

Caracterização das Estratégias de Privacidade do Instagram

Geanderson E. dos Santos¹, Marcelo W. Barbosa², Glívia A. R. Barbosa³

¹Departamento de Ciência da Computação – Universidade Federal de Minas Gerais (DCC/UFMG). Av. Antônio Carlos, 6627 - Prédio do ICEx Pampulha, Belo Horizonte, MG – Brasil.

²Instituto de Ciências Exatas e Informática – Pontifícia Universidade Católica de Minas Gerais (PUC-MG). Av. Afonso Vaz de Melo, 1.200 - Barreiro de Baixo - Belo Horizonte – MG - Brasil, CEP 30640-070

³Departamento de Computação – Centro Federal de Educação Tecnológica de Minas Gerais (DECOM/CEFET-MG). Av. Amazonas, 7675 - Nova Gameleira - Belo Horizonte, MG – Brasil.

geanderson@dcc.ufmg.br, mwerneck@pucminas.br,
gliviabarbosa@decom.cefetmg.br

Abstract. *This paper aimed to verify and characterize how Instagram has supported their users' privacy. A qualitative methodology known as Semiotic Inspection Method (SIM) is used to identify and present the privacy strategies proposed by Instagram interface designer. Following, these strategies were compared to the privacy strategies available in the literature in order to verify the equivalence degree of Instagram privacy strategies and the ones available in the literature. Finally, an online questionnaire was sent to Instagram users aiming to verify whether users feel safe using the app based on the privacy strategies. The results showed that the strategies adopted by Instagram designer have contributed to the protection of Instagram's users. Moreover, the results can help in the development and evaluation of privacy settings in other social networks.*

Resumo. *Este trabalho buscou verificar e caracterizar como o Instagram tem suportado a privacidade dos seus usuários. Para isso, o Método de Inspeção Semiótica (MIS) foi aplicado para identificar e apresentar as estratégias de privacidade propostas pelo aplicativo. Posteriormente, essas estratégias foram comparadas com os princípios de privacidade disponíveis na literatura com o intuito de verificar o grau de correspondência entre as estratégias do Instagram e os princípios de privacidade identificados na literatura. Finalmente, um questionário online foi aplicado para usuários do Instagram buscando verificar se esses usuários se sentem seguros ao utilizar esse aplicativo. Os resultados mostraram que as estratégias adotadas pelo Instagram têm contribuído para proteger seus usuários. Além disso, esses resultados contribuem para o desenvolvimento e avaliação dos recursos de privacidade de outras redes sociais.*

1. Introdução

Redes sociais *online* têm se tornado cada vez mais populares, e no Brasil essa utilização não tem sido diferente [comScore 2015]. Essa crescente adoção abre espaço para que essas redes *online* se tornem, cada vez mais, mediadoras da interação entre as pessoas de diferentes regiões, culturas e condições físicas e/ou psicológicas [Villella e Prates 2015]. Contudo, juntamente com todos os benefícios que as redes sociais *online* podem oferecer a seus usuários, surge também a preocupação com a privacidade dos usuários nessas redes [Gill *et al.* 2011][Villella e Prates 2015]. Isso porque, na maioria das vezes, o conteúdo compartilhado (e.g., informações pessoais, fotos, vídeos) refere-se a informações pessoais e verdadeiras que ao serem acessadas sem um controle podem expor seus proprietários de forma que fiquem vulneráveis a pessoas não autorizadas e/ou mal intencionadas [Gill *et al.* 2011].

Com o intuito de potencializar a privacidade dos usuários de redes sociais, projetistas e pesquisadores da área de Interação Humano Computador (IHC) têm direcionado seus esforços para avaliar e propor mecanismos que permitem a configuração de privacidade nessas redes (e.g., [Fong *et al.* 2009][Junior *et al.* 2014][Rodrigues *et al.* 2012][Villella e Prates 2015]). Porém, algumas pesquisas têm demonstrado que os modelos de configuração correntes nem sempre oferecem proteção adequada para os diferentes perfis de usuários, resultando em uma disparidade entre a privacidade desejada e a real [Liu *et al.* 2011][Villella e Prates 2015]. Diante dessa realidade é importante caracterizar quais estratégias de privacidade têm sido utilizadas por softwares sociais para oferecer proteção de seus membros e verificar se essas estratégias contribuem para a privacidade dos mesmos [Young e Quan-Haase 2009].

Motivados pela importância de pesquisas que investigam como as redes sociais *online* têm favorecido a privacidade dos usuários, e considerando o Instagram um fenômeno em termos de popularidade mundial, com cerca de 300 milhões de usuários acessando o serviço mensalmente [Instagram 2015], o objetivo desse trabalho consiste em identificar e caracterizar as estratégias de privacidade do Instagram e verificar se, de fato, essas estratégias potencializam a privacidade dos usuários durante o uso do aplicativo.

Este trabalho foi conduzido a partir de uma metodologia qualitativa que consistiu na aplicação do Método de Inspeção Semiótica (MIS) [de Souza *et al.* 2006] para identificar e apreciar as estratégias de privacidade adotadas pelo projetista na interface do Instagram. Posteriormente, essas estratégias foram comparadas com diretrizes de privacidade disponíveis na literatura a fim de verificar o grau de adequação da proposta do Instagram às mesmas. Finalmente, foi aplicado um questionário aos usuários do aplicativo para verificar se, de fato, os recursos oferecidos têm apoiado no controle de privacidade desses usuários durante o uso do Instagram.

