PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO EM ADMINISTRAÇÃO E NEGÓCIOS

VERGILIO RICARDO BRITTO DA SILVA

PREOCUPAÇÃO COM A PRIVACIDADE NA INTERNET: UMA PESQUISA EXPLORATÓRIA NO CENÁRIO BRASILEIRO

Porto Alegre
Março, 2015

VERGILIO RICARDO BRITTO DA SILVA

PREOCUPAÇÃO COM A PRIVACIDADE NA INTERNET: UMA PESQUISA EXPLORATÓRIA NO CENÁRIO BRASILEIRO

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Administração, pelo Programa de Pós-Graduação em Administração, da Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul.

Orientadora: Profª. Drª. Edimara Mezzomo Luciano

Porto Alegre

Março, 2015

Catalogação na Fonte

S586p Silva, Vergilio Ricardo Britto da
Preocupação com a privacidade na internet: uma pesquisa exploratória no cenário brasileiro / Vergilio Ricardo Britto da Silva. – Porto Alegre, 2015.
117 f.
Diss. (Mestrado) – Faculdade de Administração, Contabilidade e Economia, PUCRS.

Orientador: Profª. Drª. Edimara Mezzomo Luciano.

1. Privacidade das Informações Pessoais. 2. Internet - Privacidade. 3. Direito à Privacidade. 4. Risco à Privacidade. 5. Segurança de Informação. I. Luciano, Edimara Mezzomo. II. Título.

CDD 341.2

Bibliotecário Responsável
Ginamara de Oliveira Lima
CRB 10/1204

Vergilio Ricardo Britto da Silva

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

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Administração, pelo Mestrado em Administração e Negócios da Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul.

Aprovado em 31 de março de 2015, pela Banca Examinadora.

BANCA EXAMINADORA:

Profa. Dra. Edimara Mezzomo Luciano
Orientadora e Presidente da sessão

Prof. Dr. Maurício Gregianin Testa

Profa. Dra. Marie Anne Macadar Moron

Profa. Dra. Flávia Mori Sarti

AGRADECIMENTOS

Aos meus pais Florinda e Vergilio, que foram os meus primeiros professores, que com amor e carinho me passaram valores e princípios essenciais para que eu pudesse trilhar meu caminho.

Ao meu amor, minha esposa Viviane França, pelo amor, apoio, incentivo e por ser uma fonte de inspiração na minha vida. Por ter um papel decisivo para que eu mantivesse o foco e retomasse as forças nos momentos de cansaço, e por todas as xícaras de cafés, muito deliciosos, para que eu pudesse vencer as madrugadas de estudo.

A minhas irmãs Jaqueline, Regina, Luciana e Fernanda, meus sobrinhos Guilherme, Eduardo, Rodrigo e Leonardo, Pedro e Schruder, minhas sobrinhas Natali e Isabela, que são pessoas muito importantes na minha vida, das quais estive distante durante os últimos dois anos.

Aos meus amigos de mais de 30 anos Zezé e Andréia, com os quais compartilhei muitos momentos felizes, e com quem quero compartilhar esta vitória.

A minha orientadora Prof. Dra. Edimara Mezzomo Luciano, pela condução altamente qualificada e determinante para o desenvolvimento deste trabalho, pela compreensão, pela paciência e por ter contribuído com seu vasto conhecimento para que este objetivo fosse alcançado.

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 envolvendo Chefes 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. O grande volume de informações pessoais que são publicadas na Internet diariamente colocam em risco tais direitos. Garantir a privacidade na Internet não depende exclusivamente de tecnologias de proteção, mas principalmente da conscientização dos usuários quanto à importância de entender os riscos a que estão se expondo e conhecer as consequências destes riscos. O objetivo desta pesquisa foi identificar o grau de preocupação com a privacidade dos usuários de Internet do Brasil, relacionado com a Coleta de Dados, Uso Secundário, Erros, Acesso Indevido, Controle sobre as Informações, Consciência, Confiança e Risco, bem como identificar quais as informações os usuários percebem como mais sensíveis quanto à privacidade. 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. O instrumento de coleta de dados utilizado nesta pesquisa teve origem no estudo de Smith et al. (1996), sendo aprimorando por diversos estudos, até a versão final de Hong e Thong (2013). Foi realizada uma pesquisa de natureza exploratória descritiva com o objetivo de identificar opiniões que estão manifestas na população objeto deste estudo, que são os usuários de Internet no Brasil que, segundo pesquisa do IBGE (2013), totalizavam 77,7 milhões de usuários. Foram coletados dados nas cinco regiões do país, totalizando 1.104 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. Entre as informações apontadas como mais sensíveis estão, em ordem de maior preocupação, senhas, número de cartão de crédito, número de conta corrente e agência, saldo bancário, gastos com cartão de crédito e limite de cheque especial. Entre as informações menos sensíveis estão orientação sexual, vícios, escola onde estudou ou estuda, data de nascimento e notas escolares.

Palavras-chave: Segurança da Informação; Privacidade na Internet; Preocupação com a Privacidade; Acesso Indevido; Coleta de Dados; Uso Secundário; Controle sobre as Informações; Risco à Privacidade; Sensibilidade da Informação.

ABSTRACT

The Internet Privacy Concern - IPC is a study area that is receiving more attention nowadays due to the extensive amount of personal information being transferred through the Internet. The constant scandals of privacy invasion and espionage involving heads of state have brought more evidence for this discussion. This research addresses the topic Information Security, focusing on Internet Privacy Concern. The growth of Information and Communication Technologies usage has generated challenges for fundamental rights, namely: the right to privacy, freedom of expression and freedom of association. The large amount of personal information that is daily published on the Internet endanger those rights. Ensuring privacy on the Internet does not depend on exclusively protection technologies, but mainly of user awareness about the importance of understanding the risks they are exposing themselves and knowing the consequences of these risks. The aim of this research was to identify the degree of concern about the privacy among Internet users in Brazil, related to Data Collection, Secondary Use, Errors, Improper access, Control over The Information, Awareness, Trust and Risk, and to identify which piece of information users notice as more sensitive in relation to privacy. This research is based on theoretical studies on Privacy on the Internet, Privacy Concern and User Behavior, showing the evolution of Concern construct with the Privacy and indicate how users deal with their privacy. The data collection instrument employed in this study originated in the study of Smith et al. (1996), and has been improved by several studies up to the final version of Hong and Thong (2013). A descriptive exploratory survey was conducted aiming to identify opinions that are being manifested in the target population of this study, which are Internet users in Brazil that according to the IBGE survey (2013), totaled 77,7 million users. Data were collected in the five regions of the country, summing up 1,104 completed questionnaires. The results indicate a high degree of concern for the privacy of Internet users in Brazil, mainly in the South and South-East regions, which showed the highest concernment indexes. Among the information identified as sensitive are, in order of greatest concern, passwords, credit card number, checking account number and agency, bank balance, spending on credit card and overdraft limit. Among the less sensitive information is sexual orientation, addictions, school where they have studied, date of birth and school grades.

Keywords: Information Security; Internet privacy; Privacy Concern; Improper Access; Data Collection; Secondary Use; Control over Information; Risk of Privacy; Information Sensitivity.

LISTA DE ILUSTRAÇÕES

Figura 1 – Quantidade de dados dos usuários do Facebook configurados como públicos..... 17
Figura 2 – Percentual das pessoas que acessaram a Internet por faixa etária 21
Figura 3 – Percentual de pessoas que acessaram a Internet por região do país..... 22
Quadro 1 – Construto Preocupação com a Privacidade das Informações 35
Quadro 2 – Dimensões da escala de IUIPC..... 37
Quadro 3 – Dimensões da escala de MUIPC 37
Quadro 4 – Roteiro dos Quatro Estudos 38
Quadro 5 – Dimensões do construto de IPC..... 39
Figura 4 – Desenho da pesquisa 47
Quadro 6 – Questões submetidas à validação de face 50
Quadro 7 – Teste de KMO e Bartlett do Pré-Teste 55
Quadro 8 – Teste de KMO e Bartlett..... 67
Gráfico 1 – Scree Test 70
Figura 5 – Modelo teórico IPC 73

LISTA DE TABELAS

Tabela 1 – Dados coletados nos serviços de redes sociais e e-mails gratuítos 17
Tabela 2– Alfa de Cronbach na fase do pré-teste 54
Tabela 3 – Alfa de Cronbach dos Construtos na fase do pré-teste 55
Tabela 4 – Comunalidades das variáveis no pré-teste 56
Tabela 5 – Variância total explicada 57
Tabela 6 – Estatísticas de confiabilidade na coleta final 57
Tabela 7 – Alfa de Cronbach dos construtos 57
Tabela 8 – Faixa Etária, Renda e Gênero 58
Tabela 9 – Grau de Escolaridade e Situação Profissional 59
Tabela 10 – Horas de Navegação na Internet, Utilização de Redes sociais 59
Tabela 11 – Sensibilidade das Informações 60
Tabela 12 – Frequência de Respostas dos Construtos 62
Tabela 13 – Média da preocupação com a privacidade por região do Brasil 64
Tabela 14 – Análise descritiva estatística da amostra 66
Tabela 15 – Matriz de Correlações 67
Tabela 16 – Comunalidades 68
Tabela 17 – Variância total explicada 69
Tabela 18 – Matriz de análise fatorial de componente não-rotacionada 71
Tabela 19 – Matriz de análise fatorial de componentes rotacionadas por Varimax 72
Tabela 20 – Correlações quadradas múltiplas 74
Tabela 21 – Qui-quadrado sobre os graus de liberdade (CMIN/DF) 75
Tabela 22 – Comparações de Baseline 75
Tabela 23 – Raiz do erro quadrático médio de aproximação (RMSEA) 75
Tabela 24 – Índice de Holter 76
Tabela 25 – Validade e confiabilidade convergente 76
Tabela 26 – Cargas significativas das variáveis 77
Tabela 27 – Validade discriminante do modelo 78
Tabela 28 – Caracterização dos *clusters* identificados 78
Tabela 29 – Centro de *clusters* iniciais 80
Tabela 30 – Histórico de iterações 80
Tabela 31 – Membros dos *Clusters* 81
Tabela 32 – Médias dos *Clusters* Finais 81

Tabela 33 – Número de casos em cada cluster 82
Tabela 34 – Resultados da análise da ANOVA 83
Tabela 35 – Distância entre centroides dos *clusters* 84
Tabela 36 – Caracterização dos *clusters* pelo grau de escolaridade 84
Tabela 37 – Caracterização dos *clusters* pelas regiões do Brasil 85
Tabela 38 – Caracterização dos *clusters* pelo gênero 85
Tabela 39 – Caracterização dos *clusters* pela situação profissional 86
Tabela 40 – Caracterização dos *clusters* por faixa salarial 86
Tabela 41 – Comparação dos resultados com estudos anteriores 88

LISTA DE SIGLAS

IPC	Preocupações com a Privacidade na Internet
PNAD	Pesquisa Nacional por Amostra de Domicílios
IBGE	Instituto Brasileiro de Geografia e Estatística – IBGE
APPS	Aplicações Móveis
CIA	Agência Central de Inteligência
NSA	Agência de Segurança Nacional
CFIP	Privacidade das Informações
IUIPC	Privacidade das Informações Pessoais dos Usuários de Internet
MUIPC	*Mobile User's Concerns for Information Privacy*
TDM	Teoria do Desenvolvimento Multidimensional
FRA	European Union Agency for Fundamental Rights
TIC	Tecnologias da Informação e Comunicação
DHS	Departamento de Segurança Interna dos Estados Unidos
FIPP	Fair Information Practice Principles
CFA	Análise Fatorial Confirmatória

SUMÁRIO

1 INTRODUÇÃO 13

1.1 DELIMITAÇÃO DO TEMA E SITUAÇÃO PROBLEMÁTICA 14

1.2 OBJETIVOS 20

1.3 JUSTIFICATIVA 20

2 REFERENCIAL TEÓRICO 24

2.1 SEGURANÇA DA INFORMAÇÃO 24

2.2 PRIVACIDADE DAS INFORMAÇÕES PESSOAIS 27

2.3 RISCO À PRIVACIDADE 32

2.4 PREOCUPAÇÃO COM A PRIVACIDADE 34

2.4.1 Preocupações com a Privacidade dos Usuários de Internet 36

2.4.2 Preocupação com a Privacidade dos Usuários de Dispositivos Móveis 37

2.4.3 Preocupação com a Privacidade na Internet 38

2.4.4 Comportamento do Usuário 40

2.5 LEGISLAÇÃO SOBRE PRIVACIDADE 41

2.5.1 Estados Unidos da América 41

2.5.2 Europa 43

2.5.3 Comitê Gestor da Internet no Brasil 43

2.5.4 Marco Civil da Internet - Brasil 45

3 MÉTODO DE PESQUISA 47

3.1 ESTRUTURA DA PESQUISA 47

3.2 POPULAÇÃO E AMOSTRA 48

3.3 INSTRUMENTO DE COLETA DE DADOS 49

3.4 PRÉ-TESTE 51

3.5 COLETA DE DADOS FINAL 52

3.6 ANÁLISE DE DADOS 52

4 RESULTADOS 54
4.1 ANÁLISE DE CONFIABILIDADE DO INSTRUMENTO NO PRÉ-TESTE 54
4.2 ANÁLISE DE CONFIABILIDADE NA COLETA FINAL 57
4.3 ANÁLISE DESCRITIVA DA AMOSTRA 58
4.4 ANÁLISE DESCRITIVA UNIVARIADA 65
4.5 ANÁLISE FATORIAL EXPLORATÓRIA 67
4.6 ANÁLISE CONFIRMATÓRIA DO MODELO DE MENSURAÇÃO 73
4.7 VALIDADE CONVERGENTE E DISCRIMINANTE 76
4.8 ANÁLISE DE CLUSTERS 78
5 CONSIDERAÇÕES FINAIS 87
REFERÊNCIAS 90
ANEXO A – DADOS CONFIGURADOS COMO PÚBLICOS NO FACEBOOK 96
ANEXO B –LEGISLAÇÃO DOS EUA COM IMPLICAÇÕES NA PRIVACIDADE 97
ANEXO C – REDE NOMOLÓGICA DE IPC 98
ANEXO D – INSTRUMENTO DE PESQUISA - IPC 99
ANEXO E – MARCO CIVIL DA INTERNET NO BRASIL 100
APÊNDICE A – INSTRUMENTO DE COLETA DE DADOS FINAL 109
APÊNDICE B – COVARIÂNCIA RESIDUAL PADRONIZADA 114

1 INTRODUÇÃO

A presente pesquisa aborda o tema Segurança da Informação, mais especificamente sobre a preocupação com a privacidade na 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 foi 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 o aumento da frequência de incidentes de segurança é 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, como por 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 seguir serão abordados em sequência a delimitação do tema e situação problemática, os objetivos, o referencial teórico e o método utilizado nesta pesquisa.

1.1 DELIMITAÇÃO DO TEMA E SITUAÇÃO PROBLEMÁTICA

A segurança de Sistemas de Informação recebeu uma grande atenção e cobertura nos meios de comunicação populares ao longo dos últimos dez 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.

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. Por outro lado, a preocupação com a privacidade faz com que os usuários fiquem mais atentos em relação a seus dados pessoais.

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 permitem que 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.

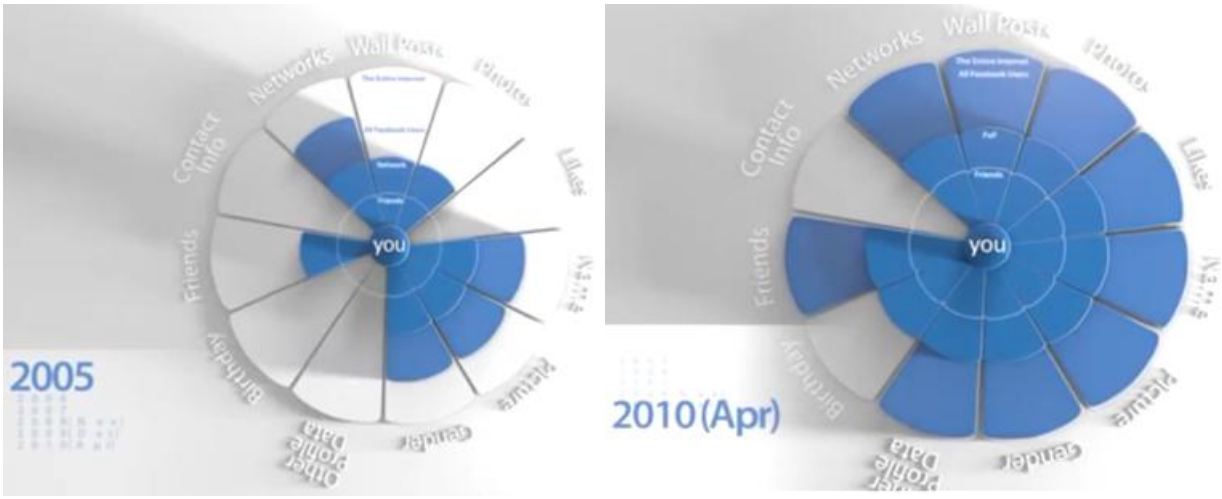
Um exemplo da abrangência das permissões que o usuário fornece para os provedores de serviços na Internet são aquelas fornecidas à rede de relacionamento profissional LinkedIn, quando o usuário concorda com os termos e políticas, onde consta:

> 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 compartilhar 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. A evolução de tais políticas de privacidade mostra que a quantidade de informações dos usuários que são definidas por padrão como públicas aumentou desde 2005, conforme indicado na Figura 1 a seguir:

Figura 1 – Quantidade de dados dos usuários do Facebook configurados como públicos



Fonte: GNT (2014)

A partir das mudanças, cuja evolução pode ser verificada no Anexo A, entende-se que caso os usuários não ajustem suas configurações de privacidades, estarão compartilhando uma considerável quantidade de informações pessoais, que poderá ser acessada por qualquer usuário da Internet. A Tabela 1 apresenta as informações que são coletadas pelas empresas provedoras de serviços de redes sociais e e-mails gratuitos.

Tabela 1 – Dados coletados nos serviços de redes sociais e e-mails gratuítos

Grupo de Informações	**Informações Coletadas**		
Informações Pessoais	Usuário Senha Nome Sobrenome Telefones Foto	Religião Etnia Orientação sexual Filhos Relacionamento Com quem mora	E-mail Sexo Data de nascimento Local de nascimento Nacionalidade
Hábitos	Fumar Beber Animal de estimação	Livros Filmes Músicas	Check-in realizado
Informações Acadêmicas	Escola onde estudou	Ano de conclusão/período	Faculdade
Profissionais	Empresa onde trabalha Perfil profissional	Profissão Salário	Cargo
Dados Técnicos	Coleta IP	Sistema Operacional Provedor de Internet	Browser Operadora de celular
Localização	Endereço CEP	País onde mora Localização	Cidade onde mora Check-in

Fonte: O autor (2015)

Os dados da Tabela 1 mostram a quantidade e os tipos de dados que são coletados ao se cadastrar ou utilizar os serviços de redes sociais e e-mails gratuitos, indicando quais dados podem ser obtidos em caso de invasão 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 W. 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). Estas permissões fazem com que empresas como o Google não possam cumprir o que afirmam em suas políticas de privacidade, que diz que não repassarão as informações coletadas sobre seus usuários exceto quando requerido por um processo legal, como uma ordem de busca, intimação ou mandado.

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).

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 norte 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.

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*.

Segundo Milne et al. (2004) segurança e privacidade em ambientes de *e-commerce* são de grande importância para os consumidores, empresas e reguladores. Os autores afirmam ainda que as violações de segurança das transmissões de Internet e dos bancos de dados permitem a utilização não autorizada de informações confidenciais dos consumidores, como por exemplo, nome, endereço, senhas e cartão de crédito, e muitas vezes podem resultar em roubo de identidade. Por outro lado, "a perspectiva de perdas de privacidade e uso indevido de informações em ambientes de e-commerce pode balançar uma eventual conveniência, tempo ou poupança financeira concedida aos consumidores" (FEATHERMAN et al., 2010, p. 220).

Os autores afirmam ainda que violações de Segurança da Informação estão ocorrendo em ritmo crescente, como por exemplo bancos, agências de crédito e processadores de pagamento continuam a sofrer perdas de informações pessoais confidenciais dos clientes.

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 Beldad et al. (2011), enquanto um usuário avaliar uma organização como confiável, ele irá considerar que as transações realizadas com esta organização seguras.

