comunicação		*“Espaço de publicação do indivíduo”*	Sistema – valor definido em tempo de design
Informação	**Expressão**	*“Tipada”*	Sistema – valor definido em tempo de design
	Conteúdo	*“Muito pessoal”*	Sistema – valor definido em tempo de design
Persistência temporal		*“Permanente”*	Sistema – valor definido em tempo de design
Audiência		*{“indivíduo”, “limitada”, “ilimitada”}*	Indivíduo
Notificação		*“Ausente”*	Sistema – valor definido em tempo de design
Discurso do sistema		*“Destaque”*	Sistema – valor definido em tempo de design
Disseminação da informação		*“Ausente”*	Sistema – valor definido em tempo de design

EXEMPLO CARINGBRIDGE: “O indivíduo compartilhar suas informações em seu website”



UFMG

Winweb

UFVJM

Obrigada!

CAPES

FAPEMIG

Maria Lúcia Bento Villela
mvillela@dcc.ufmg.br

Raquel Oliveira Prates
rprates@dcc.ufmg.br

Grupo de pesquisa:

PENSi Núcleo de Pesquisa em Engenharia Semiótica e Interação

http://pensi.dcc.ufmg.br

GLOSSÁRIO DO MODELO DE DESIGN DE PRIVACIDADE (MDP)

A explicação sobre as dimensões de privacidade do MDP, seus atributos e possíveis valores, bem como os níveis de privacidade associados a estes estão representados nas Tabelas 1, 2, 3 e 4, respectivamente.

Tabela 1. Descrição das dimensões de privacidade do MDP

Categoria	Dimensão		Explicação
Comunicação usuário-sistema-usuário	Fonte de Informação		Refere-se a quem é o responsável pelo compartilhamento de informações sobre o indivíduo dentro do sistema, ou seja, quem pode determinar como, quando e em que extensão tal informação será compartilhada.
	Espaço de Comunicação		Refere-se ao local onde a informação sobre o indivíduo será compartilhada no sistema.
	Informação do Indivíduo		Refere-se à informação sobre o indivíduo que será compartilhada no sistema. Esta dimensão é composta por uma ou mais estruturas de informação, que se subdividem nas -subdimensões "Expressão" e "Conteúdo", descritas nas próximas duas linhas.
	Estrutura da Informação	Expressão	Refere-se à forma como a informação compartilhada sobre o indivíduo é expressa dentro do sistema.
		Conteúdo	Refere-se ao nível de pessoalidade atribuído à informação sobre o indivíduo, que é compartilhada dentro do sistema.
	Persistência Temporal		Refere-se ao período de tempo em que a informação sobre o indivíduo fica disponível para a sua audiência dentro do sistema.
	Audiência		Refere-se quem terá acesso à informação sobre o indivíduo dentro do sistema.
Efeitos da Comunicação	Notificação		Diz respeito ao sistema informar adequadamente ao indivíduo quando informação sobre ele é divulgada ou acessada por outros usuários e de que forma.
	Discurso do Sistema		Está relacionada ao sistema informar outros usuários sobre a informação do indivíduo que está sendo compartilhada dentro do sistema.
	Disseminação da Informação		Está relacionada à audiência ser capaz de recompartilhar informação pessoal sobre o indivíduo com outros usuários dentro do sistema.

Tabela 2. Descrição dos atributos das dimensões de privacidade do MDP

Atributo	Descrição
Valor	Valor que a dimensão de privacidade pode assumir
Controle	Quem é o responsável por determinar o valor da dimensão e em que momento (tempo de design ou tempo de uso)

Tabela 3. Possíveis valores do atributo "controle" para todas as dimensões de privacidade do MDP

Possíveis valores para o atributo "controle"	Descrição
Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	O valor da dimensão é definido pelo designer, em tempo de design, e o valor é fixo no nível de tipo de comunicação (ou seja, o valor da dimensão será o mesmo para todas as instâncias do tipo de comunicação).
Sistema (valor definido em tempo de uso)	O valor da dimensão é definido pelo designer, mas em tempo de uso, tendo em vista que depende do valor de alguma outra dimensão ou de outro aspecto relacionado ao compartilhamento.
Outro usuário	Outro usuário é responsável por definir o valor da dimensão de privacidade, em tempo de uso.
Indivíduo	O indivíduo é responsável por definir o valor da dimensão de privacidade, em tempo de uso.
Definido em tempo de uso	Quem será o responsável por definir o valor da dimensão de privacidade será definido em tempo de uso, dependendo do valor de alguma outra dimensão ou de outro aspecto relacionado ao compartilhamento.