Os resultados dessa pesquisa permitiram constatar que o projetista do Instagram adota estratégias consideradas relevantes para potencializar a privacidade dos usuários. Nesse sentido, esse trabalho apresenta contribuições práticas e científicas para essa linha de pesquisa. Em termos práticos, os resultados reportados, bem como as estratégias de privacidade identificadas neste trabalho, podem servir de parâmetros para a melhoria e/ou

criação de mecanismos de privacidade em redes sociais *online*. Além disso, essa pesquisa alerta os designers de interface sobre a importância de oferecer configurações de privacidade adequadas aos usuários nesse ambiente *online*. Em termos científicos/metodológicos, os resultados do MIS reforçam a aplicabilidade do método, devido à sua fundamentação teórica, para identificar as estratégias de design, comunicadas na interface, que visam potencializar determinadas qualidades de uso, neste caso, a privacidade.

2. Trabalhos Relacionados

A privacidade em redes sociais é um assunto complexo que tem sido investigado por pesquisadores de diferentes áreas sob diferentes perspectivas. Por exemplo, o trabalho realizado por Johnson *et al.* (2012) alerta para o fato de que, nem sempre, configurações de privacidade são capazes de combater a ameaça interna, ou seja, pessoas que fazem parte da própria rede de amigos de um determinado usuário, mas que poderiam usar as informações que eles têm acesso para prejudicar o proprietário do perfil. Em Xavier *et al.* (2014), os autores apreciam a privacidade de usuários em redes sociais através de uma metodologia qualitativa de pesquisa. O estudo mostrou a importância dos usuários serem capazes de denunciar abusos em redes sociais.

Em uma perspectiva diferente, Hull *et al.* (2010) enfatizam como que decisões de projeto de interface podem expor informações de usuários. Eles destacam a implementação do *feed* de notícias e a inserção de aplicativos no Facebook, e como tais mudanças na interface impactaram consideravelmente na privacidade dos membros daquela rede. Outros autores têm explorado quais configurações contribuem para fornecer uma melhor privacidade para membros dessas redes *online* [Young e Quan-Haase 2009][Johnson *et al.* 2012].

Embora os trabalhos apresentados foquem em aspectos de privacidade em redes sociais *online*, não foram encontradas pesquisas que fizessem a análise feita neste estudo, caracterizando as estratégias de privacidade que têm sido adotadas pelas redes sociais *online* através de um estudo de caso no Instagram. Esse tipo de investigação é importante porque seus resultados podem apontar as vantagens e/ou limitações no uso dessas estratégias, de forma a colaborar no desenvolvimento e/ou avaliação das configurações de privacidade dos softwares sociais *online*.

3. Metodologia e Referencial Teórico

Considerando o objetivo deste trabalho, a seguinte questão de pesquisa foi investigada: “*Quais as estratégias de privacidade utilizadas pelo Instagram contribuem para proteger as informações dos usuários?*”. A metodologia adotada para responder essa pergunta consistiu em uma abordagem qualitativa, dividida em quatro etapas.

Inicialmente, foi realizado um levantamento bibliográfico com o objetivo de identificar estratégias de privacidade, presentes na literatura, que poderiam ser utilizadas como referência para verificar a adequação da proposta de privacidade do Instagram. Em seguida, a interface do Instagram foi inspecionada, seguindo o Método de Inspeção Semiótica (MIS) [de Souza e Preece 2004][de Souza *et al.* 2006][de Souza e Leitão 2009]

para identificar e apresentar as estratégias de privacidade comunicadas em sua interface.

A terceira etapa da metodologia buscou comparar as estratégias encontradas na literatura com as identificadas na interface do Instagram. Para finalizar, foi investigado junto aos usuários desse aplicativo se as estratégias identificadas contribuem para a privacidade de seus membros. Para isso foi aplicado um questionário *online* e as respostas foram analisadas de forma a caracterizar a influência das estratégias no uso do Instagram. Para um melhor entendimento dos conceitos e métodos mencionados na metodologia, a seguir o MIS será apresentado, bem como a justificativa pela escolha desse método.

3.1 Método de Inspeção Semiótica

O Método de Inspeção Semiótica (MIS) é fundamentado na Teoria da Engenharia Semiótica – uma teoria explicativa de Interação Humano Computador (IHC). A Engenharia Semiótica (EngSem) nos permite entender os fenômenos envolvidos no design, uso e avaliação de um sistema interativo [de Souza 2004]. Para a EngSem, a interface de um sistema é vista como uma comunicação, unidirecional e indireta, do projetista do sistema aos seus usuários. O objetivo dessa comunicação é transmitir aos usuários a sua visão sobre a quem o sistema se destina; que problemas ele pode resolver e como interagir com ele [de Souza 2004]. O usuário compreende a mensagem à medida que interage com a interface. Essa comunicação é conhecida como metacomunicação e sua mensagem como metamensagem. A metamensagem transmitida do projetista para o usuário é composta por signos – i.e. qualquer coisa que representa algo para alguém [Peirce 1992]. A EngSem classifica os signos em um sistema interativo como: metalinguísticos, estáticos e dinâmicos [de Souza *et al.* 2009][de Souza *et al.* 2010].

No intuito de apreciar a qualidade da comunicação entre o projetista e o usuário, a EngSem foca na avaliação da propriedade de comunicabilidade do sistema, isto é, sua capacidade de transmitir aos usuários as decisões e princípios que guiaram seu design de forma eficiente e eficaz [Prates *et al.* 2000]. Um dos métodos propostos pela EngSem para apreciação da comunicabilidade é o MIS [de Souza *et al.* 2006][de Souza *et al.* 2009][de Souza *et al.* 2010]. Para isso, um avaliador (que tenha conhecimento de IHC e Engenharia Semiótica) inspeciona o sistema com o objetivo de analisar o sistema proposto a partir da metamensagem projetista-usuário [de Souza *et al.* 2006][de Souza *et al.* 2009][de Souza *et al.* 2010].

