Revista Gestão & Tecnologia
e-ISSN: 2177-6652
revistagt@fpl.edu.br
http://revistagt.fpl.edu.br/

Desenvolvimento e validação de um instrumento para mensurar a preocupação de usuários de smartphones sobre a invasão de privacidade

Yves Wanderley Estanislau da Costa Netto
Doutorando em Administração na área de Gestão de Sistemas e Tecnologia da Informação na Universidade Federal do Rio Grande do Sul
yves.costa@gmail.com

Vergílio Ricardo Ricardo Britto da Silva
Mestre em Administração pela Pontifícia Universidade Católica do Rio Grande do Sul PUCRS Analista de Processos Pleno na Coordenadoria de Planejamento e Gestão da Pró-Reitoria de Extensão e Assuntos Comunitários da PUCRS
vrbritto@gmail.com

Antônio Carlos Gastaud Maçada
Doutor em Administração pela Universidade Federal do Rio Grande do Sul; Visiting Scholar, UTEP, Texas, El Paso, USA (1999/2000); Professor, Texas A&M, College Station, USA (2011/2012); Especialização em Economia – Universidade Federal de Pelotas
acgmacada@ea.ufrgs.br

Editor Científico: José Edson Lara
Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em 19.02.2018
Aprovado em 10.08.2018

Resumo

O uso de *smartphones* cresceu de forma consistente ao longo dos últimos anos. Na medida que os aparelhos adquiriram novas funções, aumentou a sua capacidade de suportar serviços e aplicações. Preocupações sobre a privacidade durante o uso dos equipamentos como: coleta e armazenamento de dados, localização e uso de informações por terceiros sem autorização passaram a ser comuns entre os usuários. O presente artigo apresenta um questionário composto por cinco dimensões e dezesseis itens e tem como objetivo iniciar o processo de desenvolvimento e validação de uma escala para mensurar os fatores que influenciam a preocupação dos usuários sobre invasão de privacidade durante o uso de *smartphones*. Dentre as conclusões, verificou-se que a inclusão de duas dimensões que mensuram percepções positivas relacionadas ao uso dos aparelhos (Auto Eficácia e Benefício Percebido), pode contribuir para a mensuração de como os usuários avaliam as ameaças e benefícios ao usar os *smartphones*.

Palavras Chaves: Invasão de privacidade; Smartphones; Validação de instrumento de pesquisa.

Development and validation of an instrument to measure the concern of smartphone users on the privacy invasion

Abstract

The use of smartphones grew consistently over the past few years. To the extent that the appliances acquired new functions and increased its ability to support services and applications. Concerns about privacy during its use such as collection and storage of data, location, and use of information by third parties without authorization rose among users. This article presents a questionnaire composed of five dimensions and 16 items and aims to start the process of development and validation of a scale to measure the factors that influence users' concerns about invasion of privacy during the use of smartphones. Among the findings, we found that the inclusion of two dimensions that measure positive perceptions regarding the use of the equipment (Self-efficacy and perceived benefit), can contribute to the measurement of how the users assess the threats and benefits when using smartphones.

Keywords: Privacy Invasion; Smartphones; Survey Instrument Validation.

Desarrollo y validación de un instrumento para medir la preocupación de usuarios de smartphones sobre la invasión de privacidad

Resumen

El uso de smartphones creció de forma consistente a lo largo de los últimos años. A medida que los aparatos adquirieron nuevas funciones, aumentó su capacidad para soportar servicios y aplicaciones. Preocupaciones sobre la privacidad durante el uso de equipos como: recolección y almacenamiento de datos, ubicación y uso de informaciones por terceros desautorizados se volvieron comunes entre los usuarios. El presente artículo presenta una encuesta compuesta por cinco dimensiones y dieciséis ítems y tiene como objetivo iniciar el proceso de desarrollo y validación de una escala para medir los factores que influencian la preocupación de los usuarios sobre invasión de privacidad durante el uso de smartphones. Entre las conclusiones, se verificó

que la inclusión de dos dimensiones que miden percepciones positivas relacionadas con el uso de los aparatos (Auto Eficacia y Benefício Percibido), puede contribuir a la medición de cómo los usuarios evalúan las amenazas y beneficios al usarlos.

Palabras Claves: Invasión de privacidad; Smartphones; Validación del instrumento de investigación.

1. Introdução

O crescimento no uso de *smartphones* fez surgir questões relativas à privacidade durante o uso desses aparelhos. Em relatório recente da *Global System for Mobile Communications Association (GSMA)* — a entidade internacional que reúne as operadoras de telefonia móvel — e da AT Kearney — consultoria global em gestão de negócios — verificou-se que 8 entre 10 proprietários de telefones celulares tem preocupações com a privacidade dos dados que são disponibilizados ao usar os aparelhos (Computerworld, 2017).

Com o advento da era da alta tecnologia, a privacidade da informação tem se tornado de forma evidente, uma questão política, social e legal (Westin, 2003). Nesse contexto, a Tecnologia da Informação (TI) desponta como uma das áreas onde a privacidade é mais violada, e por outro lado onde tais violações são menos percebidas (Aaker, Kumar, & Day, 2008; Dogruel, Joeckel, & Vitak, 2017; Newell, 1995).

Uma das possíveis explicações para esse fato é a permeabilidade de diferentes tecnologias no cotidiano, como por exemplo, dispositivos móveis, assistentes digitais pessoais (PDAs) e telefones celulares, ampliando significativamente o acesso à informação e, concomitantemente, aumentando os riscos de invasão de privacidade (Acquisti, Brandimarte, & Loewenstein, 2015; Tan, 2014; Xu, 2007). Sob esse contexto, as transações que ocorrem nos meios eletrônicos tendem a deixar um número muito mais expressivo de registros residuais das ações dos usuários do que em meios que não dependem de soluções digitais (Akhter, 2014; Chellappa & Sin, 2005).

Os telefones celulares evoluíram ao longo dos anos, adquirindo novas funções e ampliando sua utilidade original (La Polla, Martinelli, & Sgandurra, 2013; Lynch, 2016). Essa evolução deu origem aos *smartphones*. Apesar de fisicamente distintos, esses dispositivos podem facilitar o acesso ao mesmo tipo de dados e a muitos dos serviços e aplicações suportadas pelos computadores convencionais (Acquisti et al., 2015; Botha, Furnell, & Clarke, 2009). Mais ainda, os aparelhos complementam e em alguns casos até ultrapassam, no que tange a

funcionalidade, dispositivos mais tradicionais como computadores de mesa e laptops (Chin, Felt, Sekar, & Wagner, 2012; Pennekamp, Henze, & Wehrle, 2017).