Por outro lado, segundo Beldad et al. (2011), a relação entre o nível de experiência de Internet dos usuários e de suas percepções dos riscos em transações *online* é, de alguma forma, complexa. Corbitt e Thanasankit (2003) afirmam que a experiência das pessoas com a Internet não reduz a percepção de riscos de segurança e privacidade, enquanto que os autores Yao et al. (2007) concluíram que a fluência dos internautas com a Internet não significa que os usuários terão menos preocupações com a privacidade. Reforçando esta afirmação, os autores Miyazaki & Fernandez (2001) afirmam que as preocupações com a privacidade da informação são mais elevadas para pessoas com mais experiência na Internet.

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?

1.2 OBJETIVOS

Buscando conhecer os fatores relacionados com a situação problemática e visando atender ao tema e ao foco deste estudo, foi estabelecido o objetivo, identificar o grau de preocupação com a privacidade dos dados pessoais de usuários de Internet no Brasil. Os objetivos específicos definidos a partir do objetivo geral, são os seguintes:

a) Versionar e validar o instrumento de coleta de dados, a partir do instrumento desenvolvido por Hong e Thong (2013);
b) Identificar o grau de preocupação com a privacidade dos dados pessoais, relacionado com coleta de dados, uso secundário, erros, acesso indevido, controle sobre as informações, consciência com relação à privacidade;
c) Identificar quais as informações o usuário de Internet julga ser mais sensíveis quanto a perda de privacidade

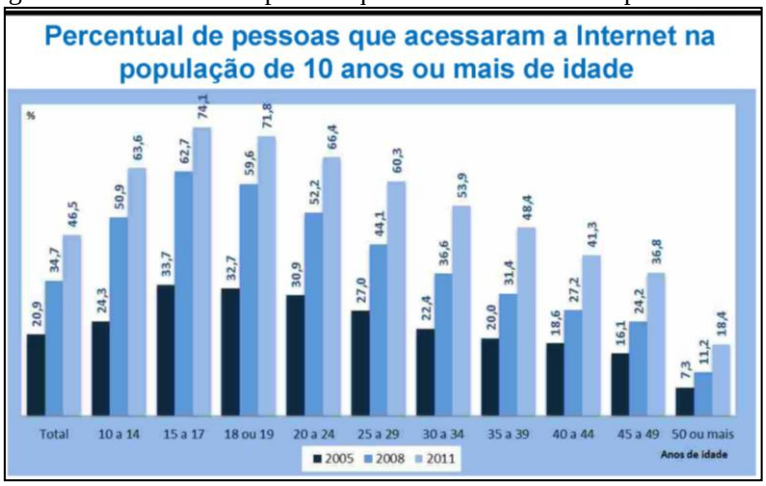
1.3 JUSTIFICATIVA

A preocupação com a privacidade das informações, de acordo com Malhotra et al. (2004), refere-se a visões subjetivas de justiça de um indivíduo no contexto da privacidade da informação, e que as preocupações com a privacidade de um indivíduo serão influenciadas por condições externas como setores da indústria, culturas e leis reguladoras. De acordo com

os autores, no entanto, a percepção de um indivíduo de tais condições externas também irá variar de acordo com suas características pessoais e experiências passadas, fazendo com que muitas vezes as pessoas tenham opiniões diferentes sobre o que é ou não justo, relativo à coleta e uso de suas informações pessoais por uma empresa. Segundo os autores, os consumidores consideram a liberação de informações pessoais como uma transação arriscada, porque eles se tornam vulneráveis a possíveis comportamentos oportunistas de uma empresa. De acordo com a FRA (2015) "o crescimento do uso das Tecnologias da Informação e Comunicação (TIC) tem criado desafios para os direitos fundamentais dos cidadãos, quais sejam: o direito à privacidade, à liberdade de expressão ou a liberdade de associação". Segundo a Agência Europeia, estes desafios variam entre preocupação com a privacidade e a potencial utilização abusiva de dados pessoais *online*, até ameaças representadas por cibercrimes ou vigilância em grande escala.

Cada vez mais pessoas têm acesso à Internet no Brasil, segundo a Pesquisa Nacional por Amostra de Domicílios - PNAD, realizada no ano de 2011 pelo Instituto Brasileiro de Geografia e Estatística - IBGE (IBGE, 2013), que afirma que "no Brasil o percentual de pessoas de 10 anos ou mais de idade que acessaram a Internet passou de 20,9% (31,9 milhões) em 2005 para 46,5% (77,7 milhões) em 2011". Ainda segundo esta pesquisa, entre os jovens o percentual de internautas é maior, como pode ser visto na Figura, 2 abaixo.

Figura 2 – Percentual das pessoas que acessaram a Internet por faixa etária

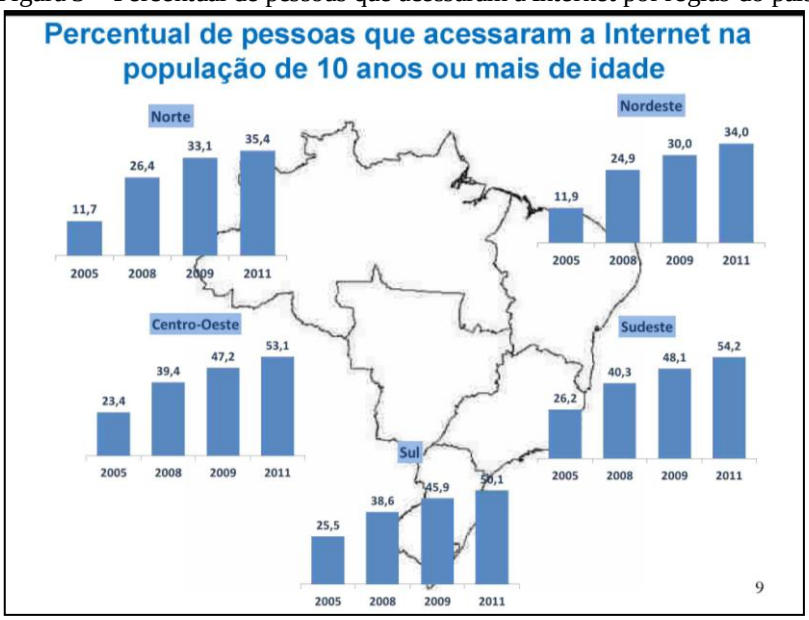


Fonte: IBGE (2013)

A pesquisa PNAD 2011 mostra, conforme Figura 2, que as mulheres eram a maioria entre os internautas de 10 a 39 anos, e que o acesso à Internet chega a 90,2% entre as pessoas com 15 anos ou mais de estudo (IBGE, 2013). A pesquisa afirma ainda que entre os estudantes do ensino superior quase a totalidade acessava a Internet em 2011, com 98,1 % dos

alunos. Como pode ser visto na Figura 3, as regiões do Brasil com maiores percentuais de pessoas que acessaram a Internet são Sudeste, Centro-Oeste e Sul respectivamente (IBGE, 2013).

Figura 3 – Percentual de pessoas que acessaram a Internet por região do país



Fonte: IBGE (2013)

De acordo com Beldad et al. (2011, p. 2235) “os usuários de Internet clamam por controle sobre qualquer informação pessoal que eles divulguem *online*, como uma tentativa de se proteger de riscos à privacidade da informação e como uma afirmação do direito de propriedade sobre ela”. Os autores afirmam ainda que as preocupações dos usuários de Internet relativas à proteção dos seus dados pessoais impulsionam a criação de limites em torno de seus dados e suas percepções sobre os riscos envolvidos na divulgação de seus dados pessoais influenciam tanto a adoção de alguns tipos de estratégias de proteção, quanto a sua intenção de recorrer a comportamentos de proteção à privacidade *online*, quer por meio de estratégias de proteção baseada em tecnologia ou ocultando e falsificando informações.

Segundo Acquist e Grossklags (2005), os usuários de Internet estão relutantes em divulgar informações pessoais identificáveis, tais como nome completo ou endereço de contato e informações financeiras, como renda e número de cartão de crédito. Os autores afirmam ainda que as solicitações de informações de perfil, por exemplo: idade, peso, orientação sexual ou política, levantaram pouca preocupação entre os usuários, quando solicitadas isoladamente, sem a possibilidade de identificar o usuário que forneceu tal informação. Ainda segundo os autores, estes pontos justificam a afirmação de que a

disposição dos usuários de divulgar os dados pessoais é determinada pelo tipo de dados solicitados pelas empresas.

De acordo com Earp et al. (2005), a privacidade das informações tem sido reconhecida como uma importante questão de gestão, e tal importância deve continuar crescendo, uma vez que o valor da informação cresce a cada dia. Para os autores, compreender e proteger a privacidade pessoal em sistemas de informação está se tornando cada vez mais importante com o uso generalizado de sistemas em rede e da Internet. Os autores afirmam ainda que essas tecnologias oferecem oportunidades de coletar grandes quantidades de informações pessoais sobre os usuários e potencialmente violar suas privacidades.

Identificar o grau de preocupação com a privacidade das informações pessoais de usuários de Internet pode chamar a atenção das pessoas para os riscos relacionados à privacidade das informações pessoais aos quais estão se expondo ao fornecer suas informações para quaisquer serviços oferecidos, bem como direcionar o aprimoramento da legislação voltada à proteção das informações pessoais na Internet. Esta pesquisa se justifica em função da crescente quantidade de informações publicadas na Internet, e da possível perda de controle dos usuários sobre estas informações após terem sido publicadas. Da mesma forma, justifica-se pelo contínuo crescimento do número de pessoas que acessam a Internet no Brasil, conforme pode ser verificado com os resultados da PNAD, realizada no ano de 2011 pelo IBGE (2013), potencializando os riscos de violação da privacidade dos usuários.

2 REFERENCIAL TEÓRICO

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

No âmbito do direito civil, a Constituição Federal de 1988, em seu Artigo 5º diz que "são invioláveis a intimidade, a vida, a honra e a imagem das pessoas, assegurando o direito e a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988). No contexto da Internet no Brasil, foi sancionado pela Presidente da República um projeto de lei intitulado Marco Civil da Internet, com o objetivo de regular o uso da Internet no país e estabelecer princípios, garantias e deveres, bem como determinar diretrizes para a atuação da União em relação ao assunto.

Os riscos relacionados à Segurança da Informação (SI), segundo Bulgurcu et al. (2010), são o principal desafio para muitas organizações, uma vez que estes riscos podem ter consequências extremas, incluindo responsabilidade corporativa, perda de credibilidade e dano monetário. Segundo os autores, assegurar a SI tornou-se uma das principais prioridades administrativas em algumas organizações. De acordo com Bulgurcu et al. (2010), muitas organizações reconhecem que os empregados são considerados frequentemente como o elo mais fraco em SI, mas também podem ser grandes trunfos para reduzir o risco à SI. Segundo os autores, empregados que cumprem as regras e regulamentos de SI da organização são a chave para fortalecer a Segurança da Informação.

A segurança da informação nas redes sociais é abordada por Verma et al. (2013), que afirmam que o surgimento das redes sociais *online* trouxe uma era que mudou todo o cenário do compartilhamento de informações *online*. Segundo os autores, a quantidade e o tamanho das informações, antes restritos por infraestrutura e serviços limitados, tais como e-mail, compartilhamento de arquivos e comunicadores instantâneos, foi amplificado com a grande variedade de serviços oferecidos pelas redes sociais.

2.1 SEGURANÇA DA INFORMAÇÃO

Segundo Luciano et al. (2012, p. 148), "a informação é fundamental para o funcionamento de grande parte das organizações, e é imprescindível que ela esteja sempre disponível". De acordo com Williams (2001) o conceito de Segurança aplica-se a todas as informações. O autor afirma ainda que segurança está relacionada à proteção de ativos

valiosos contra a perda, divulgação não autorizada ou danos. O autor define como ativos valiosos as informações gravadas, transformadas, armazenadas, compartilhadas, transmitidas em um meio eletrônico.

De acordo com Williams (2001) no ambiente global de negócios, o significado e a importância da informação são amplamente aceitos, e os sistemas de informação permeiam toda a empresa. Para Ng et al. (2008) uma vez que as empresas dependem cada vez mais de sistemas de informação para a transmissão, processamento e armazenamento de informações, tornou-se essencial proteger estas informações e garantir a disponibilidade destes sistemas. Os autores afirmam ainda que, no entanto, a crescente dependência das organizações dos sistemas de informação, bem como a facilidade de montagem de ataques tem levado a um aumento do número de incidentes de segurança e de danos causados.

Segundo Ng e Rahin (2005), em um mundo altamente interconectado, a segurança cibernética é um problema sério que requer atenção. Em consonância a isto, a Segurança da Informação tem sido uma das grandes preocupações das empresas atualmente, uma vez que a informação se tornou um dos seus maiores ativos, e segundo Puhakainen (2006) esses ativos são em grande parte eletrônicos e são processados por sistemas de informação que se comunicam sobre redes privadas e pela Internet. O autor afirma ainda que a Segurança da Informação pode ser definida em termos de confidencialidade, integridade e disponibilidade. De acordo com Johnston e Warkentin (2010, p. 549) “dentro do ambiente moderno de negócios as organizações comumente sofrem com ameaças aos dados corporativos, infraestrutura de tecnologia da informação e computação pessoal”. Os autores afirmam ainda que, além dessas ameaças, os incidentes de segurança, tais como vírus, invasões de sistema, abuso de informação privilegiada, ou outras formas de acesso não autorizado continuam a evoluir em sofisticação e impacto.

Neste contexto, Williams (2001) afirma que os dados ou informações devem ser protegidos contra danos de ameaças que podem levar a perda, falta de acesso ou divulgação ilegal destes dados ou informações. Para o autor a proteção decorre a partir de uma série de seguranças tecnológicas e não tecnológicas, tais como medidas de segurança física, verificação de antecedentes das pessoas que têm acesso às informações sensíveis, senhas, cartões inteligentes, biometria e *firewalls* devidamente implementados e gerenciados. O autor afirma ainda, que a segurança tecnológica mais avançada hoje, torna-se muitas vezes obsoleta ou inadequada em pouco tempo.

Segundo Williams (2001) o objetivo da Segurança da Informação é proteger os interesses que se baseiam nas informações e os sistemas e comunicações que entregam a

informação, de qualquer dano resultante de falhas de indisponibilidade, confidencialidade e integridade. O autor afirma ainda que a economia baseada em redes acrescentou a necessidade de confiança nas transações eletrônicas, de forma que, para a maioria das organizações, o objetivo da segurança é cumprido quando:

a) Os sistemas de informação estão disponíveis e utilizáveis quando necessários, podem adequadamente resistir a ataques e se recuperar de falhas (disponibilidade);
b) Dados e informações são divulgadas apenas para aqueles que têm o direito de saber (confidencialidade);
c) Dados e informações são protegidos contra modificações não autorizadas (integridade);
d) As transações comerciais podem ser confiáveis (autenticidade e não repúdio).

Segundo Kankanhalli et al. (2003), a gestão inadequada da preocupação com a segurança do sistema de informação é perturbadora, tendo em vista as evidências de que ocorrem significativos abusos de segurança de sistemas de informação. Segundo Williams (2001), estas são as principais atividades envolvidas na segurança da informação:

a) Desenvolvimento de Políticas: usando os objetivos de segurança e os princípios fundamentais como um *framework* em torno do qual desenvolver a política de segurança;
b) Papéis e responsabilidades: a garantia de que os papéis individuais, responsabilidades e autoridade são claramente comunicadas e entendidas por todos;
c) *Design*: desenvolvimento de uma estrutura de segurança e controle que consiste em normas, medidas, práticas e procedimentos;
d) Implementação: implementar a solução em tempo hábil e depois mantê-la;
e) Monitoramento: o estabelecimento de medidas de monitoramento, para detectar e assegurar a correção de falhas de segurança, de modo que todas as violações reais e suspeitas sejam prontamente identificadas, investigadas e se tome a ação necessária, e para assegurar a conformidade com a política, normas e práticas de segurança mínimas aceitáveis.
f) Sensibilização, Formação e Educação: promover a conscientização sobre a necessidade de proteger as informações nas habilidades necessárias para operar os sistemas de informação de forma segura, e oferecendo formação em medidas e práticas de segurança.

Por outro lado, de acordo com Ng e Rahin (2005) é imperativo estudar a segurança dos computadores domésticos ligados à Internet, uma vez que estes têm impacto direto não

somente nestes computadores, mas na segurança do ciberespaço. Os autores afirmam que computadores domésticos indefesos podem se tornar parte de redes de máquinas controladas remotamente, que são então utilizadas para atacar infraestruturas críticas. Segundo Ng e Rahin (2005) uma das maiores ameaças aos computadores domésticos são os vírus, que tem potencial para ameaçar a confidencialidade e a integridade das informações, bem como a disponibilidade de computadores e redes.

2.2 PRIVACIDADE DAS INFORMAÇÕES PESSOAIS

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, que tratou 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.

A privacidade das informações foi definida por Smith et al. (1996) como uma das questões éticas mais importantes da era da informação. Os autores afirmaram ainda que pesquisas realizadas naquela época já mostravam um aumento nos níveis de preocupação com a privacidade das informações entre os norte-americanos. A privacidade, segundo o que afirma Moor (1997), é um dos problemas mais paradigmáticos que envolve a computação. Segundo o autor, a capacidade dos computadores para manipular, armazenar indefinidamente, classificar de forma eficiente e localizar informações facilmente, faz com que os indivíduos estejam justificadamente preocupados que, em uma sociedade informatizada, a privacidade possa ser invadida, e que informações prejudiciais sobre estes indivíduos possam ser reveladas.

Existem muitas definições para privacidade da informação, mas existe uma pequena variação nos elementos destas definições que tipicamente incluem alguma forma de controle sobre o potencial uso secundário da informação pessoal (BÉLANGER e CROSSLER, 2011). De acordo com os autores, uso secundário refere-se à prática de usar dados para propósitos diferentes daqueles para os quais foram coletados originalmente.

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.

A coleta de informações pessoais dos consumidores, segundo Hui et al. (2007), é um elemento inevitável do comércio eletrônico, uma vez que os comerciantes na Internet precisam das informações pessoais dos consumidores para entregar os produtos, analisar o perfil dos consumidores e oferecer serviços personalizados. Ainda segundo os autores esta coleta de informações tem benefícios e implicações de risco. Em termos de benefícios, é possível ter acesso a serviços mais convenientes, diminuindo o tempo de transação e o custo de procura por produtos. Em termos de risco, os usuários não podem permanecer anônimos em transações pela Internet, e uma vez que fornecem seus dados, enfrentam um novo espectro de riscos de abuso com relação a suas informações, como a transferência de dados para terceiros ou uso dos dados de modos não intencionais.

Nas transações *online*, de acordo com Li (2012), como o consumidor fornece informações pessoais para o comerciante de bens e serviços, existe uma relação de agência, uma vez que para reduzir o custo causado pelo comportamento oportunista do agente, é preciso incorrer em custos de monitoramento adicional, sendo que a soma destes custos é conhecida como custos de agência. Segundo o autor, uma vez que ambos são partes com interesses próprios, e a assimetria da informação favorece o comerciante *online* que coleta e usa as informações dos clientes durante e após as operações, existem incertezas, tais como riscos de privacidade em relação ao uso da informação. Portanto, o consumidor precisa decidir se irá fornecer as informações para participar das transações, e se sim, como os potenciais riscos podem ser mitigados. Culnan e Armstrong (1999) afirmam que por outro lado, as leis e regulamentos ajudam a transferir parte do custo de agência para o comerciante, obrigando-o a aplicar intervenções para aliviar as preocupações com a privacidade dos clientes, incluindo o uso de políticas de privacidade e garantia de terceiros.

A teoria do contrato social, de acordo com Malhotra et al. (2004), sugere que o fornecimento de informações pessoais para um comerciante *online* envolve não apenas uma troca econômica, isto é, aquisição de bens e serviços, mas também um intercâmbio social, ou seja, o estabelecimento de relações, para que o contrato social, definido como as obrigações

comumente entendidas ou as normas sociais para as partes envolvidas, é fundamental para a prevenção do comportamento oportunista do comerciante, de fazer mau uso das informações do cliente. De acordo com Hoffman et al. (1999), os consumidores não podem completar as transações *online* anonimamente, de modo que eles buscam exercer uma troca social que envolve tanto um contrato econômico, quanto um contrato social para reduzir os riscos potenciais. Segundo Culnan e Armstrong (1999), se os clientes estão preocupados que o site pode não honrar o seu contrato social para proteger suas informações, eles podem optar por não se envolver na relação de troca.

