# Preocupação com a Privacidade na Internet: Uma Pesquisa Exploratória no Cenário Brasileiro

**Conference Paper** · June 2015

CITATION
1

READS
89

**3 authors:**

Odirlei Antonio Magnagnagno
Faculdade Assis Gurgacz
**3** PUBLICATIONS **1** CITATION
SEE PROFILE

Edimara Mezzomo Luciano
Pontifícia Universidade Católica do Rio Gran…
**103** PUBLICATIONS **80** CITATIONS
SEE PROFILE

Vergilio RICARDO BRITTO DA Silva
Pontifícia Universidade Católica do Rio Gran…
**8** PUBLICATIONS **1** CITATION
SEE PROFILE

# Preocupação com a Privacidade na Internet: Uma Pesquisa Exploratória no Cenário Brasileiro

**Autoria:** Vergilio Ricardo Britto-da-Silva, Edimara Mezzomo Luciano, Odirlei Antonio Magnagnagno

RESUMO

A preocupação com a privacidade na Internet (*Internet Privacy Concern* - IPC) é uma área de estudo que está recebendo maior atenção recentemente devido à enorme quantidade de informações pessoais que trafegam na internet. Os constantes escândalos de invasão de privacidade e espionagem envolvendoChefes de Estado trouxeram maior evidência para o assunto. Esta pesquisa aborda o tema Segurança da Informação, com foco na Preocupação com a Privacidade na Internet.O crescimento do uso de Tecnologias da Informação e Comunicação tem gerado desafios para os direitos fundamentais dos cidadãos, quais sejam: o direito à privacidade, à liberdade de expressão e a liberdade de associação, e o grande volume de informações pessoais que são publicadas na Internet diariamente colocam em risco tais direitos.O objetivo desta pesquisa foi identificar o grau de preocupação com a privacidade dos usuários de Internet do Brasil, relacionado com IPC e identificar clusters com características em comum. A presente pesquisa está embasada teoricamente em estudos sobre Privacidade na Internet, Preocupação com a Privacidade e Comportamento do Usuário, que mostram o a evolução do construto Preocupação com a Privacidade, bem como indicam como os usuários lidam com sua privacidade. Foi realizada uma pesquisa de natureza exploratória descritiva, com dados coletados nas cinco regiões do país, totalizando 1104 questionários completos. Os resultados indicam um alto grau de preocupação com a privacidade dos usuários de Internet do Brasil, principalmente nas regiões Sul e Sudeste, que apresentaram os maiores índices de preocupação.

**Palavras-chave:** Privacidade na Internet, Preocupação com a Privacidade, Risco à Privacidade

## 1 INTRODUÇÃO

A presente pesquisa aborda o tema Segurança da Informação, mais especificamente sobre apreocupação com a privacidadena Internet.Com o objetivo de identificar o grau de preocupação com a privacidade das informações pessoais de usuários de internet no Brasil, utilizou-se o instrumento de coleta de dados desenvolvido e validado em estudo realizado por Hong e Thong (2013), composto de oito dimensões, quais sejam: coleta de dados, uso secundário, erros, acesso indevido, controle, consciência, confiança e risco, o qual será versionado para o contexto brasileiro. Adicionalmente,verificou-se a sensibilidade das informações pessoais (tipos de informações com as quais os respondentes expressam maior preocupação com a privacidade) utilizando para tal uma lista de informações sensíveis, oriunda do estudo de Degirmenci et al. (2013). O estudo utilizou análise de clusters no intuito de identificar grupos por grau de preocupação e características pessoais, permitindo atender ao proposto no estudo.

A Segurança da Informação tem se tornado cada vez mais importante para as organizações (BOSS et al., 2009). De acordo com os autores, apesar da prevalência de medidas técnicas de segurança, os funcionários individualmente continuam a ser o elo fundamental, e muitas vezes o mais fraco,nas defesas corporativas.Quando os indivíduos optam por desconsiderar as políticas e procedimentos de segurança, a organização está em risco. Em consonância com os autores, Ng e Xu (2007) afirmam que, oaumento da frequência

de incidentes de segurançaé uma grande preocupação para as organizações, e, portanto, é importante que estas protejam suas informações contra ameaças de segurança. Segundo os autores, controles tecnológicos são importantes, mas não suficientes, e o sucesso da segurança depende também do comportamento seguro efetivo dos indivíduos.De acordo com os autores, enquanto os administradores do sistema são responsáveis pela configuração de *firewalls* e servidores de forma segura, os usuários são responsáveis pelas práticas de medidas de segurança, comopor exemplo, escolher e proteger boas senhas.Há uma série de fatores que contribuem para a segurança da informação como foi identificado no estudo de Klein (2014), que afirma que o contentamento do funcionário tem impacto significativo no seu comportamento em relação à segurança da informação. Desta forma, o importante papel do usuário em termos de comportamento envolve não apenas a sua atuação no sentido de proteger as informações da organização na qual trabalha, mas também as suas informações como indivíduo e cidadão, foco adotado nesse trabalho.

A preocupação com a privacidade na Internet (*Internet Privacy Concern* - IPC) é uma área de estudo que está recebendo maior atenção recentemente, devido à enorme quantidade de informações pessoais sendo recolhidas, armazenadas, transmitidas e publicadas na internet (HONG e THONG, 2013). Segundo Westin (1967), privacidade das informações é definida como a capacidade do indivíduo controlar quando, como e até que ponto sua informação pessoal é comunicada a outros.

A segurança de Sistemas de Informação recebeu uma grande atenção e cobertura nos meios de comunicação populares ao longo dos últimos 10 anos e, de forma alarmante, a ameaça de ataque continua a crescer (BOSS, 2009). Segundo o autor, estudo recente mostra que tem havido um aumento significativo no roubo de dados na Internet, bem como na criação de código malicioso desenvolvido especificamente para roubar informações confidenciais. Estas informações podem compor bases de dados que serão comercializados ou divulgados, ferindo a privacidade do usuário.Segundo os resultados da PNAD 2011 (IBGE, 2013) a quantidade de pessoas que acessaram a internet no Brasil passou de 31,9 milhões em 2005, para 77,7 milhões em 2011.