O crescimento na utilização dos smartphones trouxe também preocupações relativas ao uso não autorizado da informação fornecida pelos usuários (Ketelaar & van Balen, 2018). A informação pessoal no meio digital pode ser facilmente copiada, transmitida e integrada, o que por um lado pode ser benéfico pois oferece aos usuários um serviço mais personalizado, também aumenta os riscos de invasão de privacidade (Malhotra, Kim, & Agarwal, 2004).

Introna e Pouloudi (1999) destacam que uma linha tênue separa a necessidade em revelar informações para o benefício dos indivíduos e a preservação da privacidade dos mesmos, ao não permitir que tais informações sejam disponibilizadas. Verifica-se dessa forma a existência do paradoxo da privacidade (Kokolakis, 2017; Sutanto, Palme, Tan, & Phang, 2013; Xu, Li, Lau, Liao, & Fang, 2011).

Tal paradoxo apresenta vantagens e desvantagens para os usuários e as organizações, que buscam cada vez mais capturar as informações de seus clientes. Dentre as vantagens para as organizações, Dinev e Hart (2006) assinalam que os dados dos clientes se tornaram um dos principais ativos da economia digital, trazendo novas oportunidades para ampliar sua base de clientes, aumentar as taxas de retenção, personalizar os serviços e construir relacionamentos estratégicos.

Verifica-se no panorama atual que as práticas agressivas de acesso e transmissão de dados empregados por aplicações móveis e sistemas operacionais tornaram ainda mais preocupante a questão da privacidade dos usuários (Xu, Gupta, Rosson, & Carroll, 2012). Entretanto, a mensuração dos fatores que influenciam essas preocupações exige um instrumento confiável que possibilite relacionar atitudes com opções dos usuários sobre privacidade (Preibusch, 2013). Dentre os modelos propostos para mensurar tais preocupações destaca-se o modelo teórico *Mobile Users' Information Privacy Concerns* (MUIPC). O MUIPC consiste em um questionário de três dimensões e nove itens com o intuito de avaliar as preocupações sobre segurança de usuários de tais dispositivos (Xu et al., 2012).

Tendo em vista o supracitado, o objetivo do presente trabalho é iniciar o processo de desenvolvimento e validação de uma escala baseada no instrumento desenvolvido por Xu *et al.* (2012), com o propósito de mensurar os fatores que influenciam a preocupação dos usuários a respeito da invasão de privacidade durante o uso de *smartphones*. A motivação para o desenvolvimento do instrumento foi a afirmação de Xu *et al.* (2012) de que as pesquisas posteriores ao seu trabalho, poderiam examinar de que forma a relação custo-benefício

influencia os usuários no que diz respeito à tomada de decisão em fornecer informações pessoais durante o uso de telefones celulares.

Na seção seguinte é apresentado o referencial teórico relevante para o embasamento do estudo.

2. Referencial Teórico

2.1. A Privacidade e o Uso da Tecnologia

A privacidade é definida como o poder que um indivíduo possui para determinar quais informações sobre si devem ser conhecidas por terceiros (Westin, 2003). Sob esse aspecto, Pedersen (1997) assinala que a privacidade não significa evitar que o indivíduo conviva com os demais, mas sim, ter o controle do volume de contato com os outros. O controle da informação pessoal faz parte da privacidade do indivíduo (Newell, 1995). Verifica-se sua importância na medida que ao submeter informações pessoais, ele pode se sujeitar a grandes riscos (Malhotra *et al*., 2004).

Durante os 15 anos que sucederam a Segunda Guerra Mundial existia uma confiança elevada da sociedade em relação ao poder público e as organizações, a privacidade não figurava como uma preocupação relevante para as pessoas. Nos anos 70, os avanços nas tecnologias de vigilância contribuíram para a mudança desse quadro (Westin, 2003).

Orlikowski e Iacono (2001) assinalam que a sociedade tem se tornado dependente de um número cada vez maior de artefatos tecnológicos persuasivos e ao mesmo tempo invasivos. Carvalho e Vieira (2007, p. 90) apontam que "com a explosão das comunicações, a vigilância sobre os indivíduos se dá também sobre suas mensagens, sobre sua dinâmica de comunicação, como eles se movimentam no espaço informacional". O que se torna crítico ao passo que no atual estágio de desenvolvimento da internet, conhecido como Web 2.0 é possível obter diversos benefícios através do ambiente online como, por exemplo, a procura por relacionamentos afetivos, ofertas de empregos, comunicação gratuita, o que em muitas vezes implica em uma troca pela disponibilização de dados (Dienlin & Trepte, 2015; Preibusch, 2013).

Segundo Nov e Wattal (2009), é mais provável que usuários que tenham um maior nível de preocupação a respeito de privacidade na internet, sejam mais cautelosos ao acessar um determinado website ou um sistema. Haifeng Xu e Tan (2012), assinalam que durante o uso de

telefones móveis as atividades dos usuários e sua localização são ainda mais vigiadas, registradas e transmitidas para terceiros do que ao utilizarem computadores pessoais.

2.2. Do CFIP até o MUIPC: A Evolução dos Modelos para Mensurar as Preocupações sobre a Privacidade da Informação

Smith, Milberg, e Burke (1996), foram alguns dos autores pioneiros em pesquisas relativas à Preocupação com a Privacidade das Informações nas organizações. Os autores apontam que a coleta de dados por parte das empresas e o uso das informações pessoais, são as duas principais preocupações dos usuários. Junglas, Johnson, e Spitzmüller (2008), utilizaram as lentes da Teoria da Motivação para a Proteção, e verificaram que os fatores: (i) afabilidade, (ii) extroversão e (iii) abertura para novas experiências, exercem influência nas preocupações relativas à privacidade no contexto da adoção da TI.

Smith *et al*. (1996), desenvolveram o modelo *Concerns for Information Privacy* (CFIP) para identificar e mensurar as dimensões primárias das preocupações que os indivíduos têm a respeito da privacidade da informação nas organizações. O instrumento é composto por quatro dimensões com quinze itens. Stewart e Segars (2002) submeteram o instrumento a uma amostra de 355 consumidores de *shopping centers* americanos. Dentre as conclusões, verificaram que a percepção por parte dos consumidores de que suas informações seriam tratadas com cuidado e de maneira justa, influencia a CFIP. Na Tabela 1, estão expostas as dimensões do instrumento CFIP.

