XXI SEMEAD
Seminários em Administração
novembro de 2018
ISSN 2177-3866

Tem Boi na Linha? Uma Análise sobre o Paradoxo da Privacidade durante o Uso de Smartphones

YVES WANDERLEY ESTANISLAU DA COSTA NETTO
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL (UFRGS)

JOSÉ CARLOS DA SILVA FREITAS JUNIOR
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL (UFRGS)

Agradecimento à orgão de fomento:
Agradecemos a CAPES pelos recursos que tornaram possível essa pesquisa.

Tem Boi na Linha? Uma Análise sobre o Paradoxo da Privacidade durante o Uso de Smartphones

1. INTRODUÇÃO

No ano de 2014, o número de telefones móveis ultrapassou o de pessoas na face da Terra. Nos tempos atuais, o uso desses aparelhos tem crescido de forma consistente, e paralelamente, a dependência dos indivíduos neles para fins tanto recreativos como de trabalho (BOREN, 2014). Com a evolução da tecnologia na área da telefonia móvel, surgiram os *smartphones*, que são telefones móveis capazes de desempenhar com a mesma eficiência (ou em muitos casos) ultrapassar o desempenho em relação à acessibilidade e funcionalidade de computadores pessoais (PENNEKAMP; HENZE; WEHRLE, 2017).

O uso intensivo desses aparelhos tem feito com que se tornem cada vez mais indissociáveis da identidade dos usuários (LYNCH, 2016). Na medida que determinadas funcionalidades (antes restritas aos computadores pessoais) passaram as ser desempenhadas de forma preponderante nos *smartphones*, as preocupações em relação à privacidade dos dados também cresceram no contexto do uso desses aparelhos (ABDELHAMID; VENKATESAN; GAIA, 2018). No entanto, os fatores e a forma com que influenciam as preocupações dos usuários de *smartphones* em relação à privacidade ainda precisam ser melhor estudados pela academia (MELLO; ZORZO; PONTES, 2017).

Os usuários de *smartphones*, em grande parte, não tem o conhecimento necessário para tomar decisões quando se defrontam com situações em que precisam disponibilizar informações pessoais para que aproveitem de forma completa a experiência no uso de seus aparelhos (MARCELINO; SILVA, 2018). Alguns autores, a partir de situações como essas, definiram o Paradoxo da Privacidade como o fenômeno em que os usuários decidem disponibilizar informações pessoais de forma extensiva, em troca de pequenas recompensas como a maior conveniência ao usarem aplicativos em dispositivos eletrônicos (BARNES, 2006; ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2015; DIENLIN; TREPTE, 2015; KOKOLAKIS, 2017).

Foi realizada uma busca por artigos no Google Acadêmico pelos termos *"Mobile Privacy" e "Smartphone Privacy"*. Entre 2014 e 2018, o termo foi encontrado no título de 147 trabalhos. Coloca-se em evidência esse número ao constatar-se que foram encontrados — utilizando-se o mesmo indexador de busca e termos supracitados — um total de 191 trabalhos que abordaram o tema até 2014. O crescimento de forma substancial no número de trabalhos nos últimos quatro anos é uma das justificativas para a investigação proposta no presente artigo que aborda o tema da privacidade no contexto do uso de *smartphones*.

Buscando conhecer os fatores relacionados com a situação problemática e visando atender ao tema e ao foco deste estudo foi estabelecido o seguinte objetivo geral: propor e testar um modelo para analisar a relação entre os fatores que influenciam as preocupações sobre privacidade durante o uso de smartphones e o benefício percebido que a utilização desses equipamentos proporciona aos usuários. O método de pesquisa foi uma survey, submetida a uma amostra por conveniência. O questionário foi construído a partir de dimensões do instrumento de Xu et al. (2012) e da dimensão "Benefício Percebido" do trabalho de Costa Netto e Britto da Silva (2016).

Nas seções seguintes estão expostos o referencial teórico, o método de pesquisa, a análise e discussão dos resultados e as considerações finais.

2. REFERENCIAL TEÓRICO

Nessa seção são apresentados os temas relevantes para o embasamento da pesquisa.

2.1. As Preocupações sobre Privacidade no Uso de Smartphones

Da mesma forma que cresce o consumo e uso de smartphones e dispositivos similares, cresce também a quantidade de dados gerados pelos usuários durante as atividades desempenhadas na utilização de tais aparelhos. Ainda que essa enorme quantidade de dados possa ser transformada em informação para benefício dos próprios usuários, também aumentam os riscos para a privacidade desses indivíduos (SIPIOR; WARD; VOLONINO, 2014).

Os estudos sobre privacidade no uso de *smartphones* derivam de pesquisas que surgiram na medida que crescia o uso de computadores pessoais nas organizações (SMITH; MILBERG; BURKE, 1996). Nessa época, Smith, Milberg e Burke (1996) desenvolveram o instrumento *Concerns for Information Privacy* (CFIP) com o objetivo em mensurar as preocupações dos funcionários sobre suas informações pessoais que circulam no ambiente de trabalho.

Paralelamente, a revolução iniciada pela popularização da internet fez com que o foco das preocupações sobre a privacidade fosse transferido para essa esfera. Na área acadêmica, essa nova forma de se comunicar teve reflexos nas pesquisas sobre privacidade dando origem a instrumentos como o de Malhotra, Kim e Agarwal (2004). Nele, os autores utilizaram dimensões do instrumento de Smith, Milberg e Burke (1996) e construíram o *User's Information Privacy Concern* (UIPC). Esse trabalho já abrangia preocupações recentes como a de coleta e uso de informações pessoais por parte de empresas online.

Seguindo a evolução tecnológica, a ampliação da funcionalidade dos telefones móveis deu origem aos *smartphones* (PENNEKAMP; HENZE; WEHRLE, 2017). Esses, reúnem em um equipamento móvel as mesmas funcionalidades de um computador pessoal. Se antes as preocupações sobre privacidade eram restritas à experiência que o usuário tinha ao interagir com um dispositivo localizado em um determinado ambiente, agora as fronteiras de usabilidade se tornaram mais estreitas ao passo que os riscos à privacidade aumentaram significativamente (CHITKARA et al., 2017).

Na academia, o trabalho de Xu et al. (2012) refletiu essa mudança de paradigma ao abordar as preocupações sobre privacidade no contexto dos telefones móveis. Os autores testaram e validaram o instrumento *Mobile User's Concerns for Information Privacy* (MUIPC). No questionário final que deu base para a elaboração do modelo, a dimensão MUIPC é influenciada pela experiência prévia dos usuários em relação à privacidade no uso de smartphones e refletia nas dimensões: (i) Vigilância Percebida, a (ii) Intrusão Percebida e o (iii) Uso Secundário da Informação.