A evolução das tecnologias de redes móveis e *smartphones* tem proporcionado aos consumidores móveis acesso sem precedentes à internet e serviços com valor agregado mesmo em movimento (XU et al., 2012). Os autores afirmam ainda que com a rápida difusão de *smartphones*, a trajetória de crescimento de aplicações móveis (apps) é impressionante. Os riscos relacionados à privacidade das informações,em função dos acessos realizados pelos apps, foram estudados por Degirmenci (2013), que afirma que o acesso à informação pessoal, ou seja, a identidade pessoal, a localização, o conteúdo do dispositivo e do sistema e as configurações de rede, podem incitar os usuários a não instalar ou desinstalar aplicativos móveis,uma vez que estes podem representar uma ameaça à privacidade destes usuários.

As práticas agressivas de acesso e transmissão de dados empregadas por aplicações móveis e sistemas operacionais, de acordo com Xu et al. (2012), agravaram as preocupações com a privacidade entre os usuários. Segundo os autores, estas preocupações estão relacionadas com a coleta automática de dispositivos móveis, que muitas vezes ocorre sem o conhecimento do usuário,com a comunicação de informações de localização dos usuários em tempo real e com a confidencialidade dos dados recolhidos, como localização, identidade pessoal e comportamento de uso diário. De acordo com Malhotra et al. (2004), as informações pessoais em um formato digital podem ser facilmente copiadas, transmitidas e integradas, o que permite que os provedores de serviços na internet construam descrições completas dos indivíduos. Os autores sugerem que a prática de coleta de dados, legítima ou não, é o ponto de partida de várias preocupações com a privacidade das informações pessoais na internet.

Fatos veiculados na imprensa internacional no ano de 2013 mostraram o quanto a privacidade das informações pessoais está fragilizada. Em junho de 2013, através do site *The*

*Intercept*, Edward Snowden, um analista de sistemas, ex-funcionário da Agência Central de Inteligência (CIA) e ex-contratado da Agência de Segurança Nacional (NSA), dos Estados Unidos da América, revelou documentos secretos que mostram como o governo americano monitora seus cidadãos (PORTAL GLOBO.COM, 2014). Segundo tais documentos, a NSA estaria desenvolvendo um sistema para gerenciar milhões de computadores infectados por códigos espiões. Chamado de *Turbine*, o sistema teria sido criado para gerenciar os "implantes" de diferentes programas instalados pela NSA em computadores que seriam controlados. Os documentos afirmam que tais programas permitemque estes obtenham total controle do sistema infectado, acionem microfones e webcams para capturar conversas e imagens, trazendo ainda funções que registram senhas usadas na web e o histórico de navegação. Em dezembro do mesmo ano, Snowden revelou que o governo americano espionou ligações telefônicas e troca de e-mails de empresas e políticos brasileiros (PORTAL GLOBO.COM, 2014).Em função do grande volume de informações postadas na internet diariamente e do avanço das tecnologias que propiciam maior acesso a internet para uma quantidade cada vez maior de pessoas, a privacidade das informações pessoais, segundo os autores Xu et al. (2012) e Malhotra et al. (2004) está ameaçada.

Para que tenha acesso aos diversos serviços oferecidos na internet, o usuário precisa concordar com as políticas de privacidade e termos de uso associados a estes serviços, sem saber exatamente com o que está concordando, pois estes documentos são muito longos e estima-se que a maioria dos usuários não os leia, mas acabe aceitando mesmo assim, uma vez que se não aceitá-los não poderá utilizar o serviço. A partir da análise dos termos de uso e políticas de privacidade destes serviços percebe-se que os usuários estão delegando aos provedores destes serviços acesso indiscriminado a suas informações pessoais.

Em março de 2014 o canal de televisão por assinatura GNT apresentou um documentário produzido pelo cineasta e diretor Cullen Hoback, intitulado *Terms and Conditions May Apply*, que aborda estes contratos que são firmados entre os usuários e os provedores de serviços na internet, entre os quais, redes sociais e e-mails gratuitos, e as implicações associadas a eles. O documentário traz depoimentos que mostram o nível de monitoramento e acesso às informações pessoais postadas pelos usuários destes serviços, fazendo também uma análise dos termos de uso e políticas de privacidade de alguns serviços oferecidos na internet.

Um exemplo da abrangência das permissões que o usuário fornece para os provedores de serviços na internet são aquelas fornecidas à rede de relacionamento profissional Linkedin, quando o usuário concorda com os termos e políticas, onde consta:

> O usuário dá o não exclusivo, irrevogável, internacional, perpétuo, ilimitado, designável, sublicenciável, completamente quitado e sem *royalties*, direito de copiar, fazer trabalhos derivados, melhorar, distribuir, publicar, remover, reter, adicionar, processar, analisar, usar e comercializar, de qualquer forma conhecida ou descoberta no futuro, qualquer informação que o usuário fornecer, direta ou indiretamente ao Linkedin, incluindo, mas não limitado a, qualquer conteúdo do usuário, ideias, conceitos, técnicas ou dados, que o usuário envie ao Linkedin, sem qualquer aviso prévio, acordo ou compensação para o usuário ou para terceiros(LINKEDIN, 2014).

A rede social de fotos Instagram, através da qual os usuários podem copartilhar suas fotos, alterou seu acordo de usuário em janeiro de 2013, para dizer que teria o direito de vender fotos postadas para anúncios, sem compensação para seus usuários (INSTAGRAM, 2014).Segundo GNT (2014), caso o indivíduo leia o acordo de uso do iPhone, não encontrará nenhuma menção sobre grampo telefônico, mas na política de privacidade da AT&T, fornecedora do chip do iPhone no mercado americano, verá que eles dizem que podem utilizar para investigar, prevenir ou tomar medidas sobre atividades ilegais.

A partir da análise da política de privacidade do Facebook, percebe-se que quando um usuário realiza cadastro nesta rede social, por padrão algumas informações são marcadas como públicas, ficando disponíveis para todos os usuários. Caso o usuário queira compartilhar essas informações somente com seus amigos, ou não queria compartilhar tais informações, precisa redefinir suas configurações de privacidade.