Tabela 1
Dimensões do Instrumento CFIP

Dimensões	Conceito
Coleta	O usuário se preocupa que grandes quantidades de dados identificáveis estão sendo coletados e armazenados em bancos de dados
Erros	O usuário se preocupa que proteções adotadas pelas empresas para resguardar os dados pessoais, não são efetivas
Uso secundário não autorizado	O usuário se preocupa que os dados coletados pelas empresas para uma finalidade, são utilizados para outros propósitos (internamente ou compartilhadas com terceiros externamente) sem a sua autorização
Acesso não autorizado	O usuário se preocupa que seus dados são facilmente acessíveis para indivíduos não autorizados

Fonte: Smith *et al*. (1996)

Com o crescimento do uso da internet pelo grande público, as atenções referentes à privacidade foram direcionadas para esse meio. Malhotra et al. (2004) propuseram o modelo *Internet Users' Information Privacy Concern* (IUIPC) para mensurar essa nova modalidade de

preocupação dos usuários em relação à invasão de privacidade. O IUIPC se refere ao nível de preocupação que os usuários da internet têm em relação à coleta de dados e uso de informações pessoais por parte das empresas que controlam os websites. Na Tabela 2, estão expostas as dimensões do instrumento IUIPC.

Tabela 2
Dimensões do Instrumento IUIPC

Dimensões	Conceito
Coleta	O quanto o usuário se preocupa com a quantidade de dados individuais específicos possuídas por outros, relativos ao valor dos benefícios recebidos.
Controle	O quanto o usuário se preocupa em não ter o controle adequado sobre suas informações pessoais na internet.
Consciência	O quanto o usuário se preocupa em saber sobre as práticas dos sites relativas à privacidade das informações.

Fonte: Malhotra *et al*. (2004)

O crescimento no uso de telefones móveis possibilitou ao usuário a flexibilização do acesso à internet e como consequência, aumentou também a produção e armazenamento de dados pessoais (Dehling & Sunyaev, 2014). Mais uma vez, as preocupações relativas à privacidade necessitaram de um novo instrumento para serem mensuradas. Para endereçar essas novas preocupações, Xu et al. (2012) desenvolveram o modelo *Mobile Users' Concerns for Information Privacy* (MUIPC). O instrumento tem por finalidade mensurar as preocupações dos usuários de telefones móveis a respeito da privacidade de suas informações durante o uso dos aparelhos. As três dimensões do modelo MUIPC são: a (i) Vigilância Percebida, a (ii) Intrusão Percebida e o (iii) Uso Secundário da Informação.

A Vigilância Percebida ocorre na medida que as atividades de coleta de dados por aplicativos móveis e sistemas operacionais induzem à percepção de que os dados pessoais estão sendo gravados de forma intensa ou que os fornecedores estão constantemente monitorando o comportamento do usuário através de *smartphones* (Lom, Thoo, Sulaiman, & Adam, 2018; Xu *et al*., 2012).

A intrusão percebida se caracteriza por envolver necessariamente um evento em que um indivíduo tem alguma informação pessoal acessada indevidamente (Xu, Zhang, Xue, & Yeo, 2008). Os ataques através de *malwares* estão entre os responsáveis pela intrusão em *smartphones*. Verifica-se que o menor poder computacional dos *smartphones* em relação ao dos computadores pessoais torna mais complexa a prevenção desses ataques (La Polla *et al.*, 2013).

O uso secundário da informação ocorre quando uma informação pessoal coletada para um propósito, é utilizada na sequência para outra finalidade. Enquanto o uso secundário da informação é amplamente utilizado e legal, também pode ser visto como uma invasão de privacidade quando ocorre sem o conhecimento ou o consentimento do usuário (Culnan, 1993; Solove, 2007). O uso secundário da informação é uma dimensão chave para a caracterização do MUIPC, e é também uma dimensão do CFIP (Xu *et al*., 2012).

Junglas *et al.* (2008), assinalam que apesar das preocupações relativas à privacidade exercerem um papel importante na utilização da TI, os fatores responsáveis por essa influência ainda são pouco conhecidos. Xu *et al.* (2012) apontam em suas conclusões que uma extensão no seu estudo poderia verificar o MUIPC em uma rede nomológica maior e sugerem que uma dessas possibilidades é averiguar a relação entre a troca da privacidade de dados pessoais por benefícios.

No presente momento em que as pessoas utilizam com maior frequência dispositivos móveis, verifica-se também a ocorrência do Paradoxo da Privacidade. Quanto antes os indivíduos percebem os benefícios que o uso de tais soluções tecnológicas oferece, e mais disfarçados estiverem os riscos percebidos, maior a probabilidade que disponibilizem informações pessoais durante o uso dos equipamentos (Kokolakis, 2017; Wilson & Valacich, 2012).

Sob esse aspecto, verifica-se que quando um serviço oferece um alto grau de personalização e interação, os consumidores percebem com maior clareza os seus benefícios (Dienlin & Trepte, 2015; Kinard & Capella, 2006). Dentro desse contexto, Acquisti e Grossklags (2005) afirmam que os indivíduos estão dispostos a trocar a privacidade por conveniência ou negociar a liberação de informações pessoais em troca de recompensas relativamente pequenas. Nesse contexto, em um estudo a respeito da intenção de compras online, Forsythe, Liu, Shannon, e Gardner (2006), concluem que os benefícios percebidos têm relação positiva com as intenções futuras dos usuários em visitar o *website* novamente e realizar compras.

A auto eficácia consiste no julgamento que um indivíduo tem de que irá conseguir executar uma ação e obter um determinado desempenho (Compeau & Higgins, 1995). A ênfase principal de algumas teorias motivacionais da auto-eficácia é no controle e não na competência do indivíduo. Sendo que competência é entendida como a experiência no controle e na motivação para estar no controle, o que diferencia as teorias motivacionais, das teorias voltadas para a orientação ao controle, presentes nas teorias cognitivas da auto eficácia (Gecas, 1989).

De forma resumida, a mensuração da auto eficácia tem o foco na capacidade do desempenho, e não em capacidades físicas e psicológicas dos indivíduos (Zimmerman, 2000). A crença na auto eficácia por parte de um indivíduo é um fator que influencia o seu comportamento (Davis, 1989), dessa forma Bandura (1977) ressalta que o grau de convicção do indivíduo na sua efetividade diante de determinada situação o torna propenso a decidir se irá sequer cooperar com ela ou não.

Luarn e Lin (2005) verificaram que a auto eficácia tem impacto positivo na percepção da facilidade no uso de transações digitais bancárias pelos telefones celulares. Sob outro aspecto, Akhter (2014), destaca que a auto eficácia do indivíduo no uso da internet, tem impacto na preocupação relativa à privacidade.