Tabela 4. Possíveis valores do atributo "valor" para as dimensões de privacidade do MDP e seus níveis de privacidade associados

Dimensão		Possíveis valores para o atributo "valor"	Descrição	Nível de Privacidade
Fonte de Informação		*Indivíduo*	O próprio indivíduo compartilha informações sobre ele no sistema, seja explicitamente ou através de suas ações.	Alto
		Outro usuário	Outro usuário compartilha informações pessoais do indivíduo dentro do sistema.	Baixo
Espaço de Comunicação		*Espaço de perfil do indivíduo*	Espaço onde são compartilhadas informações mais estáticas, como aquelas biográficas e descritivas relacionadas a elementos de identidade do indivíduo dentro do sistema, como, por exemplo, nome, data de nascimento, endereço, etc.	Alto
		Espaço de publicação do indivíduo	Espaço controlado pelo indivíduo destinado a compartilhar informações que são mais dinâmicas, que refletem situações ou objetos que podem ser sofrer frequentes atualizações, e sobre as quais outros usuários podem interagir.	Alto
		Espaço de outro usuário	Espaço pertencente a outro usuário.	Médio-baixo
		Espaço público	Espaço público, que não pertence a nenhum usuário e pode ser acessado amplamente por todos os usuários do sistema.	Baixo
Informação do Indivíduo	Expressão	*Predefinida*	Mensagem pré-definidas pelo sistema em que os usuários apenas decidem se desejam enviá-las ou não (ex.: curtir ou confirmar a presença e um evento, no Facebook).	Não aplicável
		Tipada	Mensagem cujo significado é definido pelo sistema, mas cujo valor é definido pelo usuário (ex.: nome e data de nascimento, no Facebook).	
		Livre	Mensagem cujo significado da informação é definido pelo seu conteúdo (ex.:comentário no Facebook pode ser usado para dizer algo positivo, negativo ou mesmo algo que não está relacionado ao que o comentário se refere) .	
	Conteúdo	*Pouco pessoal*	Informação pouco pessoal, de acordo com classificação realizada por usuários em Villela et al. (2015), como local onde o indivíduo trabalha ou estuda.	Alto
		Levemente pessoal	Informação levemente pessoal, de acordo com classificação realizada por usuários em Villela et al. (2015), como opiniões políticas, lugares visitados, estado de relacionamento e conquistas pessoais do indivíduo.	Médio-alto
		Pessoal	Informação pessoal, de acordo com classificação realizada por usuários em Villela et al. (2015), como emoções positivas, aniversário e religião/crenças do indivíduo.	Médio
		Um tanto pessoal	Informação um tanto pessoal, de acordo com classificação realizada por usuários em Villela et al. (2015), como fotos de família, endereço de e-mail, fotos e emoções negativas do indivíduo.	Médio-baixo
		Muito pessoal	Informação muito pessoal, de acordo com classificação realizada por usuários em Villela et al. (2015), como problemas de relacionamento, endereço e telefone e informações relacionadas ao estado e saúde do indivíduo.	Baixo