A coleta de informações dos clientes por uma empresa é percebida como justa ou justificável somente quando ao cliente é concedido controle sobre a informação, tal como consentimento informado e direito de saída, e é informado sobre o uso pretendido da informação pela empresa (MALHOTRA et al. ,2004). Por outro lado, segundo Moor (1997) as informações sobre os usuários podem ser coletadas sutilmente, sem que estes percebam. O autor afirma ainda que a facilidade de acesso às informações faz com que outros computadores capturem e manipulem informações de forma desconhecida. Contribuindo ainda mais com este cenário que facilita a coleta de informações dos clientes, os autores Acquisti e Grossklags (2005) afirmam que os indivíduos estão dispostos a trocar a privacidade por conveniência ou negociar a liberação de informações pessoais em troca de recompensas relativamente pequenas. Outra abordagem sobre os fatores que facilitam a coleta de informações é utilizada por Li (2012), quando afirma que, outras crenças pessoais coexistem com as preocupações com a privacidade, e algumas das crenças podem favorecer a divulgação de informações pessoais, tais como os benefícios esperados, que levantam a questão de como os indivíduos comparam as várias crenças e fazem uma compensação na formação da atitude. Segundo Ajzen (1980), a atitude para com a divulgação das informações é determinada por benefícios e riscos percebidos do comportamento de divulgar, considerando que a relação de forças entre as duas crenças, em determinado contexto, determina a atitude geral da pessoa dentro desse contexto.

De um modo geral, de acordo com Li (2012), a intenção de proteção de uma pessoa é alta se a ameaça é grave e a probabilidade é alta, e a pessoa não tem a capacidade de tomar medidas preventivas eficazes para reduzir o risco. Por outro lado, a intenção de proteção é baixa, ou seja, a pessoa está disposta a fornecer informações, se a ameaça é trivial ou altamente improvável e os mecanismos de enfrentamento são eficazes. O autor afirma ainda que a Teoria do Cálculo de Privacidade (TCP) é uma abordagem comum para estudar o efeito conjunto de forças opostas sobre a percepção de privacidade e comportamento. Segundo o

autor, TCP sugere que a intenção de uma pessoa de divulgar informações pessoais se baseia em um cálculo de comportamento, ou seja, cálculo de privacidade, em que fatores potencialmente concorrentes são pesados à luz de resultados possíveis. Segundo Xu et al. (2009), mais especificamente, os consumidores realizam a análise de risco-benefício no cálculo privacidade e decidem se divulgam as informações, com base nos resultados líquidos.

Segundo Li (2012) muitos fatores de risco e benefício de segurança que influenciam o cálculo privacidade e a intenção de divulgar informações pessoais têm sido estudados na literatura, como pode ser visto a seguir.

a) Fatores que aumentam as preocupações de privacidade e desencorajam a divulgação de informações, tais como: riscos percebidos e vulnerabilidade, ansiedade causada pelo computador, experiência anterior com invasão de privacidade, personalidades como consciência social, consciência, abertura à experiência, a desconfiança cínica, paranoia, crítica social e necessidade psicológica de privacidade.
b) Fatores que atenuam as preocupações com a privacidade e incentivam a divulgação de informações, tais como: reputação do site, intervenções do fornecedor como políticas de privacidade e presença social, sensibilidade da Informação, autoeficácia e controlabilidade e personalidades como afabilidade.

Segundo o autor estes exemplos mostram que o cálculo da privacidade é um processo psicológico complexo que envolve várias considerações, sugerindo que é importante ganhar uma compreensão mais profunda desses fatores baseados em teorias adicionais.

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.

No contexto das redes sociais na Internet, conforme Shin (2010), privacidade pode ser definida como controle sobre o fluxo das informações pessoais, inclusive sobre a transferência e a troca destas informações. O autor afirma ainda que riscos inerentes à privacidade estão associados aos serviços de redes sociais na Internet, incluindo:

a) Incapacidade de controlar efetivamente o acesso às informações postadas dos usuários;

b) Incapacidade de controlar efetivamente as informações que outros postam sobre os usuários;
c) Acesso ao site sem ferramentas de verificação de identidade;
d) Roubo de identidade, embora a proteção de *software* adequada no computador dos usuários pode proteger contra abuso de terceiros sobre os dados do perfil.

Com o crescimento rápido da Internet e das tecnologias móveis, e com o aumento dos riscos de brechas de privacidade, o assunto de privacidade recebeu muita atenção de legisladores (LIGINLAL et al., 2008). O Anexo B desta pesquisa mostra um resumo da legislação norte americana com implicações para a privacidade, com foco nas seguintes questões:

a) Especifica como as informações de saúde protegidas deveriam ser administradas pelas entidades de saúde;
b) Regula a coleta e liberação das informações financeiras pessoais dos consumidores pelas instituições financeiras;
c) Regula os direitos e restrições dos país, empregados e agências do estado para acessar os registros educacionais dos estudantes;
d) Exige que todo o comerciante norte americano disponibilize as informações dos clientes para a execução da lei;
e) Requer o descarte adequado referente às informações e registros dos clientes;
f) Estabelece um novo crime federal, por exemplo, roubo qualificado de identidade;
g) Defini e especifica as exigências de notificação, procedimentos e prazos de validade das informações pessoais dos consumidores.

Foi proposto no Brasil pelo Deputado Alessandro Molon um projeto de lei, intitulado Marco Civil da Internet, com o objetivo de traçar princípios como neutralidade e privacidade dos usuários de Internet. O projeto de lei foi aprovado pelo Senado Federal no dia 22/04/2014 e sancionado pela presidente da República Dilma Roussef no dia seguinte (BBC, 2014). "O Marco Civil proíbe o acesso de terceiros a dados e correspondências ou comunicações pela rede. Também busca garantir a liberdade de expressão e a proteção da privacidade dos dados pessoais". O projeto também pretende garantir o direito de expressão dos usuários da Internet, defendendo que conteúdo publicado somente seja retirado da rede após ordem judicial (BBC, 2014). Um dos artigos mais polêmicos do projeto de lei é o de número 20, que trata da responsabilidade dos provedores de Internet sobre o conteúdo produzido por outros *sites* ou pessoas. No projeto aprovado pelos Deputados os provedores não irão responder por aquilo que seus internautas fizerem na rede. Pelo projeto inicial, as operadoras de Internet e *sites* que

grande porte deveriam armazenar todo os seus banco de dados no Brasil, mesmo que fosse uma empresa estrangeira. Esse ponto foi incluído no texto original do projeto após os escândalos de espionagem da Agência Nacional de Segurança dos Estados Unidos (NSA), mas no projeto aprovado este item foi retirado (BBC, 2014).

O Projeto de Lei pretende garantir os seguintes direitos aos usuários de Internet no Brasil (BBC, 2014):

a) Inviolabilidade e sigilo de suas comunicações. Só ordens judiciais para fins de investigação criminal podem mudar isso;
b) Não suspensão de sua conexão, exceto em casos de não pagamento;
c) Manutenção da qualidade contratada da sua conexão;
d) Informações claras nos contratos de prestação de serviços de operadoras de Internet, o que inclui detalhes sobre proteção de dados pessoais;
e) Não fornecimento a terceiros sobre registros de conexão à Internet.

A partir da aprovação do projeto de lei os provedores de Internet ficarão obrigados a manter os registros de conexão em sigilo, em ambiente seguro, por pelo menos um ano, sendo que a guarda deve ser feita de forma anônima, limitada ao registro do protocolo IP, não sendo permitida a guarda das informações dos usuários.

2.3 RISCO À PRIVACIDADE

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.

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 Milne et al. (2004, p. 219) "os consumidores que fazem negócio com empresas *online* estão vulneráveis, de forma geral, de três formas": 1) os dados em seu computador podem ser comprometidos; 2) a transferência de dados para um negócio *online* pode ser comprometida; 3) os dados armazenados pela empresa podem ser comprometidos. Os autores afirmam ainda que, quando estão conectados à Internet, as informações em seus computadores pessoais estão cada vez mais vulneráveis a invasões e roubos, sendo possível também invadir discos rígidos e rastrear as atividades realizadas na Internet.

Segundo Milne et al. (2004, p. 217) as "informações dos consumidores estão em risco quando visitam *sites* ou completam transações *online*". Os autores afirmam que, quando os consumidores fornecem informações sobre cartão de crédito e informações pessoais para *sites*, estas informações podem ser interceptadas, caso a transferência não seja criptografada, e que a privacidade também pode ser comprometida pelos *cookies* que permitem que sejam rastreados os históricos de navegação na Internet. Ainda segundo os autores, outra ameaça para a privacidade dos consumidores ocorre depois que as empresas obtêm os dados pessoais, uma vez que em alguns casos as empresas não têm mantido a promessa de não compartilhar estes dados com terceiros. No entanto as ameaças apontadas pelos autores como mais graves para o roubo de identidade incluem funcionários que roubam dados armazenados eletronicamente, ou ladrões *hackeando* os bancos de dados das empresas e roubando dados pessoais e financeiros.

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.

Beldad et al. (2011) afirmam que a perda de dinheiro e de privacidade dos dados resultantes de abuso ou uso indevido são dois riscos que podem ser esperados transações de comércio eletrônico, e que em transações de governo eletrônico o risco mais importante é a possibilidade de perder a privacidade das informações *online*, o que pode ser atribuído ao uso indevido dos dados pessoais compartilhados para utilizar um serviço fornecido pelo governo

através da Internet. Os autores afirmam ainda que os "dados pessoais podem ser acessados por terceiros não autorizados, alugados ou vendidos a outras organizações, ou apenas utilizados para fins desconhecidos para a pessoa a quem os dados dizem respeito".

2.4 PREOCUPAÇÃO COM A PRIVACIDADE

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 os autores o avanço das tecnologias da informação elevou as preocupações com a privacidade das informações e seus impactos, e motivou os pesquisadores de Sistemas de Informação (SI) a explorar este assunto, incluindo soluções técnicas para tratar estas informações. Da mesma forma, segundo Hong e Thong (2013), *Internet Privacy Concern* (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. Segundo Hong e Thong (2013) embora exista uma literatura emergente sobre IPC existe um acordo limitado sobre sua conceituação, com relação as suas dimensões-chave e estrutura fatorial. Com base na Teoria do Desenvolvimento Multidimensional (TDM) os autores identificaram conceituações alternativas sobre IPC.

Foi realizado um estudo por Smith et a. (1996), com o objetivo de desenvolver e validar um instrumento de coleta de dados para medir as preocupações dos indivíduos sobre as práticas organizacionais de privacidade da informação, pois segundo os autores, baseado em uma série de estudos preliminares, tornou-se evidente que as práticas organizacionais, as percepções dessas práticas dos indivíduos, e as respostas sociais estão intimamente ligadas de várias maneiras. Smith et al. (1996) afirmam que os pesquisadores que tentam examinar tais relações através de abordagens empíricas confirmatórias podiam ser impedidos por falta de instrumentos validados. Segundo Stewart e Segars (2002) os autores adotaram uma abordagem iterativa e sistemática em escala de desenvolvimento, que incluiu a especificação de domínio, especificação do item, inúmeros pré-testes, reespecificação e análise fatorial exploratória e confirmatória. O resultado foi um instrumento de 15 escalas que reflete quatro dimensões do construto de Preocupação com a Privacidade, quais sejam, coleta de informações pessoais, erros nas informações pessoais, uso secundário não autorizado e acesso indevido às informações pessoais (SMITH et al. 1996), conforme mostra a Quadro 1 a seguir.

Quadro 1 – Construto Preocupação com a Privacidade das Informações

Dimensões	Definição
Coleta	Preocupação de que grandes quantidades de dados pessoalmente identificáveis estão sendo coletados e armazenados em bancos de dados
Erros	A preocupação de que proteções contra erros deliberados ou acidentais em dados pessoais são inadequados
Acesso não autorizado	A preocupação de que os dados sobre os indivíduos são facilmente disponíveis para as pessoas não devidamente autorizadas a exibir ou trabalhar com estes dados
Uso secundário não autorizado	A preocupação de que a informação é recolhida a partir de indivíduos para uma finalidade, mas é usado para outra finalidade, secundária (internamente ou compartilhadas com terceiros externos) sem a autorização dos indivíduos

Autor: Smith et al. (1996)

Stewart e Segars (2002) desenvolveram um estudo para examinar empiricamente o instrumento desenvolvido por Smith et al. (1996), com o objetivo de desenvolver ainda mais o referido instrumento, examinando seu significado teórico, dimensionalidade, confiabilidade e validade, além de melhorar a comparação, acumulação e síntese dos resultados (STEWART;

SEGARS, 2002). Foram analisados modelos com um, dois, três e quatro fatores de primeira ordem e um modelo com fator de segunda ordem. Com base em uma amostra de 355 consumidores e trabalhando no âmbito da análise fatorial confirmatória, os autores examinaram a estrutura fatorial do construto Preocupação com a Privacidade das Informações (*Concern for Information Privacy - CFIP*), desenvolvido por Smith et a. (1996). Segundo os autores, os resultados implicam que um tema mais amplo de CFIP pode ser reflexo das dimensões de nível de item. Os autores afirmam ainda que uma política bem sucedida em relação privacidade da informação não deve apenas tratar "o que" e "como" a informação é recolhida e utilizada, mas também considerar a percepção de controle e justiça daqueles que fornecem as informações.

Estudos recentes foram realizados com o objetivo de desenvolver instrumentos de coleta de dados que pudessem medir com mais precisão o construto Preocupação com a Privacidade das Informações. Estes estudos mostram a evolução do construto CFIP, a partir dos estudos que serão apresentados a seguir, até o estudo mais recente realizado por Hong e Thong (2013), que apresenta um instrumento de coleta de dados validado, para medir a Preocupação com a Privacidade na Internet.

2.4.1 Preocupações com a Privacidade dos Usuários de Internet

Utilizando-se das dimensões do construto Preocupação com a Privacidade, desenvolvido por Smith et al. (1996), foi realizado por Malhotra et al. (2004) um exame teórico sobre a natureza e dimensionalidade da Preocupação com a Privacidade das Informações Pessoais dos Usuários de Internet (*Internet Users' Information Privacy Concern* - IUIPC), com o objetivo de desenvolver uma escala para a ideia multidimensional de IUIPC e propor e testar um modelo causal entre IUIPC e a intenção comportamental para a liberação de informações pessoais a pedido de um comerciante (MALHOTRA et al., 2004).

Como resultado, este estudo apresentou uma escala de IUIPC de 10 itens, com as dimensões coleta, controle e consciência, conforme Quadro 2, que segundo os autores, juntamente com a escala de CFIP, será um candidato digno a ser considerado como indicador de preocupações com a privacidade dos consumidores *online*.

Quadro 2 – Dimensões da escala de IUIPC

Dimensões	Definição
Coleta	Grau com que uma pessoa está preocupada com a quantidade de dados individuais específicos possuídas por outros, relativos ao valor dos benefícios recebidos.
Controle	Grau com que uma pessoa está preocupada em não ter o controle adequado sobre suas informações pessoais na Internet.
Consciência	Grau em que uma pessoa está preocupada em saber sobre as práticas dos *sites* relativas à privacidade das informações.

Autor: Malhotra et al. (2004)

Os autores afirmam ainda que a validade de IUIPC ainda tem que ser estabelecida em diferentes contextos da Internet, e com isso os profissionais continuarão a ter a necessidade de contar com CFIP para muitas aplicações.

De acordo com Malhotra et al. (2004), podemos conceituar IUIPC como o grau em que um usuário da Internet está preocupado com a coleta de informações pessoais por comerciantes *online*, o controle do usuário sobre as informações coletadas e a conscientização do usuário de como a informação recolhida é utilizada.

2.4.2 Preocupação com a Privacidade dos Usuários de Dispositivos Móveis

Com o objetivo de desenvolver um *framework* sobre a natureza específica das preocupações com a privacidade da informação dos consumidores móveis Xu et al. (2012) realizaram um estudo no qual desenvolveram a escala MUIPC – *Mobile User's Concerns for Information Privacy*, com três dimensões e nove itens, sendo que uma das dimensões Uso Secundário de Informações Pessoais, foi retirada inteiramente da escala de CFIP de Smith et al.. (1996). Com base na Teoria da Gestão da Privacidade na Comunicação (CPM), Xu et al. (2012) propuseram que as preocupações com a privacidade de usuários móveis estão centradas em três grandes dimensões, a saber, a vigilância percebida, intrusão percebida e uso secundário de informações pessoais, as quais são definidas na Quadro 3 a seguir.

Quadro 3 – Dimensões da escala de MUIPC

Dimensões	Definição
Vigilância Percebida	Solove (2006) definiu vigilância como a observação, o ouvir ou a gravação de atividades de um indivíduo. No ambiente móvel, os vendedores aproveitam as poderosas tecnologias de vigilância para monitorar e perfil dos consumidores. Os usuários móveis podem não utilizar aplicativos móveis por medo de que suas atividades podem ser observadas, registradas e transmitidas para diversas entidades.
Intrusão Percebida	Solove (2006) definiu intrusão como atos invasivos que perturbam a tranquilidade ou a solidão dos indivíduos. A percepção de intrusão dos titulares dos dados seria desencadeada quando os destinatários dos dados fossem capazes de tomar decisões independentes sobre estas informações pessoais.
Uso Secundário	Segundo Smith et al. (1996), a preocupação de que a informação é recolhida a partir de indivíduos para uma finalidade, mas é usado para outra finalidade secundária sem a autorização dos indivíduos

Autor: Xu et al. (2012)

Preocupação com a privacidade da informação dos usuários móveis (MUIPC), de acordo com Xu et al. (2013), é definida como preocupação com uma possível perda de privacidade, como resultado de divulgação de informações a um agente externo específico.

2.4.3 Preocupação com a Privacidade na Internet

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 quais são descritos no Quadro 4 a seguir:

Quadro 4 – Roteiro dos Quatro Estudos

Estudo 1	Estudo 2	Estudo 3	Estudo 4
1. Comparar a baseline de conceituação integrada de IPC contra duas conceituações populares na literatura. 2. Replicar estudos anteriores usando itens de instrumentos existentes	1. Examinar o impacto da formulação inconsistente de itens em instrumentos originais. 2. Validação cruzada dos resultados do estudo 1 usando uma nova amostra.	1. Resolver a formulação inconsistente de itens e adotar uma perspectiva comum na medição de IPC. 2. Avaliar as conceituações integradas alternativas de IPC com uma nova amostra.	1. Validação cruzada das conclusões do estudo 3, utilizando uma nova amostra. 2. Avaliar a validade nomológica do melhor modelo teórico adaptado de IPC identificado no estudo 3.

Fonte: Hong e Thong (2013)

Os autores afirmam ainda 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, que é o grau em que um construto comporta-se como predito dentro de um sistema de construtos relacionados, de acordo com Cronbach e Meehl (1955), 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 conforme Quadro 5 a seguir:

Quadro 5 – Dimensões do construto de IPC

Dimensões	Definição	Fonte
Coleta	Grau com que uma pessoa está preocupada com a quantidade de dados individuais específicos possuídas por outros, relativos ao valor dos benefícios recebidos (MALHOTRA et al., 2004).	Malhotra et al. (2004)
Uso secundário	A preocupação de que a informação é recolhida a partir de indivíduos para uma finalidade, mas é usado para outra finalidade, secundária (internamente ou compartilhadas com terceiros externos) sem a autorização dos indivíduos (SMITH et al., 1996).	Smith et al. (1996)
Erros	A preocupação de que proteções contra erros deliberados ou acidentais em dados pessoais são inadequados (SMITH et al., 1996).	Malhotra et al. (2004).
Acesso indevido	A preocupação de que os dados sobre os indivíduos são facilmente disponíveis para as pessoas não devidamente autorizadas a exibir ou trabalhar com estes dados (SMITH et al., 1996).	Smith et al. (1996)
Controle	Grau com que uma pessoa está preocupada em não ter o controle adequado sobre suas informações pessoais na Internet (MALHOTRA et al., 2004).	Smith et al. (1996)
Consciência	Grau em que uma pessoa está preocupada em saber sobre as práticas dos *sites* relativas à privacidade das informações (MALHOTRA et al., 2004).	Malhotra et al., (2004)
Crenças de confiança	Grau em que o usuário confia nas empresas para as quais fornece informações na Internet.	Malhotra et al., (2004)
Crenças de risco	Grau em que um usuário percebe risco em suas atividades na Internet.	Malhotra et al., (2004)

Fonte: Hong e Thong (2013)

No instrumento desenvolvido, que será utilizado para alcançar os objetivos da presente pesquisa, Hong e Thong (2013) utilizaram a mesma escala Likert de sete pontos, dos estudos de CFIP (SMITH et al., 1996) e IUIPC (MALHOTRA et al., 2004). A escala de IPC foi ajustada, mudando o termo "empresas" para "*sites* comerciais", com o objetivo estar de acordo com o contexto da Internet. Para que fosse possível analisar IPC dentro de uma rede nomológica, foram adicionadas crenças de confiança e crenças de risco ao modelo (HONG e

THONG, 2013), da mesma forma como realizado por Malhotra et al. (2004) no IUIPC. Os resultados confirmaram que o conceito de terceira ordem do construto de IPC é válido nomológicamente, bem como confirmaram que as preocupações com a privacidade na Internet (IPC) têm efeito significativo sobre as crenças de risco e sobre as crenças de confiança. Está análise fornece maior apoio para à conceituação de terceira ordem de IPC (HONG e THONG, 2013).