Segundo Gist (1987), um nível moderado à elevado de auto eficácia estimula no envolvimento mais frequente em atividades relacionadas com a tarefa e na persistência por maior tempo diante dos esforços envolvidos. Por sua vez, conduz a experiências de maior nível, que por sua vez contribuem para aumentar a auto eficácia. Mais especificamente em relação aos smartphones, Ketelaar e van Balen (2018) concluíram que a conscientização que os usuários adquirem pelo tempo de utilização, tem a capacidade em atenuar a relação entre as preocupações em relação a privacidade e o comportamento durante o uso dos aparelhos.

No que concerne os aspectos demográficos, diversos estudos apontam que usuários mais velhos tendem a se preocupar mais com à privacidade das informações do que os mais jovens. Entretanto, os estudos divergem em relação à influência do gênero nos níveis de preocupação relativas à privacidade das informações (Dehling & Sunyaev, 2014; Wang, Wang, Chen, Xie, & Lu, 2017).

Dentre os estudos que utilizaram o instrumento MUIPC como base, destaca-se a pesquisa de Degirmenci, Guhr, e Breitner (2013), em que os autores averiguaram a influência de quatro dimensões no que diz respeito ao acesso às informações pessoais no MUIPC, que são elas: (i) Identidade Pessoal, (ii) Localização, (iii) Conteúdo do Dispositivo e (iv) Configurações de Sistema e Rede. O estudo se distingue da pesquisa original de Xu *et al*. (2012), por mensurar o acesso às informações pessoais como um antecedente do MUIPC, enquanto no estudo original as experiências prévias dos usuários em relação à privacidade antecediam o MUIPC.

Dehling e Sunyaev (2014), propuseram um instrumento para mensurar as preocupações em relação à privacidade e a segurança de serviços de TI que dão apoio a pacientes hospitalares. Para realizar a pesquisa, utilizaram dimensões do CFIP e do MUIPC como por exemplo o uso

secundário de informações. No contexto dos pacientes hospitalares, o maior receio é o uso dessas informações por exemplo, por empresas de seguro ou na ocasião de uma possível promoção para o empregado. O acesso a essas informações pode ser usado de forma indevida e prejudicar o indivíduo.

O trabalho de Ryschka, Rodewyk, Ha, e Bick (2014), verificou as preocupações em relação à privacidade no uso de *smartphones*, no contexto dos serviços de localização geográfica desses aparelhos. Os autores verificaram que dentre as cinco principais preocupações, o uso secundário das informações e a vigilância percebida foram suportadas através do seu estudo qualitativo. Na seção seguinte está exposto o método de pesquisa.

3. Método de pesquisa

Esta pesquisa se caracteriza como descritiva. Pinsonneault e Kraemer (1993) assinalam que estudos desse tipo tem como propósito identificar opiniões que estão manifestas na população, bem como descrever a distribuição do fenômeno na própria população ou entre seus subgrupos.

A pesquisa foi realizada com corte transversal, sendo a coleta de dados realizada por meio de um questionário *survey* com uma escala *Likert* de cinco pontos, que segundo Pinsonneault e Kraemer (1993), tem como objetivo coletar informações sobre as características, ações ou opiniões de um grupo de pessoas, referido como população. Na escala, o valor 1 correspondia a “discordo totalmente”, enquanto o valor 5 a “concordo totalmente”.

Para atingir o objetivo da pesquisa foi utilizado como base três dimensões do instrumento desenvolvido por Xu *et al*. (2012), o qual foi traduzido e adaptado para o cenário brasileiro. Adicionalmente, foram incluídas duas dimensões desenvolvidas a partir da literatura. O instrumento final possui as seguintes dimensões: (i) vigilância percebida, (ii) intrusão percebida, (iii) uso secundário, (iv) auto eficácia e (v) benefício percebido.

Durante o processo de desenvolvimento e validação do instrumento, foi obedecida a recomendação de que para que se obtenha consistência interna satisfatória dos construtos, é necessário que ele possua ao menos três itens (Hinkin, 1998; Werts, Linn, & Jöreskog, 1974). Pelo fato do instrumento proposto ter sido adaptado a partir de um existente, foi necessário também iniciar a aplicação do questionário na fase pré-teste. Dessa forma, foi possível aferir se o instrumento possuía inconsistências que inviabilizariam a continuidade da pesquisa (Oppenheim, 2000).

A população-alvo do estudo foram estudantes universitários, sendo que foi utilizada uma amostra por conveniência ou não probabilística. Ainda que tenha se optado por esse tipo de amostra, Xu *et al.* (2012), afirmam que estudantes universitários representam apropriadamente os usuários de *smartphones*. O instrumento foi aplicado em uma amostra de 244 usuários de *smartphones* em uma universidade brasileira. As coletas — tanto para a fase de pré-teste do instrumento como para a de coleta dos dados final — foram realizadas em novembro de 2015.

Na fase pré-teste, foram obtidas 41 respostas de alunos e funcionários de um curso pré-vestibular. Posteriormente, o questionário foi submetido à alunos da universidade referida. Em uma fase inicial foram removidos os questionários que não possuíam respostas e os *outliers*, caracterizados por questionários com concentração de respostas em uma mesma escala. Na base depurada obteve-se um total de 231 questionários válidos, resultando numa taxa de respostas válidas de 94,6 %.

Os dados foram analisados seguindo os passos recomendados por Koufteros (1999). Inicialmente os dados foram tabulados no software de planilha eletrônica Excel. O software estatístico SPSS foi utilizado para a análise de dados.

4. Análise e discussão dos resultados

Os principais resultados dessa pesquisa são discutidos nessa seção. Na subseção seguinte é apresentado perfil demográfico dos respondentes e suas características em relação à experiência prévia com invasão de privacidade.

4.1. Caracterização dos Respondentes

A primeira análise da base de dados final apresenta os dados sócio demográficos dos respondentes. Conforme pode ser verificado na Tabela 3, 54,73% dos respondentes possui graduação e apenas 1,7% possui pós-graduação. Por outro lado, 26,41% responderam afirmativamente quando questionados se haviam experimentado alguma situação em que se sentiram prejudicados por terem a sua privacidade invadida. Enquanto 76,2% responderam que possuem conhecimento sobre o prejuízo para a privacidade que podem estar sujeitos caso suas informações pessoais coletadas a partir da internet sejam utilizadas. Quando questionados se conheciam alguma pessoa que havia sido prejudicada por crimes de invasão da privacidade a partir de dados coletados na internet, 44,16% responderam afirmativamente.

Os dados referentes a idade, gênero, grau de instrução, e as questões relativas à experiência prévia dos respondentes em relação à privacidade foram compilados na Tabela 3. Destaca-se dentre os dados, a faixa etária preponderante dos respondentes. Do total de 231, um percentual de 83,54% tem entre 20 e 30 anos.