Motivado pelos atos terroristas ocorridos em 11 de setembro de 2001, em 26 de outubro deste mesmo ano, o presidente dos Estados Unidos da América (EUA), George Bush, assinou o chamado Ato Patriota que permite, conforme afirmado pelo Presidente dos EUA, que os órgãos de segurança e de inteligência dos EUA vigiem todas as comunicações usadas por supostos terroristas, incluindo e-mails, internet e celulares, saibam quais os sites um usuário visitou, que buscas ele fez, sejam estrangeiros ou americanos, mesmo sem a autorização de um juiz (GNT, 2014).O monitoramento e controle realizado pelas agências de segurança dos EUA, que tem entre as justificativas prevenir ações terroristas, garantir a segurança dos cidadãos americanos e a soberania nacional, impacta não somente na privacidade dos americanos,mas também na privacidade dos usuários de serviços de redes sociais, e-mails gratuitos e outros serviços providos por corporações americanas através da internet.

O monitoramento e controle realizado pelas agências de segurança dos EUA, que tem entre as justificativas prevenir ações terroristas, garantir a segurança dos cidadãos americanos e a soberania nacional, impacta não somente na privacidade dos americanos, mas também na privacidade dos usuários de serviços de redes sociais, e-mails gratuitos e outros serviços providos por corporações americanas através da internet.Com o suposto objetivo de prevenir, as agências de segurança dos EUA monitoram as redes sociais, como pode ser visto no documentário exibido pela GNT (2014) que mostra uma entrevista realizada com um usuário irlandês da rede social Twitter, chamado Leigh Bryan, através da qual postou a seguinte mensagem para um de seus contatos: “você está livre esta semana para um encontro antes de eu sair e destruir a América?”. Vinte dias após esta mensagem ele viajou de férias para Los Angeles, e ao chegar no aeroporto e passar pela imigração é levado para uma sala e interrogado por cinco horas sobre a postagem realizada no Twitter. Segundo Leigh Bryan, ele foi questionado sobre o que ele queria dizer com destruir a América (GNT, 2014).

Muito embora a privacidade possa ser violada não apenas em informações que estão em Sistemas de Informação, mas também em conversas realizadas pessoalmente, a chegada da era da informação, segundo Stewart e Segars (2002), proporcionou às organizações acesso a uma grande variedade de informações armazenadas. No entanto, a livre troca de informações também traz de forma fácil, mas muitas vezes indesejada, o acesso às informações pessoais dos usuários. Segundo os autores, é imperativo que os pesquisadores e profissionais compreendam a natureza da preocupação com a privacidade dos dados pessoais e que seja modelado com precisão o construto no âmbito da pesquisa e no contexto de negócio. De acordo com Malhotra et al. (2004), apesar da importância da compreensão da natureza das preocupações com a privacidade das informações dos consumidores online, este tema tem recebido pouca atenção na comunidade de sistemas de informação. A falta de confiança com a privacidade das informações foi identificada anteriormente como um grande problema que dificultava o crescimento do comércio eletrônico (MALHOTRA et al., 2004). Hoje vê-se possivelmente o contrário, os consumidores compram sem se preocupar com a privacidade das informações que estão fornecendo para as empresas online.

Com a evolução das tecnologias de redes móveis e dos *smartphones*, as questões de privacidade neste contexto tornaram-se extremamente importantes, uma vez que possibilitam o acesso a um grande volume de informações pessoais, de acordo com Xu et al. (2012).A facilidade de acesso à internet decorrente destas evoluções tecnológicas tornou os consumidores provedores de conteúdo em web blogs e redes sociais, tornando suas

informações pessoais mais vulneráveis (HONG e THONG, 2013). De acordo com os autores, processos contra sites populares, tais como Google e Facebook, por violação de privacidade online, e a aplicação de instrumentos de proteção à privacidade na rede, tal como a atuação da Comissão Federal do Comércio dos Estados Unidos, são provas da crescente importância e interesse com a privacidade online.

A percepção de risco do usuário pode definir qual o comportamento deste quanto à preocupação com a privacidade, a qual pode ser deixada de lado em função da confiança em relação à empresa provedora do serviço que está sendo utilizado. Segundo Kim et al. (2008), as organizações e companhias *online* podem reagir às percepções dos riscos envolvidos em transações *online* dos usuários, afirmando que são empresas confiáveis. De acordo com Beldadet al. (2011), enquanto um usuário avaliar uma organização como confiável, ele irá considerar que as transações realizadas com esta organização seguras.

Uma vez que os usuários de internet brasileiros publicam cada vez mais informações na rede mundial de computadores, estima-se que os mesmos tenham um baixo grau de preocupação com a privacidade das informações. Esta pesquisa busca elucidar esta percepção, respondendo a seguinte questão de pesquisa: Qual o grau de preocupação com a privacidade dos dados pessoais de usuários de internet no Brasil?

## 2 REFERENCIAL TEÓRICO

Estima-se que a Privacidade na Internet está se tornando um dos grandes desafios para a Segurança da Informação. Neste capitulo são apresentados alguns conceitos necessários ao entendimento deste estudo, no qual serão apresentados termos relacionados à privacidade.

As discussões e pesquisas sobre privacidade iniciaram muito antes do surgimento da Internet ou da chamada era da informação. A preocupação com privacidade foi abordada por Aristóteles,quetratou sobre a diferença entre a esfera pública (atividade política) e a esfera privada (vida doméstica) dos indivíduos. Thomas Cooley, juiz americano, em 1873, no artigo intitulado “The Elements of Torts”, definiu a privacidade como a limitação do acesso às informações de uma dada pessoa, ao acesso à própria pessoa, à sua intimidade, envolvendo as questões de anonimato, sigilo, afastamento ou solidão, “*the rigth to be alone”*, o direito de ser deixado em paz.Segundo Westin (1967) privacidade das informações é a reivindicação dos indivíduos, grupos ou instituições para determinar por si mesmos quando, como e em que medida suas informações são comunicadas a outros.

O aumento da digitalização das informações pessoais e o avanço das tecnologias da informação, segundo Hong e Thong (2013), representam novos desafios para a privacidade das informações dos consumidores. Segundo os autores, de um lado os serviços de internet personalizados e software de *business intelligence*requerem a coleta e mineração de quantidades sem precedentes de informações pessoalmente identificáveis, de outro como os consumidores se tornaram provedores de conteúdo em *web blogs* e sites de redes sociais na internet, suas informações pessoais se tornaram mais vulneráveis.