2.4.4 Comportamento do Usuário

Segundo Luciano, Maçada e Mahmood (2010), o sucesso da Segurança da Informação depende efetivamente dos usuários, uma vez que muitas falhas de segurança têm a participação dos usuários ou funcionários. 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.

Aytes e Connolly (2003) apresentam um modelo de comportamento do usuário que enfatiza os fatores relacionados à percepção de risco do usuário e a escolha com base nessa percepção. Neste modelo, as fontes de informação (por exemplo, treinamento, mídia, colegas de trabalho, amigos, políticas, procedimentos e experiência pessoal) fornecem informações que formam o conhecimento do usuário sobre ameaças e vulnerabilidades, consciência de medidas defensivas, potenciais consequências para si e para os outros e os custos de comportamento seguro. Segundo os autores a percepção dos usuários representa um fator importante no processo de definição de comportamento, que leva ao comportamento real de usar ou não medidas preventivas.

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. De acordo com os autores isso corresponde à suposição de que, enquanto uma organização *online* é avaliada como confiável, as transações com esta organização não seriam consideradas

arriscadas. Ainda segundo os autores, 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). Por outro lado, Culnan e Armstrong (1999) afirmam que os indivíduos realizam um simples cálculo de risco benefício ao decidir divulgar suas informações pessoais, e quando os riscos são maiores, estes indivíduos não divulgam tais informações.

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. conforme os autores 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. De acordo com Beldad et al. (2011) embora os riscos de se envolver em transações mediadas por computador inundarem a Internet, os usuários ainda podem optar por realizar transações convenientes, mas possivelmente arriscadas. De acordo com os autores, usuários de Internet com altos níveis de experiência podem estar inclinados a fazer operações *online*, apesar dos seus conhecimentos sobre a profusão de riscos em transações e interações mediadas por computadores, apenas por causa da sua experiência.

2.5 LEGISLAÇÃO SOBRE PRIVACIDADE

Alguns países possuem leis específicas para regular o uso da Internet, outros aplicam as leis comuns para julgar os crimes realizados na *web*. A seguir serão apresentadas as principais iniciativas para regular a privacidade na Internet, algumas leis específicas e as leis que trataram do tema mesmo antes do advento da Internet.

2.5.1 Estados Unidos da América

De acordo com Eart et al. (2005), audiências no Congresso dos Estados Unidos na década de 1970, onde os defensores da privacidade procuraram proibir agências de crédito de utilizar as bases de dados centralizadas em computador, levaram ao reconhecimento de que as organizações têm certas responsabilidades e os indivíduos certos direitos, em relação à coleta e o uso de informações pessoais. Os autores afirmam ainda que, desde 1973, os princípios do *Fair Information Practice Principles (FIPP)*, desenvolvidos pelo Departamento de Segurança

Interna (*DHS*) dos Estados Unidos, têm servido como base para estabelecer e avaliar as leis e práticas de privacidade do país. O FIPP é composto de princípios que devem ser seguidos para garantir a privacidade dos dados pessoais coletados pelas empresas, quais sejam (DHS, 2008):

a) **Transparência**: o DHS deve ser transparente e avisar previamente o indivíduo quanto a coleta, difusão e manutenção de informações pessoais;
b) **Participação Individual**: o DHS deve envolver o indivíduo no processo de utilização de informações pessoais e, na medida do possível, buscar o consentimento individual para a coleta, utilização, difusão e manutenção de informações pessoalmente identificáveis. Deve também fornecer mecanismos apropriados de acesso, correção e reparação a respeito do uso de informações pessoais pelo DHS;
c) **Especificação de Finalidade**: o DHS deve expressar especificamente a autoridade que permite a coleta de informações pessoais e, especificamente, expressar o propósito ou propósitos para os quais se pretende utilizar estas informações;
d) **Minimização de Dados**: o DHS só deve coletar informações pessoalmente identificáveis que sejam relevantes e necessárias para cumprir a finalidades específicas e apenas reter informações pessoais pelo tempo que for necessário para cumprir tais finalidades;
e) **Limitação de Uso**: o DHS deve utilizar as informações pessoais somente para os fins especificados na notificação. O compartilhamento de informações pessoais fora do Departamento deve ser para um propósito compatível com a finalidade para a qual as informações pessoais foram coletadas;
f) **Integridade e Qualidade dos Dados**: o DHS deve, na medida do possível, garantir que as informações pessoais são precisas, adequadas, oportunas e completas;
g) **Segurança**: o DHS deve proteger as informações pessoais (em todos os meios), através de garantias de segurança adequadas, contra riscos como perda, acesso ou utilização não autorizado, destruição, modificação ou divulgação não intencional ou inadequada;
h) **Prestação de Contas e Auditoria**: o DHS deve ser o responsável pelo cumprimento destes princípios, oferecendo treinamento a todos os funcionários e prestadores de serviços que utilizam informações pessoais, e fiscalizar o uso real de informações pessoais para demonstrar a conformidade com estes princípios e todos os requisitos de proteção à privacidade aplicáveis.

2.5.2 Europa

Segundo FRA (2015) “a manutenção dos direitos fundamentais na atual sociedade da informação é uma questão fundamental para a União Europeia, e cada vez mais para *European Union Agency for Fundamental Rights* (FRA), à medida que mais e mais pessoas usam as TICs em suas vidas diárias no trabalho e em casa”. Na União Europeia a proteção de dados é um direito fundamental consagrado no artigo 8º da Carta dos Direitos Fundamentais, que é diferente do artigo 7º que trata do respeito à vida privada e familiar (FRA, 2015). A Agência Europeia afirma ainda que a União Europeia tem desempenhado na promoção do desenvolvimento e introdução de legislação nacional de proteção de dados em diversos sistemas jurídicos onde a referida legislação não era adotada (FRA, 2015). Ainda segundo a Agência, a Diretiva 95/46/CE da União Europeia sobre a proteção dos indivíduos a respeito do tratamento dos dados pessoais e a livre circulação destes dados, que é principal instrumento jurídico da União Europeia sobre a proteção dos dados, foi um instrumento fundamental neste aspecto.

De acordo com a FRA (2015) em janeiro de 2012 a Comissão Europeia propôs um pacote de reforma legislativa sobre a proteção dos dados, com o objetivo de modernizar as atuais regras, à luz da rápida evolução tecnológica e da globalização. Ainda segundo a Agência, o pacote consiste em uma proposta de Regulamento Geral sobre a proteção de dados, que deverá substituir a Diretiva de Proteção de Dados, contendo ainda disposições sobre a proteção de dados na área da cooperação policial e judiciária em matéria penal.

2.5.3 Comitê Gestor da Internet no Brasil

O Comitê Gestor da Internet no Brasil (CGI.br) foi criado pelo Decreto 4.729, de 3 de setembro de 2003, tendo como principais atribuições (PRESIDÊNCIA DA REPÚBLICA, [2003]):

a) Estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil;
b) Estabelecer diretrizes para a organização das relações entre o Governo e a sociedade, na execução do registro de Nomes de Domínio, na alocação de Endereço IP (Internet Protocol) e na administração pertinente ao Domínio de Primeiro Nível (ccTLD - country code Top Level Domain), ".br", no interesse do desenvolvimento da Internet no País;

c) Propor programas de pesquisa e desenvolvimento relacionados à Internet, que permitam a manutenção do nível de qualidade técnica e inovação no uso, bem como estimular a sua disseminação em todo o território nacional, buscando oportunidades constantes de agregação de valor aos bens e serviços a ela vinculados;
d) Promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade;
e) Articular as ações relativas à proposição de normas e procedimentos relativos à regulamentação das atividades inerentes à Internet;
f) Ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;
g) Adotar os procedimentos administrativos e operacionais necessários para que a gestão da Internet no Brasil se dê segundo os padrões internacionais aceitos pelos órgãos de cúpula da Internet, podendo, para tanto, celebrar acordo, convênio, ajuste ou instrumento congênere;
h) Deliberar sobre quaisquer questões a ele encaminhadas, relativamente aos serviços de Internet no País; e
i) Aprovar o seu regimento interno.

O CGI.br em reunião ordinária em 2009, aprovou a Resolução CGI.br/RES/2009/003/P sobre os Princípios para a Governança e Uso da Internet no Brasil, aprovando os seguintes Princípios para a Internet no Brasil (CGI.br, [2009]):

a) Liberdade, privacidade e direitos humanos: o uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática;
b) Governança democrática e colaborativa: a governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva;
c) Universalidade: o acesso à Internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos;
d) Diversidade: a diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores;
e) Inovação: a governança da Internet deve promover a contínua evolução e ampla difusão de novas tecnologias e modelos de uso e acesso;

f) Neutralidade da rede: filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento;
g) Inimputabilidade da rede: o combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos;
h) Funcionalidade, segurança e estabilidade: a estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas;
i) Padronização e interoperabilidade: a Internet deve basear-se em padrões abertos que permitam a interoperabilidade e a participação de todos em seu desenvolvimento;
j) Ambiente legal e regulatório: o ambiente legal e regulatório deve preservar a dinâmica da Internet como espaço de colaboração.

Os dez princípios aprovados pelo CGI.br (2009) serviram de base para o Projeto de Lei 2126, que foi apresentado à Câmara dos Deputados em agosto de 2011, o qual ficou conhecido como o Marco Civil da Internet. Esta iniciativa ganhou repercussão nacional e internacional, "levando o Brasil a ocupar posição de destaque por sua organização de governança multissetorial e pela elaboração de um marco regulatório que definisse os princípios-chave da Internet, livre e aberta, e as regras de proteção ao usuário" (CGI.br, [2009]).

2.5.4 Marco Civil da Internet - Brasil

O projeto de lei que deu origem a Lei nº 12.965, que ficou conhecida popularmente como o Marco Civil da Internet foi proposto pelo Ministério da Justiça do Brasil, para traçar os princípios como neutralidade e privacidade na Internet brasileira. Em outubro de 2009, em uma parceria entre a Secretaria de Assuntos Legislativos do Ministério da Justiça e o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas, foi lançada no Rio de Janeiro a primeira fase do processo colaborativo para a construção de um Marco Regulatório da Internet no Brasil, propondo à sociedade uma discussão sobre as condições de utilização da Internet em relação aos direitos e deveres de seus usuários e dos provedores de Internet, bem como sobre o papel do Poder Público. Após a formulação da Minuta do

Anteprojeto, iniciou-se a fase de debates públicos com a participação da sociedade, culminando com sua aprovação na Câmara dos Deputados no dia 25 de março de 2013.

A Lei nº 12.965, a qual pode ser verificada na integra no ANEXO E deste estudo, foi sancionada pela Presidente da República Dilma Rousseff em 23 de abril de 2014, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, e determina as diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria (CGI.br, [2014]). A Lei está dividida em cinco capítulos, quais sejam:

I. Das Disposições Gerais
II. Dos Direitos e Garantias dos Usuários
III. Da Provisão de Conexão e de Aplicações de Internet
IV. Da Atuação do Poder Público
V. Disposições Finais

O Marco Civil enfatiza o caráter de livre acesso e manifestação, característicos da Internet. Entre os direitos dos usuários estão a inviolabilidade da intimidade, da vida privada e das comunicações, salvo por determinação da justiça, a não suspensão de conexão de dados, salvo por falta de pagamento do serviço, a manutenção da qualidade da conexão contratada e o direito de solicitar a exclusão definitiva dos dados pessoais fornecidos a determinado site, após o final da relação entre as partes. Os registros de conexão e acesso somente poderão ser compartilhados com terceiros havendo o consentimento livre e expresso por parte do usuário. De acordo com a referida Lei, o direito à liberdade de expressão e a privacidade é essencial para o pleno exercício do direito de acesso à Internet (BRASIL, 2014).

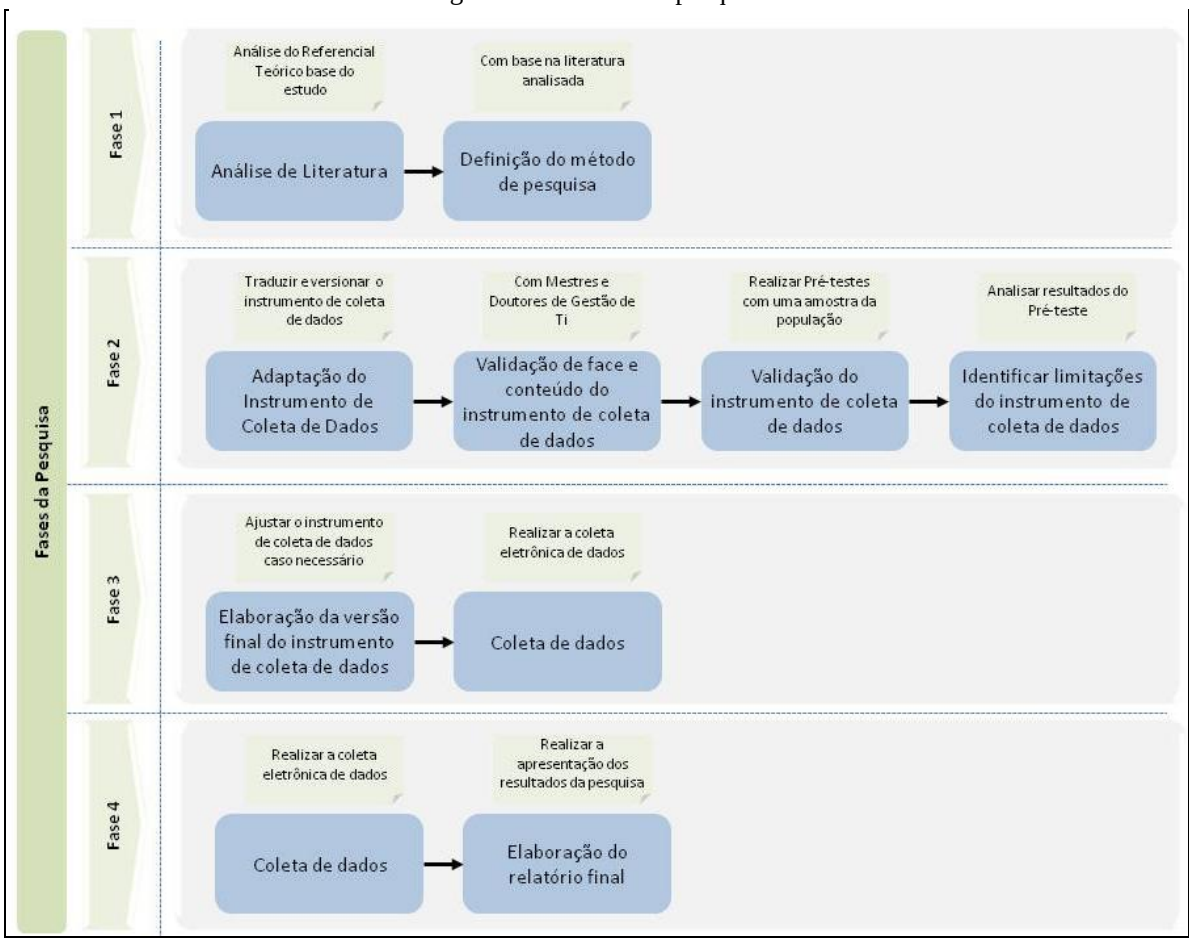
3 MÉTODO DE PESQUISA

Neste capítulo apresenta-se o método de pesquisa utilizado para alcançar os objetivos propostos anteriormente. Apresenta-se a estratégia adotada e o desenho de pesquisa, bem como o detalhamento das técnicas utilizadas para a coleta e a análise dos dados.

3.1 ESTRUTURA DA 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, somente com uma coleta de dados, com o objetivo de descrever e analisar o estado de uma ou mais variáveis. A seguir apresenta-se o desenho da pesquisa na Figura 4.

Figura 4 – Desenho da pesquisa



Fonte: O autor (2015)

Para atingir os objetivos propostos neste estudo a seguinte estrutura de pesquisa foi utilizada: a) análise do referencial teórico para embasar o estudo do tema; b) seleção do método de pesquisa; c) adaptação do questionário tipo *survey*, desenvolvido em estudo realizado por Hong e Thong (2013), conforme abordado na revisão de literatura realizada no presente estudo; d) validação de face; e) validação de face e conteúdo; f) pré-teste do questionário, com pequena amostra representativa da população; g) correção do questionário em função do resultado do pré-teste, caso necessário; h) elaboração final do questionário; i) aplicação do questionário de forma eletrônica; j) análise dos dados coletados; k) interpretação dos resultados obtidos; l) conclusões e m) relatório final, conforme descrito na Figura 4.

Conforme apresentado no desenho da pesquisa será descrito a seguir a fase 2 do método utilizado, onde foi possível o versionamento, adaptação e validação do instrumento de coleta de dados.

3.2 POPULAÇÃO E AMOSTRA

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 (HAIR et al., 2005). De acordo com Hair et al. (2009) em uma amostra não probabilística, não há método estatístico para mensurar o erro amostral e é desconhecida a probabilidade de um elemento da amostra ser escolhido. A partir de tal afirmação, não é possível a generalização das descobertas, uma vez que não há grau mensurável de confiança.

Em função da possibilidade de coleta eletrônica, optou-se por coletar dados das regiões Sul, Sudeste, Centro-Oeste, Norte e Nordeste do país, sendo que a técnica de amostragem utilizada foi a não probabilística bola-de-neve. Segundo Malhotra (2006), na amostragem bola-de-neve inicialmente escolhe-se um grupo aleatório de entrevistados, e após solicita-se que estes identifiquem outros que pertençam à população-alvo de interesse. Ainda segundo o autor, os demais entrevistados são selecionados com base nessas referências, sendo o processo executado em ondas sucessivas, o que leva a um efeito de bola-de-neve. Malhotra (2006) afirma que o objetivo principal desta técnica de amostragem é estimar características raras na população e a principal vantagem é que ela aumenta muito a possibilidade de localizar a característica desejada na população.

Para atender os objetivos desta pesquisa utilizou-se a técnica de amostragem bola-de-neve selecionando-se aleatoriamente os pesquisadores, que posteriormente distribuíram o instrumento de pesquisa. Segundo Malhotra (2006) em populações acima de 10.000, uma amostra de 200 seria suficiente para pesquisas exploratórias. Sendo assim, a quantidade coletada em cada região é suficiente para retratá-las individualmente.

Não foram considerados os questionários incompletos, restando no final um total de 1.104 questionários respondidos completos, sendo 202 da Região Sul, 204 do Norte, 240 do Nordeste, 211 do Centro-Oeste e 247 da Região Sudeste do Brasil.

3.3 INSTRUMENTO DE COLETA DE DADOS

Uma vez que o projeto de pesquisa envolve a coleta de informações de uma grande amostra de indivíduos, o que se faz necessário para que possam ser atendidos os objetivos gerais e específicos deste estudo, foi utilizada uma *survey*, de acordo com as indicações de Hair et al. (2007). Uma pesquisa do tipo *survey*, segundo Pinsonneault e Kraemer (1993), tem como objetivo coletar informações sobre as características, ações ou opiniões de um grupo de pessoas, referido como população. Foi aplicado um questionário estruturado com questões pré-definidas, que segundo os autores, é a principal forma de coleta de informações, e cujas respostas constituem os dados a serem analisados.

Para atender os objetivos deste estudo, foi utilizado o instrumento de coleta de dados desenvolvido por Hong e Thong (2013), composto de seis dimensões de IPC, com dezoito questões, uma dimensão de crenças de confiança e uma dimensão de crenças de risco, cada uma com quatro questões. O instrumento pode ser verificado no Anexo D deste estudo. 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), e da mesma forma como utilizado no estudo realizado por Hong e Thong (2013).

O instrumento foi traduzido do inglês para o português por uma professora de inglês, Licenciada em Letras Inglês pela PUCRS, e posteriormente do português para o inglês, por outra professora Licenciada em Letras Inglês pela PUCRS, com o objetivo de identificar possíveis falhas de tradução. 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 foram inseridas questões de sensibilidade da informação, oriundas do estudo de Degirmenci (2013), com o objetivo de identificar com quais os tipos de informação os respondentes têm maior preocupação relacionada à privacidade, e na terceira parte do instrumento foram inseridas questões sócio demográficas, com o objetivo de caracterizar a amostra. As variáveis do instrumento de coleta de dados utilizado nesta pesquisa são descritas no Quadro 5.