Tabela 3

Perfil Demográfico dos Respondentes e Experiência Prévia com Privacidade no Uso de Smartphones

Perfil Demográfico e Caraterísticas de Uso de Smartphones	Número	Porcentagem
Gênero		
Masculino	**121**	**52,38**
Feminino	110	47,62
Idade (anos)		
20 ⊦ 25	**95**	**41,12**
25 ⊦ 30	**98**	**42,42**
30 ⊦ 35	17	7,35
35 ⊦ 40	12	5,19
40 ⊦ 45	5	2,16
45 ⊦ 50	1	0,43
50 ⊦ 70	3	1,42
Grau de Instrução		
Segundo Grau completo	104	45
Graduação	**123**	**54,7**
Pós-graduação	4	1,7
Você já se sentiu prejudicado por ter sua privacidade invadida em meios eletrônicos		
Sim	60	26,41
Não	**171**	**73,59**
Você tem conhecimento sobre o potencial prejuízo que o uso indevido das suas informações pessoais coletadas a partir da Internet pode causar a sua privacidade?		
Sim	**176**	**76,2**
Não	55	23,8
Você conhece alguém que foi prejudicado por crime de invasão de privacidade a partir de dados coletados na internet?		
Sim	102	44,16
Não	**129**	**55,84**

Fonte: Dados da Pesquisa (2015)

Na seção seguinte é apresentado o processo de validação do instrumento a partir das dimensões do instrumento de Xu *et al*. (2012) e dos construtos "Auto Eficácia e Benefício Percebido.

4.2. Validação do Instrumento

A fase pré-teste teve início com a verificação e remoção de *outliers*. Na sequência, foi calculado o Alfa de Cronbach do instrumento. O coeficiente obtido de 0,824, portanto, acima de 0,7, indica a confiabilidade do instrumento (Hair Jr, Gabriel, & Patel, 2014). Concomitantemente, foi aferida a correlação de item-total corrigido (CITC) dos itens. Dois deles, apresentaram CITC inferior a 0,300 e foram mantidos, contrariando as recomendações de Pedhazur e Schmelkin (1991). Nesse caso, foi seguida a orientação de Koufteros (1999), de que apesar da retirada de um item que apresenta CITC inferior a 0,300 tornar o modelo mais robusto, também retira dele a capacidade de mensuração que o item ofereceria.

A segunda justificativa para a inclusão de tais itens se deve à natureza exploratória da pesquisa. O terceiro ponto considerado para a manutenção dos dois itens foi a recomendação de Werts *et al*. (1974) de que são necessários ao menos três itens por construto para que seja possível realizar a análise fatorial exploratória, permitindo a existência de graus de liberdade satisfatórios para que se verifique a unidimensionalidade deles. Esse passo adquire uma importância ainda mais pronunciada na medida que o cálculo do alfa de Cronbach é efetuado assumindo-se a unidimensionalidade dos construtos (Gerbing & Anderson, 1988).

Na etapa seguinte, foi executado o teste de KMO, o que indica se a amostra é adequada, e o teste de esfericidade de Bartlett. O KMO aferido foi de 0,625. Coeficientes acima de 0,6 indicam a adequação da amostra para proceder a análise fatorial (Malhotra, 2012). O teste de esfericidade de Bartlett foi significativo a .000 e obteve-se um índice de 332,196. O teste avalia a presença de correlação entre os itens. Diante de ambos os resultados, verifica-se que a análise fatorial exploratória poderia ser executada (Norusis, 1993).

Após a análise de confiabilidade e fidedignidade do instrumento, a verificação da adequação da amostra permitiu que se desse o prosseguimento à execução da análise fatorial nos blocos. Nessa fase, verificou-se que todos os itens que compõe cada construto, mensuram apenas uma dimensão.

Na Tabela 4, verifica-se o intervalo de CITC dos itens assim como o coeficiente de Alfa de Cronbach por construtos para averiguar a consistência interna do questionário.

Tabela 4
CITC dos itens e Alfa de Cronbach dos construtos na Fase Pré-Teste

Construtos	Número de Itens	Instrumento na Fase Pré-Teste	Alfa de Cronbach
Vigilância Percebida	3	0,23-0,60	0,717
Intrusão Percebida	3	0,52-0,60	0,817
Uso Secundário	3	0,55-0,61	0,834
Auto eficácia	4	0,14-0,35	0,743
Benefício Percebido	3	0,37-0,47	0,741

Fonte: Dados da Pesquisa (2015)

Na amostra final, a relação entre respondentes e questionários é de 14,44 por itens, acima da recomendação de Hair Jr et al. (2014), que aponta que a relação deve ser de 5 a 10 respondentes por itens, e de Kline (2011) que defende que o estudo das equações estruturais necessita de pelo menos 200 respondentes. Hinkin (1998) assinala que 150 observações deveriam ser suficientes para que se obtenha um resultado confiável na análise fatorial exploratória, desde que a correlação dos itens seja razoavelmente forte.

Com a base de dados devidamente transposta para o meio digital, uma nova verificação da fidedignidade do instrumento foi feita com a amostra total de respondentes. Foi utilizado o software estatístico SPSS para a execução de todas as análises anteriores e posteriores. O alfa de Cronbach do instrumento final dessa vez foi de 0,826 e apenas um dos itens apresentou CITC inferior a 0,300.

O item foi mantido no instrumento final. Verificou-se um ligeiro aprimoramento no coeficiente de Alfa de Cronbach e no CITC dos itens (com exceção do item "Auto eficácia 4"). Nesse item, os respondentes deveriam apontar o grau de concordância com a afirmação de que possuíam conhecimento sobre os tipos de crime de invasão de privacidade que podem ser cometidos a partir dos dados disponibilizados durante o uso do *smartphone*

Na Tabela 5 são apresentados os itens que compõe os construtos e suas cargas latentes. Adicionalmente são apresentados o coeficiente de confiabilidade composta, o alfa de Cronbach e a variância média extraída de cada dimensão.