A avaliação da interação de um sistema utilizando o MIS consiste em cinco etapas [de Souza *et al.* 2006]: (1) inspeção dos signos metalinguísticos; (2) inspeção dos signos estáticos; (3) inspeção dos signos dinâmicos; (4) contraste e comparação entre as mensagens identificadas em cada uma das inspeções e (5) apreciação da qualidade da metacomunicação. Nos passos de 1 a 3, o especialista deve ser capaz de reconstruir a metamensagem proposta pelo projetista a partir dos signos inspecionados. No passo 4, o especialista contrasta as mensagens geradas nos passos anteriores e, a partir desta análise, explora a possibilidade do usuário atribuir significados diferentes a um mesmo objeto (signo). Finalmente, no passo 5, o especialista gera uma versão unificada da metamensagem e registra a sua apreciação final da qualidade do sistema.

Embora originalmente o MIS tenha sido proposto para avaliar a comunicabilidade de um sistema, uma revisão na literatura realizada por [Reis e Prates 2011], revelou que, devido à sua fundamentação teórica, esse método também pode ser utilizado para identificar as estratégias de *design* comunicadas na interface que visam potencializar determinadas qualidades de uso. Neste sentido, trabalhos como o realizado por Coutinho *et al.* (2011) identificam estratégias sonoras para orientação em jogos, através da aplicação do MIS. Já o trabalho realizado por Barbosa *et al.* (2011) utilizou o MIS para identificar estratégias de sociabilidade em redes sociais. Os autores Silva, Marcelle e Oliveira (2014), utilizaram o MIS para identificar estratégias de marketing (MKT) em sites de hotel, e, no trabalho feito por [Silva *et al.* 2015], o MIS é utilizado para identificar estratégias de *gamificação* em aplicativos educacionais. Todas essas evidências justificam a utilização do MIS na identificação de estratégias no *design* de interação.

4. Apreciação da Proposta de Privacidade do Instagram

Projetistas de softwares sociais *online* não podem controlar a interação social que acontece entre os usuários dentro dessas redes sociais. Contudo, decisões de interface podem auxiliar no controle de privacidade dos usuários desses softwares [Strater e Lipford 2008][Hull *et al.* 2010]. Devido ao crescimento abrupto do Instagram e a possibilidade de divulgar informações pessoais através desse aplicativo, este trabalho buscou avaliar a interface do Instagram para identificar e caracterizar sua proposta de privacidade. Para isso foi realizada uma avaliação utilizando o MIS, cujo objetivo foi identificar as decisões do projetista que refletem em estratégias de privacidade descritas na literatura.

A avaliação foi realizada no período de sete dias (entre 05/09/2015 e 11/09/2015) e foi conduzida por dois autores desse trabalho, sendo que ambos já haviam realizado outras avaliações de interface no contexto de softwares sociais *online* utilizando o método em questão [Barbosa *et al.* 2013]. O escopo da avaliação foi limitado à versão em Inglês do aplicativo do Instagram e às seguintes tarefas: (1) pesquisar e seguir usuários, (2) publicar e visualizar conteúdo, (3) interagir socialmente com os seguidores através dos recursos do sistema como *chat* (mensagem) e envio de fotos/vídeos, e (4) configurar aspectos de privacidade relacionados as três tarefas anteriores. A seguir, são apresentados os principais resultados da primeira etapa dessa pesquisa.

5. Proposta de Privacidade do Instagram

A partir da aplicação do MIS, verificou-se que o propósito do projetista em relação ao Instagram é oferecer um espaço para interação e compartilhamento de fotos e vídeos. O sistema dispõe de políticas e termos de uso que, conforme relatado pelo próprio projetista em sua metamenagem, devem ser seguidas porque, *“Ao usar o nosso Serviço, você entende e concorda que estamos fornecendo uma plataforma para você publicar e compartilhar conteúdo, incluindo fotos, comentários e outros materiais (“Conteúdo do usuário”). Isso significa que outros Usuários podem pesquisar por, ver, usar ou compartilhar qualquer Conteúdo do usuário que você disponibilize publicamente através do Serviço, em consonância com os termos e condições desta Política de Privacidade e nossos Termos de uso.”* [Instagram 2015].

Qualquer pessoa que possui e-mail ou uma conta no Facebook, e aceitar a política de privacidade e termos de uso pode criar uma conta no Instagram. Ao criar um perfil, é necessário informar apenas um nome de usuário e senha. A partir da interação com o aplicativo, diversas outras informações poderão ser inseridas no perfil, tais como: Nome, Website, Biografia, Telefone e Sexo. Além disso, é possível disponibilizar uma imagem, cujo objetivo é identificar visualmente o proprietário do perfil, essa imagem também pode ser importada de outras redes sociais (e.g., Facebook e Twitter).

Para que a interação entre os membros aconteça, o projetista do Instagram oferece um recurso de pesquisa e recomendação de pessoas. Para interagir com outros integrantes do Instagram, o proprietário do perfil tem duas opções: (1) seguir outros membros do Instagram ou (2) permitir que outros membros o siga. Devido a questões de privacidade, usuários podem tornar seus perfis privados. Essa opção permite que o proprietário do perfil receba uma requisição de usuários que o queiram seguir, ou seja, ele pode aprovar ou não que outros usuários tenham acesso ao seu perfil (i.e., conceder visualização a suas fotos/vídeos).