A vigilância percebida ocorre quando os indivíduos percebem que suas atividades estão sendo observadas, ouvidas e registradas (SOLOVE, 2007). Com o advento da internet e a evolução da tecnologia móvel, essa preocupação se tornou cada vez mais frequente na medida que a mobilidade proporcionada pelos *smartphones* proporcionou a possibilidade de que a vigilância passasse a ser efetuada em qualquer lugar que o usuário estiver portando o seu aparelho (MELLO; ZORZO; PONTES, 2017; ABDELHAMID; VENKATESAN; GAIA, 2018).

A intrusão percebida se difere da vigilância percebida ao passo que nessa situação o indivíduo, apesar de perceber que existem ações que estão oferecendo riscos à sua privacidade, ainda não tem a consciência de como tais ações podem se configurar em riscos. A intrusão percebida nos meio online é uma extensão do que ocorre no mundo físico quando o indivíduo sente que o seu espaço pessoal foi invadido (SOLOVE, 2007; XU et al., 2012).

O uso secundário de informações ocorre quando os indivíduos percebem que suas informações pessoais foram coletadas para um propósito mas utilizadas para outro (SMITH; MILBERG; BURKE, 1996). Ainda que a utilização de informações secundárias ocorra de forma extensiva por empresas e órgãos governamentais, no momento que não há o consentimento ou

o conhecimento por parte dos usuários, essa prática passa a ser percebida como uma ameaça. Enquanto o uso secundário de informações é amplamente utilizado e legal, também pode ser percebido como uma invasão de privacidade (CULNAN, 1993; SOLOVE, 2007).

As preocupações em relação a privacidade no meio online podem ser atenuadas pela percepção por parte dos usuários de que ao trocarem a flexibilização das fronteiras do seu espaço pessoal privado terão algum tipo de benefício pessoal (TADDICKEN, 2014; DIENLIN; TREPTE, 2015; KOKOLAKIS, 2017). Na seção seguinte, essa discussão tem continuidade na apresentação do paradoxo da privacidade.

2.2. O Paradoxo da Privacidade

O crescimento no número de atividades tanto de negócios como de lazer no meio online foi acompanhado de uma necessidade crescente de que os usuários forneçam informações pessoais, o que aumenta o risco de que ocorra a invasão de privacidade (DIENLIN; TREPTE, 2015; KOKOLAKIS, 2017). Essa relação "perde-ganha" foi definida em tempos recentes como o paradoxo da privacidade (AWAD; KRISHNAN, 2006; BARNES, 2006; XU et al., 2011; SUTANTO et al., 2013; TADDICKEN, 2014) Segundo Kokolakis (2017) a compreensão de como ocorre o paradoxo da privacidade pode ampliar o debate ético e legal sobre a privacidade da informação, trazendo esse importante tema para um debate mais profundo no seio da sociedade moderna.

O termo "paradoxo da privacidade" foi mencionado por Barnes (2006) e na ocasião a autora evidenciava a forma contraditória como as pessoas disponibilizam informações no ambiente das plataformas de mídias sociais como se estivessem em ambientes privados (DIENLIN; TREPTE, 2015). Barnes (2006) ressaltou em seu trabalho que as preocupações que os indivíduos alegavam ter em relação à privacidade eram, naquele momento, dissonantes do comportamento que exibiam ao expor informações sensíveis de forma bastante aberta nesses ambientes. Em um trabalho que tinha como foco as mídias sociais, Taddicken (2014) concluiu que a percepção do benefício em termos de relevância social influenciava a intenção dos indivíduos em disponibilizar informações pessoais ao usar tais soluções tecnológicas. No mesmo contexto, Young e Quan-Haase (2013) concluíram que os benefícios sociais percebidos durante o uso de mídias sociais tem flexibilizado, de forma gradual, as preocupações relacionadas à privacidade nesse meio, resultando em maior tolerância para que empresas como o Facebook coletem, compilem e utilizem dados pessoais para fins de propaganda na plataforma social.

A combinação entre o uso de smartphones e mídias sociais expõe de forma clara a ocorrência do paradoxo da informação. Na medida que ambos artefatos de TI proporcionam o engajamento social e aumentam o senso de pertencimento (KIM; WANG; OH, 2016), por outro lado reduzem, muitas vezes sem que os usuários percebam, o nível de preocupação em relação a privacidade de informações consideradas sensíveis por eles.

Nos últimos anos, a maior compreensão sobre a natureza da internet e dos riscos relacionados à privacidade que a exposição de informações pessoais pode representar para os indivíduos, tem feito com que ocorra uma mudança gradual no comportamento das pessoas em relação ao comportamento em relação à privacidade online (ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2015). Ainda assim, os diversos benefícios sociais, emocionais e econômicos ainda desempenham um papel na flexibilização das preocupações relativas à privacidade.

Na sequência, são apresentados o modelo de pesquisa e as hipóteses a serem testadas.

3. MODELO DE PESQUISA E DESENVOLVIMENTO DE HIPÓTESES

O desenvolvimento das hipóteses se baseou no modelo MUIPC de Xu et al. (2012) e na dimensão Benefício Percebido do trabalho de Costa Netto e Britto Da Silva (2016), o que tornou possível analisar empiricamente o processo de formação do fenômeno do paradoxo da privacidade(WILSON; VALACICH, 2012; HÉRAULT; BELVAUX, 2014; TADDICKEN, 2014; DIENLIN; TREPTE, 2015; KOKOLAKIS, 2017).

O grau de maleabilidade que as preocupações sobre privacidade estão sujeitas por ações de empresas e intervenções governamentais foi um dos temas de discussão do artigo de Acquisti, Brandimarte e Loewenstein (2015). Sob esse aspecto, no ambiente virtual, quanto maior o grau de personalização e interação, maior os usuários percebem os benefícios de um determinado serviço (KINARD; CAPELLA, 2006). A percepção dos indivíduos sobre os benefícios que as soluções tecnológicas têm no seu cotidiano influencia a forma com que eles decidem disponibilizar informações pessoais para desfrutar da conveniência e praticidade no uso da tecnologia (LEE; CRANAGE, 2011; SUTANTO et al., 2013). Aliado a isso, quanto mais os riscos à sua privacidade estiverem disfarçados, menor a percepção de intrusão na sua privacidade (WILSON; VALACICH, 2012; ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2015). No trabalho de Lee e Cranage (2011) os autores verificaram que a percepção de utilidade de usuários de websites de agências de viagem tem a capacidade em reduzir as preocupações em relação a privacidade. Mais especificamente em relação ao uso de aplicativos móveis, Xu et al. (2009) concluíram em seu estudo que os indivíduos que utilizam de forma mais frequente aplicativos em dispositivos móveis tendem a ter um nível menor de preocupação em relação a privacidade ao utilizar soluções digitais. Tendo em vista o exposto, a seguinte hipótese é definida:

Hipótese 1: O Benefício Percebido pelo uso de Smartphones tem uma relação negativa na Intrusão Percebida pelos usuários desses equipamentos.