Uma vez que foi utilizado um instrumento de coleta de dados de outra pesquisa, foram realizadas validações deste instrumento, conforme indicado por Hoppen et al. (1996). O Quadro 6 apresenta as questões submetidas à análise de face e conteúdo, agrupadas pelos construtos, com a identificação das variáveis associadas.

Quadro 6 – Questões submetidas à validação de face

	Questões
Coleta	COL1 - Geralmente me incomoda quando *sites* comerciais/governo me pedem informações pessoais COL2 - Quando *sites* comerciais/governo me pedem informações pessoais, às vezes penso duas vezes antes de fornecê-las. COL3 - Estou preocupado que os *sites* comerciais/governamentais estejam recolhendo muita informação pessoal sobre mim.
Uso Secundário	USEC1 - Eu estou preocupado que quando eu dou informações pessoais a um site comercial / governo por algum motivo, o site use as informações para outros objetivos. USEC2 - Estou preocupado que os *sites* comerciais/governo vendam as minhas informações pessoais em seus bancos de dados para outras empresas. USEC3 - Estou preocupado que os *sites* comerciais/governo compartilhem minhas informações pessoais com outras empresas sem a minha autorização.
Erros	ERR1 - Estou preocupado que os *sites* comerciais/governo não tomem medidas suficientes para ter certeza de que as minhas informações pessoais em seus arquivos são precisas. ERR2 - Estou preocupado que os *sites* comerciais/governo não tenham procedimentos adequados para corrigir erros em minhas informações pessoais. ERR3 - Estou preocupado que os *sites* comerciais/governo não dediquem tempo e esforço suficiente para verificar a exatidão de minhas informações pessoais em seus bancos de dados.
Acesso Indevido	ACI1 - Estou preocupado que bancos de dados de *sites* comerciais/governo que contenham as minhas informações pessoais não sejam protegidos contra o acesso não autorizado. ACI2 - Estou preocupado que os *sites* comerciais/governo não dediquem tempo e esforço suficiente para impedir o acesso não autorizado a minhas informações pessoais. ACI3 - Estou preocupado que os *sites* comerciais/governo não tomem medidas suficientes para se certificar de que pessoas não autorizadas possam acessar minhas informações pessoais em seus computadores.
Controle	CTRL1 - Geralmente me incomoda quando eu não tenho controle sobre as informações pessoais que eu forneço a *sites* comerciais/governo. CTRL2 - Geralmente me incomoda quando eu não tenho controle ou autonomia sobre as decisões sobre como as minhas informações pessoais são coletadas, utilizadas e compartilhadas por *sites* comerciais/governo. CTRL3 - Estou preocupado quando o controle é perdido ou involuntariamente reduzido como resultado de uma operação de marketing com *sites* comerciais/governo.
Consciência	CONS1 - Estou preocupado quando uma divulgação clara e visível não está incluída na política de privacidade on-line de *sites* comerciais/governo. CONS2 - Geralmente me incomoda quando eu não estou ciente ou bem informado sobre como as minhas informações pessoais serão utilizadas por *sites* comerciais/governo. CONS3 - Geralmente me incomoda quando *sites* comerciais/governamentais que buscam a minha informação on-line não divulgam a forma como os dados são recolhidos, processados e utilizados.

Crenças de confiança	CONF1 - *Sites* Comerciais/governamentais, em geral, seriam dignos de confiança para lidar com as minhas informações pessoais. CONF2 - *Sites* Comerciais/governamentais manteriam meus melhores interesses em mente ao lidar com as minhas informações pessoais. CONF3 - *Sites* Comerciais/governamentais cumpririam suas promessas relacionadas com as minhas informações pessoais. CONF4 - *Sites* Comerciais/governamentais são, em geral, previsíveis e consistentes em relação ao uso das minhas informações pessoais.
Crenças de Risco	RISC1 - Em geral, seria arriscado fornecer os meus dados pessoais para *sites* comerciais/governo. RISC2 - Haveria alto potencial de perda associado com fornecer os meus dados pessoais para *sites* comerciais/governo. RISC3 - Haveria muita incerteza associada com fornecer os meus dados pessoais para *sites* comerciais/governo. RISC4 - Abastecer *sites* comerciais/governo com as minhas informações pessoais envolveria muitos problemas inesperados.

Fonte: Hong e Thong (2013)

A validação de face, com o objetivo de avaliar se a forma do instrumento de pesquisa está adequada (HOPPEN et al., 1996), e a validação de conteúdo, que segundo Malhotra (2006) é uma avaliação da exatidão com que o conteúdo de uma escala representa a medição em andamento, foram realizadas com três doutores da Área de Administração, Linha de Pesquisa Gestão da Informação, do Programa de Pós-Graduação em Administração da PUCRS, e com um doutorando do referido programa. Como resultado da validação de face e de conteúdo, sendo substituídas algumas palavras com o objetivo de facilitar o entendimento por parte dos respondentes. O instrumento de coleta de dados final desta pesquisa pode ser verificado no APÊNDICE A deste documento.

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). Os resultados obtidos no pré-teste serão apresentados no capítulo dos resultados deste estudo.

3.4 PRÉ-TESTE

A etapa de pré-testes possibilita identificar e eliminar problemas potenciais para aperfeiçoamento do instrumento de coleta de dados, sendo possível testar os enunciados, os conteúdos, o formato e a sequência das perguntas, bem como o entendimento das questões e das instruções fornecidas (MALHOTRA, 2010).

Segundo Malhotra (2010), o pré-teste é a aplicação do questionário em uma pequena amostra de entrevistados, os quais devem ter o mesmo perfil dos entrevistados da pesquisa real em termos de características, familiaridade com o assunto e atitudes e comportamentos. Ainda de acordo com o autor, a quantidade de respondentes necessária para o pré-teste é

pequena, variando entre 15 e 30 respondentes. Os dados para o pré-teste foram coletados de forma eletrônica, através da ferramenta Qualtrics, entre os dias 18/11/2014 e 20/11/2014.

A validação através do pré-teste foi realizada a partir da aplicação do instrumento de coleta de dados em uma amostra de 64 usuários de Internet, não probabilística, com a técnica bola-de-neve, a partir da divulgação do instrumento nas redes sociais Facebook, Linkedin, Twitter, Google+. Foram desconsiderados os respondentes que não preencheram totalmente o questionário, restando 53 respondentes válidos e completos.

3.5 COLETA DE DADOS FINAL

Utilizou-se uma *survey* publicada em www.pucrs.qualtrics.com, a qual foi encaminhada para pesquisadores de Gestão da Informação de todo o país, solicitando que os mesmos distribuíssem para seus contatos e para seus alunos. O *link* da pesquisa foi divulgado em diversas redes sociais, tais como Facebook, LinkedIn, Twitter e Google +, com o objetivo de coletar dados em todas as regiões do Brasil. A coleta foi realizada através de um questionário autoadministrado com 26 questões, as quais foram adaptadas para o contexto brasileiro. Participaram da análise fatorial confirmatória, uma questão de sensibilidade da informação e demais questões sócio-demográficas, que permitiram a identificação do perfil do respondente através de análises estatísticas descritivas. Uma vez que não se obteve sucesso na coleta de dados nas regiões sudeste, centro-oeste, norte e nordeste, totalizando apenas 92 questionários respondidos, optou-se por contratar uma empresa especializada em coleta de dados para pesquisas acadêmicas. A coleta de dados final foi realizada entre os dias 05/12/2014 e 06/01/2015.

3.6 ANÁLISE DE DADOS

Para obter os resultados desta pesquisa foram as seguintes análises estatísticas foram realizadas: análise de confiabilidade do instrumento de coleta de dados, análise descritiva da amostra, análise descritiva univariada, análise fatorial exploratória, análise confirmatória do modelo de mensuração, análise da validade convergente e discriminante.

A Análise de Cluster, ou Análise de Agrupamentos, segundo Hair et al. (2006, p. 430), "é uma análise multivariada cuja finalidade principal é agregar objetos com base nas características que eles possuem". Buscou-se identificar na amostra comportamentos que pudessem caracterizar os grupos.

Os *clusters* foram definidos a partir dos dados coletados, com o objetivo de examinar relações de interdependência entre todo o conjunto de variáveis, para possibilitar a classificação dos objetos em grupos relativamente homogêneos com base no conjunto de variáveis. Foram utilizadas as seguintes estatísticas associadas à análise de cluster, seguindo as recomendações de Malhotra (2010):

a) **Esquema de aglomeração**: para fornecer informações sobre os objetos a serem combinados em cada estágio do procedimento hierárquico de aglomeração;
b) **Centroide de cluster**: para identificar os valores médios das variáveis em um cluster;
c) **Associação a um cluster**: para indicar o cluster a que pertence cada objeto;
d) **Distância entre centros de cluster**: para indicar o grau de separação dos pares individuais de cluster.
e) **Matriz de coeficientes de semelhança / distância**: para apresentar as distâncias pareadas entre objetos.

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.

O próximo capítulo apresenta os resultados obtidos a partir da aplicação do método descrito acima.

4 RESULTADOS

Este capítulo apresenta os resultados obtidos a partir dos dados coletados através do instrumento de coleta de dados, que pode ser verificado no APÊNDICE A desta pesquisa.

Uma vez que um dos objetivos desta pesquisa é a validação de um instrumento de coleta de dados, são apresentadas neste capítulo as análises que validam o instrumento utilizado neste estudo. Os procedimentos metodológicos utilizados para análise dos dados coletados foram os seguintes: a) Pré-teste do instrumento de coleta de dados; b) Análise descritiva da amostra; c) Análise descritiva univariada; d) Análise de confiabilidade; d) Análise exploratória; e) Análise confirmatória; f) Análise de validade convergente e G) Análise de cluster.

4.1 ANÁLISE DE CONFIABILIDADE DO INSTRUMENTO NO PRÉ-TESTE

A validação de confiabilidade do instrumento de coleta de dados foi realizada através do Alfa de Cronbach, utilizando-se o *software* SPSS Statistics, versão 21, uma vez que, segundo Kline (2011), esta estatística mede a confiabilidade interna e o grau de consistência das respostas entre os itens dentro de uma medida.

Tabela 2– Alfa de Cronbach na fase do pré-teste

Alfa de Cronbach	Nº de itens
,871	26

Fonte: O autor (2015)

O resultado do coeficiente Alfa de Cronbach, o qual pode ser verificado na Tabela 2 acima, demonstra que o instrumento de coleta de dados tem consistência interna, uma vez que, segundo Hinkin (2009), esta medida de confiabilidade varia entre 0 e 1, sendo que os valores de 0,60 e 0,70 considerados o limite inferior de confiabilidade. Os índices do coeficiente Alfa de Cronbach obtidos indicaram que não seria necessário retirar questões do instrumento, conforme pode ser verificado na Tabela 3 a seguir.

Tabela 3 – Alfa de Cronbach dos Construtos na fase do pré-teste

Construto	Variáveis / Questões	Alfa de Cronbach
Coleta de dados (COL)	COL1, COL2 e COL3	0,690
Uso secundário (USEC)	USEC1, USEC2 e USEC3	0,740
Erro (ERR)	ERR1, ERR2 e ERR3	0,875
Acesso indevido (ACI)	ACI1, ACI2 e ACI3	0,786
Controle (CTRL)	CTRL1, CTRL2 e CTRL3	0,813
Consciência (CONS)	CONS1, CONS2 e CONS3	0,903
Confiança (CONF)	CONF1, CONF2, CONF3 e CONF4	0,800
Risco (RISC)	RISC1, RISC2, RISC3 e RISC4	0,871

Fonte: O autor (2015)

Os índices obtidos no Teste de KMO e Bartlett, que indicam o grau de suscetibilidade ou o ajuste dos dados à análise fatorial, indicando o nível de confiança que pode ser obtido dos dados quando tratados pelo método multivariado de análise fatorial (HAIR et al., 2009), e apresentam resultados consistentes, conforme pode ser verificado no Quadro 7 abaixo.

Quadro 7 – Teste de KMO e Bartlett do Pré-Teste

Medida Kaiser-Meyer-Olkin de adequação de amostragem.		,741
Teste de esfericidade de Bartlett	Qui-quadrado aprox.	1010,576
	df	325
	Sig.	,000

Fonte: O autor (2015)

De acordo com Malhotra (2006), valores do índice de KMO inferiores a 0,6 indicariam que a análise fatorial poderia ser inadequada.

A próxima validação realizada foi a análise multivariada, por meio da Análise Fatorial Exploratória das variáveis, com o objetivo de verificar a estrutura dos fatores que compõem as escalas, com análise do componente principal e rotação varimax (HAIR et al., 2009). Esta análise confirmou que não seria necessário realizar modificações nas escalas.

Tabela 4 – Comunalidades das variáveis no pré-teste

Construtos	Variável	Comunalidade
Coleta	COL1	,801
	COL2	,751
	COL3	,787
Uso Secundário	USEC1	,797
	USEC2	,903
	USEC3	,870
Erros	ERR1	,817
	ERR2	,906
	ERR3	,750
Acesso Indevido	ACI1	,823
	ACI2	,855
	ACI3	,844
Controle	CTRL1	,830
	CTRL2	,777
	CTRL3	,679
Consciência	CONS1	,824
	CONS2	,767
	CONS3	,846
Confiança	CONF1	,632
	CONF2	,880
	CONF3	,788
	CONF4	,725
Risco	RISC1	,737
	RISC2	,719
	RISC3	,856
	RISC4	,654

Fonte: O autor (2015)

Por meio da Análise Fatorial pode-se verificar a cumunalidade das variáveis que, de acordo com Hair et al. (2005), representa o índice de variância em uma única variável, explicados pelos valores extraídos. Os resultados, conforme Tabela 4, mostram que os valores estão acima de 0,5, portanto satisfatórios (MALHOTRA, 2006). Segundo o autor, valores de cumunalidade abaixo de 0,5 indicam que as variáveis não fornecem explicação suficiente para o que está mensurando, sendo necessárias amostras maiores.

A Tabela 5 apresenta a variância explicada da análise, indicando que 77,919% da variância foi explicada por estes componentes, indicando que entre os 8 componentes originais, os sete componentes listados seriam suficientes.

Tabela 5 – Variância total explicada

Componente	Valores próprios iniciais			Somas de extração de carregamentos ao quadrado			Somas rotativas de carregamentos ao quadrado		
	Total	% de variância	% cumulativa	Total	% de variância	% cumulativa	Total	% de variância	% cumulativa
1	8,975	34,521	34,521	8,975	34,521	34,521	5,178	19,915	19,915
2	3,107	11,950	46,470	3,107	11,950	46,470	3,544	13,632	33,547
3	2,415	9,287	55,758	2,415	9,287	55,758	2,696	10,369	43,916
4	2,024	7,787	63,544	2,024	7,787	63,544	2,611	10,043	53,960
5	1,580	6,077	69,622	1,580	6,077	69,622	2,394	9,206	63,165
6	1,149	4,418	74,040	1,149	4,418	74,040	1,985	7,636	70,801
7	1,009	3,880	77,919	1,009	3,880	77,919	1,851	7,118	77,919
Método de extração: análise do componente principal.									

Fonte: O autor (2015)

A partir das análises realizadas no pré-testes pode-se verificar que o instrumento de coleta de dados está adequado para realizar a coleta de dados final.

4.2 ANÁLISE DE CONFIABILIDADE NA COLETA FINAL

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, como pode ser verificado na Tabela 6 abaixo.

Tabela 6 – Estatísticas de confiabilidade na coleta final

Alfa de Cronbach	Alfa de Cronbach com base em itens padronizados	N de itens
,950	,954	26

Fonte: O autor (2015)

A seguir é apresentado na Tabela 7 o coeficiente Alfa de Cronbach de cada construto na coleta de dados final.

Tabela 7 – Alfa de Cronbach dos construtos

Construto	Variáveis / Questões	Alfa de Cronbach
Coleta de dados (COL)	COL1, COL2 e COL3	0,836
Uso secundário (USEC)	USEC1, USEC2 e USEC3	0,925
Erro (ERR)	ERR1, ERR2 e ERR3	0,883
Acesso indevido (ACI)	ACI1, ACI2 e ACI3	0,945
Controle (CTRL)	CTRL1, CTRL2 e CTRL3	0,847
Consciência (CONS)	CONS1, CONS2 e CONS3	0,907
Confiança (CONF)	CONF1, CONF2, CONF3 e CONF4	0,926
Risco (RISC)	RISC1, RISC2, RISC3 e RISC4	0,901

Fonte: O autor (2015)

De acordo com Hair et al. (2009) valores de Alfa de Cronbach a partir de 0,6 são aceitáveis para pesquisas exploratórias. Segundo o recomendado por Hair et al. (2009), os valores apresentados na Tabela 7 indicam que os itens utilizados na presente pesquisa medem adequadamente os construtos, uma vez que apresentam Alfa de Cronbach acima de 0,8.

4.3 ANÁLISE DESCRITIVA DA AMOSTRA

A seguir será apresentada a caracterização da amostra, composta de 1.104 respondentes, de acordo com a análise descritiva realizada. Os respondentes foram caracterizados pelo gênero, faixa etária, situação profissional, grau de escolaridade e renda familiar mensal.

Tabela 8 – Faixa Etária, Renda e Gênero

		Região					**Totais**
		Norte	**Nordeste**	**Centro-Oeste**	**Sudeste**	**Sul**	
Faixa Etária	19 a 24 anos	59	70	75	58	29	**291**
	25 a 35 anos	107	113	91	114	86	**511**
	36 a 49 anos	29	46	40	56	62	**233**
	50 anos ou mais	9	11	5	19	25	**69**
Familiar Mensal	Até R$ 1.449,99	65	84	42	32	13	**236**
	R$1.450,00 a R$2.899,99	81	67	69	85	28	**330**
	R$2.900,00 a R$7.249,99	41	57	73	86	86	**343**
	R$7.250,00 a R$14.499,99	10	26	19	32	46	**133**
	R$14.500,00 ou mais	7	6	8	12	29	**62**
Gênero	M	66	91	67	97	101	**422**
	F	138	149	144	150	101	**682**
Totais		**204**	**240**	**211**	**247**	**202**	1.104

Fonte: O autor (2015)

A Tabela 8 mostra que a maioria dos respondentes (61,8%) que compõem a amostra é do sexo feminino, com maior concentração de respondentes na faixa etária de 25 a 35 anos, totalizando 46,3%. Quanto a região do país, a amostra está bem distribuída entre as cinco regiões, sendo que apenas na região Sul as mulheres não são maioria. Percebe-se na referida tabela, que a renda familiar dos respondentes se concentra entre R$ 1.450,00 e R$ 7.249,99, com um total de 61% de ocorrência. A Tabela 9 a seguir apresenta o grau de escolaridade e situação profissional referentes a amostra.

Tabela 9 – Grau de Escolaridade e Situação Profissional

		Região					Totais
		Norte	Nordeste	Centro-Oeste	Sudeste	Sul	
Escolaridade	Ensino Médio	112	126	115	123	46	**522**
	Graduação	73	78	65	94	76	**386**
	Pós-Grad Lato Sensu	14	20	26	9	36	**105**
	Mestrado	5	12	3	11	29	**60**
	Doutorado	0	4	2	10	15	**31**
Situação Profissional	Empregado	90	100	114	118	145	**567**
	Empresário	5	8	8	15	9	**45**
	Profissional Liberal	27	28	9	25	16	**105**
	Estudante	28	46	26	33	13	**146**
	Servidor Público	19	24	27	17	13	**100**
	Outro	35	34	27	39	6	**141**
Totais		**204**	**240**	**211**	**247**	**202**	1.104

Fonte: O autor (2015)

A Tabela 9 apresenta a situação profissional dos respondentes, entre as informações 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. A partir dos resultados pode-se verificar que 47,3% dos respondentes possuem apenas Ensino Médio. A Tabela 10 a seguir mostra os resultados referentes à utilização de redes sociais e navegação na Internet.