Tabela 5
Cargas Latentes, Variância Média Extraída e Confiabilidade Composta de Itens e Construtos

Construto/Dimensão/Item	Cargas latentes	valor-t*	AC[a]	CC[b]	VME[c]
Intrusão Percebida (IP)			0,83	0,898	0,747
Eu sinto que, como resultado da minha utilização de aplicativos do celular, terceiros tem acesso a mais informações sobre mim do que eu gostaria. (IP1)	,702	39,914			
Eu acredito que, como resultado da minha utilização de aplicativos do celular, informações que eu considero privadas sobre mim, estão agora mais facilmente disponíveis para terceiros do que eu gostaria. (IP2)	,787	40,476			
Eu sinto que, como resultado da minha utilização de aplicativos do celular, minha privacidade pode ser invadida. (IP3)	,850	42,638			
Uso Secundário das Informações (US)			0,82	0,892	0,733
Eu me preocupo que os aplicativos do celular possam usar minhas informações pessoais para outros fins sem me avisar previamente ou mesmo sem receber minha autorização (US1)	,718	42,366			
Quando forneço informações pessoais para utilizar aplicativos do celular, me preocupo que tais aplicativos possam usar minhas informações para outros fins (US2)	,812	45,095			
Eu me preocupo que os aplicativos do celular possam compartilhar as minhas informações pessoais com terceiros sem receber a minha autorização (US3)	,825	45,123			
Vigilância Percebida (VP)			0,76	0,762	0,620
Eu me preocupo que a localização do meu telefone celular esteja sendo monitorada por pelo menos uma parte do tempo de uso do aparelho. (VP1)	,856	37,719			
Eu me preocupo que os aplicativos do meu telefone celular estejam recolhendo uma grande quantidade de informações sobre mim. (VP2)	,498	36,864			
Eu me preocupo que os aplicativos do meu telefone celular possam ser usados para monitorar minhas atividades durante o uso do aparelho. (VP3)	,622	37,464			
Benefício Percebido (BP)			0,77	0,775	0,552
Eu acredito que a acessibilidade proporcionada por aplicativos para comunicação no celular facilita a maneira como me comunico. (BP1)	,790	46,168			
Eu sinto que a acessibilidade proporcionada por aplicativos de comunicação no celular, facilita a maneira como me comunico. (BP2)	,881	37,061			
Eu sinto que a acessibilidade proporcionada por aplicativos de comunicação no celular estimulam a me comunicar pelo aparelho. (BP3)	,776	39,346			
Auto Eficácia (AE)			0,82	0,705	0,52
Você tem conhecimento do tipo de autorização que está fornecendo a partir do aceito dos termos de uso dos aplicativos no seu smartphone (AE1)	,762	29,029			
Você sabe como se prevenir para que os aplicativos do seu smartphone não compartilhem seus dados com terceiros (AE2)	,837	27,870			
Você tem conhecimento sobre como atuar na necessidade de reparação de dano a sua privacidade	,866	28,470			

cometida a partir dos dados disponibilizados no seu smartphone (AE3)		
Você tem conhecimento sobre os tipos de crime de invasão de privacidade que podem ser cometidos a partir dos dados disponibilizados no seu smartphone (AE4)	,738	35,865

Fonte: Dados da Pesquisa (2015)
Nota: a – Alfa de Cronbach; b – Confiabilidade Composta; c – Variância Média Extraída

* valor t para teste de duas caudas: * 1.96 (nível de significância:95%)

O alfa de Cronbach e o coeficiente de confiabilidade composta são os dois métodos mais utilizados para avaliar a confiabilidade interna e o grau de consistência das respostas entre os itens (Fornell & Larcker, 1981; Kline, 2011) e indicam que os itens de cada construto convergem no sentido de medir apenas a uma dimensão (Hair, Babin, Money, & Samouel, 2005).

Nos resultados apresentados na Tabela 5, tanto o alfa de Cronbach quanto os coeficientes de confiabilidade composta apresentam índices superiores a 0,70 para todos os construtos, o que indica a boa confiabilidade do instrumento proposto (Fornell & Larcker, 1981; Hair, Black, Babin, Anderson, & Tatham, 1998).

A validade convergente foi analisada pelos coeficientes da Variância Média Extraída (VME) de cada variável latente. O coeficiente para cada variável latente deve ser superior a 0,5, indicando que há mais variância do que erro no construto analisado (Hair et al., 1998; Koufteros, 1999). Dessa forma, verifica-se que os indicadores do questionário mensuram no mínimo a metade da variabilidade da variável latente.

O segundo critério de mensuração utilizado se refere ao peso de cada indicador na variável latente a que se destina, devendo ser superior a 0,71 (raiz quadrada de 0,5) (Lewis & Byrd, 2003). Verifica-se dessa forma, que o indicador contribui com pelo menos metade de sua variância para a composição da variável latente.

As cargas dos indicadores dos construtos devem ser maiores nos próprios construtos a serem medidos, do que nos outros construtos. Os resultados dispostos na Tabela 6 demonstram a análise dos componentes principais usando a Rotação Varimax em que constam as cargas dos indicadores.

Tabela 6
Resultado da Análise dos Componentes Principais usando a Rotação Varimax

Itens	Vigilância Percebida	Intrusão Percebida	Uso Secundário	Auto Eficácia	Benefício Percebido
VIPER1	0,856	0,182	0,054	0,049	-0,054
VIPER2	0,498	0,315	0,570	0,094	-0,042
VIPER3	0,622	0,254	0,551	0,039	0,092
INPER1	0,294	0,702	0,307	-0,043	0,046
INPER2	0,139	0,787	0,378	-0,003	0,112
INPER3	0,097	0,850	0,188	0,064	0,092
USSEC1	0,008	0,417	0,718	-0,059	0,127
USSEC2	0,302	0,110	0,812	0,081	0,112
USSEC3	-0,076	0,283	0,825	0,046	0,024
AUTOE1	0,086	0,124	0,049	0,762	0,026
AUTOE2	0,021	0,045	0,028	0,837	-0,051
AUTOE3	0,061	-0,038	0,007	0,866	0,108
AUTOE4	-0,055	-0,095	0,017	0,738	0,086
BENPC1	0,249	-0,035	-0,044	0,080	0,790
BENPC2	-0,057	0,131	0,050	0,039	0,881
BENPC3	-0,256	0,139	0,241	0,054	0,776

Fonte: Dados da Pesquisa (2015)

Na Tabela 7, estão dispostos os autovalores, que correspondem a soma das cargas dos fatores ao quadrado, assim como a porcentagem de variância explicada de cada fator e sua porcentagem cumulativa.

Verifica-se dessa forma que os fatores demonstram grande poder de explicação da variância pelo instrumento.

Tabela 7
Análise Fatorial Intrabloco

Construtos	Autovalores (Soma dos quadrados das cargas)	% Variância Explicada	% Variância Explicada Cumulativa
Vigilância Percebida	1,724	10,777	10,777
Intrusão Percebida	2,363	14,772	25,549
Uso Secundário	2,825	17,657	43,206
Auto Eficácia	2,618	16,360	59,566
Benefício Percebido	2,089	13,054	72,62

Fonte: Dados da Pesquisa (2015)

A validade discriminante foi verificada pela mensuração da relação entre a raiz quadrada da variância média extraída (VME) e a correlação entre os fatores. A raiz quadrada da VME de uma variável latente deve ser maior que as correlações com as demais variáveis latentes,

indicando que os indicadores que medem uma das variáveis latentes não se confundem com as demais (Fornell & Larcker, 1981). A raiz quadrada da VME é representada pelos valores na diagonal. Os resultados obtidos estão expostos na Tabela 8. Adicionalmente verificam-se a média e o desvio padrão dos construtos.