Os principais recursos oferecidos para interação e compartilhamento de conteúdo entre o proprietário do perfil e seus seguidores são compartilhamento de fotos/vídeos, mensagens diretas, e envio direto de fotos e vídeos. É importante destacar que o Instagram fornece uma gama de ferramentas para edição do conteúdo antes de ser postado. Membros podem compartilhar conteúdo com outros membros, desde que eles tenham permissão para isso. Além disso, é possível incluir informações como localização, título do conteúdo, ou mesmo marcar seguidores. Outras redes sociais estão vinculadas a opção de compartilhamento, por essa razão, esse conteúdo (i.e., foto ou vídeo), pode aparecer diretamente em outras redes sociais, tais como: Facebook, Twitter, Tumblr e Flickr.

Em relação ao conteúdo multimídia compartilhado (i.e., fotos e vídeos) na tela principal do aplicativo, é permitido que usuários curtam, comentem, ou mesmo enviem uma publicação para outros membros. Além disso, a/o foto/vídeo pode ser compartilhada em outras redes sociais após sua publicação. Caso o usuário deseje desfazer da postagem, ou mesmo queira modificar alguma coisa. É possível editar e deletar publicações.

Conforme mencionado anteriormente, além do compartilhamento de conteúdo entre o proprietário do perfil e seus seguidores, é possível interagir socialmente através de mensagens diretas. O mecanismo de mensagem diretas possibilita um bate-papo entre o dono do perfil e outro membro do Instagram. Além disso, caso seja do interesse dos interlocutores, é possível adicionar outras pessoas à conversa. O conteúdo da conversa é gravado, para posterior visualização e, além disso, é possível anexar fotos ou vídeos à interação. Novamente, o menu de notificações ajuda a manter a privacidade dos usuários do Instagram, uma vez que eles podem impedir que não seguidores os enviem mensagens diretamente.

Com o intuito de garantir uma boa interação entre os usuários que mantem contato através do Instagram, o projetista notifica cada membro sobre as atualizações que ocorrem em seu perfil, por exemplo, quando um contato curte a foto do dono do perfil uma mensagem é enviada ao mesmo, o usuário recebe uma notificação para que tenha a

oportunidade de fornecer um feedback para a pessoa ou o grupo que interagiu com ele (e.g., responder uma mensagem, curtir um conteúdo, aceitar uma solicitação para seguir).

O menu de notificações é uma das principais decisões do projetista, pois essa função é utilizada no controle sobre a exibição de conteúdo compartilhado no perfil de um usuário. Esse recurso é essencial para manter uma boa privacidade dos usuários dessa rede. Entretanto, o menu de notificações não é a única ferramenta que favorece a privacidade no Instagram. Fotos e vídeos indevidamente postados por seguidores e não seguidores podem ser reportados para os administradores do Instagram pelo dono do perfil. Seguidores hostis também pode ser bloqueados pelo dono do perfil, com o intuito de proteger a rede de amigos do proprietário da conta. A Figura 1 ilustra evidências da proposta do projetista para a interface do Instagram.

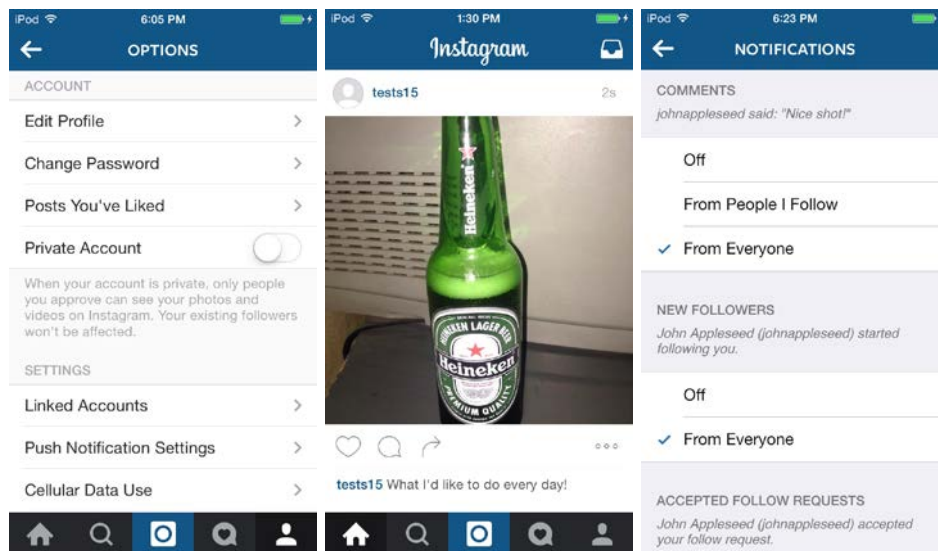


Figura 1 – Proposta do Projetista do Instagram

5.1. Estratégias de Privacidade Identificadas

Uma vez identificada a proposta do projetista em relação a privacidade no Instagram, este trabalho buscou verificar se as decisões comunicadas na interface são compatíveis com as estratégias que, de acordo com a literatura [Young e Quan-Haase 2009][Johnson *et al.* 2012][Xavier *et al.* 2014], podem ser consideradas fatores motivacionais para usuários em ambientes sociais. A Tabela 1 lista as estratégias de privacidades recomendadas na literatura.