No cenário das nas Redes Sociais, segundo Shin (2010), privacidade pode ser definida como o controle sobre o fluxo de informações pessoais, incluindo a transferência e troca de informações. O autor afirma ainda que a proteção da privacidade do usuário passa a ser o principal objetivo para os provedores destes serviços, e que os dados pessoais de usuários dos serviços de redes sociais tornam-se disponíveis ao público de forma sem precedentes, e que estes usuários enfrentam uma possível perda de controle sobre seus dados publicados na internet. Segundo o autor conversas entre usuários podem ser pesquisadas, registradas indefinidamente, replicadas e alteradas, podendo inclusive ser acessadas por outros usuários.

De acordo com Featherman et al. (2010, p.220) “risco à privacidade é a avaliação evolutiva subjetiva das perdas potenciais para a privacidade das informações confidenciais de identificação pessoal, incluindo a avaliação do potencial de uso indevido destas informações”,

o que segundo os autores podem resultar em roubo de identidade. Um exemplo disto é mostrado na pesquisa de Belanger et al. (2002) que afirma que as razões mais citadas para um consumidor rejeitar uma transação *online* eram a falta de informação de privacidade e a potencial perda de controle sobre informações confidenciais. Os autores afirmam ainda que muitas vezes os consumidores podem não utilizar um e-serviço devido aos riscos à privacidade.De acordo com Wartofsky (1986) as pessoas podem ou não estar cientes que estão em risco, podendo voluntariamente assumir riscos, ou terem riscos impostos a elas. O autor afirma ainda que os riscos podem ser classificados como conscientes ou inconscientes, voluntários ou involuntários e calculáveis ou incalculáveis.

Segundo Beldad et al. (2011) o compartilhamento online de informações pessoais dificilmente é considerado seguro. Os dados pessoais com relativo valor econômico podem ser explorados pela organização que coleta esses dados ou por terceiros externos. Os autores afirmam ainda que o uso secundário dos dados pode ter consequências adversas para a pessoa a quem os dados dizem respeito. Assim não é surpreendente que divulgação de dados pessoais no ambiente digital seria considerada arriscada.

De acordo com Beldad et al. (2011) a percepção de risco associada a divulgação de informações pessoais não seria tão alta se estes dados não fossem avaliados como muito sensíveis e se a divulgação destes dados não fossem resultar em consequências negativas para a pessoa a quem os dados dizem respeito. Os autores afirmam ainda que muitas vezes os usuários são privados da possibilidade de saber como os seus dados pessoais são utilizados pelas empresas, e que a coleta não autorizada e o uso secundário de dados pessoais tem sido identificados como fatores críticos que desencadeiam as preocupações com a privacidade das informações pessoais.

A Preocupação com a Privacidade das Informações (CFIP) tem sido objeto de estudo há muitos anos. Desde Smith et al. (1996), foram realizados alguns estudos com objetivos diversos envolvendo a privacidade das informações pessoais. Moor (1997) afirma que quando uma informação é digitalizada, ela trafega fácil e rapidamente para muitos pontos, fazendo com que a recuperação desta informação seja rápida e conveniente. De acordo com o autor, as legítimas preocupações com a privacidade surgem quando essa velocidade e conveniência levam à exposição indevida das informações pessoais. Complementarmente a isso, Smith et al. (1996), afirmam que os usuários de Internet  com preocupações com a privacidade estão preocupados não somente com as práticas de coleta de dados das empresas, mas também com o uso de suas informações pessoais. Som e Kim (2008) afirmam que os usuários com alto nível de preocupação com a privacidade das informações acreditam que o uso indevido das informações pessoais destes provedores de serviços na internet pode resultar em perdas consideráveis.

Muitos provedores de serviços na internet exigem que os usuários façam um cadastro de suas informações pessoais como uma condição para que possam utilizar o serviço oferecido (SOM e KIM, 2008). Segundo os autores, em função da preocupação destes usuários com a privacidade de suas informações pessoais, os usuários por vezes decidem não utilizar tal serviço, ou fornecer informações falsas no cadastro. De acordo com os autores, os usuários de internet podem perceber ameaças à privacidade de suas informações pessoais simplesmente quando os provedores de serviços na internet solicitam que sejam fornecidas informações pessoais e em outros modos mais sutis na interação com estes provedores.

A preocupação com a privacidade na internet, de acordo com Bélanger e Crossler (2011), representa a percepção dos indivíduos do que acontece com as informações que eles fornecem na internet. Segundo Hong e Thong (2013), preocupação com a privacidade na Internet (IPC) é uma área de estudo que está recebendo maior atenção, devido à enorme quantidade de informações pessoais sendo coletadas, armazenadas, transmitida, e publicada na Internet. Segundo Malhotra et al. (2004), IPC é o grau em que o usuário da internet está

preocupado com as práticas de sites, relacionadas com a coleta e uso de suas informações pessoais.

Hong e Thong (2013) realizaram um estudo com os objetivos de desenvolver uma conceituação integrada de IPC, realizada através da revisão da literatura prévia para identificar as dimensões de menor ordem, e validar a conceituação desenvolvida através de quatro estudos empíricos em grande escala, envolvendo cerca de 4.000 usuários de internet. Os autores afirmam que IPC foi desenvolvido teoricamente para ter uma relação negativa com as crenças de confiança e uma relação positiva com as crenças de risco. Segundo os autores, indivíduos com maiores preocupações com a privacidade são menos propensos a confiar em *websites* no tratamento de suas informações pessoais e são mais propensos a achar que é arriscado fornecer informações pessoais para *websites*.

Segundo Hong e Thong (2013) IPC consiste em um fator geral de terceira ordem (IPC), com dois fatores de segunda ordem, quais sejam Gestão da Interação e Gestão da Informação e seis fatores de primeira ordem, que são Coleta, Uso Secundário, Erros, Acesso Indevido, Controle e Consciência. O componente Gestão da Interação é composto pelas dimensões Coleta, Uso Secundário e Controle, e descreve como um indivíduo gerencia a sua interação com os outros, enquanto o componente Gestão da Informação engloba as dimensões Erros e Acesso Indevido, e descreve como um indivíduo gerencia a sua informação pessoal. A dimensão Consciência está vinculada diretamente ao fator geral de terceira ordem IPC, mesmo sendo um fator de primeira ordem.