Tabela 8
Correlações entre as Variáveis Latentes

Construtos latentes	Construtos latentes				
	AE	**BP**	**IP**	**US**	**VP**
Auto Eficácia (AE)	**0,801**				
Benefício Percebido (BP)	0,121	**0,825**			
Intrusão Percebida (IP)	0,052	0,216	**0,865**		
Uso Secundário de Informações (US)	0,083	0,240	0,621	**0,856**	
Vigilância Percebida (VP)	0,129	0,075	0,592	0,616	**0,830**
Média	2,580	3,283	3,430	3,711	3,373
D.P.	1,269	1,231	1,243	1,249	1,349

Fonte: Dados da Pesquisa (2015)

Os valores da raiz quadrada da VME dos construtos, dispostos nas diagonais são superiores aos valores das correlações entre os construtos, indicando a adequação em relação à validade discriminante.

Na última seção são apresentadas as principais conclusões da pesquisa.

5. Considerações Finais

O objetivo da pesquisa foi atingido ao passo que os resultados obtidos indicam que a inclusão de duas dimensões baseadas na literatura pode contribuir para a elaboração de novos instrumentos para auxiliar pesquisadores interessados em investigar o comportamento dos usuários de *smartphones* no que diz respeito às preocupações com a invasão de privacidade. O escopo do trabalho não foi a proposição de um modelo. Entretanto, a validação do instrumento com as duas dimensões propostas pode oferecer aos pesquisadores dessa área uma nova vertente a ser explorada na busca da compreensão de como ocorre o paradoxo da privacidade durante o uso de smartphones

Apesar dos resultados da validade convergente, discriminante e a verificação da unidimensionalidade dos construtos indicarem que o instrumento é adequado para a mensuração daquilo que se propõe, durante a fase pré-teste, os coeficientes CITC de dois itens não alcançaram o índice mínimo defendido pela literatura (Pedhazur & Schmelkin, 2013). Após

a análise dos componentes principais, a dimensão "Vigilância Percebida" apresentou dois itens com cargas inferiores a 0,71, o que demonstra que o critério para explicação de pelo menos metade da variância do indicador, não foi satisfeito. Além desse item, um dos itens da dimensão "Intrusão Percebida" também não satisfez ao mesmo critério.

O índice de CITC inferior a 0,300 de dois itens na fase pré-teste e um no instrumento fina, podem ter sido influenciados pela diferença cultural do questionário ao aplicá-lo no contexto sociocultural brasileiro. Pelo fato da escala utilizada como base ter sido traduzida e adaptada para a língua portuguesa é possível que tenha ocorrido alguma discrepância por diferenças culturais e pelo viés do tradutor. Para averiguar essa questão, em pesquisas futuras seria importante fazer a tradução da escala final para o inglês e submeter a um nativo da língua inglesa para a validação.

Com relação às limitações do trabalho, pode ser citada a submissão do questionário apenas a uma amostra por conveniência, o que impede que a pesquisa possa ser generalizada. Outra limitação foi não incluir o construto "intenção comportamental" do MUIPC que verifica a intenção do usuário em fornecer informações pessoais no uso do aparelho nos próximos 12 meses.

No que concerne as pesquisas futuras, a inclusão de novos itens por construto pode aprimorar o instrumento. Um número maior de itens permitirá aferir quais representam com maior fidedignidade cada dimensão, remover aqueles que apresentarem os menores índices CITC e aumentar a variância explicada por construto. Posteriormente, uma nova análise dos componentes principais possibilitará aumentar a variância explicada no conjunto de dados (Hair *et al*., 2005).

O trabalho de Degirmenci *et al*. (2013), apresenta o acesso às informações pessoais como um antecedente do MUIPC. De forma análoga, a pesquisa de Ryschka et al. (2014) e de Dehling e Sunyaev (2014), apontam que o uso de informações pessoais é um dos fatores que mais influenciam nas preocupações dos usuários relativas à privacidade das informações. Uma possibilidade para novas pesquisas é verificar se as dimensões propostas pelo presente trabalho, Auto Eficácia e Benefício Percebido, atuam como moderadores no MUIPC. A depuração do instrumento e a sua aplicação em amostras representativas em abrangência nacional, podem contribuir para a compreensão dos fatores que influenciam a preocupação de usuários de *smartphones* em relação a privacidade no cenário brasileiro. Para aferir tais questões, novas pesquisas serão necessárias.

Referências

Aaker, D. A., Kumar, V., & Day, G. S. (2008). *Marketing research*: John Wiley & Sons.

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

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy, 3*(1), 26-33.

Akhter, S. (2014). Privacy concern and online transactions: the impact of internet self-efficacy and internet involvement. *Journal of Consumer Marketing, 31*(2), 118-125.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review, 84*(2), 191.

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2009). From desktop to mobile: Examining the security experience. *Computers & Security, 28*(3-4), 130-137.

Carvalho, C. A., & Vieira, M. M. F. (2007). *O poder nas organizações*: Thomson.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information technology and management, 6*(2-3), 181-202.

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). *Measuring user confidence in smartphone security and privacy.* Paper presented at the Proceedings of the Eighth Symposium on Usable Privacy and Security.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *Mis Quarterly*, 189-211.

Computerworld. (2017, 09 Abr. 2017). Mais privacidade e segurança nas comunicações móveis envolve decisões políticas, diz estudo. Retrieved 20 Jul. 2018, 2018, from http://computerworld.com.br/2017/4/9/mais-privacidade-e-seguranca-nas-comunicacoes-moveis-envolve-decisoes-politicas-diz-estudo

Culnan, M. J. (1993). " How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *Mis Quarterly*, 341-363.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Mis Quarterly*, 319-340.

Degirmenci, K., Guhr, N., & Breitner, M. H. (2013). Mobile applications and access to personal information: A discussion of users' privacy concerns.

Dehling, T., & Sunyaev, A. (2014). *Information Security and Privacy of Patient-Centered Health IT Services: What Needs to Be Done?* Paper presented at the System Sciences (HICSS), 2014 47th Hawaii International Conference on.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297.

Dinev, T., & Hart, P. (2006). Privacy concerns and levels of information exchange: An empirical investigation of intended e-services use. *E-Service, 4*(3), 25-60.

Dogruel, L., Joeckel, S., & Vitak, J. (2017). The valuation of privacy premium features for smartphone apps: The influence of defaults and expert recommendations. *Computers in Human Behavior*.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of marketing research*, 382-388.