Tabela 1 - Estratégias de Privacidade identificadas na Literatura

Estratégias Privacidade		
Cód. Estratégia	Descrição	Referência
E01	Ocultar informações pessoais ou prover falsas informações sobre mim	[Young e Quan-Haase 2009]
E02	Excluir determinadas informações pessoais	[Young e Quan-Haase 2009]

E03	Possibilitar comunicação privada entre usuários	[Young e Quan-Haase 2009]
E04	Permitir a alteração das configurações "default" do sistema	[Young e Quan-Haase 2009]
E05	Remover informações que outros usuários postaram sobre mim	[Young e Quan-Haase 2009]
E06	Desmarcar-se de determinados posts	[Young e Quan-Haase 2009] [Johnson <i>et al.</i> 2012]
E07	Restringir acesso à certas informações pessoais	[Young e Quan-Haase 2009]
E08	Proteger rede de amigos	[Johnson <i>et al.</i> 2012]
E09	Bloquear usuários indesejados	[Young e Quan-Haase 2009]
E10	Denunciar abusos	[Xavier <i>et al.</i> 2014]
E11	Alterar status de um post	[Johnson <i>et al.</i> 2012]
E12	Criar listas customizadas de contatos	[Johnson <i>et al.</i> 2012]
E13	Manter mais de uma conta	[Johnson <i>et al.</i> 2012]

A partir da aplicação do MIS foi possível identificar que o projetista utiliza 11 das 13 estratégias de privacidade já conhecidas na literatura, ou seja, observou-se que o projetista atendeu 85% das estratégias levantadas na literatura para endereçar privacidade. A Tabela 2 apresenta as estratégias de privacidade propostas pela literatura, as decisões do projetista identificadas pelo MIS e exemplos de aplicação destas estratégias no aplicativo. É importante ressaltar que uma estratégia pode remeter a uma ou mais decisões do projetista da interface.

Tabela 2 - Estratégias de Privacidade x Decisão do Projetista

Cod. Estratégia	Cod. Decisão Projetista	Decisão do Projetista	Exemplo de Aplicação no Instagram
E01	DP01	Permitir deixar em branco praticamente qualquer informação sobre o usuário, alteração livre dessas informações e não conferir a veracidade da mesma	Usuários somente precisam informar <i>username</i> e <i>password</i> . Todas as outras informações do perfil podem ficar em branco ou serem alteradas
E02			
E03	DP02	Permitir o envio de mensagens diretas para qualquer usuário	Usuários podem mandar mensagem para qualquer pessoa conectada ao Instagram

E04	DP03	Permitir alteração das configurações padrão do sistema	Usuários podem alterar diversas configurações de privacidade no menu de configurações
E05	DP04	Permitir a remoção de fotos/vídeos postados por seguidores	Usuários podem remover-se de qualquer foto/vídeo postado por outros usuários
E06			
E07	DP05	Permitir perfil privado	Usuários podem configurar o perfil como privado fazendo novos seguidores precisarem de uma aprovação
E08			
E09			
E10	DP06	Permitir o bloqueio de seguidores	Seguidores podem ser bloqueados através de uma opção dentro de seus perfis
E11	DP07	Permitir reportar qualquer post no Instagram	Usuários podem reportar para os administradores qualquer foto/vídeo postado na comunidade
E12	DP08	Permitir a edição de uma foto/vídeo	Usuários podem editar uma foto ou vídeo postados
E13			
	DP00	Instagram falha nessa estratégia	Nulo

A Figura 4 apresenta como algumas decisões do projetista podem aparecer na interface do aplicativo.

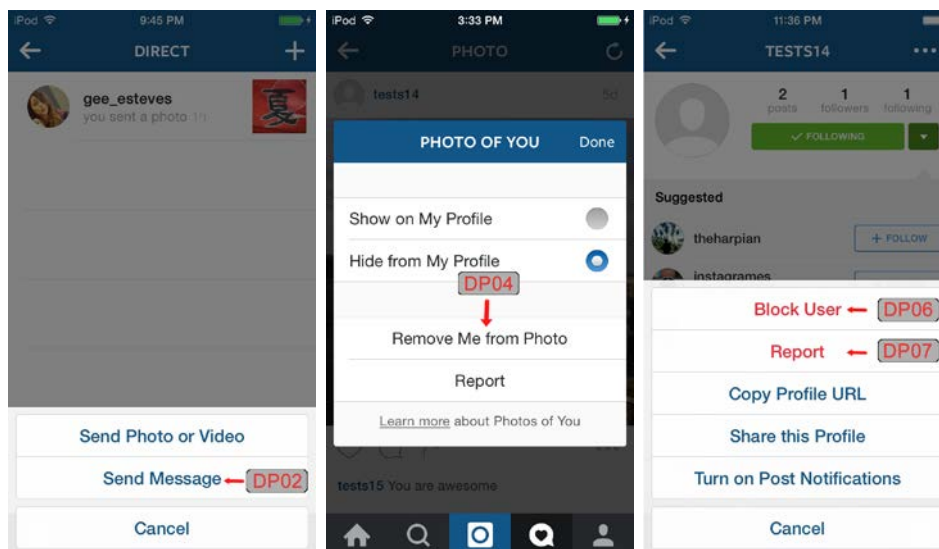


Figura 2 – Decisões do Projetista na interface do Instagram

6. Análise das Configurações de Privacidade do Instagram sob a Perspectiva dos Usuários

Com o objetivo de investigar junto aos usuários do Instagram se eles percebem e adotam as estratégias de privacidade identificadas na análise anterior, foi aplicado um questionário *online* composto por 14 questões de múltipla escolha. As questões foram divididas de tal forma que fosse possível caracterizar: (1) o perfil dos participantes da pesquisa, (2) se os usuários sentem-se seguros quando utilizam o aplicativo, e (3) quais as decisões do projetista são mais relevantes para manter os usuários seguros. O questionário ficou disponível para acesso durante uma semana, entre os dias 6 a 12 de Outubro de 2015. O mesmo foi divulgado por meio de redes sociais, e-mails e fóruns de discussões sobre o Instagram.