Experiências prévias negativas em relação a privacidade podem influenciar indivíduos a não expor informações sensíveis em ambientes online (BANSAL; ZAHEDI; GEFEN, 2010). Em uma pesquisa que tinha como foco a compreensão de como os usuários de serviços de tecnologia baseados em localização percebiam os benefícios e riscos durante sua utilização, Xu et al. (2009) concluíram que indivíduos que tiveram experiências anteriores com — tanto sendo expostos como vítimas de abusos no uso de informações pessoais — tem maiores preocupações em relação a privacidade tendem a serem mais cautelosos quando precisam disponibilizar informações pessoais no ambiente online. No contexto da área de saúde, Bansal, Zahedi e Gefen (2010) concluíram em seu estudo que a experiência prévia em relação a invasão de privacidade dos usuários de planos de saúde tem uma relação positiva com as preocupações sobre privacidade, dentre elas, a percepção de intrusão no uso desses serviços. A partir do supracitado, a seguinte hipótese é proposta:

Hipótese 2: A Experiência Prévia em relação à Invasão de Privacidade tem uma influência positiva na intrusão percebida pelos usuários de Smartphones.

Ryschka et al. (2014), em estudo qualitativo. sobre os serviços de localização geográfica de smartphones concluíram que que dentre as cinco principais preocupações analisadas, as duas principais foram: o uso secundário das informações e a vigilância percebida. O uso secundário de informações ocorre quando sem a anuência dos detentores da informação, terceiros passam a utilizá-la para outros fins. Quando o detentor da informação percebe a sua ocorrência, ele a interpreta como uma forma de intrusão na sua privacidade. O aumento na percepção de intrusão, aumenta também a sensação de vigilância por parte dos usuários (CULNAN, 1993; SOLOVE, 2007; LOM et al., 2018).

No trabalho de Dinev, Hart e Mullen (2008) os autores concluíram que quando os usuários concordavam que a vigilância de suas atividades era importante para a segurança da população, as pessoas tinham níveis menores de preocupações em relação à privacidade. Essa relação refletia na maior propensão a disponibilizar informações pessoais. Entretanto quando não havia a percepção de que a vigilância de suas atividades refletia em benefícios, os usuários apresentavam um nível maior de preocupação em relação à privacidade.

Das três dimensões que formam o *Mobile User's Information Privacy Concerns* (MUIPC), a Vigilância Percebida é a que se posiciona no nível mais elevado de consciência dos usuários de smartphones. Como foi demonstrado nos resultados do trabalho de Xu et al. (2012), a dimensão Vigilância Percebida tem a maior influência no MUIPC e também na intenção futura dos usuários em utilizar os smartphones.

Ante o exposto, três hipóteses foram definidas para verificar a relação entre as três dimensões, posicionando a Vigilância Percebida como antecedente do Uso Secundário de Informações e da Intrusão Percebida:

Hipótese 3: O Uso Secundário de Informações de usuários de smartphones tem uma relação positiva com a Intrusão Percebida pelo uso desses equipamentos.

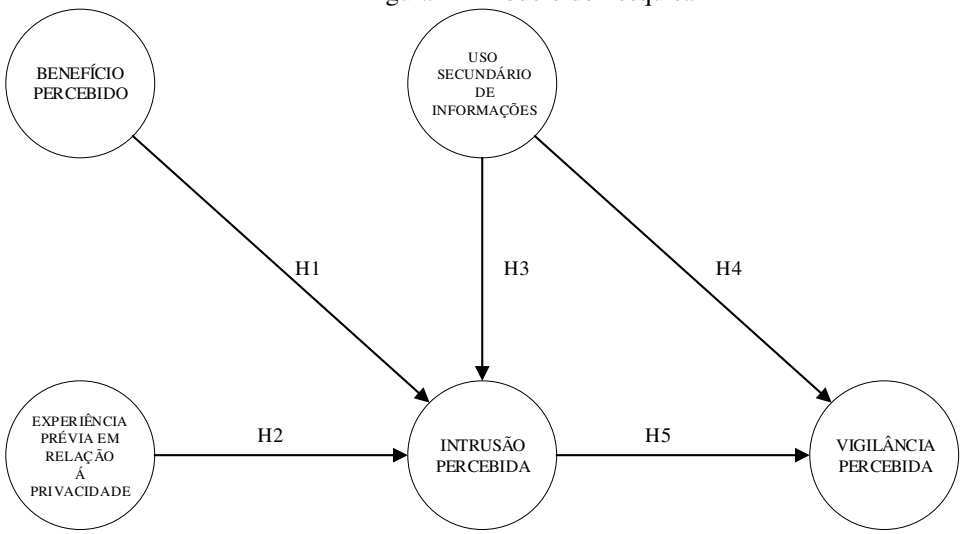
Hipótese 4: O Uso Secundário de Informações de usuários de smartphones tem uma relação positiva com a Vigilância Percebida pelo uso desses equipamentos.

Hipótese 5: A Intrusão Percebida por usuários de smartphones tem uma relação positiva com a Vigilância Percebida pelo uso desses equipamentos.

Na Figura 1 está exposto o modelo de pesquisa. O modelo tem como objetivo analisar a relação entre os fatores que influenciam as preocupações sobre privacidade durante o uso de smartphones e o benefício percebido pela personalização e conveniência que a utilização desses equipamentos proporciona aos usuários.

Através do teste da relação entre os construtos, e em especial à análise do coeficiente de caminhos das dimensões: (i) Benefício Percebido em Intrusão Percebida e (ii) Intrusão Percebida em Vigilância Percebida, o modelo tem o objetivo em predizer que o benefício percebido pelo uso de smartphones influencia negativamente a percepção de intrusão e indiretamente a percepção de vigilância dos usuários durante o uso do aparelho. Adicionalmente, o modelo tem por objetivo predizer que o Uso Secundário de Informações e a Intrusão Percebida têm influência positiva e direta na Vigilância Percebida.

Figura 1 – Modelo de Pesquisa



Fonte: Os Autores (2018)

Na seção seguinte está exposto o método utilizado no trabalho. Nele, a pesquisa é classificada e os métodos de coleta e análise são apresentados.

4. MÉTODO DE PESQUISA

A presente pesquisa, de caráter exploratório, foi realizada em corte transversal. Os dados de 117 respondentes foram coletados entre junho e meados de julho de 2018 por meio de um link para uma survey disponibilizada nas plataformas Kwiksurveys (KWIKSURVEYS, 2018) e Google Forms (GOOGLE FORMS, 2018). Ao final da coleta, os dados foram compilados em uma planilha do Excel.

