PryMeVis: Uma ferramenta para Modelagem de Design de Privacidade

Maria Lúcia Bento Villela[1,2], Lidia Silva Ferreira[1], Diego Augusto de Faria Barros[1], Raquel Oliveira Prates[1], Raquel Cardoso de Melo Minardi[1]

[1] DCC – ICEx, Universidade Federal de Minas Gerais, Belo Horizonte – MG, Brasil

[2]DECOM – FACET, UFVJM, Diamantina – MG, Brasil

{mvillela, lidiaferreira, diego.barros, rprates, raquelcm}@dcc.ufmg.br

Abstract. *The Privacy Design Model (PDM) is a descriptive model that aims at helping designers to model personal information disclosure in Social Network Sites (SNSs). This model takes into account different aspects that influence the level of privacy being offered to users. In this paper we propose PryMeVis - an online tool that allows the creation of visual representations for the models of personal information disclosure in SNSs created using PDM. A preliminary evaluation was conducted and presented, and the results indicate that it can be an important tool to support designers in using PDM to model privacy in SNSs.*

Resumo. *O Modelo de Design de Privacidade (MDP) é um modelo descritivo que tem o propósito de ajudar designers a modelarem o compartilhamento de informações pessoais em Redes Sociais Online (RSOs), considerando diferentes aspectos que influenciam o nível de privacidade a ser oferecido ao usuário. Neste artigo, propomos a PryMeVis - uma ferramenta online que permite a criação de visualizações correspondentes aos modelos de compartilhamento de informações pessoais em RSOs, criados com o uso do MDP. Além disso, apresentamos também uma avaliação preliminar de tal ferramenta, com os resultados indicando que a mesma pode ser importante para apoiar designers no uso do MDP para a modelagem de privacidade em RSOs.*

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, através das Redes Sociais Online (RSOs). 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.

Com isso, estudos que buscam fornecer um melhor entendimento sobre a relação entre privacidade e RSOs têm sido conduzidos. Também foi identificada a necessidade de ferramentas para apoiarem designers na tomada de decisões sobre aspectos de privacidade

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

que devem ser considerados nesses sistemas. Nesse sentido, [Villela and Prates 2015] propôs o Modelo de Design de Privacidade (MDP), que consiste em uma ferramenta epistêmica[2] 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.

Existe porém, um número considerável de decisões a serem tomadas durante o design do compartilhamento de informações pessoais em uma RSO usando o MDP. Além disso, uma vez que o designer toma todas as decisões necessárias, pode ser difícil ter uma visão geral dos possíveis estados de privacidade definidos como consequência de suas decisões. A fim de facilitar a visão geral das decisões do designer ao fazerem uso do MDP, bem como dos possíveis estados de privacidade resultantes, [Villela 2016] propôs uma representação visual para o modelo. Assim, o objetivo deste trabalho é apresentar a ferramenta PryMeVis (acrônimo para *PRivacY design model Visualization*), que se propõe a apoiar o uso do MDP, ao fazer uso da sua representação visual para a confecção de modelos de compartilhamento de informações pessoais em RSOs. Além disso, com o objetivo de verificar o valor e a utilidade dessa representação visual, a mesma foi avaliada, juntamente com a versão inicial da ferramenta PryMeVis, com designers de sistemas, que consistem em seus potenciais usuários. Foi verificado, a partir dessas avaliações, que o uso da ferramenta de visualização PryMeVis enriquece a experiência de designers de RSOs, ao projetarem o compartilhamento de informações pessoais nesses sistemas e visualizarem o impacto de suas decisões na privacidade dos usuários.

Na próxima seção, apresentamos os trabalhos relacionados a este estudo. Na seção 3, são apresentados o Modelo de Design de Privacidade (MDP), suas dimensões e sua representação visual. Na seção 4, apresentamos a ferramenta PryMeVis, seguida de uma avaliação preliminar da representação visual do MDP e da primeira versão da ferramenta, na Seção 5. Por fim, na Seção 6, são apresentadas as considerações finais deste trabalho, bem como os trabalhos futuros que podem ser explorados a partir do mesmo.

2. Trabalhos Relacionados

A maior parte das pesquisas sobre privacidade em RSOs consiste em estudos empíricos e tem se dedicado principalmente à compreensão de diferentes aspectos relacionados à privacidade no compartilhamento de informação pessoal nesses ambientes [Stutzman and Hartzog 2012, Bevan et al. 2015]. Por outro lado, poucos estudos têm contribuído com modelos teóricos ou conceituais para tratar privacidade no design de tecnologias online [Belanger and Crossler 2011]. Nesse sentido, algumas ferramentas conceituais têm sido propostas com a finalidade de aumentar a flexibilidade que RSOs oferecem ao seus usuários, a fim de lidarem com aspectos específicos de privacidade [Pang and Zhang 2015, Tierney and Subramanian 2014], como o controle de acesso e o gerenciamento de compartilhamento .