Ao todo 62 pessoas participaram da pesquisa. Dos participantes, cerca de 3% foram classificados na faixa etária entre 13 e 18 anos, 77% declararam estar na faixa entre 19 e 30 anos e 19% estão na faixa entre 31 e 55 anos. Embora houvesse as opções que representavam menores de 12 anos e maiores de 56 anos não foram obtidas respostas para esses perfis. Quanto às redes sociais utilizadas, além do Instagram, 97% utilizam o Facebook e o WhatsApp, 79% o Youtube, 71% o Twitter, e 53% o Google+. Outros 10% citaram outras redes sociais, tais como o SnapChat e o LinkedIn.

6.1. Análise das Configurações de Privacidade no Instagram

Inicialmente, os participantes foram questionados se eles se preocupam com questões de privacidade quando utilizam o Instagram, 82% dos participantes afirmaram se preocupar com essa questão durante o uso do aplicativo, enquanto 18% disseram não se importar com privacidade no Instagram.

Nesse sentido, os participantes foram questionados se conheciam as configurações de privacidade do Instagram e se sabem aplicá-las em seus perfis. Conforme demonstrado na Figura 3, embora a maioria (56%) dos participantes afirme conhecer e aplicar os recursos de privacidade em seus perfis, 44% afirmaram não adotar as configurações por razões como, por exemplo, a falta de conhecimento sobre sua existência ou sobre como acessá-las na interface.

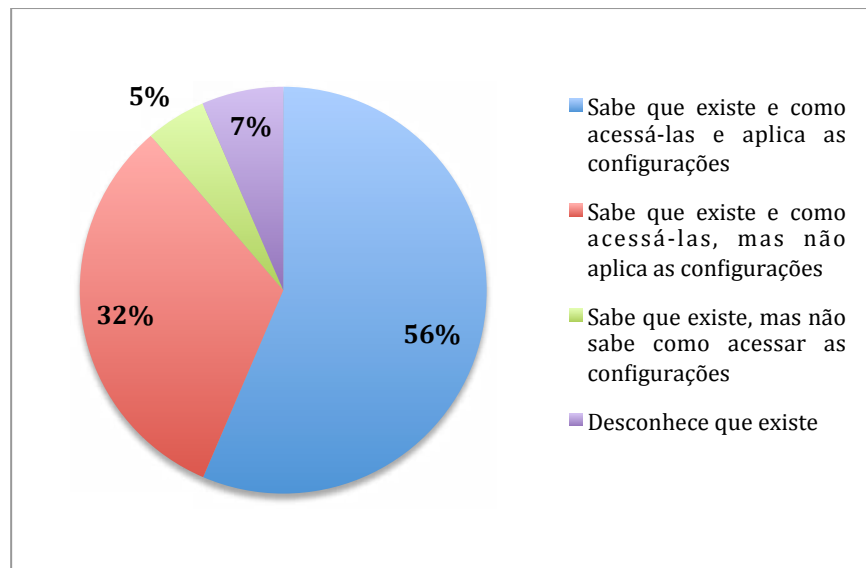


Figura 3 – Grau de conhecimento sobre as Configurações de Privacidade

Fonte: Dados da Pesquisa

Na sequência, os participantes que afirmaram aplicar as configurações de privacidade foram questionados sobre quais recursos eles utilizam. O gráfico da Figura 4 apresenta os resultados obtidos. É possível notar que a principal estratégia de privacidade adotada pelos usuários (42%) refere-se a configurar a visibilidade do perfil para privado. As demais opções são utilizadas por, no máximo, 37% dos participantes. Esse resultado chama atenção para o uso limitado que esses usuários têm feito das possibilidades que o Instagram oferece para resguardar a privacidade no aplicativo.

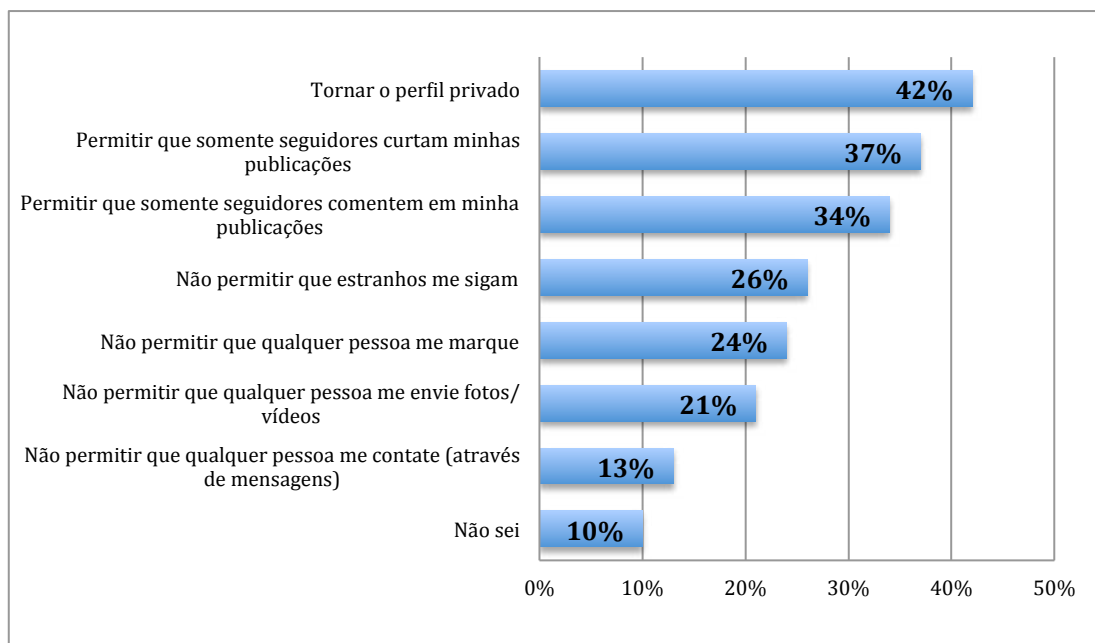


Figura 4 - Configurações de Privacidade do Instagram adotadas pelos Participantes