Inicialmente foram expostas questões para identificar características demográficas dos participantes, quais são: (i) idade, (ii) profissão, (iii) quantos anos utilizam telefones móveis e (iv) tempo diário de uso do aparelho. As questões do questionário survey foram apresentadas em uma escala do tipo Likert de sete pontos. Nas questões que se referiam à Experiência Prévia com Privacidade, a posição 1 correspondia "Nunca" e a posição 7 a "Com Frequência". Nos demais itens, a posição 1 correspondia à "Discordo Totalmente" e a posição 7 à "Concordo Totalmente". Para aumentar a validade e a confiabilidade do instrumento, o questionário foi submetido previamente à dois mestres e um doutorando, que apresentaram sugestões de melhoria.

Para o desenvolvimento do questionário, foram utilizadas as dimensões: (i) Experiência Prévia com Privacidade. (ii) Vigilância Percebida, (iii) Intrusão Percebida e (iv) Uso Secundário de Informações (XU et al., 2012). Adicionalmente, para verificar a influência da acessibilidade e conveniência que os smartphones proporcionam à vida dos usuários, foi incluída a dimensão Benefício Percebido (COSTA NETTO; BRITTO DA SILVA, 2016).

As dimensões haviam sido traduzidas, adaptadas e validadas para o contexto do uso de smartphones no trabalho de Costa Netto e Britto Da Silva (2016). Na versão final do questionário, 15 itens apresentaram os índices recomendados para que fosse possível prosseguir com os testes de validade e confiabilidade do instrumento (HINKIN, 1998; KOUFTEROS, 1999).

A amostra foi definida por conveniência, portanto, não probabilística. Entretanto, a ubiquidade dos smartphones no dia a dia das pessoas, — inclusive no Brasil, que no ano de 2016, foi estimado pelo Instituto Brasileiro de Geografia e Estatística (IBGE) que 95% da população já acessava a internet por esse meio (FOLHA DE SÃO PAULO, 2018) — contribuiu para mitigar essa limitação ao passo que a condição para que respondente pudesse participar da pesquisa foi a de que possuísse um smartphone e utilizasse aplicativos ao usar o aparelho. O número final de respostas válidas foi de 95 questionários.

A estimativa do número mínimo de respostas foi feita através do software GPower (FAUL et al., 2007) utilizando-se os parâmetros recomendados por Cohen (1992) para o método de regressão linear múltipla. O número de respostas obtidas foi superior ao mínimo de 71 respostas necessárias. Tendo em vista que segundo a recomendação de Hair et al. (2016) são necessárias ao menos 5 respostas por item, o número obtido (95) é superior ao recomendado (75).

O teste de normalidade indicou que os dados não são normalizados. Esse resultado justifica a escolha do método de análise PLS-SEM (HAIR et al., 2016). Adicionalmente, a segunda justificativa para a escolha do método foi devido ao caráter preditivo e exploratório da pesquisa (HAIR et al., 2016). As hipóteses propostas no modelo foram testadas seguindo as recomendações de Hair et al. (2016). No presente trabalho os dados foram analisados através dos softwares de análise estatística SPSS e SmartPLS. Adicionalmente, o Excel foi utilizado para tabular a base de dados.

Na seção seguinte estão dispostos os resultados da coleta e análise dos dados obtidos conforme especificado no método.

5. ANÁLISE E DISCUSSÃO DOS RESULTADOS

Nesta seção são discutidos os principais resultados dessa pesquisa. Na subseção seguinte, o perfil demográfico dos respondentes e suas características são apresentados.

5.1. Caracterização dos Respondentes

Um total de 117 pessoas responderam à pesquisa. Entretanto, após a retirada dos questionários incompletos e dos *outliers* esse número foi reduzido a 95 respondentes. A média de idade dos respondentes foi de 31,7 anos. Em termos de gênero, obteve-se uma porcentagem relativamente balanceada (45,27% de homens e 54,73% de mulheres). Em relação ao grau de instrução, a grande maioria (54,73%) dos respondentes tem graduação, na segunda colocação, 33,68% dos respondentes possuem pós-graduação.

Adicionalmente foram apresentadas questões referentes ao tempo que utilizam telefones móveis e quantas horas utilizam o aparelho por dia. Uma porcentagem expressiva (60%) afirmou que utilizam telefones móveis há mais de 10 anos. Em relação ao tempo de uso diário, 40 % o utilizam entre 5 e 10 horas diariamente. Na Tabela 1 os dados são apresentados de forma mais detalhada.

Tabela 1 - Perfil Demográfico dos Respondentes e Características de Uso dos Aparelhos

Perfil Demográfico e Caraterísticas de Uso de Smartphones	**Número**	**Porcentagem**
Gênero		
Masculino	43	45,27
Feminino	**52**	**54,73**
Idade (anos)		
16 ⊦ 20	11	11,57
20 ⊦ 25	**23**	**24,21**
25 ⊦ 30	17	17,89
30 ⊦ 35	8	8,42
35 ⊦ 40	9	9,47
40 ⊦ 45	9	9,47
45 ⊦ 50	5	5,26
50 ⊦ 70	13	13,68
Grau de Instrução		
Segundo Grau completo	9	9,47
Graduação	**52**	**54,73**
Especialização	2	2,10
Pós-graduação	32	33,68
Tempo (em anos) de utilização de telefones móveis?		
De 1 a 5 anos	6	6,31
De 5 a 10 anos	32	33,68
Mais de 10 anos	57	60
Tempo (em horas) diário de utilização de telefones móveis?		
Menos de uma hora	3	3,15
De 1 a 5 horas	36	37,89
De 5 a 10 horas	**38**	**40**
Mais de 10 horas	21	22,10

Fonte: Dados da Pesquisa (2018)

Na seção seguinte é apresentada a validação do instrumento e a estimação do modelo estrutural.

5.2. Validação do Instrumento e Estimação do Modelo Estrutural

A validação do instrumento teve início na fase pré-teste em que foram obtidas 32 respostas com alunos de graduação de uma faculdade de administração. De um total de 21 itens analisados, foram retirados seis que apresentaram índices de correlação item-total corrigido inferiores a 0,300, seguindo as recomendações de Pedhazur e Schmelkin (2013).

Para cada construto, foram obtidos três itens válidos, permitindo que a análise fatorial exploratória pudesse ser feita. Conforme asseveram Werts; Linn e Jöreskog (1974), a manutenção de três itens garante que se obtenha graus de liberdade adequados para aferir a unidimensionalidade de cada construto. Esse cuidado se torna essencial na medida que a mensuração do alfa de Cronbach do instrumento assume que cada construto seja unidimensional (GERBING; ANDERSON, 1988).