Os resultados confirmam que a conceituação de terceira ordem do IPC tem validade nomológica, conforme pode ser observado no Anexo C, e é um determinante significativo tanto nas crenças de confiança quanto nas crenças de risco (HONG e THONG, 2013). Os autores afirmam ainda que a pesquisa realizada ajuda a resolver inconsistências nas dimensões subjacentes chaves do IPC e na formulação dos itens originais em instrumentos anteriores de IPC. Segundo os autores, a pesquisa realizada contribui para uma melhor compreensão da conceituação do IPC, e forneceu um instrumento confiável e válido para a investigação sobre IPC. O instrumento desenvolvido por Hong e Thong (2013) foi criado com base no construto CFIP (Smith et al., 1996) e IUIPC (Malhotra et al., 2004), e é composto por seis dimensões, quais sejam Coleta, Uso Secundáro, Erros, Acesso Indevido, Controle e Consciência.

Segundo Puhakainen (2006), ao implementar suas soluções de segurança da informação as organizações têm normalmente focado em medidas de segurança técnica e de procedimento. O autor afirma ainda que, no entanto, isso não é suficiente, e que um sistema de segurança da informação efetivo exige que os usuários estejam informados e utilizem as medidas de segurança disponíveis, de acordo com o descrito nas políticas de segurança da informação de suas organizações. De acordo com Denning (1999) o treinamento é uma parte importante na defesa da informação. A autora propõe programas de treinamento de sensibilização para a segurança dos sistemas de informação como um meio de informar funcionários sobre as políticas de segurança, torná-los conscientes dos riscos e perdas potenciais, e ensinar-lhes a utilização adequada das práticas de segurança.

Segundo Beldad et al. (2011) as empresas podem combater as percepções dos usuários sobre os riscos envolvidos em transações *online*, afirmando que são empresas confiáveis. Os autores afirmam ainda que isso corresponde à suposição de que, enquanto uma organização *online*é avaliada como confiável, as transações com esta organização não seriam consideradas arriscadas. Os autores afirmam ainda que, é importante notar que a percepção de riscos varia de acordo com o contexto da operação e do tipo de organização envolvida. Percepções de risco em *e-commerce* e *e-government*, por exemplo, são significativamente diferentes, com os usuários percebendo mais riscos no primeiro do que no segundo (BELANGER e CARTER, 2008).

Para Trcek et al. (2007) tornou-se evidente nos últimos anos que a tecnologia por si só não pode fornecer a segurança adequada para os sistemas de informação. Os autores afirmam que o fator principal e mais importante para garantir a segurança é o humano, e que em cada sistema de informação há uma complexa interação entre a tecnologia e o fator humano, fazendo com que seja necessário instrumentalizar os responsáveis pela segurança para abordar estas questões de forma rigorosa.

## 3 MÉTODO DE PESQUISA

A pesquisa tem uma natureza exploratória descritiva, que segundo Pinsonneault e Kraemer (1993), tem como propósito identificar opiniões que estão manifestas na população, bem como descrever a distribuição do fenômeno na população ou entre subgrupos da população ou, ainda, fazer uma comparação entre essas distribuições. Foi realizada uma pesquisa de corte transversal, com o objetivo de descrever e analisar o estado de uma ou mais variáveis.

A população-alvo utilizada para este estudo foram os usuários de internet no Brasil, que segundo a Pesquisa Nacional de Amostra de Domicílios de 2011 (IBGE, 2013) totalizava 77,7 milhões de usuários. Para a coleta dos dados utilizou-se uma amostragem não probabilística, seguindo o indicado por Hair et al. (2005), utilizando para a coleta de dados a técnica bola-de-neve. Foram coletados dados nas regiões Sul, Sudeste, Centro-Oeste, Norte e Nordeste do país. Não foram considerados os questionários incompletos, restando no final um total de 1104 questionários respondidos completos. Utilizou-se o instrumento de coleta de dados desenvolvido por Hong e Thong (2013), Foi utilizada uma escala do tipo Likert com variação de sete pontos, entre 1 (discordo totalmente) e 7 (concordo totalmente), para obter maior precisão quanto à intensidade com a qual a pessoa concorda ou discorda da afirmação, conforme recomendação de Hair et al. (2005).Alguns termos foram adaptados ao contexto brasileiro, para melhor compreensão por parte dos respondentes, quais sejam: commercial/government websites, foi traduzido apenas como websites. Na segunda parte do questionário foraminseridas questões de sensibilidade da informação, oriundas do estudo de Degirmenci (2013), com o objetivo de identificarcom quais os tipos de informação os respondentes têm maior preocupação relacionada à privacidade, e na terceira parte do instrumento foram inseridas questõessócio demográficas, com o objetivo de caracterizar a amostra.Após da validação do instrumento de coleta de dados foi realizado um pré-teste, com uma amostra da população-alvo, com o objetivo de identificar e corrigir erros potenciais, seguindo as recomendações de Malhotra (2006).A coleta de dados final foi realizada entre os dias 05/12/2014 e 06/01/2015.

A confiabilidade do instrumento de coleta de dados foi verificada através do coeficiente Alfa de Cronbach, obtendo-se o valor de 0,950 para o conjunto das 26 variáveis que mensuram os construtos.De acordo com Hair et al. (2009) valores de Alfa de Cronbach a partir de 0,6 são aceitáveis para pesquisas exploratórias.

Os resultados indicam que a maioria dos respondentes (61,8%) que compõem a amostra é do sexo feminino, sendo que a maior concentração de respondentes está na faixa etária de 25 a 35 anos, totalizando 46,3% da amostra. As mulheres são maioria também dentro de todas as regiões do país. Quanto a situação profissional dos respondentes pode-se verificar que 51,4% estão empregados, 13,2% são estudantes sem atividade profissional e 12,8% marcaram como resposta a opção “Outro”, sendo que os respondentes que marcaram tal opção descreveram sua situação como: aposentados, desempregado, professores, consultores e estagiários. Os resultados mostram também que 47,3% dos respondentes possuem apenas Ensino Médio Completo (26% - Graduação em Andamento e 21,3% Ensino Médio Completo).Quando questionados se utilizavam alguma rede social, através de uma questão de

múltipla escolha, 97,8% dos respondentes afirmaram que sim, totalizando 1081 respostas positivas. Percebe-se que apenas 100 respondentes não utilizam a rede social Facebook. A partir das análises realizadas foi possível identificar quais as informações apontadas pelos respondentes como mais sensíveis quanto a privacidade.