Tabela 10 – Horas de Navegação na Internet, Utilização de Redes sociais

		Região					Totais
		Norte	**Nordeste**	**Centro-Oeste**	**Sudeste**	**Sul**	
Horas por semana que navega na Internet	**até 10h**	63	62	42	42	40	**249**
	10h a 20h	39	56	50	67	61	**273**
	21h e 30h	33	42	42	42	32	**191**
	mais de 30h	69	80	77	96	69	**391**
Utiliza Rede Social	**Sim**	199	239	209	243	191	**1.081**
	Não	5	1	2	4	11	**23**
Redes Sociais que mais utiliza	**Instagram**	112	127	127	115	76	**557**
	Twitter	60	92	53	84	48	**337**
	Youtube	126	165	137	172	112	**712**
	Facebook	193	234	202	232	183	**1.044**
	Linkedin	36	63	44	86	82	**311**
	Flickr	4	7	5	10	3	**29**
	Outra	23	28	29	27	8	**115**

Fonte: O autor (2015)

A partir da Tabela 10 pode-se perceber que 35,4% dos respondentes navegam na Internet por mais de 30 horas por semana e, a grande maioria dos respondentes, 64,6%, navega até 30 horas por semana. Importante salientar que os resultados apontam o tempo que os usuários navegam na Internet, não o tempo em que ficam conectados. 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. Este resultado mostra a grande popularidade das redes sociais entre os usuários de Internet do Brasil. Os resultados obtidos na questão sobre quais redes sociais eram mais utilizadas. Percebe-se que apenas 100 respondentes não utilizam a rede social Facebook. Quanto às horas semanais que os respondentes navegam nas redes sociais, os resultados indicam que a maior concentração, que totaliza 40,8%, navega até 10 horas por semana. Os 1,2% indicados como ausentes referem-se aos respondentes que não utilizam nenhuma rede social.

A partir das análises realizadas foi possível identificar quais as informações apontadas pelos respondentes como mais sensíveis quanto à privacidade, sendo os resultados apresentados na Tabela 11.

Tabela 11 – Sensibilidade das Informações

Informação	Muitíssimo Preocupado	Muito Preocupado	Preocupado	Preocupado em Parte	Nada Preocupado	Média	Desvio padrão
Senhas	**822**	**135**	94	28	25	4,54	0,918
Número de cartão de crédito	**806**	**150**	90	27	31	4,52	0,947
Número de conta corrente e agência	**740**	**153**	132	45	34	4,38	1,044
Saldo bancário	**712**	**169**	137	47	39	4,33	1,072
Gastos com cartão de crédito	**696**	**165**	154	45	44	4,29	1,099
Limite do cheque especial	**661**	**167**	142	65	69	4,16	1,225
Localização pelo celular	**573**	**223**	192	66	50	4,09	1,154
Endereço residencial	**569**	**235**	205	55	40	4,12	1,101
Salário	**525**	208	**223**	76	72	3,94	1,24
Telefone	**505**	**231**	227	89	52	3,95	1,187
Fotos	**462**	232	**241**	111	58	3,84	1,22
Empresa onde trabalha	**296**	231	**270**	133	174	3,31	1,392
Cargo	**240**	189	**296**	163	216	3,07	1,403
Notas escolares	229	185	**253**	175	**262**	2,95	1,451
Data de nascimento	215	162	**269**	174	284	2,86	1,448
Escola onde estuda/estudou	203	172	**234**	163	332	2,77	1,481
Vícios	201	138	**240**	148	377	2,67	1,499
Orientação sexual	167	111	**193**	129	504	2,37	1,503

Fonte: O autor (2015)

Os resultados apresentados indicam uma forte preocupação com relação às informações 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.

A análise dos Construtos Coleta, que tem o objetivo de identificar o grau com que uma pessoa está preocupada com a quantidade de dados individuais específicos em poder de outros (MALHOTRA et al., 2004), tem os resultados apresentados na Tabela 12, e demonstram um grau elevado de preocupação com a privacidade relacionada com a coleta de dados, uma vez que o percentual da amostra que indicou que concorda, ou concorda totalmente com cada questão foi de 60,15% para COL1, 70,7% para COL2 e 65,3% para COL3. A média obtida para cada variável foi de 5,54, 5,89 e 5,69 consecutivamente, e a média do construto foi de 5,71.

Tabela 12 – Frequência de Respostas dos Construtos

Construtos	Variáveis	Regiões do Brasil					Gênero		Média	Média	Desvio Padráo
		Norte	Nordeste	Centro-Oeste	Sudeste	Sul	Masc	Fem			
Coleta	COL1	5,20	5,31	5,24	5,57	6,42	5,59	5,51	5,54	5,71	1,66
	COL2	5,61	5,75	5,84	6,10	6,15	5,84	5,93	5,89		1,54
	COL3	5,50	5,55	5,67	5,94	5,78	5,62	5,74	5,69		1,6
Uso Secundário	USEC1	5,63	5,77	5,78	5,97	6,04	5,75	5,90	5,84	**5,79**	1,52
	USEC2	5,50	5,74	5,50	5,75	5,87	5,56	5,75	5,68		1,64
	USEC3	5,53	5,80	5,69	5,98	6,07	5,77	5,85	5,85		1,57
Erros	ERR1	5,42	5,48	5,48	5,58	5,50	5,47	5,51	5,49	5,31	1,71
	ERR2	5,31	5,38	5,35	5,45	5,61	5,39	5,44	5,42		1,68
	ERR3	5,13	5,14	5,09	5,13	4,54	4,91	5,09	5,02		1,82
Acesso Indevido	ACI1	5,69	5,85	5,73	6,13	6,17	5,80	6,00	5,92	**5,86**	1,49
	ACI2	5,53	5,84	5,60	6,03	6,02	5,69	5,89	5,81		1,56
	ACI3	5,53	5,85	5,66	6,06	6,03	5,71	5,91	5,84		1,52
Controle	CTRL1	5,50	5,63	5,61	5,94	5,81	5,60	5,77	5,7	5,65	1,62
	CTRL2	5,49	5,72	5,55	5,96	6,00	5,64	5,82	5,75		1,57
	CTRL3	5,26	5,46	5,43	5,67	5,64	5,36	5,58	5,5		1,68
Consciência	CONS1	5,49	5,63	5,62	5,82	5,47	5,42	5,73	5,7	5,65	1,62
	CONS2	5,65	5,71	5,67	6,06	5,88	5,70	5,86	5,75		1,57
	CONS3	5,70	5,70	5,64	5,91	5,65	5,59	5,81	5,5		1,68
Confiança	CONF1	4,54	3,94	4,35	3,62	3,06	3,74	3,99	3,9	4,09	2,09
	CONF2	4,74	4,33	4,53	3,77	2,97	4,02	4,10	4,07		2,02
	CONF3	4,81	4,30	4,59	3,93	3,23	4,21	4,15	4,17		1,89
	CONF4	4,66	4,28	4,73	4,10	3,39	4,32	4,18	4,23		1,92
Risco	RISC1	5,44	5,49	5,53	5,60	5,29	5,34	5,56	5,48	5,27	1,67
	RISC2	5,04	5,18	5,23	5,02	4,71	4,97	5,09	5,04		1,69
	RISC3	5,36	5,38	5,40	5,49	5,30	5,32	5,43	5,39		1,64
	RISC4	5,12	5,26	5,30	5,23	4,82	5,06	5,21	5,15		1,68

Fonte: O autor (2015)

Os resultados do Construto Uso Secundário, que busca identificar o grau de preocupação de que a informação recolhida para uma finalidade é usada para outra finalidade, sem a autorização dos indivíduos (SMITH et al., 1996), indicam um grau elevado de preocupação com a privacidade relacionada ao uso secundário das informações fornecidas, uma vez que o percentual da amostra que indicou que concorda ou concorda totalmente com cada questão foi de 68,8% para USEC1, 65,4% para USEC2 e 69,9% para USEC3. A média obtida para cada variável foi de 5,84, 5,68 e 5,85 consecutivamente.

O Construto Erros tem por objetivo identificar a preocupação de que as proteções contra erros deliberados ou acidentais em dados pessoais são inadequados (SMITH et al., 1996). Os resultados demonstram um grau de preocupação com a privacidade, relacionado com erros, menos acentuado em relação aos construtos Coleta e Uso Secundário. As respostas se concentraram em concordo ou concordo totalmente da seguinte forma para as variáveis: ERR1 60,2%, com média de 5,49; ERR2 56,8%, com média de 5,42 e; ERR3 47,7%, com

média de 5,02. Os resultados demonstram ainda que a variável ERR3 apresentou baixo grau de preocupação com a privacidade relacionada ao construto em questão, uma vez que 52,3% da frequência de resposta para esta variável distribuí-se entre discordo totalmente e concordo em parte.

O Construto Acesso indevido tem por objetivo de identificar o grau de preocupação dos usuários de que seus dados estejam prontamente disponíveis para as pessoas não devidamente autorizadas (SMITH et al., 1996). Responderam que concordam ou concordam totalmente para a variável ACI1 70,9% da amostra, para ACI2 70,2% e para ACI3 68,5%, com médias respectivas de 5,92, 5,81 e 5,84.

O Construto Controle buscou identificar o grau com que o respondente está preocupado em não ter o controle adequado sobre suas informações pessoais na Internet (MALHOTRA et al., 2004). Os resultados obtidos, apresentados na Tabela 12, indicam um grau elevado de preocupação com a privacidade relacionada com o construto, uma vez que responderam concordo ou concordo totalmente 66,9% para CTRL1, 66,6% para CTRL2 e 60,3% para CTRL3. As médias obtidas para cada variável também indicam o alto grau de preocupação, com 5,7 para CTRL1, 5,75 CTRL2 e 5,5 para CTRL3. Os resultados indicam ainda que 10,8%, 9,2% e 12,5% respectivamente indicaram algum nível de discordância com as questões apresentadas.

O Construto Consciência buscou identificar o grau em que o usuário está preocupado em saber sobre as práticas dos *sites* relativas à privacidade das informações (MALHOTRA et al., 2004). Os resultados da análise deste construto apresentados na Tabela 12 indicam um grau elevado de preocupação com a privacidade relacionada ao construto, uma vez que o percentual da amostra que indicou que concorda ou concorda totalmente com cada questão foi de 66,9,8% para CONS1, 66,6% para CONS2 e 60,3% para CONS3. A média obtida para cada variável foi de 5,7, 5,75 e 5,5 consecutivamente.

O Construto Crenças de Confiança tem como objetivo medir o grau em que um usuário confia nas empresas para as quais fornece informações na Internet (MALHOTRA et al., 2004). Os resultados obtidos indicam uma percepção mais neutra com relação ao construto. A variável CONF1 apresentou um percentual de 31,7% de respostas entre discordo e discordo totalmente, sendo que o maior percentual de respostas para está variável é de 18,8% que discordam totalmente. As demais variáveis apresentaram resultados maiores para a opção neutra, tendo CONF2 19,1%, CONF3 24,5% e CONF4 21,1% de respostas neutras. Importante salientar que todas as variáveis obtiveram percentual de respostas entre neutro e discordo totalmente acima de 50%, indicando uma tendência de desconfiança relacionada ao construto.

O Construto Crença de Risco tem como objetivo identificar o grau em que um usuário percebe risco em suas atividades na Internet (MALHOTRA et al., 2004). Os resultados apresentados indicam uma média percepção de risco à privacidade associado ao construto. A variável RISC1 com 58,2% de respostas entre cocordo e concordo totalmente e RISC3 com 44,8%, apresentaram os maiores índices percentuais de percepção de risco, as demais variáveis obtiveram 44,8% para RISC2 e 48,4% para RISC4, fortalecendo a percepção de médio grau de preocupação relacionada ao construto. A Tabela 13 apresenta as médias e os desvios-padrão de cada variável, por Região do Brasil.

Tabela 13 – Média da preocupação com a privacidade por região do Brasil

Variáveis	Norte		Nordeste		Centro-Oeste		Sudeste		Sul		Total
	Média	Desvio padrão	Média	Desvio padrão	Média	Desvio padrão	Média	Desvio padrão	Média	Desvio padrão	Média
COL1	5,20	1,828	5,31	1,701	5,24	1,885	**5,57**	1,541	**6,42**	,814	5,54
COL2	**5,61**	1,782	**5,75**	1,521	**5,84**	1,606	**6,10**	1,412	**6,15**	1,288	5,89
COL3	5,50	1,749	**5,55**	1,648	5,67	1,663	**5,94**	1,456	**5,78**	1,463	5,69
USEC1	**5,63**	1,713	**5,77**	1,506	**5,78**	1,534	**5,97**	1,456	**6,04**	1,332	5,84
USEC2	5,50	1,780	**5,74**	1,553	5,50	1,674	**5,75**	1,675	**5,87**	1,502	5,68
USEC3	**5,53**	1,749	**5,80**	1,538	**5,69**	1,626	**5,98**	1,522	**6,07**	1,371	5,82
ERR1	5,42	1,772	5,48	1,721	5,48	1,702	**5,58**	1,716	5,50	1,637	5,49
ERR2	5,31	1,750	5,38	1,650	5,35	1,671	5,45	1,705	**5,61**	1,596	5,42
ERR3	5,13	1,829	5,14	1,720	5,09	1,761	5,13	1,889	4,54	1,858	5,02
ACI1	**5,69**	1,566	**5,85**	1,550	**5,73**	1,530	**6,13**	1,382	**6,17**	1,336	5,92
ACI2	**5,53**	1,709	**5,84**	1,504	**5,60**	1,671	**6,03**	1,465	**6,02**	1,395	5,81
ACI3	**5,53**	1,703	**5,85**	1,493	**5,66**	1,567	**6,06**	1,410	**6,03**	1,384	5,84
CTRL1	5,50	1,769	**5,63**	1,655	**5,61**	1,636	**5,94**	1,526	**5,81**	1,492	5,70
CTRL2	5,49	1,769	**5,72**	1,545	**5,55**	1,633	**5,96**	1,504	**6,00**	1,336	5,75
CTRL3	5,26	1,814	5,46	1,674	5,43	1,658	**5,67**	1,608	**5,64**	1,646	5,50
CONS1	5,49	1,752	**5,63**	1,547	**5,62**	1,467	**5,82**	1,530	5,47	1,725	5,61
CONS2	**5,65**	1,564	**5,71**	1,505	**5,67**	1,459	**6,06**	1,330	**5,88**	1,425	5,80
CONS3	**5,70**	1,680	**5,70**	1,468	**5,64**	1,481	**5,91**	1,450	**5,65**	1,571	5,73
CONF1	4,54	2,069	3,94	2,137	4,35	1,952	3,62	2,096	**3,06**	1,838	3,90
CONF2	4,74	1,909	4,33	2,034	4,53	1,863	3,77	2,053	**2,97**	1,740	4,07
CONF3	4,81	1,842	4,30	1,926	4,59	1,731	3,93	1,957	**3,23**	1,561	4,17
CONF4	4,66	1,960	4,28	1,923	4,73	1,780	4,10	1,946	**3,39**	1,666	4,23
RISC1	5,44	1,779	5,49	1,629	5,53	1,528	**5,60**	1,681	5,29	1,722	5,48
RISC2	5,04	1,895	5,18	1,609	5,23	1,479	5,02	1,741	4,71	1,689	5,04
RISC3	5,36	1,709	5,38	1,585	5,40	1,608	**5,49**	1,662	5,30	1,639	5,39
RISC4	5,12	1,909	5,26	1,544	5,30	1,537	5,23	1,741	4,82	1,623	5,15

Fonte: O autor (2015)

Os resultados apresentados na Tabela 13 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.

De acordo com a análise por região, os resultados indicam que a região com maior grau de preocupação com a privacidade é o Sudeste, obtendo resultados mais expressivos em 95,45% das variáveis. Por outro lado a região com menor grau de confiança é a região Sul, cujas respostas para cada variável estão distribuídas entre discordo totalmente e discordo em parte com os seguintes percentuais: CONF1 com 62,87%, CONF2 com 64,36%, CONF3 com 55,45% e CONF4 com 50,99%. Os resultados indicam ainda que as regiões Sudeste e Sul são as que apresentaram maior grau de preocupação com a privacidade. Por outro lado, os resultados indicam que a região Centro-Oeste é a menos preocupada com a privacidade, a região Norte a mais confiante, e a região Sul foi a que apresentou os menores resultados quanto a preocupação relacionada ao construto Risco, com respostas entre concordo e concordo totalmente de 51,98% para RISC1, 34,65 % para RISC2, 52,97% para RISC3 e 37,62% dos respondentes para RISC4.

Os resultados da análise cruzada dos construtos com a variável gênero indicam que as mulheres possuem maior grau de preocupação com a privacidade em todos os construtos, apresentando os seguintes médias percentuais de respostas entre concordo e concordo totalmente para cada construto: Coleta 66,57%, Uso Secundário 69,40, Erros 57,23%, Acesso Indevido 73,02%, Controle 67,69%, Consciência 68,23% e Risco 68,23% das respostas. Com relação a Confiança, os resultados indicam que as mulheres confiam menos do que os homens.

4.4 ANÁLISE DESCRITIVA UNIVARIADA

A Análise Descritiva Univariada foi realizada através da estatística descritiva com frequência simples, médias e desvio padrão da escala, e através dos itens das escalas de mensuração, incluindo média e desvio padrão, conforme pode ser verificado na Tabela 14. Por meio da Análise Univariada é possível verificar o padrão médio das respostas obtidas para cada variável observável.

Tabela 14 – Análise descritiva estatística da amostra

	Média		Desvio padrão	Variância	Assimetria		Kurtosis	
	Estatística	Modelo padrão	Estatística	Estatística	Estatística	Modelo padrão	Estatística	Modelo padrão
COL1	5,54	,050	1,662	2,762	-1,017	,074	,156	,147
COL2	5,89	,046	1,538	2,365	-1,441	,074	1,319	,147
COL3	5,69	,048	1,602	2,568	-1,189	,074	,597	,147
USEC1	5,84	,046	1,516	2,297	-1,336	,074	1,117	,147
USEC2	5,68	,049	1,642	2,696	-1,171	,074	,458	,147
USEC3	5,82	,047	1,573	2,474	-1,399	,074	1,217	,147
ERR1	5,49	,051	1,709	2,919	-1,028	,074	,128	,147
ERR2	5,42	,050	1,676	2,808	-,892	,074	-,093	,147
ERR3	5,02	,055	1,823	3,323	-,637	,074	-,617	,147
ACI1	5,92	,045	1,486	2,208	-1,450	,074	1,467	,147
ACI2	5,81	,047	1,560	2,434	-1,340	,074	,975	,147
ACI3	5,84	,046	1,522	2,318	-1,331	,074	1,038	,147
CTRL1	5,70	,049	1,622	2,630	-1,271	,074	,817	,147
CTRL2	5,75	,047	1,573	2,474	-1,272	,074	,894	,147
CTRL3	5,50	,051	1,682	2,829	-1,045	,074	,247	,147
CONS1	5,61	,048	1,605	2,575	-1,086	,074	,383	,147
CONS2	5,80	,044	1,461	2,135	-1,208	,074	,876	,147
CONS3	5,73	,046	1,528	2,333	-1,124	,074	,432	,147
CONF1	3,90	,063	2,088	4,360	,063	,074	-1,289	,147
CONF2	4,07	,061	2,025	4,099	-,028	,074	-1,222	,147
CONF3	4,17	,057	1,894	3,585	-,070	,074	-1,004	,147
CONF4	4,23	,058	1,918	3,680	-,104	,074	-1,057	,147
RISC1	5,48	,050	1,668	2,783	-,942	,074	,004	,147
RISC2	5,04	,051	1,692	2,864	-,526	,074	-,603	,147
RISC3	5,39	,049	1,638	2,684	-,857	,074	-,059	,147
RISC4	5,15	,051	1,680	2,821	-,609	,074	-,524	,147

Fonte: O autor (2015)

Verificou-se a normalidade através da análise de assimetria e curtose. Segundo Malhotra (2006, p. 446) assimetria é “a característica de uma distribuição que mede a sua simetria em relação à média” e, ainda segundo os autores, curtose “é uma medida do achatamento relativo da curva definida pela distribuição de frequência”. De acordo com Kline (2011), valores de assimetria superiores a 3 podem ser tidos como bastante assimétricos e valores de curtose superiores a 10 sugerem um problema, e valores superiores a 20 um problema mais grave. Com base nas recomendações de Kline (2011), os valores apresentados na Tabela 38 representam uma assimetria negativa e uma distribuição leptocúrtica, com valores de curtose maiores que a distribuição normal. Somente as variáveis do construto confiança apresentaram valores simétricos

4.5 ANÁLISE FATORIAL EXPLORATÓRIA

Realizou-se a análise exploratória dos dados coletados com o objetivo de descrever e explorar as características principais dos resultados, bem como de explicar a correlação e covariância destes dados. Os resultados das análises são apresentados a seguir. Inicialmente verificou-se a fatorabilidade da matriz de correlações da amostra, através da inspeção da matriz de correlações.