No instrumento final, o alfa de Cronbach resultou em um índice de 0,785, portanto, acima da recomendação de Hair et al. (2005). Adicionalmente, o teste de KMO resultou em um índice de 0,745 e foi significante a 0,000. Índices acima de 0,6 demonstram a adequação da amostra para proceder a análise fatorial (MALHOTRA, 2012). Finalmente, o teste de esfericidade de Bartlett resultou em um índice de 546,487 e foi significativo a 0,000 (NORUSIS, 1993).

Em seguida, foi efetuada a purificação da base de dados, seguindo as recomendações de Koufteros (1999). Para isso, foram removidos questionários com respostas incompletas e que possuíam um percentual de 50 % de respostas concentradas no mesmo item. De um total de 117 respostas obtiveram-se 95 questionários válidos, e, portanto, aptos a serem analisados.

A estimação do modelo estrutural foi feita pela verificação da validade discriminante, validade convergente, pela confiabilidade composta dos itens, variância média extraída (VME) e validade dos construtos. Para a validade discriminante foi adotado o critério de Fornell e Larcker (1981).

Enquanto para a validade convergente, verificou-se que a confiabilidade composta de todos os construtos resultou em índices acima de 0,7 e a VME acima de 0,5, indicando que cada construto explica ao menos 50% da variável a ser observada (BAGOZZI; YI, 1988). Na Tabela X são apresentados: os construtos, os itens, as cargas latentes, o valor

Tabela 2 – 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]**
Experiência Prévia com Privacidade (EP)			0,76	0,772	0,536
Com que frequência você passou por situações em que suas informações pessoais foram usadas por uma empresa ou um website de comércio eletrônico sem a sua autorização? (EP1)	,570	2,91			
Com que frequência você passou por situações em que suas informações pessoais foram usadas por fabricantes de aplicativos de telefones móveis, sem a sua autorização? (EP2)	,806	5,095			
No último ano, tomei conhecimento (através de notícias e de amigos) de situações em que ocorreu o uso, ou potencial mal-uso, de informações coletadas durante o uso de telefones móveis (EP3)	,797	5,727			
Intrusão Percebida (IP)			0,72	0,859	0,615
Eu sinto que terceiros têm acesso à mais informações sobre mim do que eu gostaria por decorrência do uso de aplicativos do meu telefone celular. (IP1)	,779	13,603			
E acredito que informações que considero privadas sobre mim estão mais facilmente disponíveis para terceiros do que eu gostaria por decorrência do uso de aplicativos do meu telefone celular. (IP2)	,794	12,740			

Construto/Dimensão/Item	Cargas latentes	valor-t*	AC[a]	CC[b]	VME[c]
Sinto que, a minha privacidade pode ser invadida com maior facilidade por decorrência da utilização de aplicativos no meu celular. (IP3)	,780	15,415			
Uso Secundário das Informações (US)			0,754	0,859	0,672
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)	,818	13,096			
Quando forneço informações pessoais para utilizar aplicativos do celular, me preocupo que tais aplicativos possam usar minhas informações para outros fins (US2)	,885	48,584			
Eu me preocupo que os aplicativos do celular possam compartilhar as minhas informações pessoais com terceiros sem receber a minha autorização (US3)	,753	8,571			
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)	,611	4,956			
Eu me preocupo que os aplicativos do meu telefone celular estejam recolhendo uma grande quantidade de informações sobre mim. (VP2)	,882	34,699			
Eu me preocupo que os aplicativos do meu telefone celular possam ser usados para monitorar minhas atividades durante o uso do aparelho. (VP3)	,841	20,833			
Benefício Percebido (BP)			0,77	0,775	0,552
Creio que ao usar aplicativos no meu telefone móvel eu caso uma boa impressão nas pessoas (BP1)	,869	6,068			
A utilização de aplicativos no meu telefone móvel faz com que me sinta mais próximo de amigos e parentes (BP2)	,440	1,996			
A utilização de aplicativos no meu telefone móvel faz com que me sinta aceito pelas pessoas (BP3)	,840	4,262			

Fonte: Dados da Pesquisa (2018)

a – Alfa de Cronbanch; b – Confiabilidade Composta; c – Variância Média Extraída

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

Na Tabela 3 encontra-se a o modelo de mensuração e a validade discriminante do modelo.

Tabela 3 – Modelo de Mensuração

Construtos latentes	CC	VME	Construtos latentes				
			BP	EP	IP	US	VP
BP	0,775	0,552	**0,748**				
EP	0,772	0,536	0,143	**0,741**			
IP	0,859	0,615	-0,218	0,356	**0,782**		
US	0,859	0,672	-0,134	0,233	0,723	**0,820**	
VP	0,762	0,620	0,003	0,373	0,777	0,792	**0,788**
Média			3,891	3,992	5,512	5,589	5,256
D.P.			1,749	1,888	1,443	1,502	1,636

Fonte: Dados da Pesquisa (2018)

Observa-se na Tabela 3 que os índices nas diagonais são maiores do que os abaixo das respectivas colunas, demonstrando-se assim a validade discriminante dos construtos. A raiz quadrada de VME de uma variável latente deve ser maior que as correlações com as demais variáveis latentes, indicando que os itens que medem uma das variáveis latentes mensuram apenas a dimensão da qual fazem parte (FORNELL; LARCKER, 1981).

No passo seguinte foi utilizado o método de *bootstrapping* com 5000 amostras seguindo as recomendações de Hair et al. (2016). A análise de colinearidade foi feita observando-se o Fator de Inflação da Variância (VIF). Segundo (HAIR et al., 2016) os valores entre 0.2 e 5 indicam que não há uma influência negativa da colinearidade entre os itens. Os valores tanto das variáveis independentes como as dependentes oscilaram entre 1,06 e 1,69.

Na sequência foi efetuada a análise dos coeficientes dos caminhos. A um nível de significância de 95% ($p<0,05$) dois dos caminhos demonstraram serem significantes. A um nível de significância de 99% ($p<0,001$) os outros três também demonstraram ser significantes. Na Tabela 4 são apresentadas as hipóteses e os índices que apontam a significância dos caminhos.