Dimensão	Possíveis valores para o atributo "valor"	Descrição	Nível de Privacidade
Persistência Temporal	*Instantânea*	Informação pessoal do indivíduo é disponibilizada no sistema apenas por um período muito curto de tempo (tipicamente em tempo real, apenas para os usuários que estão logados no sistema no momento em que a informação é compartilhada)	Alto
	Limitada	Informação pessoal do indivíduo é disponibilizada no sistema por um período limitado de tempo (geralmente curto).	Médio-alto
	Ilimitada em uma direção	Informação pessoal do indivíduo é disponibilizada no sistema por um período ilimitado de tempo, iniciando a partir do presente em direção ao passado ou ao futuro. Considerando como presente o momento em que o usuário torna-se parte da audiência da informação, este valor indica que o usuário tem acesso a toda informação compartilhada com a audiência da qual ele faz parte (em qualquer momento anterior ao momento presente) ou o usuário tem acesso apenas às informações compartilhadas com a audiência da qual ele faz parte a partir do momento em que ele começa a fazer parte da mesma (exemplo: grupos no WhatsApp).	Médio-baixo
	Permanente	Uma vez que a informação é compartilhada no sistema, ela será sempre acessível para a sua audiência.	Baixo
Audiência	*Indivíduo*	Apenas o próprio indivíduo possui acesso à informação, indicando um nível máximo de privacidade, por um lado, mas, por outro lado, um nível mínimo de interação, dado que ninguém, além do indivíduo, terá acesso à informação.	Alto
	Selecionada	O usuário decide quem serão os usuários que farão parte do grupo que irá formar a audiência da informação.	Médio-alto
	Limitada	Abrange todo o conjunto de usuários do sistema.	Médio
	Ilimitada	Abrange todos os usuários do sistema e até mesmo que não é usuário do mesmo.	Médio-baixo
	Desconhecida	O indivíduo não sabe quem fará parte da audiência de sua informação.	Baixo
Notificação	*Completa*	O sistema sempre notifica o indivíduo quando outros usuários interagem de alguma forma com a sua informação, como, por exemplo, no Facebook, quando outros usuários curtem, comentam ou compartilham a mesma.	Alto
	Parcial	O sistema notifica o indivíduo apenas sobre uma parte das interações de outros usuários com a sua informação.	Médio
	Ausente	O sistema não fornece ao indivíduo nenhuma notificação sobre a interação de outros usuários com a sua informação.	Baixo
Discurso do Sistema	*Ausente*	Sistema não gera nenhuma comunicação sobre o compartilhamento de uma informação do indivíduo.	Alto
	Destaque	Sistema apresenta informação do indivíduo a outros usuários à qual estes já possuem acesso, porém dá destaque à mesma.	Médio
	Novo	Sistema processa informação do indivíduo, gerando informação nova sobre o mesmo.	Baixo

Dimensão	Possíveis valores para o atributo "valor"	Descrição	Nível de Privaci-dade
Dissemina-ção da In-formação	*Ausente*	Não é permitida à audiência da informação do indivíduo recompartilhá-la com outras pessoas.	Alto
	Limitada	Informação sobre o indivíduo pode ser compartilhada por sua audiência, porém de uma maneira restrita, apenas para uma audiência adicional limitada.	Médio
	Ilimitada	Informação sobre o indivíduo pode ser compartilhada pela sua audiência, sem nenhuma restrição.	Baixo

Avaliação do uso do MDP

Nome do participante: _____ Identificação: _____

Agora que você foi apresentado aos conceitos básicos do Modelo de Design de Privacidade (MDP), você irá utilizá-lo como ferramenta de análise dos aspectos de privacidade relacionados ao compartilhamento de informações pessoais em RSOs. Para guia-lo nesta tarefa, considere o seguinte cenário:

CENÁRIO

Você está trabalhando em uma equipe que está fazendo a modelagem do compartilhamento de informação pessoal no Facebook, de acordo com as dimensões de privacidade do MDP, a fim de identificar aspectos que possam despertar questões de privacidade. Assim, já foram identificadas as oportunidades de compartilhamento de informação pessoal no sistema, às quais chamamos de "tipo de comunicação" no Facebook, como, por exemplo, o indivíduo compartilhar informação sobre si mesmo em seu perfil ou sua linha do tempo, ou outro usuário compartilhar informação sobre o indivíduo em sua linha do tempo.

Você deverá realizar as tarefas descritas nas páginas seguintes.

Tarefa 1

A sua primeira tarefa é modelar um dos tipos de comunicação do Facebook:

- *"O indivíduo compartilhar informação sobre si mesmo em sua linha do tempo"*

Para isso, utilize as dimensões de privacidade do MDP[1], preenchendo a Tabela 1, abaixo.

Tabela 1. Modelagem do tipo de comunicação do Facebook:
"O indivíduo compartilhar informação sobre si mesmo em sua linha do tempo"

Atributo / Dimensão		Valor*	Controle
Fonte de informação			
Espaço de comunicação			
Informação	**Expressão**		
	Conteúdo		
Persistência temporal			
Audiência			
Notificação			
Discurso do sistema			
Disseminação da informação			

* coloque os valores que a dimensão poderá assumir entre chaves, caso a dimensão tenha seu valor definido em tempo de uso, levando em consideração os valores limites em relação ao nível de privacidade (ou seja, os valores referentes ao maior e ao menor nível de privacidade possível para dimensão)

Você terá aproximadamente 45 minutos para realizar esta tarefa.

[1] No glossário do MDP, que foi entregue a você junto com este cenário, você encontra a explicação sobre as dimensões de privacidade, seus atributos e possíveis valores, bem como os níveis de privacidade associados a cada um destes.