Fonte: Dados da pesquisa

6.2. Discussão dos Resultados

Como mostrado pela (Tabela 2), o Instagram adota 11 das 13 estratégias propostas pela literatura, ou seja, aproximadamente 85% das estratégias são atendidas. Esse pode ser considerado um fator positivo nesta rede social, porque como mostrado por [Young e Quan-Haase 2009][Jonhson *et al.* 2012], a adoção dessas estratégias pode favorecer para que o ambiente *online* se torne mais seguro. Contudo, o fato do Instagram não atender duas estratégias (E12 – Criar listas customizadas de contatos e E13 – Manter mais de uma conta) pode afetar aspectos de privacidade que deveriam ser considerados no design do aplicativo. Por exemplo, suponha que um usuário X poste uma foto pessoal para seus seguidores. Um usuário mal-intencionado que o segue no Instagram, toma posse daquele arquivo e o usa para prejudicar o usuário X de alguma forma, como por exemplo, postando a foto em um site para adultos denegrindo a imagem do usuário X. Entre as várias formas de evitar tal problema, a implementação de E12 poderia ter incentivado o usuário X a postar essa foto somente para seus amigos mais próximos [Strater e Lipford 2008].

A partir da análise das configurações de privacidade oferecidas pelo aplicativo, com a utilização que os usuários têm feito das configurações, nota-se que o recurso mais utilizado não atinge metade dos usuários (42% tornar o perfil privado). Isso indica que, embora o aplicativo disponibilize diversos recursos para garantir a privacidade de seus usuários, esses recursos têm sido usados de forma limitada, tornando as pessoas vulneráveis na rede. Uma hipótese para essa limitação de uso, é a falta de clareza na interface sobre como aplicar essas configurações nos perfis.

Dessa forma, a triangulação dos resultados indica que as estratégias existentes na literatura para endereçar privacidade podem ser úteis para oferecer recursos que potencializem a segurança dos usuários. No entanto, conforme já alertado por [Xavier *et al.* 2014][Rodrigues *et al.* 2012][Fong *et al.* 2009], e também evidenciado neste trabalho, esses recursos contribuem para privacidade somente quando são bem comunicados na interface, caso contrário, os usuários negligenciarão a utilização dos mesmos, e a possível segurança que tais recursos podem oferecer para membros de redes sociais *online* não serão aproveitadas em sua totalidade.

7. Conclusão

Este trabalho buscou apreciar e caracterizar as estratégias de privacidade adotadas em redes sociais e investigar se os usuários percebem e utilizam os recursos oferecidos. Os principais resultados apresentados e discutidos indicam que apesar do Instagram fazer uso da maioria das estratégias de privacidade, por meio das possibilidades de configurações oferecidas, os recursos disponíveis nem sempre são percebidos e utilizados através da interface.

Embora o estudo tenha sido realizado no Instagram, os resultados apresentados e discutidos são relevantes também para outros softwares sociais e/ou sistemas colaborativos que lidem, sobretudo com informações pessoais de usuários. A relevância deste tipo de investigação pode ser sustentada pelo argumento apresentado por [Willinger *et al.* 2010], onde os autores destacam a importância de apreciar e caracterizar as estratégias de interação, bem como a forma como diversos tipos de usuários estão interagindo, de forma a

verificar e endereçar os problemas que podem afetar na interação dos mesmos com esses sistemas [Willinger *et al.* 2010].

Sendo assim, esse artigo apresenta contribuições técnicas e científicas para as áreas de Sistemas Colaborativos, IHC e afins. Em termos científicos/metodológicos, os resultados do MIS reforçam a aplicabilidade do método, tendo em vista à sua fundamentação teórica, com o objetivo de identificar as estratégias de design, comunicadas na interface de sistemas colaborativos, que visam potencializar determinadas qualidades de uso, neste caso, a privacidade dos usuários. Em termos práticos, os resultados reportados, assim como as estratégias de privacidade identificadas neste trabalho, podem servir de parâmetros para a melhoria e/ou desenvolvimento de mecanismos de privacidade em redes sociais *online*. Além disso, essa pesquisa alerta os projetistas de interface sobre a importância de oferecer configurações de privacidade adequadas aos usuários em ambientes *online*.

Nesse sentido, como trabalhos futuros, poderia ser investigada a possibilidade de identificar signos na interface que permitem classificar as possibilidades de privacidade oferecidas por softwares sociais. Isso ajudaria no projeto e avaliação de outros sistemas/aplicativos que busquem manter seus usuários seguros. Além disso, seria interessante explorar como as estratégias de privacidade podem influenciar na interação do usuário.