Com o objetivo de apoiar designers em suas decisões sobre aspectos de privaci-

[2]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].

dade a serem considerados no design de RSOs, modelos conceituais são propostos, como o de [Romero et al. 2013] e o de [Epstein et al. 2015]. O primeiro consiste em um modelo que visa apoiar o design de mecanismos que permitem ao indivíduo coordenar sua privacidade enquanto comunica com outro usuário em um canal exclusivo, em RSOs, considerando especificamente sua disponibilidade para comunicação. O segundo consiste em um *framework* voltado para o projeto e avaliação de aspectos relacionados ao compartilhamento de dados capturados automaticamente nesses sistemas, com foco específico nas respostas e reações da audiência à informação compartilhada. Esses modelos se assemelham à proposta do MDP, no sentido de apoiar as decisões do designer sobre como projetar aspectos específicos do sistema, considerando a privacidade dos seus usuários. No entanto, os focos desses modelos, além de serem distintos entre si, são distintos do foco do MDP, que se propõe a apoiar designers a refletirem sobre diferentes aspectos relacionados ao compartilhamento de informações pessoais em RSOs, considerando o impacto de suas decisões nos níveis de privacidade oferecidos aos usuários pelo sistema.

Um ponto que merece ser destacado é que esses modelos conceituais para o apoio do design de privacidade não oferecem quaisquer tipos de ferramentas que ajudem na sua utilização por parte de designers, possibilitando a visualização dos modelos de design criados. As ferramentas de visualização existentes, relacionadas a privacidade em RSOs, são voltadas basicamente para o usuário final, com o intuito de permiti-lo gerenciar a sua privacidade ou aumentar a sua consciência sobre a sua exposição nesses sistemas. Contribuindo para o gerenciamento de privacidade por parte do usuário final, [Gao and Berendt 2013] apresenta uma ferramenta que possibilita aos usuários manusearem de forma eficiente os seus círculos de amizade, ao permiti-los colocar seus contatos em grupos, a fim de gerenciar o que será compartilhado com os mesmos. [Paul et al. 2012], por sua vez, desenvolveram uma interface melhorada para as configurações de privacidade do Facebook, possuindo como principal recurso a aplicação de um código de cores para grupos diferentes de audiências, com o objetivo de melhorar o acesso e a usabilidade oferecida. Visando aumentar a consciência sobre a exposição dos usuários em RSOs, [Mazzia et al. 2012] apresentam uma ferramenta que permite ao usuário entender a visibilidade de seu perfil nesses sistemas. Também dentro desta categoria estão as ferramentas que simulam efeitos de configuração, possibilitando ao usuários prever as consequências de suas escolhas [Pereira Junior et al. 2014, Malandrino et al. 2013]. Nessa mesma linha, [Schlegel et al. 2011] propuseram e avaliaram um mecanismo intuitivo para sumarizar e controlar a exposição de usuários em plataformas móveis. Por fim, [Wang et al. 2015] apresentam uma ferramenta de visualização interativa que ajuda os usuários a compreenderem e explorarem seus próprios traços de personalidade, derivados de seus dados de mídia social, e configurarem suas preferências de privacidade.

Como podemos perceber, embora tais ferramentas consistam em propostas para o tratamento de aspectos específicos de privacidade na interface de RSOs, seus focos são distintos do que estamos propondo nesta pesquisa, um vez que elas são voltadas para o usuário final e não para o designer, no sentido de ajudá-lo a tomar decisões, em tempo de design, sobre como tratar questões de privacidade na interface desses sistemas.

3. Modelo de Privacidade para Design (MDP)

O MDP [Villela and Prates 2015, Villela 2016] é um modelo descritivo que considera o compartilhamento de informações pessoais em RSOs como uma comunicação entre usuá-

rios mediada pelo sistema. Tal comunicação pode ocorrer tanto na forma direta (quando o próprio indivíduo[3] 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 [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. Assim, o compartilhamento de informações em interações envolvendo duas ou mais pessoas que se comunicam exclusivamente entre si, em um canal exclusivo, não é tratado pelo MDP.

O MDP é estruturado por meio de *dimensões de privacidade* que descrevem diferentes aspectos relacionados à privacidade no compartilhamento de informações pessoais em RSOs, conforme mostrado na Figura 1. Esses são aspectos sobre os quais o designer deve pensar, e que podem impactar o estado de privacidade dos usuários de RSOs. Para cada uma dessas dimensões, um conjunto de possíveis valores é definido, remetendo a níveis distintos de privacidade para o indivíduo.