Tabela 4 - Teste de Hipóteses da relação entre os construtos

Hipóteses	Caminho	Coeficiente do Caminho	Erro Padrão	Estatística t (a)	Valor p	Decisão
H1	BP -> IP	-0,163	0.074	2,205*	0,027	Suportado
H2	EP -> IP	0,218	0.078	2,800*	0,005	Suportado
H3	US-> IP	0,647	0.063	10,232**	0,000	Suportado
H4	US-> VP	0,483	0,103	4,670**	0,000	Suportado
H5	IP-> VP	0,428	0,101	4,221**	0,000	Suportado

Fonte: Dados da Pesquisa (2018)

(a) valor t para teste de duas caudas: * 1.96 (nível de significância: 95%), ** 2,57 (nível de significância: 99%)

A hipótese 1 foi confirmada empiricamente através do coeficiente de caminho significante a 95% ($\beta= -0,163$) indicando a influência negativa do *benefício percebido (BP)* na intrusão percebida (IP) no uso de smartphones. A hipótese 2 também foi confirmada ($\beta=0,218$) indicando que há uma influência positiva da experiência prévia com privacidade (EP) na intrusão percebida (IP) no uso de smartphones.

As três últimas hipóteses foram confirmadas a um nível de significância de 99% ($p<0,001$). A hipótese 3 foi confirmada ($\beta=0,647$) indicando a influência positiva da percepção do Uso Secundário de Informações (US) na Intrusão Percebida (IP). A hipótese 4 foi confirmada a um nível de significância de 99% ($\beta= 0,483$) indicando a influência positiva da percepção do Uso Secundário de Informações (US) na Vigilância Percebida (VP). Finalmente, a última hipótese, H5, também foi confirmada ($\beta=0,428$) indicando a influência positiva da Intrusão Percebida na Vigilância Percebida (VP).

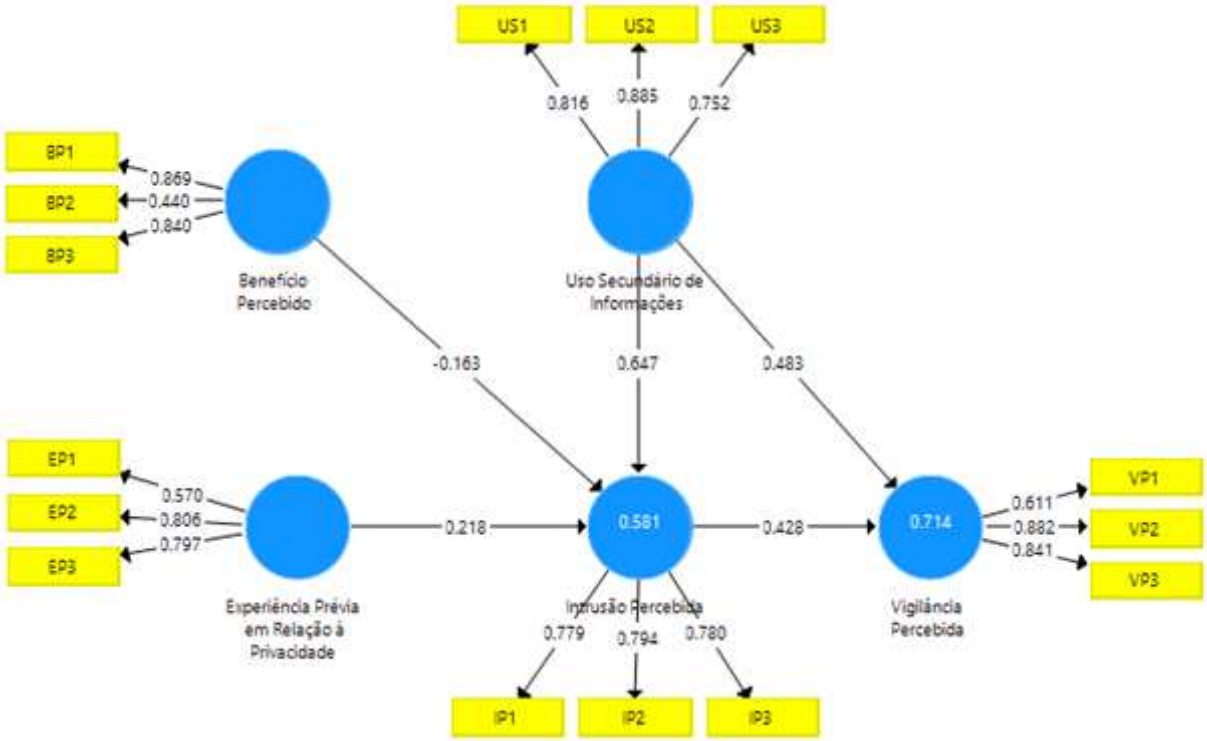
O cálculo do índice de Stone-Geisser (Q^2) confirmou a relevância preditiva do modelo ao passo que a validação cruzada dos construtos endógenos —Vigilância Percebida (VP) e Intrusão Percebida (IP) — apresentou valores acima de zero (HAIR et al., 2016). Um cuidado adicional na validação do modelo foi a realização do teste de um fator de Harman.

Os construtos foram analisados pelo software SPSS e todos os itens foram reduzidos a um fator. A variância explicada pelo conjunto de itens obteve uma porcentagem de 24,97%, portanto, inferior ao índice de 50% (BAGOZZI; YI, 1991; PODSAKOFF et al., 2003). O resultado do teste indica que a variância do modelo é atribuída aos construtos e não ao método de mensuração adotado.

Na Figura 2 verifica-se o modelo com suas cargas latentes, coeficientes de caminho e a variância explicada pelos construtos endógenos. Os construtos endógenos, Intrusão Percebida e Vigilância Percebida apresentaram respectivamente um coeficiente de determinação ($R^{2)}$ de 0,581 e 0,714. O coeficiente de determinação ajustado de ambos os construtos resultou em

0,567 e 0,708. Conforme explica Hair et al. (2005), essa pequena diferença demonstra que não há uma grande superestimação do poder explicativo do modelo.

Figura 2 – Modelo Final da Pesquisa



Fonte: Os Autores (2018)

Verifica-se na Figura 2 que 58,1 % da variância do construto latente endógeno Intrusão Percebida (IP) é explicada pela experiência prévia em relação à privacidade (EP), o uso secundário de informações (US) e pelo benefício percebido (BP). Esse último, influenciando negativamente a percepção de intrusão. Enquanto 71,4% da variância do construto endógeno Vigilância Percebida (VP) é explicada pelas variáveis Intrusão Percebida e Uso Secundário de Informações.

Na Tabela 5 verificam-se os efeitos totais das variáveis exógenas nas variáveis endógenas. O benefício percebido no uso de smartphones tem um efeito direto e negativo (β =-0,163) na Intrusão Percebida e indireto e negativo (β =-0,07) na Vigilância Percebida (VP).

Tabela 5 – Efeitos Totais das Variáveis endógenas nas Variáveis Exógenas

	BP	EP	IP	US	VP
Benefício Percebido (BP)			-0,163		-0,070
Experiência Prévia em Relação a Privacidade (EP)			0,218		0,093
Intrusão Percebida (IP)					0,428
Uso Secundário de Informações (US)					
Vigilância Percebida (VP)			0,647		0,760

Fonte: Dados da Pesquisa (2018)

A análise dos coeficientes dos caminhos demonstra que a Intrusão Percebida (IP) é influenciada positivamente pela Experiência Prévia em Relação à Privacidade (EP).