Tarefa 2

Agora você deverá fazer uma dupla com outro participante e comparar os modelos criados por vocês, na tarefa anterior, referentes ao tipo de comunicação do Facebook: “O indivíduo compartilhar informação sobre si mesmo em sua linha do tempo”. Realize então as seguintes tarefas:

a) Caso tenha havido quaisquer diferenças na modelagem, registre-as nas tabelas que lhes serão entregue separadamente.

b) Para cada uma dessas diferenças, vejam se conseguem chegar a um consenso e também registre-o nas tabelas que lhes foram entregues.

c) A partir da discussão que tiveram, crie uma nova modelagem, agora utilizando a ferramenta de visualização do MDP, que pode ser acessada a partir do seguinte link:

http://homepages.dcc.ufmg.br/~lidiaferreira/mdp_beta/modeling_privacy/

Como essa ferramenta não permite que você coloque um intervalo de valores para as **dimensões cujo valor é definido em tempo uso**, você deverá criar duas **visualizações** para esta modelagem, uma considerando os valores referentes aos **níveis máximos de privacidade** e outra considerando os valores referentes aos **níveis mínimos de privacidade**. Nessas novas visualizações, **registre as dimensões (atribuindo valores e/ou controles pra as mesmas) para as quais houve consenso** (antes ou depois da discussão). Caso não cheguem a um consenso sobre uma ou mais dimensões, deixe o seu valor e/ou controle correspondente em branco.

- **Visualização dos níveis máximos de privacidade** - criar uma visualização considerando os valores referentes aos **níveis máximos de privacidade** que cada uma dessas dimensões pode assumir em tempo de uso

    i. Na caixa “Nome da Comunicação”, digitar o texto “[IniciaisDupla] – Máximo”;

    ii. Após concluir a visualização, efetuar a captura de tela da mesma e salvar em arquivo com o nome “[IniciaisDupla] – Maximo.jpg”

- **Visualização dos níveis mínimos de privacidade** - clicar sobre o botão “Novo” e então criar outra visualização considerando os valores referentes aos **níveis mínimos de privacidade** que cada uma dessas dimensões pode assumir em tempo de uso.

    i. Na caixa “Nome da Comunicação”, digitar o texto “[IniciaisDupla] – Mínimo”;

    ii. Após concluir a visualização, efetuar a captura de tela da mesma e salvar em arquivo com o nome “[IniciaisDupla] – Minimo.jpg”

Vocês terão aproximadamente 45 minutos para fazer isso.

Tarefa 3

Serão apresentadas as modelagens de dois tipos de comunicação referentes ao compartilhamento de informações pessoais em duas RSOs distintas, de acordo com as dimensões do MDP. Mantendo a mesma dupla composta para a execução da tarefa anterior, discutam e registrem, por escrito, nas folhas que lhes serão entregue separadamente, as diferenças de privacidade que conseguem perceber a partir dessas modelagens, e suas implicações na privacidade do sistema como um todo.

Vocês terão aproximadamente 20 minutos para realizar esta tarefa.

Tarefa 4

Das duas RSOs mostradas na tarefa 3, uma é de propósito geral e a outra é profissional. Vocês conseguiriam identificar qual delas é a de propósito geral e qual delas é a profissional? Justifique (registrem sua resposta na folha que lhe serão entregue separadamente).

Vocês terão aproximadamente 10 minutos para realizar esta tarefa.

TAREFA 3

Modelos de Privacidade da Rede Social Online 1

Tipo de comunicação 1: O indivíduo compartilhar informação em seu perfil

Atributo / Dimensão		Controle	Valor*
Fonte de informação		Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	*"Indivíduo"*
Espaço de comunicação		Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	*"Espaço de perfil do indivíduo"*
Informação do indivíduo	**Expressão**	Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	"*tipada"*
	Conteúdo	Sistema (valor definido em tempo de uso)	{"*pouco pessoal", "levemente pessoal", "pessoal", "um tanto pessoal", "muito pessoal"*}
Persistência temporal		Sistema – valor fixo no sistema (valor definido em tempo de design)	*"Permanente"*
Audiência		Definido em tempo de uso	"*ilimitada"* ou {"*indivíduo", "selecionada", "limitada", ilimitada"*}
Notificação		Sistema – valor fixo no sistema (valor definido em tempo de design)	*"Completa"*
Discurso do sistema		Sistema – valor fixo no sistema (valor definido em tempo de design)	*"Destaque"*
Disseminação da informação		Sistema (valor definido em tempo de uso)	{"*ausente", "ilimitada"}*

*Quando os valores aparecem entre chaves, indica-se que a dimensão terá seu valor definido em tempo de uso, podendo assumir qualquer um desses.