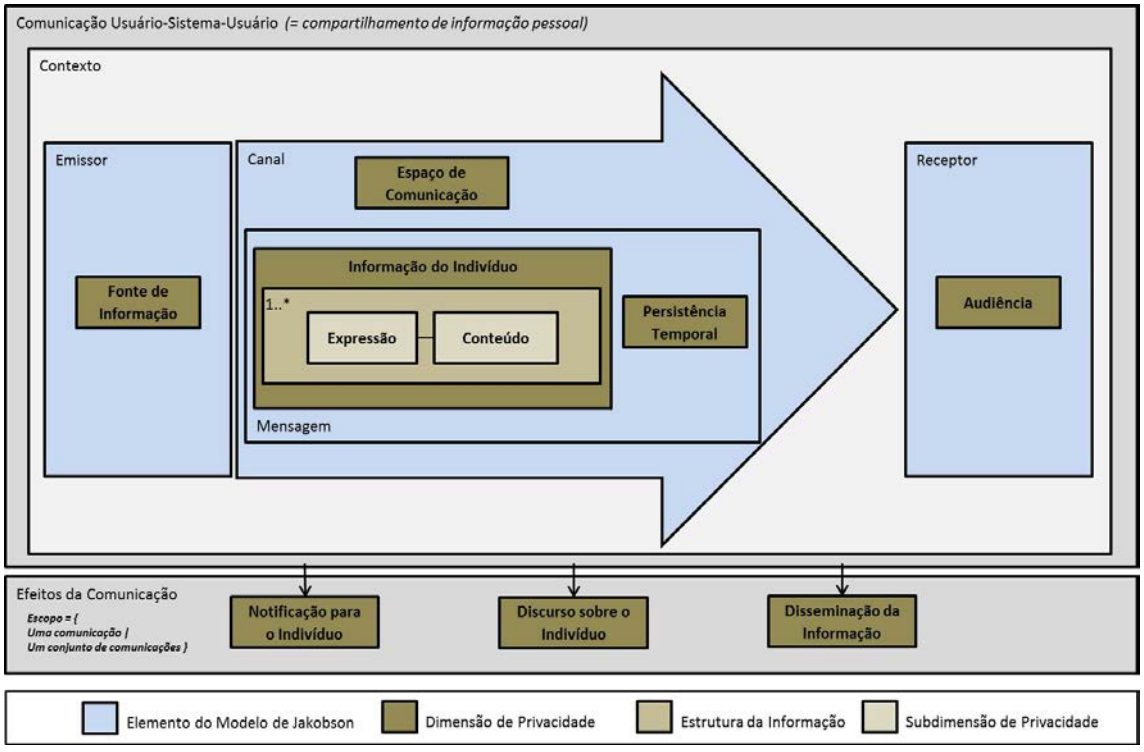

Figura 1. O modelo de design de privacidade (MDP)

O MDP considera os elementos **contexto**, **controle** e **estado de privacidade** relativos à privacidade no compartilhamento de informações pessoais. O **contexto** está relacionado a normas culturais, éticas e morais que governam compartilhamento de informações pessoais em RSOs e funciona como um pano-de-fundo, tendo em vista que as

[3]Usamos o termo "indivíduo" para nos referirmos ao usuário cuja informação está sendo compartilhada dentro da RSO.

decisões do designer sobre como tratar as dimensões de privacidade, no que se refere à forma como serão atribuídos valores às mesmas, são baseadas no contexto no qual o sistema é projetado. O elemento **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 uma das dimensões, a quem deverá ser concedido o controle sobre o valor da mesma: ao *usuário* ou ao *sistema*. O **estado de privacidade** é obtido a partir dos níveis de privacidade relacionados a cada uma das dimensões do MDP. 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. Dessa forma, as decisões do designer em relação ao controle e valor para as dimensões de privacidade determinam os possíveis estados de privacidade que o usuário pode atingir durante o uso do sistema.

3.1. Dimensões de Privacidade

As dimensões de privacidade do MDP foram definidas com base na literatura e em estudos empíricos sobre o compartilhamento de informação e privacidade em RSOs[4]. Essas dimensões são estruturadas em dois níveis: *comunicação usuário-sistema-usuário* e *efeitos da comunicação*, que serão explicados a seguir.

3.1.1. Dimensões de Comunicação Usuário-Sistema-Usuário

A comunicação usuário-sistema-usuário diz respeito à comunicação entre usuários que ocorre através do sistema, com o seu conteúdo consistindo de informações pessoais. As dimensões deste nível modelam os elementos que constituem o compartilhamento de informação pessoal em RSOs, e serão detalhadas a seguir.

Fonte de Informação: Esta dimensão diz respeito a quem pode determinar como, quando e em que extensão a informação pessoal do indivíduo será compartilhada no sistema. Os possíveis valores dessa dimensão são *"indivíduo"*, quando o indivíduo explicitamente compartilha informações sobre ele com outros usuários, ou executa ações que indiretamente podem caracterizá-lo, ao revelar suas opiniões, pontos de vista ou mesmo traços de sua personalidade dentro do sistema; e *"outro usuário"*, sendo que, neste caso, 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 se refere ao local onde a informação sobre o indivíduo é compartilhada dentro do sistema. O compartilhamento de informações pessoais pode ocorrer em um dos seguintes espaços: *"espaço de perfil do indivíduo"*, que refere-se ao espaço onde são compartilhadas informações mais estáticas, relacionadas a elementos de identidade do indivíduo dentro do sistema; *"espaço de publicação do indivíduo"*, que 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; *"espaço de outro usuário"*, que refere-se a um espaço que pertence a outro usuário do sistema, onde também podem ser compartilhadas

[4]As explicações sobre como foram geradas as dimensões do MDP estão apresentadas em [Villela and Prates 2015]

informações pessoais do indivíduo; e *"espaço público"*, que diz respeito a um espaço que não pertence especificamente a nenhum usuário e pode ser acessado por todos os usuários e, em alguns casos, também por pessoas fora do sistema.