Tabela 15 – Matriz de Correlações

	COL1	COL2	COL3	USEC1	USEC2	USEC3	ERR1	ERR2	ERR3	ACI1	ACI2	ACI3	CTRL1	CTRL2	CTRL3	CONS1	CONS2	CONS3	CONF1	CONF2	CONF3	CONF4	RISC1	RISC2	RISC3	RISC4
COL1	**1,000**																									
COL2	,594	**1,000**																								
COL3	,596	,699	**1,000**																							
USEC1	,530	,668	,766	**1,000**																						
USEC2	,463	,583	,672	,771	**1,000**																					
USEC3	,481	,621	,682	,812	,829	**1,000**																				
ERR1	,380	,451	,535	,599	,653	,677	**1,000**																			
ERR2	,367	,436	,504	,541	,594	,588	,760	**1,000**																		
ERR3	,292	,347	,462	,475	,525	,508	,658	,727	**1,000**																	
ACI1	,481	,615	,683	,728	,688	,743	,604	,591	,517	**1,000**																
ACI2	,462	,591	,671	,704	,705	,751	,606	,592	,547	,840	**1,000**															
ACI3	,465	,589	,682	,702	,691	,722	,592	,589	,517	,839	,875	**1,000**														
CTRL1	,435	,574	,626	,597	,619	,629	,526	,542	,498	,679	,689	,695	**1,000**													
CTRL2	,515	,560	,590	,616	,597	,627	,515	,506	,457	,624	,630	,649	,641	**1,000**												
CTRL3	,452	,480	,553	,554	,585	,598	,555	,547	,511	,618	,629	,631	,571	,731	**1,000**											
CONS1	,393	,532	,559	,593	,596	,606	,532	,523	,519	,631	,623	,618	,603	,670	,676	**1,000**										
CONS2	,471	,598	,600	,649	,585	,647	,522	,508	,465	,677	,658	,668	,614	,698	,662	,763	**1,000**									
CONS3	,441	,556	,586	,658	,605	,657	,542	,502	,488	,673	,675	,671	,598	,665	,620	,733	,799	**1,000**								
CONF1	-,027	-,010	,030	-,016	,055	,003	,147	,176	,223	-,022	,010	,017	,042	,009	,108	,102	,056	,097	**1,000**							
CONF2	,014	,044	,070	,019	,072	,045	,191	,213	,273	,046	,067	,071	,070	,076	,138	,151	,108	,156	,763	**1,000**						
CONF3	-,001	,027	,068	,042	,071	,044	,164	,188	,248	,030	,042	,037	,062	,021	,094	,105	,076	,113	,751	,783	**1,000**					
CONF4	,032	,085	,100	,072	,101	,086	,190	,206	,252	,068	,096	,089	,078	,051	,133	,121	,102	,161	,700	,753	,802	**1,000**				
RISC1	,339	,441	,493	,522	,490	,474	,449	,423	,379	,507	,501	,503	,441	,487	,477	,475	,518	,545	,154	,240	,207	,252	**1,000**			
RISC2	,308	,358	,450	,434	,457	,443	,464	,431	,481	,442	,475	,476	,443	,453	,537	,488	,459	,502	,255	,327	,285	,336	,688	**1,000**		
RISC3	,380	,445	,499	,501	,502	,501	,443	,427	,414	,526	,543	,547	,472	,556	,538	,526	,569	,591	,118	,207	,179	,204	,699	,731	**1,000**	
RISC4	,334	,386	,449	,449	,485	,468	,427	,433	,464	,486	,481	,486	,462	,489	,516	,505	,490	,518	,179	,253	,199	,220	,614	,702	,741	**1,000**

Fonte: O autor (2015)

Os resultados da matriz de correlações indicam que mais de 50% dos fatores apresentam coeficiente de correlação superior a 0,30, conforme recomendado por Hair et al. (2009), quanto maior a quantidade de valores superiores a 0,30, mais favorável é a matriz.

O Quadro 8 apresenta a medida de adequação da amostra de Kaiser-Meyer-Olkin (KMO), que segundo Hair et al. (2009) é um índice utilizado para avaliar a adequação da análise fatorial. O valor de ,957 obtido na análise indica, ainda segundo os autores, que a análise fatorial é adequada.

Quadro 8 – Teste de KMO e Bartlett

Medida Kaiser-Meyer-Olkin de adequação de amostragem.		,957
Teste de esfericidade de Bartlett	Qui-quadrado aprox.	26222,819
	df	325
	Sig.	,000

Fonte: O autor (2015)

O Teste de Esfericidade de Bartlett's, também apresentado na Tabela 16, apresenta um valor grande e corresponde a um nível de significância pequeno, que segundo Malhotra

(2006), indica uma baixa probabilidade de que a matriz seja uma matriz de identidade. A Tabela 16 apresenta os valores das comunalidades, que segundo Malhotra (2006), trata-se da proporção da variância que uma variável compartilha com as demais variáveis, e é também a proporção de variância explicada pelos fatores.

Tabela 16 – Comunalidades

	Inicial	Extração
COL1	1,000	,554
COL2	1,000	,710
COL3	1,000	,726
USEC1	1,000	,756
USEC2	1,000	,709
USEC3	1,000	,765
ERR1	1,000	,755
ERR2	1,000	,784
ERR3	1,000	,750
ACI1	1,000	,762
ACI2	1,000	,761
ACI3	1,000	,752
CTRL1	1,000	,615
CTRL2	1,000	,649
CTRL3	1,000	,613
CONS1	1,000	,620
CONS2	1,000	,686
CONS3	1,000	,677
CONF1	1,000	,786
CONF2	1,000	,828
CONF3	1,000	,851
CONF4	1,000	,811
RISC1	1,000	,690
RISC2	1,000	,785
RISC3	1,000	,815
RISC4	1,000	,746
Método de extração: análise do componente principal.		

Fonte: O autor (2015)

Os resultados apresentados na Tabela 16 são considerados satisfatórios, uma vez que nenhuma variável apresentou índice inferior 0,4. Índices abaixo deste valor indica que não fornece explicação suficiente para o que está mensurando (MALHOTRA, 2006).

Realizou-se a extração dos fatores com objetivo de determinar quais os fatores melhor representam o padrão de correlação entre as variáveis observadas. A Tabela 17 apresenta a total variância explicada, cujo método de extração utilizado foi o de análise do componente principal.

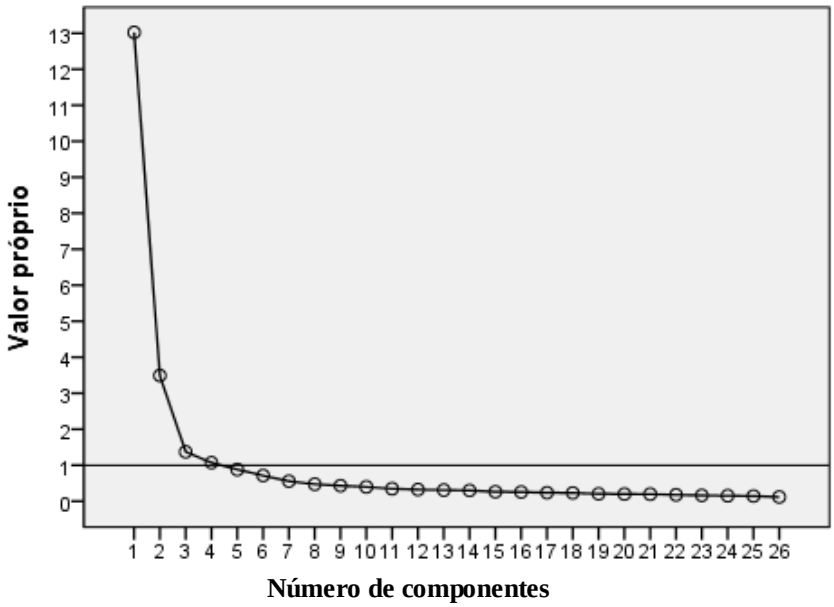
Tabela 17 – Variância total explicada

Componente	Valores próprios iniciais			Somas de extração de carregamentos ao quadrado		
	Total	% de variância	% cumulativa	Total	% de variância	% cumulativa
1	13,024	50,091	50,091	13,024	50,091	50,091
2	3,491	13,427	63,518	3,491	13,427	63,518
3	1,372	5,275	68,793	1,372	5,275	68,793
4	1,070	4,114	72,907	1,070	4,114	72,907
5	,878	3,378	76,286			
6	,711	2,736	79,021			
7	,555	2,134	81,156			
8	,470	1,809	82,964			
9	,432	1,662	84,626			
10	,397	1,526	86,152			
11	,346	1,332	87,484			
12	,322	1,240	88,724			
13	,308	1,186	89,910			
14	,297	1,141	91,052			
15	,263	1,011	92,063			
16	,253	,973	93,036			
17	,237	,910	93,946			
18	,231	,887	94,834			
19	,203	,781	95,615			
20	,196	,755	96,370			
21	,196	,754	97,124			
22	,177	,682	97,805			
23	,161	,619	98,424			
24	,151	,581	99,005			
25	,144	,552	99,557			
26	,115	,443	100,000			

Fonte: O autor (2015)

Utilizando-se o critério de raiz latente, que segundo Hair et al. (2009), indica que devem ser mantidos os fatores com autovalores maiores do que 1,0. Desta forma foram mantidos quatro componentes, os quais representam 72,907% da variância explicada das 26 variáveis. Realizou-se análises forçadas com 8, 7, 6 e 5 fatores, mas os melhores resultados foram encontrados com os 4 fatores identificados. No estudo original de Hong e Thong (2013) os resultados foram semelhantes.

Gráfico 1 – Scree Test



Fonte: O autor (2015)

O Gráfico 1 ilustra a dispersão dos componentes no *Scree test*, e a linha de referência que parte do eixo y indica os fatores com valores maiores que 1.

Na Tabela 18 apresenta-se a matriz fatorial não-rotacionada da análise de componentes. Pode-se verificar as cargas fatoriais para os quatro fatores extraídos, bem como as comunalidades de cada variável. A primeira linha de números abaixo de cada coluna apresenta a soma das cargas fatoriais ao quadrado (autovalores) de cada fator, e indica a importância relativa destes fatores na explicação da variância associada ao conjunto de variáveis. A soma dos quadrados para os quatro fatores são 13,024, 3,491, 1,372 e 1,070. A solução fatorial extrai os fatores na ordem de sua importância com o fator 1 explicando a maior parte da variância, o fator 2 explicando bem menos, e assim por diante ao longo de todos os 26 fatores. Na extremidade à direita da linha está o valor 18,957, que representa o total dos quatro autovalores, o que representa o total de variância extraída pela solução fatorial.

Os percentuais de traço explicados por cada um dos quatro fatores (50,091%, 13,427%, 5,275% e 4,114%), apresentados na Tabela 18, foram obtidos dividindo-se a soma dos quadrados (autovalores) pelo traço para o conjunto de variáveis. O índice para a solução geral mostra que 72,907% da variância total é representado pela informação contida na solução fatorial da solução, em termos de quatro fatores. De acordo com Hair et al. (2009) o índice para a solução é alto, estando as variáveis estreitamente relacionadas umas com as outras.

Tabela 18 – Matriz de análise fatorial de componente não-rotacionada

Variáveis	**Fator**				**Comunalidades**
	1	**2**	**3**	**4**	
COL1	**,594**	-,172	,040	**,413**	,554
COL2	**,718**	-,170	,085	,399	,710
COL3	**,794**	-,137	,103	,258	,726
USEC1	**,825**	-,185	,135	,151	,756
USEC2	**,817**	-,114	,169	-,029	,709
USEC3	**,838**	-,164	,187	,010	,765
ERR1	**,746**	,060	,267	-,352	,755
ERR2	**,725**	,099	,288	-,**408**	,784
ERR3	**,673**	,194	,217	-,**460**	,750
ACI1	**,846**	-,179	,120	,010	,762
ACI2	**,851**	-,148	,122	-,029	,761
ACI3	**,848**	-,150	,101	-,004	,752
CTRL1	**,771**	-,115	,087	,016	,615
CTRL2	**,787**	-,135	-,075	,074	,649
CTRL3	**,776**	-,017	-,070	-,072	,613
CONS1	**,786**	-,027	-,042	-,010	,620
CONS2	**,812**	-,090	-,062	,120	,686
CONS3	**,815**	-,027	-,076	,081	,677
CONF1	,140	**,854**	,162	,104	,786
CONF2	,209	**,875**	,093	,106	,828
CONF3	,178	**,880**	,150	,147	,851
CONF4	,220	**,848**	,123	,165	,811
RISC1	**,681**	,174	-,**443**	-,002	,690
RISC2	**,669**	,308	-,**470**	-,149	,785
RISC3	**,719**	,135	-,**527**	-,045	,815
RISC4	**,674**	,195	-,**483**	-,142	,746
					Total
Soma de quadrados (autovalor)	13,024	3,491	1,372	1,070	18,957
Percentual de traço	50,091%	13,427%	5,275%	4,114%5	72,907%

Método de extração: Análise do Componente principal.
a. 4 componentes extraídos.
Traço = 26 (soma de autovalores)

Fonte: O autor (2015)

Uma vez que a matriz fatorial não-rotacionada não tem um conjunto de cargas fatoriais completamente limpo, com cargas cruzadas substanciais ou não maximizava as cargas de cada variável em um fator, utilizou-se a técnica de rotação Varimax para melhorar a interpretação, sendo seus impactos sobre a solução fatorial geral e sobre as cargas fatoriais apresentados na Tabela 19.

Tabela 19 – Matriz de análise fatorial de componentes rotacionadas por Varimax

Variáveis	Componente				Comunaliddes
	1	2	3	4	
COL2	**,827**				,710
COL3	**,801**				,726
USEC1	**,787**				,756
COL1	**,732**				,554
USEC3	**,725**		,450		,765
ACI1	**,719**		,424		,762
ACI3	**,701**		,429		,752
ACI2	**,693**		,458		,761
CONS2	**,689**				,686
USEC2	**,668**		,464		,709
CTRL2	**,654**				,649
CONS3	**,649**	,418			,677
CTRL1	**,641**				,615
CONS1	**,584**				,620
CTRL3	**,534**	**,426**			,613
RISC3		**,810**			,815
RISC2		**,789**			,785
RISC4		**,781**			,746
RISC1		**,719**			,690
ERR2			**,776**		,784
ERR3			**,766**		,750
ERR1	,410		**,732**		,755
CONF3				**,916**	,851
CONF2				**,893**	,828
CONF4				**,890**	,811
CONF1				**,880**	,786
					Total
Soma de quadrados (autovalor)	8,052	3,876	3,629	3,398	18,955
Percentual de traço	30,971%	14,909%	13,957%	13,070%	72,907%

Método de rotação: Varimax com normalização de Kaiser.
Rotação convergida em 6 iterações.
Cargas fatoriais menores que 0,40 não foram impressas, e as variáveis foram agrupadas por carga em cada fator .

Fonte: O autor (2015)

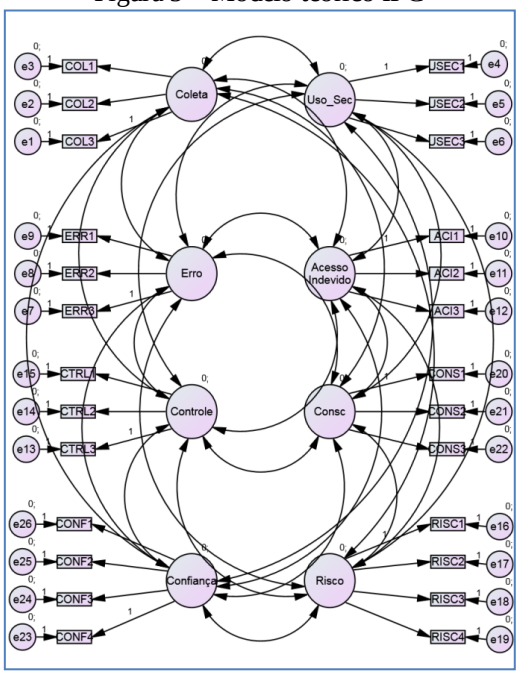
Pode-se verificar na Tabela 19 que a quantidade total de variância extraída na solução rotacionada é a mesma da não-rotacionada, 72,907%. Da mesma forma, as comunalidades para cada variável não são alteradas quando é aplicada a técnica de rotação. Por outro lado, duas alterações são apresentadas. A variância é redistribuída, fazendo com que o percentual

de variância de cada fator apresente valores diferentes. Na solução fatorial rotacionada Varimax o primeiro fator explica 30,971% da variância, enquanto que na solução não-rotacionada explica 50,091%. Da mesma forma, os demais fatores também apresentam valores diferentes. O poder explicativo mudou sensivelmente para uma distribuição mais equilibrada em função da rotação.

4.6 ANÁLISE CONFIRMATÓRIA DO MODELO DE MENSURAÇÃO

Segundo Hair et al. (2009), uma das maiores vantagens da Análise Fatorial Confirmatória (CFA) é a sua capacidade para avaliar a validade de construto de uma teoria de mensuração proposta. Ainda segundo os autores, CFA é uma maneira de testar o quão bem as variáveis medidas representam um número menor de construtos. Com o objetivo de confirmar a teoria de mensuração, realizou-se a CFA através do Software SPSS Amos 21, cujos resultados são apresentados a seguir.

Figura 5 – Modelo teórico IPC



Fonte: Hong e Thong (2013)

A Tabela 20 apresenta as correlações quadradas múltiplas para cada variável medida. Estes valores, segundo Hair et al. (2009, p. 629), representam o grau em que a variância da variável medida é explicada por um fator latente.

Tabela 20 – Correlações quadradas múltiplas

Escalas	Estimate
CONF1	,698
CONF2	,775
CONF3	,817
CONF4	,749
CONS3	,774
CONS2	,808
CONS1	,719
RISC4	,677
RISC3	,775
RISC2	,711
RISC1	,629
CTRL1	,602
CTRL2	,710
CTRL3	,656
ACI3	,864
ACI2	,870
ACI1	,823
ERR1	,743
ERR2	,779
ERR3	,634
USEC3	,845
USEC2	,778
USEC1	,794
COL1	,459
COL2	,650
COL3	,782

Fonte: O autor (2015)

De acordo com Hair et al. (2009) não são fornecidas regras específicas para realizar a interpretação dos valores de correlação tais como os apresentados na Tabela 20, uma vez que, segundo os autores, em um modelo de mensuração semelhante elas são uma função das estimativas de carga. Ainda segundo os autores, as regras para as estimativas de cargas fatoriais tendem a produzir o mesmo diagnóstico. Sendo assim, os valores apresentados são significantes (HAIR et al., 2009).

A seguir são apresentados os valores de resíduos padronizados no Apêndice B. De acordo com Hair et al. (2009), resíduos se referem às diferenças individuais entre termos de covariância. Ainda segundo os autores, os resíduos padronizados não são dependentes do real intervalo da escala de medição, o que os tornam úteis no diagnóstico de problema com um modelo de mensuração.

De acordo com Hair et al. (2009), os resultados podem ser positivos ou negativos, dependendo se a covariância estimada está abaixo ou acima da correspondente covariância. Ainda segundo os autores, valores inferiores a 2,5 não sugerem um problema, resíduos maiores que 4,0 sinalizam um alerta vermelho e sugerem um grau de erro potencialmente

inaceitável e valores entre 2,5 e 4,0 podem não sugerir quaisquer mudanças no modelo. Apenas três valores apresentados no Apêndice B, obtiveram valores próximos de 4,0, indicando que os resultados apresentados estão adequados. A seguir são apresentados os valores dos índices de ajuste do modelo, os quais foram obtidos através da ferramenta SPSS Amos 21.

Tabela 21 – Qui-quadrado sobre os graus de liberdade (CMIN/DF)

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	106	1282,474	271	,000	4,732
Saturated model	377	,000	0		
Independence model	52	26450,635	325	,000	81,387

Fonte: O autor (2015)

Segundo Hair et al. (2005), valores de qui-quadrado sobre os graus de liberdade (CMIN/DF) inferiores a 3 são preferíveis, mas abaixo de 5 são toleráveis. Na presente pesquisa, conforme apresentado na Tabela 21, os resultados indicam que o grau de liberdade está dentro de valores toleráveis.

Tabela 22 – Comparações de Baseline

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,952	,942	,961	,954	,961
Saturated model	1,000		1,000		1,000
Independence model	,000	,000	,000	,000	,000

Fonte: O autor (2015)

Segundo Hair et al. (2009) a equação para cálculo do Índice de Ajuste Comparativo (*CFI*) está normatizada para valores entre 0 e 1, sendo que valores mais altos indicam um melhor ajuste. Ainda segundo os autores, o Índice de Tucker-Lewis (TLI) não é normatizada, e, assim seus valores podem ficar abaixo de 0 ou acima de 1, sendo que na maioria das vezes o índice produz valores semelhantes ao CFI. Para o Índice de ajuste normalizado (NFI) valores maiores que 0,95 são desejados (HAIR et al., 2009). Os valores apresentados na Tabela 25 determinam um ótimo ajuste para os índices de CFI, TLI e NFI, indicando adequação dos dados.