Referências

- Barbosa, G. A. R.; Prates, R. O. e Corrê, L. 2011. Análise da sociabilidade de comunidades online para os usuários surdos: Um estudo de caso do orkut. In Proc. of the X IHC & CLIHC '11, (2011), 235-245.
- Barbosa, G. A. R.; Santos, G. E.; and Victor M. de O. Pereira, V. M. O. 2013. Caracterização qualitativa da sociabilidade no Facebook. In Proceedings of the 12th Brazilian Symposium on Human Factors in Computing Systems (IHC '13). Brazilian Computer Society, Porto Alegre, Brazil, Brazil, 72-81.
- comScore. 2015. The State of Social Media in Brazil and the Metrics that Really Matter. comScore Presentation. Disponível em: <https://goo.gl/l3dg8U>.
- Coutinho, F.; Prates, R. O.; Chaimowicz, L. An analysis of information conveyed through audio in an fps game and its impact on deaf players experience. In: IEEE. Games and Digital Entertainment (SBGAMES), 2011 Brazilian Symposium on. [S.l.], 2011. p. 53–62.
- de Souza, C.S. and Preece, J. 2004. A Framework for Analyzing and Understanding Online Communities. In: Interacting with Computers, Amsterdam, v. 16(3), (2004), 579-610.
- de Souza, C. S., Leitão, C. F., Prates, R. O., and da Silva, E. J. 2006. The semiotic inspection method. In: Proc. of IHC 2006, SBC, (2006), 148-157.
- de Souza, C. S., and Leitão, C. F. Semiotic engineering methods for scientific

- research in HCI. Morgan & Claypool Publishers, Editor: John M. Carroll, 2009.
- 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
- Fong, P. W., Anwar, M. and Zhao, Z. 2009. A privacy preservation model for facebook-style social network systems. In *Computer Security - ESORICS*, Springer Berlin Heidelberg, 303-320.
- Gill, A. J., Vasalou, A., Papoutsis, C., and Joinson, A. (2011) “Privacy Dictionary: A Linguistic Taxonomy of Privacy for Content Analysis”. In *Proceedings of CHI 2011*, Session: Privacy May 7-12, 2011, Vancouver, BC, Canada.
- Hull, G., Lipford, H. R. and Latulipe, C. 2011. Contextual gaps: privacy issues on Facebook. *Ethics and Inf. Technol.* 13, 4 (December 2011), 289-302.
- Instagram. 2015. Press News. Disponível em: <https://instagram.com/press/>
- Johnson, M., Egelman, S. and Steven M. Bellovin. 2012. Facebook and privacy: it's complicated. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. ACM, New York, NY, USA, , Article 9 , 15 pages.
- Junior, M. P., 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*, ACM, 63-72.
- Leitão, C. F., de Souza, F. C. S. and Barbosa, C. M. de A. 2007. Face-to-face sociability signs made explicit in CMC. In *Proc. of the 11th IFIP TC 13 international conference on Human-computer interaction (INTERACT'07)*, (2007), 5-18
- Liu, Y., Gummadi, K. P. and Mislove, A. 2011. Analyzing Facebook Privacy Settings: User Expectations vs Reality. In *Proceedings of Internet measurement conference*, ACM, 61-70.
- Peirce, C.S. *The Essential Peirce*. Indiana University Press, Bloomington, 1992.
- Prates, R. O., de Souza, C. S., Barbosa, S. D. J. 2000. A method for evaluating the communicability of user interfaces. *interactions*. 7(1), (2000), 31-38.
- Preece, J. 2001(a). *Online communities: Usability, Sociability, Theory and Methods*. In R. Earnshaw, R. Guedj, A. van Dam and T. Vince (Eds) *Frontiers of Human-Centred Computing, Online Communities and Virtual Environments*.
- Reis, S. de S. and Prates, R. O. 2011. Applicability of the Semiotic Inspection Method: a Systematic Literature Review. In: *Proc. of X IHC & V CLIHC'11*, (2011), 177-186.

- Rodrigues, K. R. H., Canal, M. C., Xavier, R. A. C., Alencar, T. S., and Neris, V. P. A. 2012. Avaliando aspectos de privacidade no Facebook pelas lentes de usabilidade, acessibilidade e fatores emocionais. In Companion Proceedings of the 11th Brazilian Symposium on Human Factors in Computing Systems (IHC '12).
- Silva, J. C. R.; Oliveira, E, R; and Barbora, G. A. R. Pereira, V. M. O. 2015. Caracterização de Estratégias de Gamificação em Aplicativos Móveis Educacionais: Um Estudo de Caso do Aplicativo Duolingo. In Proceedings of the 14th Brazilian Symposium on Human Factors in Computing Systems (IHC '15). Brazilian Computer Society, Porto Alegre, Brazil.
- Strater, C. and Lipford, H. R. 2008. Strategies and struggles with privacy in an online social networking community. In Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1 (BCS-HCI '08), Vol. 1. British Computer Society, Swinton, UK, UK, 111-119.
- Villella, M. L. B., and Prates, R. O. 2015. Supporting Designers in Modeling Privacy for Social Network Sites. In Proceedings of 15th Brazilian Symposium on Human Factors in Computing Systems. (IHC'15). November 03-06, 2015.
- Willinger, W., Rejaie, R., Torkjazi M., Valafar, M., Maggioni, M. 2010. Research on online social networks: time to face the real challenges. SIGMETRICS Perform. Eval. Rev. 37, 3, pp. 49--54 (2010)
- Xavier S. I. R., Maria L. B. Villela, Raquel O. Prates, Marcos O. Prates, Antônio A. P. Prates, and Alexandre A. Cardoso. 2014. Migrando das redes sociais offline para as redes sociais online: o que houve com a privacidade?. In Proceedings of the 13th Brazilian Symposium on Human Factors in Computing Systems (IHC '14). Sociedade Brasileira de Computação, Porto Alegre, Brazil, Brazil, 265-274.
- Young, A. L., and Quan-Haase A. 2009. Information revelation and internet privacy concerns on social network sites: a case study of facebook. In Proceedings of the fourth international conference on Communities and technologies (C&T '09). ACM, New York, NY, USA, 265-274.