Informação do Indivíduo: Esta dimensão diz respeito à informação que é compartilhada no sistema 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 nos formatos: *"predefinido"*, que é o formato das informações que 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; *"tipado"*, que é o formato das informações que possuem o seu significado definido pelo sistema, em tempo de design, mas são fornecidas pelos usuários, em tempo de uso; e *"livre"*, que é o formato da informação que tem o seu significado definido pelo próprio usuário, em tempo de uso, a partir do seu conteúdo. A subdimensão **conteúdo** refere-se ao nível de pessoalidade da informação sobre o indivíduo que está sendo compartilhada, que diz respeito a quão pessoal ela é [Villela et al. 2015]. Dessa forma, a subdimensão **conteúdo**, pode assumir os seguintes valores no MDP: *"pouco pessoal"*, *"levemente pessoal"*, *"pessoal"*, *"um tanto pessoal"* e *"muito pessoal"*.

Persistência Temporal: Diz respeito ao período de tempo durante o qual a informação sobre o indivíduo fica acessível à sua audiência no sistema. No MDP, a persistência temporal da informação pessoal do indivíduo pode assumir os seguintes valores: *"instantânea"*, quando a informação sobre o indivíduo fica disponível apenas para a audiência que está acessando o sistema no momento em que a mesma é compartilhada; *"limitada"*, quando a informação fica disponível para a audiência por um período limitado (e geralmente curto) de tempo; *"ilimitada em uma direção"*, quando a informação fica visível para a sua audiência por um período ilimitado de tempo, a partir do momento em que é disponibilizada (tempo presente) e prossegue em direção ao passado ou ao futuro; e, por fim, *"permanente"*, quando a informação compartilhada fica sempre acessível à sua audiência, enquanto ela não for excluída pelo usuário.

Audiência: Esta dimensão se refere a quem terá acesso à informação, sobre o indivíduo, compartilhada no sistema. O valor para a dimensão pode ser: *"indivíduo"*, indicando que 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; *"selecionada"*, quando o usuário decide quem serão os usuários que farão parte do grupo que irá formar a audiência da informação; *"limitada"*, quando abrange todo o conjunto de usuários do sistema; *"ilimitada"*, quando abrange, além dos usuários do sistema, outras pessoas externas ao mesmo; e *"desconhecida"*, quando o indivíduo ao qual a informação se refere não tem conhecimento de quem poderá ter acesso à mesma.

3.1.2. Dimensões de Efeitos da Comunicação

Os efeitos da comunicação 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 desse nível.

Notificação para o indivíduo: Esta dimensão diz respeito ao sistema informar adequadamente ao indivíduo quando a informação sobre ele é divulgada ou acessada por outros usuários, e de que forma isso acontece. Os seus valores podem ser: *"completa"*, caso o indivíduo receba, para cada informação pessoal sua que é compartilhada, um completo relatório sobre as interações de outros usuários com a mesma; *"parcial"*, caso o indivíduo seja informado apenas sobre uma parte das interações de outros usuários com sua informação; e *"ausente"*, quando o sistema não fornece ao indivíduo nenhuma informação sobre as interações de outros usuários com sua informação.

Discurso sobre o indivíduo: Dimensão relacionada ao sistema tomar a iniciativa de gerar compartilhamentos de informações do indivíduo. Remetendo a níveis decrescentes de privacidade, os valores para esta dimensão podem ser: *"ausente"*, se o sistema não gera qualquer comunicação a partir de um ou mais compartilhamentos de informações pessoais do indivíduo; *"destaque"*, quando o sistema apresenta informações sobre o indivíduo às quais os usuários já possuem acesso, porém de forma destacada, trazendo-as à atenção dos usuários; e *"novo"*, caso o sistema processe uma ou mais informações pessoais do indivíduo que são compartilhadas, gerando nova informação sobre o mesmo.

Disseminação da Informação: Esta dimensão está relacionada à audiência ser capaz de (re)compartilhar informação pessoal do indivíduo, referindo-se à possibilidade de uma informação pessoal do indivíduo se espalhar através da rede. Tal fato pode gerar problemas de privacidade, devido ao alcance inesperado, por parte do indivíduo, de suas informações [Pereira Junior et al. 2014]. Os valores que essa dimensão pode assumir são: *"ausente"*, quando não é permitida à audiência da informação recompartilhá-la com outras pessoas; *"limitada"*, quando a informação compartilhada sobre o indivíduo pode ser propagada de uma maneira restrita, apenas para uma audiência adicional limitada; e *"ilimitada"*, quando a informação sobre o indivíduo pode ser recompartilhada indistintamente pela audiência, sem nenhuma restrição.

3.2. Representação Visual do MDP

Com o objetivo de auxiliar designers na utilização do MDP, permitindo-os visualizar o impacto de suas decisões no estado de privacidade que o sistema oferece aos seus usuários, foi proposta uma representação visual para o mesmo. Nessa representação visual, cada oportunidade de compartilhamento de informação pessoal no sistema é caracterizada como um "tipo de comunicação" e é representada por um *"honeycomb"*. Esse *"honeycomb"* é formado por hexágonos que representam cada uma das dimensões de privacidade do MDP, cuja disposição remete ao seu posicionamento na na estrutura do MDP, como mostrado na Figura 2. No centro do *"honeycomb"* é colocada a descrição referente ao tipo de comunicação que o mesmo representa.