Tipo de comunicação 2: O indivíduo compartilhar informação em seu espaço

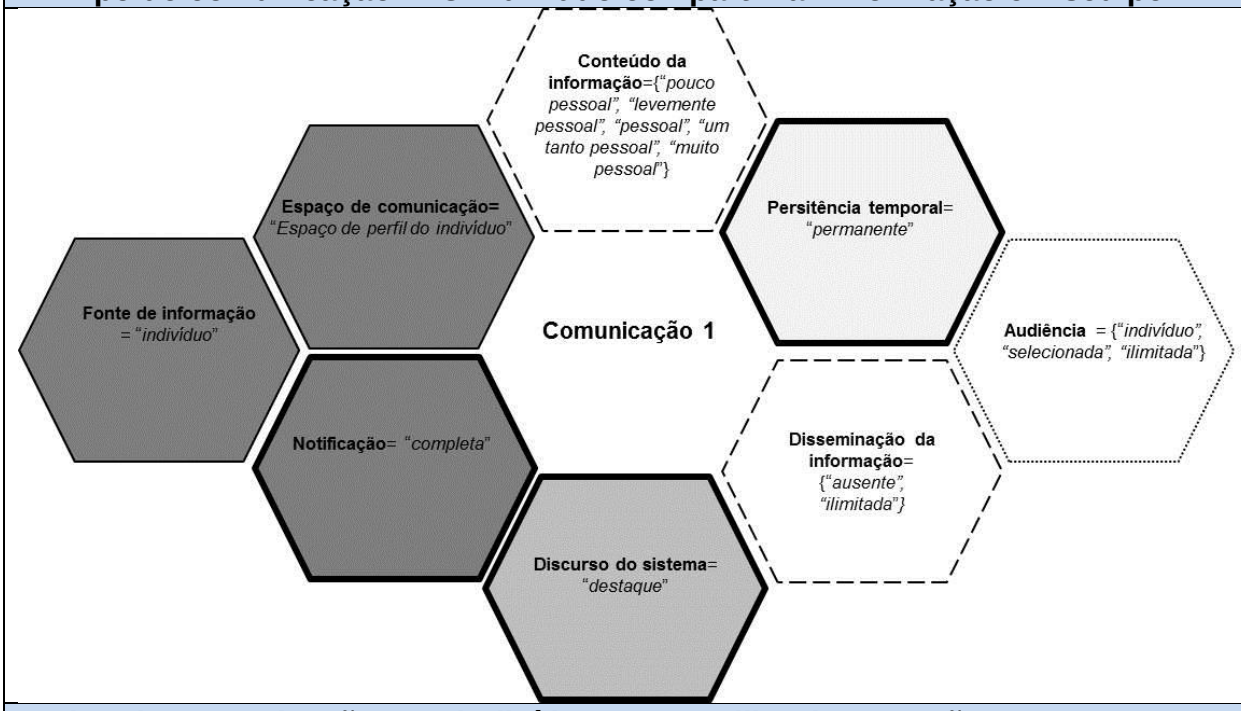
Dimensão \ Atributo		Controle	Valor*
Fonte de informação		Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	*"Indivíduo"*
Espaço de comunicação		Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	*"Espaço de publicação do indivíduo"*
Informação do indivíduo	**Expressão**	Indivíduo	{"*tipada", "livre"*}
	Conteúdo	Definido em tempo de uso	{"*pouco pessoal", "levemente pessoal", "pessoal", "um tanto pessoal", "muito pessoal"*}
Persistência temporal		Sistema – valor fixo no sistema (valor definido em tempo de design)	*"Permanente"*
Audiência		Indivíduo	{"*indivíduo", "selecionada", "limitada", ilimitada"*}
Notificação		Sistema – valor fixo no sistema (valor definido em tempo de design)	*"Completa"*
Discurso do sistema		Sistema – valor fixo no sistema (valor definido em tempo de design)	*"Destaque"*
Disseminação da informação		Definido em tempo de uso	{"*ausente", "limitada", "ilimitada"*}

*Quando os valores aparecem entre chaves, indica-se que a dimensão terá seu valor definido em tempo de uso, podendo assumir qualquer um desses.