6. CONSIDERAÇÕES FINAIS

Considera-se que o objetivo geral da presente pesquisa foi atingido ao passo que o modelo proposto foi testado e validado. No artigo de Xu et al. (2012), os autores posicionam as variáveis Benefício Percebido (BP), Vigilância Percebida (VP) e Intrusão Percebida (IP) como formadores do construto MUIPC — que propuseram para a mensurar as preocupações sobre privacidade de usuários de smartphones — mas a relação entre esses três construtos não havia sido analisada de forma empírica até o momento. No presente artigo a relação entre as três variáveis é apresentada. Uma outra contribuição do artigo é demonstrar que a influência da Experiência Prévia em relação à Privacidade ocorre de forma direta na Intrusão Percebida. Finalmente, a terceira contribuição do artigo é demonstrar que o Benefício Percebido pelos usuários de *smartphones* influenciam diretamente (e negativamente) a intrusão percebida e indiretamente (e negativamente) a vigilância percebida. Essas contribuições demonstram empiricamente a existência do chamado "Paradoxo da Privacidade". Ainda que a influência indireta do Benefício Percebido na Vigilância Percebida seja pequena (β =-0,07), a inclusão do construto como uma variável independente e capaz de influenciar a preocupação com privacidade de usuários de smartphones, abre um caminho para que novos estudos possam ampliar a compreensão de quais benefícios têm maior capacidade em reduzir a percepção de usuários de smartphones sobre os riscos envolvidos no uso do aparelho.

O artigo contribui para a pesquisa na área de segurança da informação ao auxiliar na compreensão de como ocorre o cálculo de privacidade que usuários de *smartphones* fazem quando decidem disponibilizar informações sensíveis para a utilização dos aparelhos. Em última instância, a compreensão de como ocorre essa decisão pode influenciar também na intenção futura de uso de smartphones.

Sob esse aspecto faz-se mister ressaltar que a contribuição do artigo também se estende para os *practitioners*, dentre eles, fabricantes de smartphones e de aplicativos para o uso nesses dispositivos. A compreensão de como ocorre a percepção dos usuários sobre os riscos à privacidade pode auxiliar na ocasião do desenvolvimento de sistemas operacionais e aplicativos para o uso nos aparelhos. Essa contribuição pode reverter em um aumento da transparência dos termos de uso dos sistemas e aplicativos e das permissões que os usuários necessitam fornecer para a utilização, aumentando a consciência dos indivíduos e encorajando o uso continuado dos aparelhos.

Como limitação do trabalho é possível apontar a submissão do questionário à uma amostra por conveniência. Entretanto, foram tomadas as precauções recomendadas pela literatura para mitigar os possíveis vieses que esse tipo de amostra pode introduzir nos resultados da pesquisa.

Segundo Acquisti, Brandimarte e Loewenstein (2015), o comportamento em relação a privacidade é influenciado por fatores internos e externos. Como sugestão de pesquisas futuras, é possível investigar como características pessoais, por exemplo, narcisismo, extroversão e timidez, influenciam nas preocupações em relação à privacidade dos indivíduos.

Por fim, o presente artigo espera que a sua pequena contribuição possa jogar luzes sobre como aprimorar a relação das pessoas com a tecnologia (mais especificamente com os *smartphones*) ao ampliar a conscientização de que apesar dos diversos benefícios que trazem para o nosso dia-a-dia, ainda assim, se configuram em uma pequena janela em que nossos pensamentos, anseios, dados e informações podem ser observados, coletados e utilizados por uma gama inimaginável de indivíduos, e por isso, devem ser devidamente resguardados.

REFERÊNCIAS

ABDELHAMID, Mohamed; VENKATESAN, Srikanth; GAIA, Joana. Do Privacy Concerns Affect Information Seeking via Smartphones? In: M. GUPTA, R. Sharman, J. Walp, & P.

Mulgund (Ed.). **Information Technology Risk Management and Compliance in Modern Organizations**. Hershey, PA: IGI Global, 2018. p.301-314.

ACQUISTI, Alessandro; BRANDIMARTE, Laura; LOEWENSTEIN, George. Privacy and human behavior in the age of information. **Science,** v. 347, n. 6221, p. 509-514, 2015.

AWAD, Naveen Farag; KRISHNAN, M. S. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. **MIS Quarterly,** v. 30, n. 1, p. 13-28, 2006.

BAGOZZI, Richard P; YI, Youjae. On the evaluation of structural equation models. **Journal of the Academy of Marketing Science,** v. 16, n. 1, p. 74-94, 1988.

_____. Multitrait-multimethod matrices in consumer research. **Journal of Consumer Research,** v. 17, n. 4, p. 426-439, 1991.

BANSAL, Gaurav; ZAHEDI, Fatemeh "Mariam"; GEFEN, David. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. **Decision Support Systems,** v. 49, n. 2, p. 138-150, 2010.

BARNES, Susan B. A privacy paradox: Social networking in the United States. **First Monday,** v. 11, n. 9, 2006.

BOREN, Zachary Davies. There Are Officially More Mobile Devices than People in the World. 2014. **The Independent**. UK, 7 Outubro, 2014. Disponível em: <https://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html> . Acesso em: 15 Jul. 2018.

CHITKARA, Saksham et al. Does this App Really Need My Location?: Context-Aware Privacy Management for Smartphones. ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2017.

COHEN, Jacob. A power primer. **Psychological bulletin,** v. 112, n. 1, p. 155, 1992.

COSTA NETTO, Yves; BRITTO DA SILVA, Vergílio. **Validação de um Instrumento para Mensurar a Preocupação de Usuários de Smartphones sobre a Invasão de Privacidade**. XL ENANPAD. ANPAD. Costa do Sauípe: ANPAD, 2016.

CULNAN, Mary J. " How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. **MIS Quarterly**, p. 341-363, 1993.

DIENLIN, Tobias; TREPTE, Sabine. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. **European Journal of Social Psychology,** v. 45, n. 3, p. 285-297, 2015.

DINEV, Tamara; HART, Paul; MULLEN, Michael R. Internet privacy concerns and beliefs about government surveillance – An empirical investigation. **The Journal of Strategic Information Systems,** v. 17, n. 3, p. 214-233, 2008.

FAUL, Franz et al. G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. **Behavior research methods,** v. 39, n. 2, p. 175-191, 2007.