Para cada uma das dimensões de privacidade representadas no *"honeycomb"*, os valores que a mesma pode assumir, em tempo de design, estão associados a tons de uma determinada cor. Na representação em papel, foram utilizados tons de cinza. Assim, quanto mais escuro for o tom de cinza, maior é o nível de privacidade associado ao valor da dimensão. Caso o valor para a dimensão seja definido em tempo de uso, o hexágono correspondente fica sem preenchimento (equivalente à cor branca na representação) 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

Figura 2. Disposição das dimensões de privacidade do MDP na representação visual de um tipo de comunicação

valores. Assim, 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 na tonalidade mais escura da cor e aquele que remete ao nível mínimo de privacidade é mapeado na tonalidade mais clara. Nesse caso, o valor referente ao nível intermediário de privacidade para a dimensão em questão será mapeado na tonalidade intermediária.

Neste ponto, vale salientar que a dimensão **informação do indivíduo** é representada no *"honeycomb"* apenas através de sua subdimensão **conteúdo**, tendo em vista 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 dos hexágonos, na representação visual do MDP, 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 também 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 representa também quem tem o controle sobre a dimensão, ou seja, quem pode definir os seus valores, como mostrado na Figura 3.

	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

Figura 3. Bordas representando o momento em que o valor para a dimensão é definido e quem tem controle sobre ela

Considerando os tipos de comunicação referentes a todas as oportunidades de compartilhamento de informação pessoal dentro de um sistema, a visualização fornece ao designer uma ideia geral das diferenças nos níveis 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.

4. PryMeVis

Com o objetivo de facilitar a criação e avaliação da representação visual e do próprio MDP, desenvolvemos a PryMeVis, uma ferramenta para modelagem e criação de uma representação visual online do MDP[5]. Nessa ferramenta, o designer pode modelar cada tipo de comunicação referente a uma oportunidade de compartilhamento de informação pessoal dentro da RSO, fornecendo valores para os atributos "controle" e "valor" de cada dimensão do MDP. Com base nos valores fornecidos através da interação direta com a interface, PryMeVis representa visualmente os tipos de comunicação, como mostrado na Figura 4. A única diferença entre a representação visual apresentada na seção anterior e a utilizada na PryMeVis é o uso da paleta sequencial[6] de cores com diferentes intensidades em tons de azul, ao invés dos tons de cinza, que ocorre puramente por questão estética. Também foi utilizado o padrão *fade* (em tom de cinza) para representar o valor "não aplicável" na visualização.

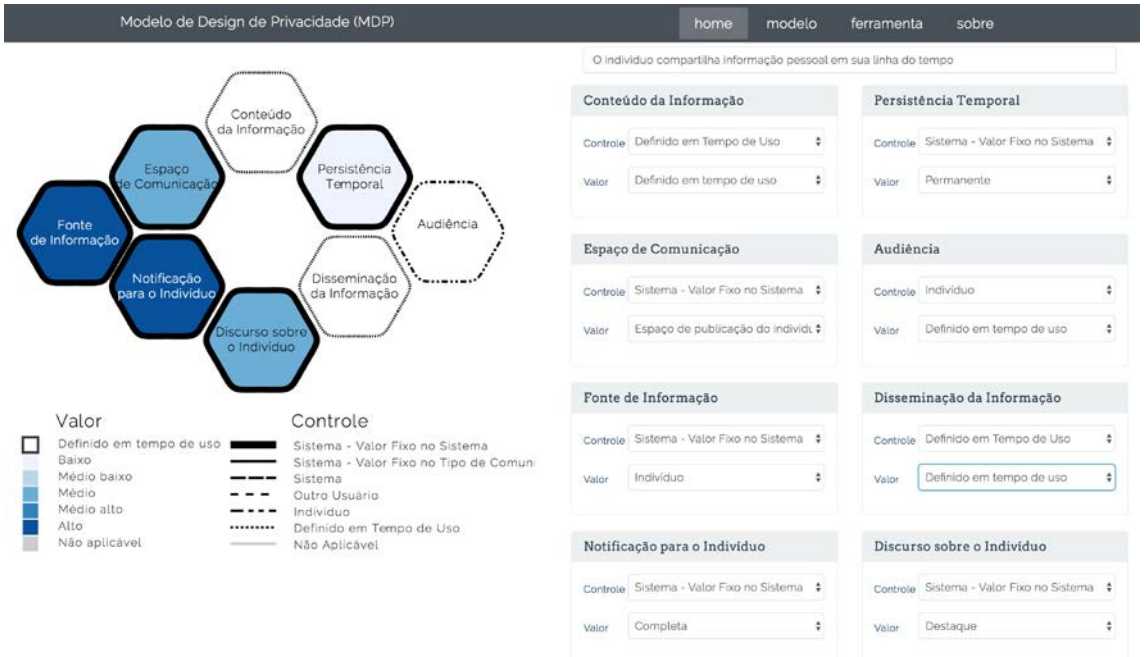

Figura 4. Protótipo da ferramenta de visualização do MDP: versão inicial

[5]Disponível em `pensi.dcc.ufmg.br/applications/`
[6]Paleta sequencial ColorBrewer: `colorbrewer2.org`