Forsythe, S., Liu, C., Shannon, D., & Gardner, L. C. (2006). Development of a scale to measure the perceived benefits and risks of online shopping. *Journal of Interactive Marketing, 20*(2), 55-75.

Gecas, V. (1989). The social psychology of self-efficacy. *Annual review of sociology, 15*(1), 291-316.

Gerbing, D. W., & Anderson, J. C. (1988). An updated paradigm for scale development incorporating unidimensionality and its assessment. *Journal of marketing research*, 186-192.

Gist, M. E. (1987). Self-efficacy: Implications for organizational behavior and human resource management. *Academy of management review, 12*(3), 472-485.

Hair, J., Babin, B., Money, A., & Samouel, P. (2005). *Fundamentos de métodos de pesquisa em administração*: Bookman Companhia Ed.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (1998). *Multivariate data analysis* (Vol. 5): Prentice hall Upper Saddle River, NJ.

Hair Jr, J. F., Gabriel, M. L. D. d. S., & Patel, V. K. (2014). Modelagem de Equações Estruturais Baseada em Covariância (CB-SEM) com o AMOS: Orientações sobre a sua aplicação como uma Ferramenta de Pesquisa de Marketing. *REMark, 13*(2), 43.

Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questionnaires. *Organizational research methods, 1*(1), 104-121.

Introna, L., & Pouloudi, A. (1999). Privacy in the information age: Stakeholders, interests and values. *Journal of Business Ethics, 22*(1), 27-38.

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387-402.

Ketelaar, P. E., & van Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior, 78*, 174-182.

Kinard, B. R., & Capella, M. L. (2006). Relationship marketing: the influence of consumer involvement on perceived service benefits. *Journal of Services Marketing, 20*(6), 359-368.

Kline, R. B. (2011). *Principles and Practice of Structural Equation Modeling* (3rd ed.): Guilford Press.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134. doi: https://doi.org/10.1016/j.cose.2015.07.002

Koufteros, X. A. (1999). Testing a model of pull production: a paradigm for manufacturing research using structural equation modeling. *Journal of Operations Management, 17*(4), 467-488.

La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. *IEEE communications surveys & tutorials, 15*(1), 446-471.

Lewis, B. R., & Byrd, T. A. (2003). Development of a measure for the information technology infrastructure construct. *European Journal of Information Systems, 12*(2), 93-109.

Lom, H. S., Thoo, A. C., Sulaiman, Z., & Adam, S. (2018). Moderating Role of Mobile Users' Information Privacy Concerns Towards Behavioural Intention and Use Behaviour in Mobile Advertising. *Advanced Science Letters, 24*(6), 4259-4264. doi: 10.1166/asl.2018.11584

Luarn, P., & Lin, H.-H. (2005). Toward an understanding of the behavioral intention to use mobile banking. *Computers in Human Behavior, 21*(6), 873-891.

Lynch, M. (2016, 19 Feb. 2016,). Leave My IPhone Alone: Why Our Smartphones Are Extensions of Ourselves., from www.theguardian.com/technology/2016/feb/19/iphone-apple-privacy-smartphones-extension-of-ourselves.

Malhotra, N. K. (2012). *Pesquisa de marketing: uma orientação aplicada*: Bookman Editora.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research, 15*(4), 336-355.

Newell, P. B. (1995). Perspectives on privacy. *Journal of Environmental Psychology, 15*(2), 87-104.

Norusis, M. J. (1993). *SPSS: SPSS for Windows, base system user's guide release 6.0*: SPSS Inc.

Nov, O., & Wattal, S. (2009). *Social computing privacy concerns: antecedents and effects.* Paper presented at the Proceedings of the SIGCHI conference on human factors in computing systems.

Oppenheim, A. N. (2000). *Questionnaire design, interviewing and attitude measurement*: Bloomsbury Publishing.

Orlikowski, W. J., & Iacono, C. S. (2001). Research commentary: Desperately seeking the "IT" in IT research—A call to theorizing the IT artifact. *Information systems research, 12*(2), 121-134.

Pedersen, D. M. (1997). Psychological functions of privacy. *Journal of Environmental Psychology, 17*(2), 147-156.

Pedhazur, E. J., & Schmelkin, L. P. (1991). Measurement, design, and analysis: An integrated analysis: Hillsdale: Erlbaum.

Pedhazur, E. J., & Schmelkin, L. P. (2013). *Measurement, design, and analysis: An integrated approach*: Psychology Press.

Pennekamp, J., Henze, M., & Wehrle, K. (2017). A survey on the evolution of privacy enforcement on smartphones and the road ahead. *Pervasive and Mobile Computing*.

Pinsonneault, A., & Kraemer, K. (1993). Survey research methodology in management information systems: an assessment. *Journal of management information systems, 10*(2), 75-105.

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies, 71*(12), 1133-1143.

Ryschka, S., Rodewyk, B., Ha, K.-H., & Bick, M. (2014). A qualitative investigation of risk perceptions in the case of check-in services.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *Mis Quarterly*, 167-196.

Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev., 44*, 745.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information systems research, 13*(1), 36-49.

Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *Mis Quarterly, 37*(4).

Tan, C. (2014). *Empirical Study on Acceptance Level of Mobile Transaction Due To Privacy Invasion*: eprints.intimal.edu.my.

Wang, C., Wang, C., Chen, Y., Xie, L., & Lu, S. (2017). *Smartphone Privacy Leakage of Social Relationships and Demographics from Surrounding Access Points.* Paper presented at the Proceedings - International Conference on Distributed Computing Systems.

Werts, C. E., Linn, R. L., & Jöreskog, K. G. (1974). Intraclass reliability estimates: Testing structural assumptions. *Educational and Psychological measurement, 34*(1), 25-33.

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

Wilson, D., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus.

Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. *ICIS 2007 proceedings*, 125.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy.

Xu, H., & Tan, B. C. Y. (2012). Why Do I Keep Checking Facebook: Effects of Message Characteristics On the Formation of Social Network Services Addiction. *ICIS 2012 Proceedings*.

Xu, K., Li, J., Lau, R., Liao, S., & Fang, B. (2011). An Effective Method of Discovering Target Groups on Social Networking Sites. *ICIS 2011 Proceedings*.

Xu, Y., Zhang, C., Xue, L., & Yeo, L. L. (2008). Product Adoption in Online Social Network. *ICIS 2008 Proceedings*.

Zimmerman, B. J. (2000). Self-efficacy: An essential motive to learn. *Contemporary educational psychology, 25*(1), 82-91. doi: 10.1006/ceps.1999.1016