Os resultados indicam uma forte preocupação com relação àsinformações de senhas, apontadas por 822 (74%) respondentes, número de cartão de crédito 806 (73%), número de conta corrente e agência 740 (67%), saldo bancário 712 (64%) e gastos com cartão de crédito 696 (63%). De acordo com as análises realizadas, os homens demonstraram maior preocupação (responderam como muito preocupado ou muitíssimo preocupado) com as informações de senhas (86,02%), número de cartão de crédito (85,07%), saldo bancário (77,96%), número de conta corrente e agência (77,96%), limite de cartão de crédito (76,07%), limite do cheque especial (71,33%), e a informação apontada como de menor preocupação foi a orientação sexual, com 25,12% dos homens respondendo estar muito ou muitíssimo preocupado. Os resultados obtidos para o gênero feminino indicam uma maior preocupação (responderam muito preocupado ou muitíssimo preocupado) com relação ao número de cartão de crédito (87,54%), senhas (87,10%), número de conta corrente e agência (82,70%), saldo bancário (80,94%), limite de cartão de crédito (79,18%) e limite de cheque especial (77,27). A informação indicada como menos sensível pelas mulheres foi a orientação sexual, com 25,22% dos respondentes indicando como muito ou muitíssimo preocupado.

## 4 RESULTADOS

Para realizar a análise de cluster, através do software SPSS Statistics, versão 21, utilizou-se a análise de agrupamentos k médias, que é um método não hierárquico, que segundo Hair et al. (2009, p. 454) apresenta vantagens em relação as técnicas hierárquicas, tais como: “os resultados são menos suscetíveis a observações atípicas nos dados”. As estatísticas aplicadas foram centros de agrupamento inicial, ANOVA e informações de agrupamento para cada caso, tendo sido definido o número de quatro agrupamentos para a análise.

Foram identificados quatro clusters, conforme pode ser visto na Tabela 1, sendo que o 1 e 2 apresentaram maior grau de preocupação com a privacidade. Nas variáveis dos construtos Coleta, Uso Secundário, Erros, Acesso Indevido e Risco, os clusters 1 e 2 apresentaram valores muito similares, entre 6 e 7. As exceções estão nas variáveis ERR3, RISC2 e RISC4, nas quais o cluster 1 apresentou valores de preocupação inferior. A principal diferença entre estes clusters está nas variáveis do construto Confiança. Os resultados indicam que o cluster 1 tem grau de confiança muito baixo, enquanto que o cluster 2 apresentou alto grau de confiança com relação ao construto. O cluster 4 apresentou neutralidade com relação a confiança, enquanto que o cluster 3 apresentou grau de preocupação muito baixo em relação ao mesmo construto. Contrario senso, os clusters 3 e 4 apresentaram graus de preocupação muito baixos ou inexistentes, com valores entre 2 e 3.

Tabela 1 – Número de casos em cada cluster

| Cluster | Número de casos |
|---|---|
| 1 | 374 |
| 2 | 326 |
| 3 | 315 |
| 4 | 89 |
| Total | 1104 |

Fonte: O autor (2015)

Os resultados apresentados pelo construto coleta, que busca identificar o grau em que um usuário está preocupado com a quantidade de dados específicos do indivíduo em pose de websites (MALHOTRA et al.,2004), indicam elevado grau de preocupação relacionado a este construto.

O construto Uso Secundário, que busca identificar o grau em que um usuário está preocupado que informações pessoais são coletadas por sites para uma finalidade, mas são usadas para o outro objetivo secundário, sem autorização do indivíduo (SMITH et al., 1996), apresenta resultados que indicam o alto grau de preocupação relacionado ao construto.

O construto controle, que tem como objetivo identificar o grau em que um usuário está preocupado que ele não tem controle adequado sobre suas informações pessoais mantidas por sites (MALHOTRA et al.,2004), apresenta valores médios que indicam alto grau de preocupação.

O construto Erros, que busca identificar o grau em que um usuário está preocupado com proteções inadequadas contra erros deliberados ou acidentais em dados pessoais recolhidos pelos sites (SMITH et al., 1996), apresenta valores médios altos, que indicam elevado grau de preocupação relacionado a este construto.

O construto Acesso Indevido, que busca identificar o grau em que um usuário está preocupado que as informações pessoais mantidas por sites estão prontamente disponíveis para as pessoas, não devidamente autorizadas a exibir ou trabalhar com os dados (SMITH et al., 1996), apresenta resultados que indicam alta preocupação com o acesso indevido.

O construto Consciência, que tem como objetivo identificar o grau em que um usuário está preocupado com sua consciência sobre as práticas dos sites relacionados à privacidade da informação (MALHOTRA et al.,2004), apresenta resultados que indicam alto grau de preocupação com relação a este construto.

O construto Crenças de Confiança, que busca identificar o grau em que um usuário confia nas empresas para as quais fornece informações na Internet (MALHOTRA et al.,2004), apresentou valores que indicam que os usuários têm um grau de confiança neutro

O construto Crenças de Risco, que busca identificar o grau em que um usuário percebe risco em suas atividades na Internet (MALHOTRA et al.,2004), apresenta resultados que indicam alto grau de preocupação com o risco.

Os resultados apresentados indicam que os usuários de Internet das Regiões Sul e Sudeste do Brasil apresentam maior grau de preocupação com a privacidade, por outro lado, as Regiões Norte e Nordeste apresentaram baixo grau de preocupação. Utilizou-se para a medição do grau de preocupação a escala Likert utilizada no instrumento de coleta de dados.

Com relação às questões de sensibilidade da informação, o cluster 2 demonstrou alto grau de preocupação com a maioria das informações, indicando estar muito preocupado ou preocupadíssimo com relação às informações (graus 4 e 5). Os clusters 1 e 3 apresentaram resultados muito similares, demonstrando alto grau de preocupação com muitas das informações, e contrario senso, o cluster 4 apresentou menor grau de preocupação. As informações indicadas como mais sensíveis quanto à privacidade para todos os clusters foram senha, número de cartão de crédito e saldo bancário.