Inicialmente, foi implementada uma versão online simplificada da ferramenta, fazendo uso da biblioteca Java Script D3.js (que manipula documentos baseados em dados) e do framework Bootstrap[7]. O design foi pensado para ser limpo, responsivo e focado na visualização, priorizando sua disposição na interface e exibindo em uma mesma tela todos os campos que devem ser preenchidos para a construção da visualização, a fim de facilitar a interação e compreensão da modelagem. Isso implicou no fato de o designer poder modelar apenas um tipo de comunicação por vez. Uma limitação da versão inicial da ferramenta é a impossibilidade de armazenar a visualização gerada, tendo o usuário que tirar um *screen shot* da mesma se quiser guardá-la. Entretanto, apesar das limitações, os resultados obtidos com a avaliação PryMeVis (que será apresentada na Seção 5) mostram que a mesma atendeu ao seu principal objetivo, que é servir como um apoio à utilização do MDP e visualização das modelagens geradas com o seu uso.

Após a avaliação da versão inicial da PryMeVis, foram definidos os casos de uso que representam um cenário chave de seu uso por designers, no sentindo de aprimorá-la. Nesse cenário, o usuário faz seu cadastro na ferramenta, cria uma modelagem referente a uma determinada RSO e cadastra os tipos de comunicações que representam as oportunidades de compartilhamento de informação pessoal no sistema. Dessa forma, é permitido ao usuário fazer a modelagem da RSO usando o MDP, podendo este acessar posteriormente os dados modelados através da PryMeVis. Foram definidas também funcionalidades desejáveis (que ainda não foram implementadas) a serem incorporadas à sua próxima versão. Um ponto importante é a implementação de um sistema de ajuda nos moldes proposto por [Silveira et al. 2004], que possa ser utilizado pelos usuários para entenderem melhor ou tirarem dúvidas sobre aspectos relativos ao MDP. Com isso, o designer poderia aprender sobre o MDP durante sua interação com a PryMeVis, de uma maneira didática e rápida. Além disso, é de grande interesse pesquisar maneiras alternativas de visualizar, filtrar e comparar as redes modeladas, bem como suas comunicações. Atualmente, a PryMeVis permite que se veja a modelagem de cada tipo de comunicação da RSO separadamente. Porém, a possibilidade de selecionar diferentes tipos de comunicação para visualização em uma mesma tela, por exemplo, pode permitir a comparação dos mesmos no que tange aos níveis de privacidade oferecidos pela RSO aos seus usuários, o que pode ter um valor significativo para o designer.

5. Avaliação da Representação Visual e PryMeVis

Após o MDP ter sido proposto, foi realizada uma avaliação inicial do mesmo junto a designers de sistemas, que consistem em seus potenciais usuários [Villela 2016]. Dentre os objetivos dessa avaliação, pretendia-se coletar indicadores tanto sobre a capacidade da representação visual do MDP, quanto sobre a primeira versão da ferramenta PryMeVis atender a seus propósitos, no sentido de apoiar o uso do MDP. Neste trabalho focamos apenas na parte da avaliação relacionada a estes objetivos, que será descrita a seguir.

5.1. Avaliação Realizada

A avaliação aconteceu em dezembro de 2015 e envolveu seis participantes, designers de sistemas de informação. Além disso, todos eram usuários frequentes de RSOs, acessando esses sistemas mais de uma vez por dia, com exceção de um participante que acessava menos de uma vez por semana. Todos os participantes já haviam alterado suas configurações

[7]Site do D3 (`d3js.org`) e do Bootstrap (`getbootstrap.com`)

de privacidade nesses sistemas, ao menos para estabelecer uma configuração padrão para o compartilhamento de suas informações. A avaliação foi realizada em uma única sessão, com duração aproximada de três horas e meia, e consistiu de três etapas: apresentação do MDP, execução das tarefas e realização de grupo focal.

Na apresentação do MDP, foi informado aos participantes o objetivo da avaliação e coletado o consentimento dos mesmos, através da assinatura do termo de consentimento. Os participantes também responderam a um questionário com questões sobre a sua experiência no uso de RSOs e em design de IHC, dentre outros aspectos. A primeira etapa foi encerrada com uma apresentação completa sobre o MDP, com exemplos do seu uso na modelagem de uma RSO existente. Em seguida, na segunda etapa da avaliação, cada participante recebeu material impresso contendo uma visão geral do MDP: sua representação gráfica e uma breve descrição de cada dimensão e seus possíveis valores, bem como as possíveis definições para o controle, e os níveis de privacidade associados ao valores das dimensões. Foi então solicitado aos participantes que executassem quatro tarefas. Dentre elas, as que estavam relacionadas à representação visual eram: (a) usar o protótipo da ferramenta PryMeVis para gerar um modelo consolidado de um tipo de comunicação do Facebook, resultante da discussão em pares realizada a partir de modelos gerados individualmente com o MDP para esse tipo de comunicação; e (b) comparar duas RSOs distintas a partir de seus modelos MDP, buscando identificar diferenças entre as mesmas no que tange à privacidade relacionada ao compartilhamento de informação pessoal - para isso, os participantes receberam as representações tabular e visual equivalentes dessas RSOs[8]. Por fim, na terceira etapa da avaliação, foi realizado com os participantes um grupo focal sobre as tarefas realizadas, quando tiveram oportunidade de falar, dentre outros pontos, de suas opiniões sobre a utilidade da representação visual do MDP, bem como da ferramenta PryMeVis.