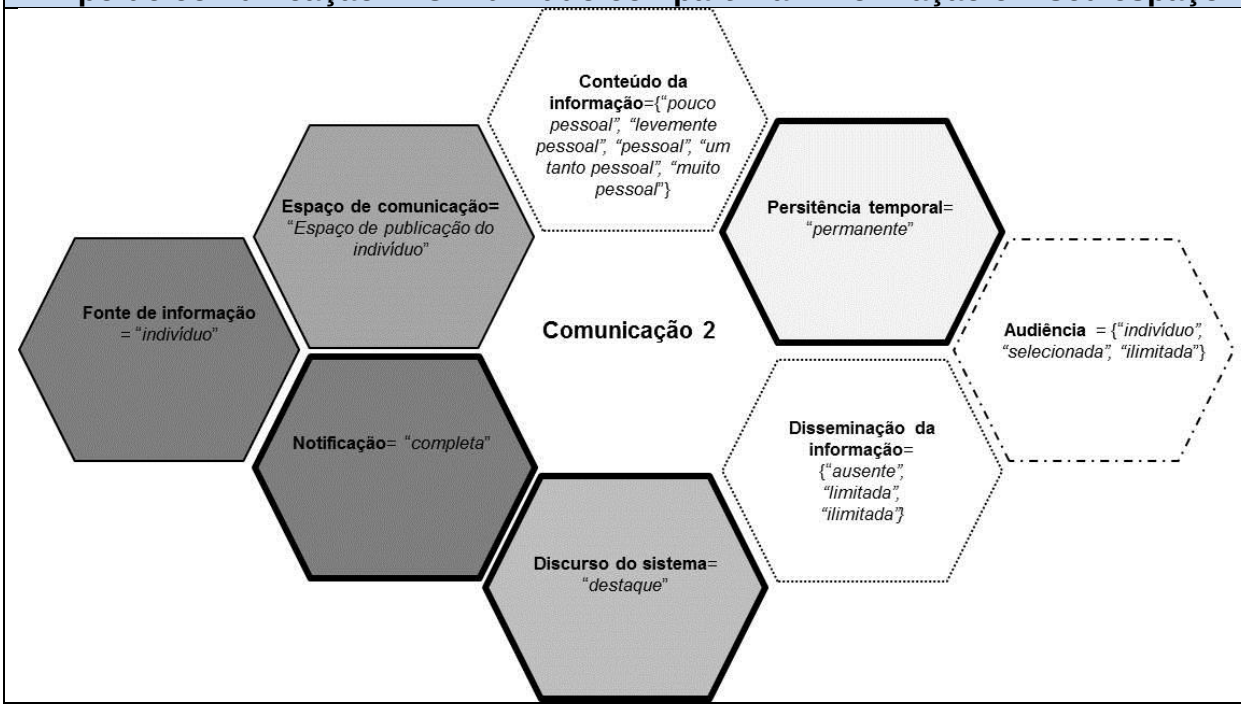
TAREFA 3

Modelos de Privacidade da Rede Social Online 1

Tipo de comunicação 1: O indivíduo compartilhar informação em seu perfil



Tipo de comunicação 2: O indivíduo compartilhar informação em seu espaço



TAREFA 3

Modelos de Privacidade da Rede Social Online 2

Tipo de comunicação 1: O indivíduo compartilhar informação em seu perfil

Atributo / Dimensão		Controle	Valor*
Fonte de informação		Sistema – valor fixo no sistema (valor definido em tempo de design)	*"Indivíduo"*
Espaço de comunicação		Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	*"Espaço de perfil do indivíduo"*
Informação do indivíduo	**Expressão**	Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	"*tipada"*
	Conteúdo	Sistema (valor definido em tempo de uso)	{"*pouco pessoal", "levemente pessoal", "muito pessoal"*}
Persistência temporal		Sistema – valor fixo no sistema (valor definido em tempo de design)	*"Permanente"*
Audiência		Definido em tempo de uso	{*"selecionada", "limitada", ilimitada"*}
Notificação		Na**	*Na*
Discurso do sistema		Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	*"Ausente"*
Disseminação da informação		Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	*"Ausente"*