Os valores das distâncias dos centroides indicam uma boa compactação entre os grupos. Segundo os dados, a maior distância está entre os clusters 1 e 2 em relação ao cluster 4. Através dos resultados da análise de variância ANOVA, pode-se identificar quais as variáveis contribuíram mais para a definição dos clusters. De acordo com Hair et al. (2009) as variáveis que mais contribuem para a formação dos cluster são aquelas que apresentam maior quadrado médio do cluster e menor quadrado médio do erro. As variáveis dos construtos de IPC foram determinantes na formação dos clusters, sendo que àquelas que apresentaram

valores mais significativos foram USEC2, USEC3, ACI1, ACI2, ACI3, CTRL3, CONF1, CONF2, CONF3 E CONF4.

Segundo os resultados o cluster 1 tem maior percentual de membros com gradação completa, sendo 27% do total, o cluster 2 é formado em 30% de membros com graduação em andamento e 27% com graduação completa. O cluster 3 tem resultado mais expressivo de 30% dos membros com graduação em andamento, e o cluster 4 possui 29% dos membros com ensino médio completo. A seguir é apresentada a Tabela 49, que mostra a descrição dos clusters em relação às regiões do Brasil. O cluster 1 é formado principalmente por usuários de Internet do Nordeste, com 27%, e da região Sul, com 33%, o cluster 2 é formado por 31% de usuários da região Norte, o cluster 3 apresentou maior distribuição entre as regiões do país sendo 24% Nordeste, 23% Centro-Oeste, 22% Sudeste, 17% Sul e 15% Norte, por fim, o cluster 4 apresentou 31% para aregião Norte, sendo este o valor mais expressivo para este cluster. Pode perceber a partir dos resultados que a região Sul está mais concentrada no cluster 1, com 33%, a região Norte nos cluster 2 e 4, com 31% em cada, e as demais regiões têm uma distribuição mais espalhada entre os clusters.

As mulheres são maioria em todos os clusters, totalizando 63% no cluster 1, 66% no cluster 2, 54% no cluster 3 e 67% no cluster 4. Os usuários de Internet que compõem cada cluster apontaram a situação profissional "empregado" com maior frequência, sendo percentualmente 51% no cluster 1, 49% no cluster 2, 55% no cluster 3 e 47% no cluster 4. Quanto à faixa salarial, os resultados indicam uma grande concentração de membros do cluster 1 com renda de R$ 14.500,00 ou mais, com percentual de 33% dos membros. O cluster 2 apresentou maior concentração de membros com renda de R$ 2.900,00 a R$ 7.249,99, com 31%, o cluster 3 apresentou maior concentração com renda de R$ 1.450,00 a R$ 2.899,99, com 24% e o cluster 4 apresentou maior concentração de membros com renda de R$ 2.900,00 a R$ 7.249,99, com 31%. As características dos agrupamentos apresentadas são apresentadas na Tabela 2a seguir.

Tabela2– Caracterização dos clusters identificados

| | | **Clusters** | | | |
|---|---|---|---|---|---|
| | | **1 - Cluster Estou de Olho** | **2 - Cluster Estou Ligado, Mas Estou Contigo** | **3 - Cluster Estou Numa Boa** | **4 - Cluster Estou Tranquilo e Encaro Todas** |
| **Descrição** | | **Preocupados e desconfiados** | **Preocupados e confiantes** | **Cientes e indiferentes** | **Despreocupados e corajosos** |
| **Características predominantes** | **Preocupação com a privacidade** | Alto grau de preocupação | Alto grau de preocupação | Baixo grau de preocupação | Baixíssimo grau de preocupação |
| | **Confiança** | Desconfiados | Confiantes | Indiferentes | Pouquíssimo confiante |
| | **Risco** | Cuidadosos | Muito cuidadosos | Indiferentes | Corajosos |
| | **Renda** | R$ 14.500,00 ou mais | De R$ 2.900,00 a R$ 7.249,99 | Até R$ 2.899,99 | De R$ 2.900,00 a R$ 7.249,99 |
| | **Escolaridade** | Graduados | Graduandos | Graduandos | Ensino médio |
| | **Região** | Sul/sudeste | Norte | Centro-oeste/nordeste/sudeste | Norte |
| | **Gênero** | Feminino | Feminino | Feminino/masculino | Feminino |

Fonte: O autor (2015)

Percebem-se características bem distintas entre os clusters. De acordo com os resultados apresentados na Tabela 2, percebem-se dois clusters com alto grau de preocupação

com a privacidade e outros dois clusters com graus de preocupação bastante inferiores. Apesar do cluster "Estou de Olho", cujos resultados indicam como desconfiados, ter sido formado pelas regiões Sul (123 pessoas) e Sudeste (102 pessoas), os resultados mostram que a região Sul tem alto grau de desconfiança e a Sudestes alto grau de confiança com relação às práticas de privacidade realizadas pelos sites.

Os resultados mostram que a região Norte do país está divida, uma vez que o cluster 2, dos preocupados e confiantes, e o cluster 4, dos despreocupados e corajosos são formados em maior quantidade por usuários desta região. Outro aspecto importante é que as mulheres tem maior participação na formação de três dos quatro clusters, sendo que somente no cluster 3 a quantidade de homes e mulheres foi muito parecida.

Com relação à renda, os dados mostram um resultado interessante. O cluster 1, dos preocupados e confiantes, formado em sua maior parte por usuários da região sul (123) e sudeste (102), tem maior quantidade de casos de usuários dentro da maior faixa de renda utilizada neste estudo e maior grau de escolaridade entre os clusters. Pode-se verificar que a medida que a faixa salarial dos clusters diminui, o nível de confiança diminui.

## 5 CONTRIBUIÇÕES

O presente estudo fornece um panorama do comportamento do usuário de Internet no contexto brasileiro em relação a preocupação com a privacidade das informaçõespessoais. Uma vez que a legislação brasileira que busca garantir direitos e deveres fundamentais para os usuários de Internet no Brasil, bem como estabelecer os limites das responsabilidades dos provedores de acesso à Internet e traçar diretrizes para a atuação do Estado ainda é muito incipiente, este estudo fornece subsídios direcionadores para o aprimoramento de tal legislação, identificando as maiores preocupação dos usuários.