O material coletado durante a realização das tarefas consistiu dos modelos gerados pelas duplas de participantes com o uso da ferramenta PryMeVis, do registro por escrito (efetuado pelas mesmas duplas de participantes formadas na tarefa anterior) das diferenças percebidas entre as duas RSOs comparadas, e dos discursos dessas duplas enquanto realizavam as tarefas. Esses materiais foram analisados para a presente avaliação, bem como os discursos de todos os participantes durante a realização do grupo focal.

5.2. Resultados

Conforme mencionado, a avaliação coletou dados sobre o uso da ferramenta PryMeVis e também sobre a representação visual do MDP. Tal representação foi avaliada a partir da tarefa de comparação entre duas RSOs distintas, que foi realizada pelos participantes com base na versão impressa da representação visual dos modelos MDP das mesmas.

Sobre a ferramenta PryMeVis, todos os participantes conseguiram utilizá-la facilmente e entender de maneira imediata como o modelo MDP deveria ser criado dentro da mesma. As dúvidas que surgiram durante o seu uso foram principalmente em relação ao MDP (relacionadas à definição das dimensões e seus valores), e não sobre a PryMeVis em si. Os participantes apontaram algumas inconsistências 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 PryMeVis, sendo alguns deles

[8]Geradas por um especialista no MDP, através da modelagem reversa dos seus tipos de comunicação.

já previstos, embora ainda não implementados na sua versão inicial usada na avaliação. Por exemplo, a inclusão de um sistema de ajuda, com a explicação sobre as dimensões de privacidade e os possíveis valores para seus atributos valor e controle.

Sobre a representação visual, os participantes destacaram que esta os ajudou a entenderem melhor a modelagem que fizeram com o MDP e os seus efeitos, bem como a terem uma visão mais clara das relações entre as dimensões dentro do modelo. Isso foi apontado pelo participante P4: *"olhando a colméia [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, foi observado que todos os seis participantes, organizados em três duplas, preferiram utilizar a representação visual à tabular. Além disso, alguns deles, aos discutirem com seus pares, expressaram a razão por tal preferência, como pode ser visto na fala de P6, por exemplo, ao discutir com P3: *"Eu acho que essa tabela é irrelevante [...]. O desenho [referindo-se à representação visual] é muito bom [...]. Gostei, resolve o problema"*. P1, durante as discussões no grupo focal, 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 do MDP foi apontado pelos participantes como sendo de grande importância para o entendimento dos níveis de privacidade oferecidos pelas RSOs modeladas e, logo, para diferenciá-las no que tange à privacidade. A fala de P6 ilustra este ponto: *"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"*. Um problema apontado pelos participantes foi o uso da cor branca (ou ausência de preenchimento do hexágono correspondente à dimensão de privacidade) para indicar que o valor da dimensão será definido em tempo de uso. Segundo eles, o usuário pode incorretamente associar o "branco" 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"*.

Houve também sugestões que extrapolam o propósito da ferramenta, como foi o caso de P6, que sugeriu estender o protótipo para fornecer feedback sobre aspectos na RSO modelada que seriam críticos em relação à privacidade do indivíduo, com base nos

valores atribuídos às dimensões do MDP. No entanto, o atendimento dessa sugestão vai além do objetivo da ferramenta, uma vez que requer a inclusão no MDP de um componente semântico que possa identificar situações em que seria relevante alertar o designer sobre o impacto de suas decisões, caracterizadas pela combinação de valores atribuídos às dimensões, no nível de privacidade a ser oferecido pelo sistema aos seus usuários.

Assim, de uma forma geral, percebemos que a representação visual se mostra como um importante suporte ao uso e entendimento do MDP, melhorando a percepção dos designers sobre os efeitos das suas modelagens na forma como a privacidade relacionada ao compartilhamento de informações pessoais é tratada em uma RSO. No entanto, alguns pontos ainda precisam ser melhorados a fim de proporcionar uma representação mais adequada, no caso específico do efeito da atribuição de valores em tempo de uso nos níveis de privacidade proporcionados pelo sistema aos seus usuários. Os resultados também indicam que vale a pena investir para que a versão da PryMeVis aqui apresentada possa evoluir para se tornar uma ferramenta robusta de apoio ao designer no uso do MDP. O fato dos participantes terem levantado pontos que já haviam sido previstos para a ferramenta (como a necessidade de inclusão de um sistema de ajuda) reforça e justifica a importância da implementação desses recursos, como incremento funcional para tornar mais eficiente o seu uso e, consequentemente, o uso do MDP.