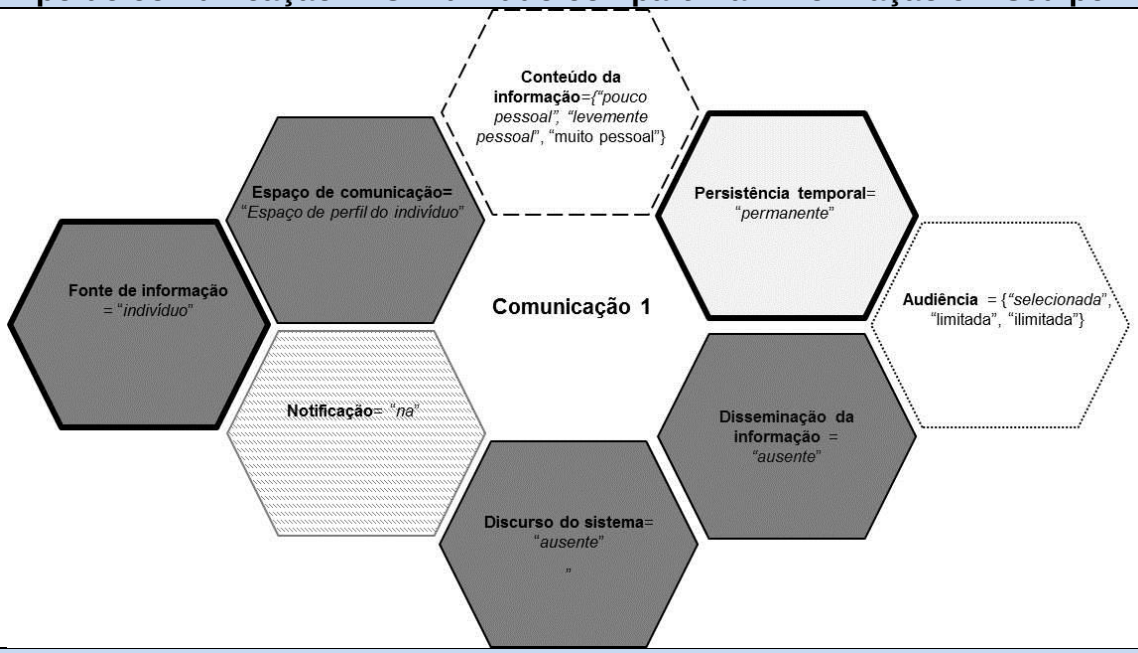
*Quando os valores aparecem entre chaves, indica-se que a dimensão terá seu valor definido em tempo de uso, podendo assumir qualquer um desses.
** Não aplicável.

Tipo de comunicação 2: O indivíduo compartilhar informação em seu espaço			
Dimensão / **Atributo**		**Controle**	**Valor**
Fonte de informação		Sistema – valor fixo no sistema (valor definido em tempo de design)	*"Indivíduo"*
Espaço de comunicação		Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	*"Espaço de publicação do indivíduo" e "Espaço público"*
Informação do indivíduo	**Expressão**	Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	"*tipada"*
	Conteúdo	Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	"*Pouco pessoal"*
Persistência temporal		Sistema – valor fixo no sistema (valor definido em tempo de design)	*"Permanente"*
Audiência		Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	"*ilimitada"*
Notificação		Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	*"parcial"*
Discurso do sistema		Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	*"Destaque"*
Disseminação da informação		Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)	*"ilimitada"*