Os resultados apresentados neste estudo podem levar os usuários de Internet no Brasil a uma reflexão sobre a importância de preservar a privacidade de suas informações pessoais e a reavaliar seu comportamento e a forma como expõem estas informações na Internet. É possível ainda conhecer os riscos a que estes usuários estão se expondo ao publicar suas informações pessoais e informações pessoais de terceiros, podendo levar a um comportamento de privacidade mais seguro.

Uma vez que não foram encontradas pesquisas realizadas com o objetivo de identificar as preocupações com a privacidade dos usuários de Internet no Brasil, este estudo pode servir de ponto de partida para novas pesquisas, bem como ser utilizado para comparar os resultados do contexto brasileiro, com pesquisas futuras realizadas em outros países.

## REFERÊNCIAS

ACQUISTI, A.; GROSSKLAGS, J. Privacy and rationality in individual decision making. **Security & Privacy, IEEE**. v. 3, n. 1, p. 26-33, 2005a.

AJZEN, I.;.FISHBEIN, M. Understanding Attitudes and Predicting Social Behavior, **Prentice-Hall**. Englewood-Cliffs, NJ, 1980.

AYTES, K. CONNOLLY, T. A research Model for Investigating Human BehaviorRelated toComputer Security. Americas Conference on Information Systems: 2027-2031. 2003.

BBC. Entenda as polêmicas sobre o Marco Civil da Internet. Disponível em: <http://www.bbc.co.uk/portuguese/noticias/2014/03/140219_marco_civil_internet_mm.shtml >. Acesso em: 19/04/2014.

BELANGER, F.; HILLER, J.S.; SMITH, W.J. Trustworthiness in electronic commerce: the role ofprivacy, security, and site attributes.**Journal of Strategic Information Systems**.v. 11 n. 3/4, p. 245 – 70, 2002.

BELANGER, F.; CARTER, L. Trust and risk in e-government adoption. **Journal of Strategic Information Systems**, v. 17, n. 2, p. 165–176, 2008.

BELANGER, F.; CROSSLER, R.E. Privacy in the Digital Age: A Review ofInformation Privacy Research in Information Systems. **Mis Quarterly**.v. 35, n. 4, p. 1017 – 1041, 2011.

BELDAD, A.; JONG, M.; STEEHOUDER, M. I trust not therefore it must be risky:Determinants of the perceived risks of disclosing personal data for e-government transactions. **Computers in Human Behavior**. vol.27, n. 6, p.2233 – 2242, 2011.

BOSS, S.R., KIRSCH, L.J., ANGERMEIER, I., SHINGLER, R.I., BOSS, R.W.; If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. **European Journal of Information Systems**. v. 18, p. 151–164, 2009.

DEGIRMENCI, K.; GUHR, N.; BREITNER, M. H. Mobile applications and access topersonal information: A discussion of users' privacy concerns. **Thirty Fourth International Conference on Information Systems**. Milan, s/n., 2013.

DENNING, D. E.Information warfare and security. **ACM Press**, USA, 1999.

GNT. Quem é Edward Snowden, o ex-agente que vazou documentos secretos dos EUA. Disponível em:<http://revistaepoca.globo.com/Mundo/noticia/2013/06/quem-e-edward-snowden-o-ex-agente-que-vazou-documentos-de-espionagem-dos-eua.html>.Acesso em: 06/04/2014.

HAIR JR., J.F; BLACK, W.C.; BABIN, B.J.; ANDERSON, R.E.; TATHAM, R.L.**Análise Multivariada de Dados**. 6 ed. Porto Alegre: Bookman, 2009.

HAIR JR, J. F.; HULT, G. T. M.; RINGLE, C.; SARSTEDT, M.**A primer on partial least squares structural equation modeling (PLS-SEM)**. SAGE Publications, Incorporated, 2013.

HONG, W.Y. ; THONG, J.Y.L. Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. **MIS Quarterly**. v. 37, n. 1, p. 275, 2013.

IBGE. Pesquisa Nacional de Amostra de Domicílios 2011. Rio de Janeiro, 16 de maio de 2013.

MALHOTRA, NK ; KIM, SS ; AGARWAL, J. 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.

MALHOTRA, N. K. Pesquisa de Marketing - Uma Orientação Aplicada. 4 ed. Porto Alegre: Bookman, 2006.

MOOR, J.H.; Towards a Theory of Privacy in the Information Age. **Computers and Society**. 1997.

Ng, B. Y., Xu, Y. Studying Users' Computer Security Behavior Using the Health Belief Model.**PACIS**. p. 45, 2007.

PINSONNEAULT, A.; KRAEMER K. L.; *Survey* research methodology in management information systems: an assessment.**Journal of Management Information Systems**. v. 10, n. 2, p. 75 – 105, 1993.

PUHAKAINEN, P. A design theory for information security awareness. Acta University of Oulu. Oulu – Finland, 2006.

SHIN, D.H. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. **Interacting with Computers**. v. 22, n. 5, p. 428 – 438,2010.

SMITH, H. J.; MILBERG, S. J.; BURKE, S. J. Information Privacy: Measuring Individuals' Concerns About Organizational Practices. MIS Quarterly, v. 20, n. 2, p. 167-196, 1996.

SOM, J.; KIM, S.S. Internet Users' Information Privacy-ProtectiveResponses: a Taxonomy and a Nomological Model. **Mis Quarterly**,v. 32, n. 3, p. 503 – 529, 2008.

STEWART, K.A. SEGARS, A.H.; An empirical examination of the concern for information privacy instrument. **Information Systems Research**, v. 13, n. 1, p. 36 – 49, 2002.

TRCEK, D.; TROBEC, R.; PAVES, N.; TASIC, J.F. Information systems security and human behavior. **Behaviour & Information Technology**. v. 26, n. 2, p. 113 – 118, 2007.

XU, H. et al. Measuring mobile users' concerns for information privacy. **Thirty Third International Conference on Information Systems (ICIS)**. Orlando: [s.n.]. 2012.

WARTOFSKY, M. W. Risk, relativism, and rationality. **New York, NY: Plenum Press**. p. 131–153, 1986.

WESTIN, A. F.; **Privacy and Freedom**, New York: Atheneum, 1967.