6. Conclusão

Esse trabalho tem por objetivo apresentar PryMeVis, uma ferramenta online para apoio ao uso do MDP, que consiste em um modelo descritivo para auxiliar designers na elaboração e avaliação do modelo de privacidade de RSOs, relacionada ao compartilhamento de informações pessoais. Tal ferramenta foi criada para facilitar o uso da representação visual do MDP, permitindo que designers criem modelos para o compartilhamento de informações pessoais em RSOs de forma mais eficiente, ao atribuir valores para as dimensões do MDP e visualizar o impacto de suas decisões nos estados de privacidade que podem ser alcançados pelos usuários dentro do sistema.

O propósito da avaliação de um protótipo ainda simplificado da PryMeVis (em relação à sua proposta) foi coletar indicadores iniciais sobre a utilidade da representação visual do MDP, além de informações que pudessem ajudar na definição da direção a ser seguida no desenvolvimento da ferramenta e do investimento requerido para tal. Assim, os resultados mostraram a importância da representação visual como suporte ao uso e entendimento do MDP, uma vez que melhora a percepção dos designers acerca dos efeitos de suas decisões, relativas à modelagem do compartilhamento de informações pessoais, nos níveis de privacidade oferecidos pelo sistema aos seus usuários. A avaliação também nos indicou alguns pontos que precisam ser melhorados em tal representação, especificamente no que tange às dimensões que possuem seus valores definidos em tempo de uso. Além disso, os resultados da avaliação também nos indicaram novos aspectos a serem considerados na ferramenta PryMeVis, como a inclusão de um sistema de ajuda, no sentido de que possa se tornar uma ferramenta robusta a ser oferecida a designers de RSOs para apoio ao aprendizado e uso do MDP.

A refatoração da PryMeVis está em andamento, com o objetivo de gerar uma ferramenta de modelagem mais efetiva no suporte ao uso do MDP. Por se tratar de um ferramenta com maior nível de interação, a arquitetura inicial foi modificada, sendo agora

baseada na abordagem “modelo, visão, controle” (MVC), através do arcabouço Ruby on Rails. Esta decisão visou garantir o baixo acoplamento e alta coesão do sistema, aumentando sua qualidade e tornando-o escalável. A interface e a visualização, assim como na versão inicial, continuaram empregando os padrões abertos de desenvolvimento web (HTML5, CSS3, JavaScript e SVG), além da biblioteca D3.js e Bootstrap. O banco de dados foi modelado possibilitando o armazenamento de mais de uma representação por vez, facilitando o acesso do designer a suas análises.

Os próximos passos consistem em finalizar o desenvolvimento da PryMeVis e disponibilizá-la a designers e interessados na aplicação do MDP. Um sistema de ajuda robusto e que permite ao designer entender a lógica de funcionamento do MDP durante a modelagem está sendo projetado. Além disso, uma segunda avaliação que contemple a interação completa com a ferramenta (não se atendo apenas à modelagem de tipos de comunicação) deve ser realizada, a fim de consolidar as decisões de projeto tomadas.

7. Agradecimentos

Agradecemos aos participantes da avaliação por sua colaboração; às agências CNPq e FAPEMIG, bem como ao InWeb (MCT/CNPq 573871/2008- 6) e MASWeb (FAPEMIG/PRONEX APQ-01400-14) por seu apoio financeiro parcial a esta pesquisa.

Referências

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

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

Bevan, J., Cummings, M., Kubiniec, A., Mogannam, M., Price, M., and 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.

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

Epstein, D. A., Jacobson, B. H., Bales, E., McDonald, D. W., and Munson, S. A. (2015). From "nobody cares"to "way to go!": A design framework for social sharing in personal informatics. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, CSCW ’15, pages 1622–1636, New York, NY, USA. ACM.

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

Kosinski, M., Stillwell, D., and 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.

Malandrino, D., Petta, A., Scarano, V., Serra, L., Spinelli, R., and Krishnamurthy, B. (2013). Privacy awareness about information leakage: Who knows what about me?

In *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society*, WPES '13, pages 279–284, New York, NY, USA. ACM.

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

Pang, J. and 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., and Strufe, T. (2012). C4ps: Colors for privacy settings. In *Proceedings of the 21st International Conference on World Wide Web*, WWW '12 Companion, pages 585–586, New York, NY, USA. ACM.

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

Romero, N. A., Markopoulos, P., and Greenberg, S. (2013). Grounding privacy in mediated communication. *Comput. Supported Coop. Work*, 22(1):1–32.

Schlegel, R., Kapadia, A., and Lee, A. J. (2011). Eyeing your exposure: Quantifying and controlling information sharing for improved privacy. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 14:1–14:14, New York, NY, USA. ACM.

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

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

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

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

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

Villela, M. L. B. V. (2016). *Um Modelo de Design de Privacidade para o Compartilhamento de Informacoes Pessoais em Redes Sociais Online*. PhD thesis, Departamento de Ciencia da Computacao, UFMG.

Wang, Y., Gou, L., Xu, A., Zhou, M. X., Yang, H., and Badenes, H. (2015). Veilme: An interactive visualization tool for privacy configuration of using personality traits. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 817–826, New York, NY, USA. ACM.