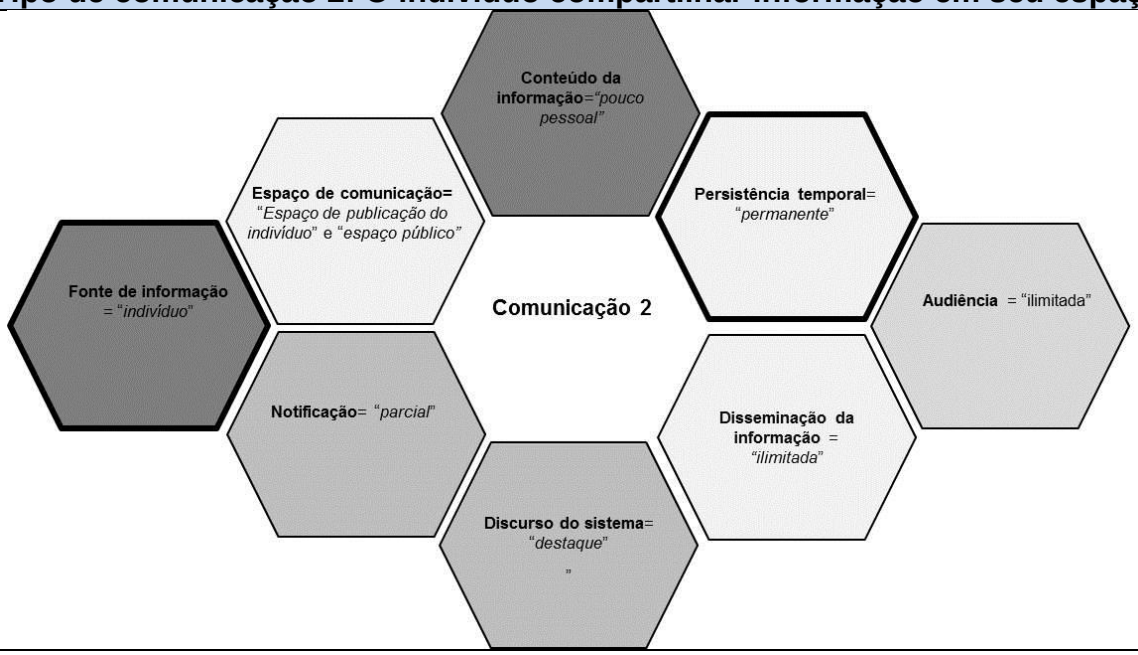
TAREFA 3

Modelos de Privacidade da Rede Social Online 2

Tipo de comunicação 1: O indivíduo compartilhar informação em seu perfil



Tipo de comunicação 2: O indivíduo compartilhar informação em seu espaço



Legenda:

Controle (representado pelas bordas do hexágono):


Sistema – valor fixo no sistema (valor definido em tempo de design)


Sistema – valor fixo no tipo de comunicação (valor definido em tempo de design)


Sistema (valor definido em tempo de uso)


Outro usuário (valor definido em tempo de uso)


Indivíduo (valor definido em tempo de uso)


Definido em tempo de uso


Não aplicável

Valor (representado pelo preenchimento do hexágono):


Nível alto de privacidade


Nível médio-alto de privacidade


Nível médio de privacidade


Nível médio-baixo de privacidade


Nível baixo de privacidade


Definido em tempo de uso


Não aplicável

ROTEIRO DO GRUPO FOCAL

Blocos	Principais Itens
I. Compreensão dos participantes sobre cada uma das dimensões, seu controle e os valores que as mesmas podem assumir	1. Falar sobre a facilidade/dificuldade em: a. Compreender as dimensões de privacidade (fazer a pergunta genérica, mas, para ajudar o respondente, em seguida passar por cada dimensão, verificando se alguma gera mais dificuldade que as outras. b. Compreender o controle sobre as dimensões (mesmo comentário acima). c. Compreender os possíveis valores das dimensões (mesmo comentário acima) 2. Você teve dificuldade em definir controle e valores para as dimensões, devido a outros fatores que não sejam a compreensão das dimensões, controle e valores que as mesmas podem assumir. Que fatores são esses? 3. O material de apoio o ajudou?
II. Explorar o uso do MDP na modelagem do compartilhamento de informações pessoais em RSOs	4. Quais os pontos positivos de fazer a análise usando o MDP? 5. Quais os pontos negativos de fazer a análise usando o MDP?
III. Potencial do uso do MDP despertar reflexões nos participantes sobre aspectos de privacidade envolvidos no compartilhamento de informações pessoais em RSOs	6. O uso do MDP o fez pensar em aspectos de privacidade envolvidos no compartilhamento de informações pessoais sobre os quais você não havia pensando antes? a. Em caso positivo, que aspectos são esses?
IV. A visualização como suporte ao uso do MDP	7. Você achou que a visualização foi útil para registrar a modelagem consolidada da dupla? Por que?
	8. Na hora de analisar as modelagens dos dois sistemas, na tarefa 3, o que você usou: a visualização ou as tabelas ou ambos? Por que ou Para que?
	a. Se preferir tabela, a visualização o ajudou ou não? Como? b. A visão geral ou cada dimensão?
	9. Você acha que a ferramenta utilizada foi uma boa forma de gerar a visualização?
V. Impressões sobre o MDP	10. Aqui só foi explorado o uso do MDP na análise de RSOs, mas a proposta é que ele seja usado no design para ajudar o designer a tomar decisões sobre privacidade enquanto está projetando o sistema. Neste cenário, você acha que o MDP seria uma ferramenta útil ou não? b. Explorar os benefícios e desafios.