FOLHA DE SÃO PAULO. 95% dos internautas brasileiros usaram celular para acessar em 2016, diz IBGE. 2018. **Folha de São Paulo**, São Paulo, 21 Fevereiro 2018. Disponível em: <https://www1.folha.uol.com.br/mercado/2018/02/95-dos-brasileiros-usaram-celular-para-acessar-a-web-no-fim-de-2016-diz-ibge.shtml> . Acesso em: 17 Jul. 2018

FORNELL, Claes; LARCKER, David F. Structural equation models with unobservable variables and measurement error: Algebra and statistics. **Journal of Marketing Research**, p. 382-388, 1981.

GERBING, David W; ANDERSON, James C. An updated paradigm for scale development incorporating unidimensionality and its assessment. **Journal of Marketing research**, p. 186-192, 1988.

GOOGLE FORMS. Google Forms. 2018. Disponível em: < https://www.google.com/forms/about/ >. Acesso em: 16 Jul. 2018.

HAIR, Joseph et al. **Fundamentos de métodos de pesquisa em administração**. Bookman Companhia Ed, 2005.

HAIR, Joseph F et al. **A primer on partial least squares structural equation modeling (PLS-SEM)**. Sage Publications, 2016.

HÉRAULT, S; BELVAUX, B. Privacy paradox et adoption de technologies intrusives Le cas de la géolocalisation mobile. **Décisions Marketing**, n. 74, 2014.

HINKIN, Timothy R. A brief tutorial on the development of measures for use in survey questionnaires. **Organizational research methods,** v. 1, n. 1, p. 104-121, 1998.

KIM, Yonghwan; WANG, Yuan; OH, Jeyoung. Digital media use and social engagement: How social media and smartphone use influence social activities of college students. **Cyberpsychology, Behavior, and Social Networking,** v. 19, n. 4, p. 264-269, 2016.

KINARD, Brian R; CAPELLA, Michael L. Relationship marketing: the influence of consumer involvement on perceived service benefits. **Journal of Services Marketing,** v. 20, n. 6, p. 359-368, 2006.

KOKOLAKIS, Spyros. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. **Computers & Security,** v. 64, p. 122-134, 2017.

KOUFTEROS, Xenophon A. Testing a model of pull production: a paradigm for manufacturing research using structural equation modeling. **Journal of Operations Management,** v. 17, n. 4, p. 467-488, 1999.

KWIKSURVEYS. 2018. Kwiksurveys. Disponível em: < https://kwiksurveys.com/ >. Acesso em: 16 Jul. 2018.

LEE, Chung Hun; CRANAGE, David A. Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites. **Tourism Management,** v. 32, n. 5, p. 987-994, 2011.

LOM, H. S et al. Moderating Role of Mobile Users' Information Privacy Concerns Towards Behavioural Intention and Use Behaviour in Mobile Advertising. **Advanced Science Letters,** v. 24, n. 6, p. 4259-4264, 2018.

LYNCH, Michael. Leave My IPhone Alone: Why Our Smartphones Are Extensions of Ourselves. 2016. **The Guardian**. UK, 19 Fevereiro 2016. Disponível em: < <www.theguardian.com/technology/2016/feb/19/iphone-apple-privacy-smartphones-extension-of-ourselves. >. Acesso em: 10 Jul. 2018.

MALHOTRA, Naresh K. **Pesquisa de marketing: uma orientação aplicada**. Bookman Editora, Porto Alegre, 2012.

MALHOTRA, Naresh K; KIM, Sung S; AGARWAL, James. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. **Information systems Research,** v. 15, n. 4, p. 336-355, 2004.

MARCELINO, Luis; SILVA, Catarina. **Location Privacy Concerns in Mobile Applications**. In: Rocha Á., Reis L. (ORGS) Developments and Advances in Intelligent Systems and Applications. Studies in Computational Intelligence, vol 718. Springer, Cham 2018. p. 241-249

MELLO, José S.; ZORZO, Sérgio D; PONTES, Diego R.G. **Mobile privacy: users' expectations about the behavior of mobile apps**. In: Twenty-third Americas Conference on Information Systems, Boston: ACIS, 2017.

NORUSIS, Marija J. **SPSS: SPSS for Windows, base system user's guide release 6.0**. SPSS Inc., 1993.

PEDHAZUR, Elazar J.; SCHMELKIN, Liora P. **Measurement, design, and analysis: An integrated approach**. Psychology Press, 2013.

PENNEKAMP, J; HENZE, M; WEHRLE, K. A survey on the evolution of privacy enforcement on smartphones and the road ahead. **Pervasive and Mobile Computing**, v.42, p. 58-76, 2017.

PODSAKOFF, Philip M et al. Common method biases in behavioral research: a critical review of the literature and recommended remedies. **Journal of applied psychology,** v. 88, n. 5, p. 879, 2003.

RYSCHKA, Stephanie et al. A qualitative investigation of risk perceptions in the case of check-in services. In: Twentieth Americas Conference on Information Systems, Savannah, GA: ACIS, 2014.

SIPIOR, Janine C; WARD, Burke T.; VOLONINO, Linda. Privacy concerns associated with smartphone use. **Journal of Internet Commerce**,v. 13, n. 3-4, p.177-193, 2014.

SMITH, H Jeff; MILBERG, Sandra J; BURKE, Sandra J. Information privacy: measuring individuals' concerns about organizational practices. **MIS Quarterly**, p. 167-196, 1996.

SOLOVE, Daniel J. I've got nothing to hide and other misunderstandings of privacy. **San Diego L. Rev.,** v. 44, p. 745, 2007.

SUTANTO, Juliana et al. Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. **MIS Quarterly,** v. 37, n. 4, 2013.

TADDICKEN, Monika. The 'privacy paradox'in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. **Journal of Computer-Mediated Communication,** v. 19, n. 2, p. 248-273, 2014.

WERTS, Charles E; LINN, Robert L; JÖRESKOG, Karl G. Intraclass reliability estimates: Testing structural assumptions. **Educational and Psychological measurement,** v. 34, n. 1, p. 25-33, 1974.

WILSON, Dave; VALACICH, Joseph S. Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. In: Thirty Third International Conference on Information Systems, Orlando, FL: ICIS, 2012.

XU, Heng et al. Measuring mobile users' concerns for information privacy. In: Thirty Third International Conference on Information Systems, Orlando, EUA: ICIS, 2012.

XU, Heng et al. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. **Decision Support Systems,** v. 51, n. 1, p. 42-52, 2011.

XU, Heng et al. The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. **Journal of management information systems,** v. 26, n. 3, p. 135-174, 2009.

YOUNG, Alyson Leigh; QUAN-HAASE, Anabel. PRIVACY PROTECTION STRATEGIES ON FACEBOOK. **Information, Communication & Society,** v. 16, n. 4, p. 479-500, 2013.