Tabela 23 – Raiz do erro quadrático médio de aproximação (RMSEA)

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,058	,055	,061	,000
Independence model	,270	,267	,273	,000

Fonte: O autor (2015)

Segundo Hair et al. (2009) o Índice RMSEA representa o quanto um modelo se ajusta à população, não somente à amostra utilizada para a estimação. Valores abaixo de 0,08 são desejáveis e valores abaixo de 0,5 ótimos. Na presente pesquisa, de acordo com o indicado por Hair et al. (2009), os valores apresentados na Tabela 23 estão ótimos, indicando que o modelo se ajusta muito bem a população, não apenas à amostra utilizada para a estimação.

Tabela 24 – Índice de Holter

Model	HOELTER .05	HOELTER .01
Default model	267	283
Independence model	16	17

Fonte: O autor (2015)

A Tabela 24 apresenta os resultados do Índice de Hoelter, que indica a adequação do tamanho da amostra com 95% e 99% de confiança. De acordo com Hair et al. (2013), um valor acima de 200 indica que o modelo representa bem os dados amostrais.

4.7 VALIDADE CONVERGENTE E DISCRIMINANTE

A Tabela 25 apresenta os valores da Média de Variância Extraída (AVE), que se referem à validade convergente. Os resultados são bastante significativos, ficando bem acima do recomendado por Hair et al. (2013), que é no mínimo 0,50.

Tabela 25 – Validade e confiabilidade convergente

Construto	**AVE**	**Composite Reliability**	**Alpha de Cronbach**
ACESSO INDEVIDO	0.901	0.965	0.945
COLETA	0.753	0.901	0.836
CONFIANÇA	0.819	0.948	0.926
CONSCIENCIA	0.843	0.942	0.907
CONTROLE	0.766	0.907	0.847
ERRO	0.810	0.928	0.883
RISCO	0.772	0.931	0.901
USO SECUNDÁRIO	0.869	0.952	0.925

Fonte: O autor (2015)

A validade convergente foi analisada através da extração do fator e cargas significantes, conforme apresentado na Tabela 25.

Tabela 26 – Cargas significativas das variáveis

Variáveis	CONSTRUTOS							
	Acesso_Ind	**Coleta**	**Confiança**	**Consciência**	**Controle**	**Erro**	**Risco**	**Uso_Sec**
ACI1	**0.940**							
ACI2	**0.954**							
ACI3	**0.954**							
COL1		**0.812**						
COL2		**0.884**						
COL3		**0.904**						
CONF1			**0.889**					
CONF2			**0.918**					
CONF3			**0.919**					
CONF4			**0.893**					
CONS1				**0.903**				
CONS2				**0.928**				
CONS3				**0.923**				
CTRL1					**0.830**			
CTRL2					**0.906**			
CTRL3					**0.888**			
ERR1						**0.894**		
ERR2						**0.919**		
ERR3						**0.887**		
RISC1							**0.852**	
RISC2							**0.885**	
RISC3							**0.907**	
RISC4							**0.870**	
USEC1								**0.923**
USEC2								**0.931**
USEC3								**0.944**

Fonte: O autor (2015)

Os resultados apresentados na Tabela 26 mostram que a carga fatorial de cada variável, em seu respectivo fator, foi significante.

A validade discriminante, segundo Hair et al. (2006), “é o grau em que um construto é verdadeiramente diferente dos demais”. Ainda segundo os autores, um grau elevado de validade discriminante “oferece evidência de que um construto é único e captura alguns fenômenos que outras medidas não conseguem”.

Tabela 27 – Validade discriminante do modelo

	Acesso_Ind	Coleta	Confiança	Consciência	Controle	Erro	Risco	Uso_Sec
ACESSO_IND	**0.949**							
COLETA	0.717	**0.867**						
CONFIANÇA	0.053	0.049	**0.905**					
CONSCIENCIA	0.752	0.668	0.137	**0.918**				
CONTROLE	0.779	0.704	0.095	0.803	**0.875**			
ERRO	0.670	0.544	0.254	0.619	0.656	**0.900**		
RISCO	0.598	0.542	0.283	0.641	0.638	0.551	**0.879**	
USO_SEC	0.807	0.762	0.058	0.727	0.736	0.682	0.583	**0.932**

Fonte: O autor (2015)

Os resultados apresentados na Tabela 27 evidenciam que os construtos são únicos e verdadeiramente diferente dos demais, de acordo com o indicado por (HAIR et al., 2009).

4.8 ANÁLISE DE CLUSTERS

A análise de cluster realizada identificou a formação de quatro agrupamentos na amostra utilizada, sendo as características destes agrupamentos apresentadas na Tabela 28 a seguir.

Tabela 28 – 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	Até R$ 2.899,99
	Escolaridade	Graduados	Graduandos	Graduandos	Ensino médio
	Região	Sul/sudeste	Norte	Centro-oeste/nordeste/sudeste	Norte
	Gênero	Feminino (237)	Feminino (214)	Feminino (171) / masculino (144)	Feminino (60)
Total de casos		**374**	**326**	**315**	**89**

Fonte: O autor (2015)

Percebem-se características bem distintas entre os *clusters*. De acordo com os resultados apresentados na Tabela 28, 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 dividida, 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 têm maior participação na formação de três dos quatro *clusters*, sendo que somente no cluster 3 a quantidade de homens e mulheres foi muito parecida.

Com relação à renda, os dados mostram um resultado interessante. O cluster 1, dos preocupados e desconfiados, 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.

A Tabela 29 apresenta as sementes de agrupamento, ou centroide inicial, que é o ponto de partida para realizar os agrupamentos. Os valores foram definidos automaticamente pelo software. Os agrupamentos resultantes da análise de cluster são construídos a partir destes centros (sementes) iniciais. Com o objetivo de facilitar a leitura, optou-se por apresenta a Tabela 29 com as variáveis dispostas em duas colunas.

Tabela 29 – Centro de *clusters* iniciais

Variáveis	**Cluster**				**Variáveis**	**Cluster**			
	1	**2**	**3**	**4**		**1**	**2**	**3**	**4**
COL1	7	5	1	6	RISC1	7	7	3	5
COL2	7	7	4	1	RISC2	7	7	1	1
COL3	7	6	1	1	RISC3	7	7	1	1
USEC1	7	7	5	1	RISC4	7	7	2	7
USEC2	7	7	7	1	Escola onde estuda/estudou	1	5	1	1
USEC3	7	7	7	1	Notas	1	5	5	1
ERR1	7	7	7	1	Empresa onde trabalha	1	5	1	1
ERR2	7	1	7	2	Cargo	1	5	5	1
ERR3	7	1	1	1	Salário	1	5	5	1
ACI1	7	1	6	1	Endereço residencial	5	5	5	1
ACI2	7	1	1	1	Localização pelo celular	1	5	5	1
ACI3	7	1	1	1	Senhas	5	5	5	2
CTRL1	7	1	7	1	Telefones	1	5	5	1
CTRL2	7	1	1	1	Fotos	1	5	1	1
CTRL3	7	1	2	1	Data de nascimento	1	5	1	1
CONS1	7	7	2	1	Orientação sexual	1	5	4	1
CONS2	7	7	1	1	Vícios	1	4	2	1
CONS3	7	7	2	1	Número de CC/agência	1	5	5	1
CONF1	1	7	2	7	Saldo bancário	1	5	5	1
CONF2	7	7	1	7	Limite do cheque especial	1	5	5	1
CONF3	7	7	2	7	Número de cartão de crédito	1	5	5	1
CONF4	7	7	2	7	Gastos com cartão de crédito	1	5	5	1

Fonte: O autor (2015)

A Tabela 30 apresenta o histórico de iterações, com a indicação da variação dos centros dos *clusters* em cada iteração realizada na formação destes *clusters*.

Tabela 30 – Histórico de iterações

Iteração	Alteração em centros de cluster			
	1	2	3	4
1	12,881	13,511	13,675	11,560
2	,944	1,618	1,516	1,196
3	,946	2,450	,694	,378
4	1,273	1,960	,548	,955
5	,642	,832	,480	,795
6	,291	,263	,283	,821
7	,147	,124	,164	,366
8	,095	,090	,188	,543
9	,047	,020	,112	,203
10	0,000	,023	,066	,195
11	0,000	0,000	0,000	0,000

Fonte: O autor (2015)

Os resultados apresentados na Tabela 30 indicam que o algoritmo de iterações encerrou na iteração 10. Importante salientar que o algoritmo é encerrado no momento em que

não há mais uma variação significativa dos centroides após a distribuição dos objetos nos *clusters*. A seguir apresenta-se a Tabela 31, que indica os membros de cada cluster.

Tabela 31 – Membros dos *Clusters*

Número de caso	Cluster	Distância
1	1	8,394
2	1	7,017
3	3	9,876
4	1	5,671
5	1	5,327
segue....		

Fonte: O autor (2015)

A Tabela 31 é apresentada de forma ilustrativa com os 12 primeiros respondentes distribuídos entre os *clusters*, em função da extensão da tabela completa, uma vez que a amostra total é de 1.104 casos. A Tabela 30 apresenta também a distância entre o objeto e o centro do cluster. Apresenta-se a seguir as médias para cada variável.

Tabela 32 – Médias dos *Clusters* Finais

Variáveis	***Clusters***				**Variáveis**	***Clusters***			
	1	**2**	**3**	**4**		**1**	**2**	**3**	**4**
COL1	**6,17**	6,09	4,85	3,26	RISC1	5,87	**6,47**	4,72	2,88
COL2	**6,54**	6,52	5,23	3,24	RISC2	5,16	**6,37**	4,19	2,71
COL3	**6,47**	6,46	4,84	2,64	RISC3	5,84	**6,43**	4,51	2,76
USEC1	**6,68**	6,52	4,98	2,88	RISC4	5,45	**6,34**	4,25	2,76
USEC2	6,47	**6,57**	4,68	2,6	Escola onde estuda/estudou	2,45	3,57	2,53	2,09
USEC3	**6,67**	6,58	4,96	2,51	Notas	2,61	3,75	2,65	2,45
ERR1	6,1	**6,51**	4,52	2,67	Empresa onde trabalha	3,22	3,99	2,93	2,53
ERR2	5,95	**6,43**	4,48	2,8	Cargo	2,89	3,75	2,8	2,26
ERR3	5,35	**6,29**	4,02	2,49	Salário	**4,03**	**4,41**	3,59	3,07
ACI1	**6,75**	6,63	5,09	2,79	Endereço residencial	**4,44**	**4,42**	3,67	3,3
ACI2	**6,67**	6,62	4,89	2,57	Localização pelo celular	**4,41**	**4,42**	3,63	3,19
ACI3	**6,67**	6,61	4,93	2,71	Senhas	**4,78**	**4,72**	**4,28**	3,82
CTRL1	6,45	**6,54**	4,77	2,82	Telefones	**4,24**	**4,29**	3,52	3,01
CTRL2	**6,6**	6,52	4,77	2,89	Fotos	**4,06**	**4,27**	3,43	2,81
CTRL3	6,27	**6,44**	4,42	2,58	Data de nascimento	2,67	3,51	2,65	2,09
CONS1	6,36	**6,48**	4,62	2,83	Orientação sexual	1,81	3,14	2,27	2,28
CONS2	**6,58**	6,52	4,9	3,04	Vícios	2,29	3,48	2,41	2,28
CONS3	6,47	**6,58**	4,78	2,82	Nº conta corrente / agência	**4,69**	**4,62**	**4**	3,49
CONF1	2,22	**5,95**	3,86	3,56	Saldo bancário	**4,65**	**4,47**	**4,03**	3,55
CONF2	2,41	**6,22**	4,05	3,18	Limite do cheque especial	**4,51**	**4,43**	3,75	3,21
CONF3	2,64	**6,1**	4,15	3,63	Nº de cartão de crédito	**4,84**	**4,7**	**4,17**	3,71
CONF4	2,79	**6,14**	4,22	3,33	Gastos cartão de crédito	**4,61**	**4,53**	3,93	3,34

Fonte: O autor (2015)

Os valores apresentados na Tabela 32 possibilitaram identificar o grau de preocupação com a privacidade relacionado a cada cluster, bem como a percepção de sensibilidade das informações pessoais. A Tabela ainda que os *clusters* 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.

Com relação às questões de sensibilidade da informação, o cluster 2 demonstra 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 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. A seguir apresenta-se o número de casos agrupados em cada cluster.

Tabela 33 – Número de casos em cada cluster

Cluster	**Número de casos**
1	374
2	326
3	315
4	89
Total	1.104

Fonte: O autor (2015)

Os dados da Tabela 33 indicam que todos os casos da população foram distribuídos de forma mais uniforme entre os *clusters* 1 e 3. Os resultados mostram também que o cluster 4 possui uma quantidade muito inferior de casos comparado com os demais. A seguir apresenta-se a Tabela 34, com os resultados da ANOVA.

Tabela 34 – Resultados da análise da ANOVA

Variáveis	Cluster		Erro		F	Sig.
	Quadrado Médio	df	Quadrado Médio	df		
COL1	287,497	3	1,985	1100	144,803	,000
COL2	350,049	3	1,417	1100	247,075	,000
COL3	491,361	3	1,235	1100	397,997	,000
USEC1	475,843	3	1,006	1100	473,085	,000
USEC2	550,888	3	1,201	1100	458,640	,000
USEC3	556,878	3	,962	1100	578,713	,000
ERR1	493,777	3	1,581	1100	312,405	,000
ERR2	441,950	3	1,610	1100	274,507	,000
ERR3	483,691	3	2,013	1100	240,255	,000
ACI1	504,975	3	,836	1100	603,735	,000
ACI2	563,072	3	,905	1100	622,043	,000
ACI3	528,571	3	,883	1100	598,829	,000
CTRL1	483,311	3	1,319	1100	366,493	,000
CTRL2	497,850	3	1,123	1100	443,447	,000
CTRL3	545,100	3	1,350	1100	403,861	,000
CONS1	482,759	3	1,265	1100	381,609	,000
CONS2	441,347	3	,938	1100	470,740	,000
CONS3	493,152	3	,995	1100	495,683	,000
CONF1	815,301	3	2,149	1100	379,445	,000
CONF2	869,405	3	1,739	1100	499,965	,000
CONF3	701,614	3	1,682	1100	417,221	,000
CONF4	676,902	3	1,844	1100	367,169	,000
RISC1	388,036	3	1,732	1100	224,024	,000
RISC2	431,097	3	1,696	1100	254,147	,000
RISC3	427,305	3	1,526	1100	280,091	,000
RISC4	419,546	3	1,685	1100	249,031	,000
Escola estuda/estudou	102,284	3	1,920	1100	53,273	,000
Notas	100,977	3	1,835	1100	55,036	,000
Empresa onde trabalha	84,109	3	1,714	1100	49,063	,000
Cargo	81,297	3	1,752	1100	46,404	,000
Salário	60,880	3	1,376	1100	44,250	,000
Endereço residencial	63,795	3	1,042	1100	61,215	,000
Localização p/celular	70,446	3	1,144	1100	61,560	,000
Senhas	33,003	3	,756	1100	43,678	,000
Telefones	68,315	3	1,226	1100	55,738	,000
Fotos	75,652	3	1,286	1100	58,840	,000
Data de nascimento	72,139	3	1,905	1100	37,874	,000
Orientação sexual	105,182	3	1,977	1100	53,203	,000
Vícios	100,406	3	1,980	1100	50,708	,000
Número CC/Agência	56,842	3	,937	1100	60,663	,000
Saldo bancário	42,325	3	1,037	1100	40,804	,000
Limite cheque especial	67,059	3	1,321	1100	50,773	,000
Número cartão de crédito	49,135	3	,766	1100	64,165	,000
Gastos cartão de crédito	59,115	3	1,051	1100	56,256	,000

Fonte: O autor (2015)

Através dos resultados da análise de variância ANOVA, apresentados na Tabela 35, pode-se identificar quais as variáveis contribuíram 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. Neste sentido, pode-se perceber que as variáveis dos construtos de IPC foram determinantes na formação dos *clusters*, sendo que as que apresentaram valores mais significativos foram USEC2, USEC3, ACI1, ACI2, ACI3, CTRL3, CONF1, CONF2, CONF3 E CONF4. A seguir apresenta-se a Tabela 35 com valores das distancias dos centroides dos *clusters* finais, que é a distância dos centros de formação de cada cluster.

Tabela 35 – Distância entre centroides dos *clusters*

Cluster	1	2	3	4
1		7,999	8,317	17,014
2	7,999		9,977	18,926
3	8,317	9,977		9,384
4	17,014	18,926	9,384	

Fonte: O autor (2015)

Os valores apresentados na Tabela 35 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, o que pode ser percebido também na Tabela 32. A seguir apresenta-se a Tabela 36 com a caracterização dos membros dos *clusters* em relação ao grau de escolaridade.

Tabela 36 – Caracterização dos *clusters* pelo grau de escolaridade

Grau de escolaridade	**Clusters**				**Totais**
	1	**2**	**3**	**4**	
Ensino Médio Completo	57	85	67	26	**235**
Graduação em Andamento	76	96	94	20	**287**
Graduação Completa	101	89	71	19	**280**
Pós-graduação em Andamento (Esp./MBA)	32	14	20	6	**72**
Pós-graduação Completa (Esp./MBA)	46	25	26	8	**105**
Mestrado em Andamento	14	5	10	6	**34**
Mestrado Completo	26	5	9	1	**41**
Doutorado em Andamento	8	4	5	2	**19**
Doutorado Completo	16	2	12	1	**31**
Totais	**376**	**325**	**314**	**89**	1.104

Fonte: O autor (2015)

Os resultados apresentados na Tabela 36 mostram que 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 37, que mostra a descrição dos *clusters* em relação às regiões do Brasil.

Tabela 37 – Caracterização dos *clusters* pelas regiões do Brasil

Regiões	**Cluster**				**Totais**
	1	**2**	**3**	**4**	
Centro-Oeste	45	**76**	**72**	18	**211**
Nordeste	**75**	**73**	**75**	17	**240**
Norte	29	**100**	47	28	**204**
Sudeste	**102**	65	68	12	**247**
Sul	**123**	12	53	14	**202**
Totais	**374**	**326**	**315**	**89**	1.104

Fonte: O autor (2015)

Os resultados apresentados na Tabela 37 evidenciam que os *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 a região 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*. A seguir apresenta-se na Tabela 38 com a caracterização dos membros dos *clusters* em relação ao gênero.

Tabela 38 – Caracterização dos *clusters* pelo gênero

Gênero	**Cluster**				**Totais**
	1	**2**	**3**	**4**	
Masculino	137	112	144	29	**422**
Feminino	237	214	171	60	**682**
Totais	**374**	**326**	**315**	**89**	1.104

Fonte: O autor (2015)

Os resultados da Tabela 38 mostram que as mulheres são maioria em todos os cluster, totalizando 63% no cluster 1, 66% no cluster 2, 54% no cluster 3 e 67% no cluster 4. A seguir apresenta-se a Tabela 39 com a caracterização dos *clusters* pela situação profissional.

Tabela 39 – Caracterização dos *clusters* pela situação profissional

Situação Profissional	**Cluster**				**Totais**
	1	**2**	**3**	**4**	
Empregado(a)	**192**	**161**	**172**	**42**	**567**
Empresário(a)	19	11	11	4	**45**
Estudante (Sem atividade profissional)	43	41	53	9	**146**
Profissional Liberal	41	29	23	12	**105**
Servidor(a) Público(a)	34	31	27	8	**100**
Outro	45	53	29	14	**141**
Totais	**374**	**326**	**315**	**89**	1.104

Fonte: O autor (2015)

Os resultados apresentados na Tabela 39 indicam que 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. A seguir apresenta-se a Tabela 40 com a caracterização dos membros dos *clusters* em relação à faixa salarial.

Tabela 40 – Caracterização dos *clusters* por faixa salarial

Faixa Salarial	**Cluster**				**Totais**
	1	**2**	**3**	**4**	
Até R$ 1.449,99	45	76	72	18	**211**
De R$ 1.450,00 a R$ 2.899,99	75	73	**75**	17	**240**
De R$ 2.900,00 a R$ 7.249,99	29	**100**	47	**28**	**204**
De R$ 7.250,00 a R$ 14.499,99	102	65	68	12	**247**
R$ 14.500,00 ou mais	**123**	12	53	14	**202**
Totais	**374**	**326**	**315**	**89**	1.104

Fonte: O autor (2015)

Os resultados da Tabela 40 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%. O capítulo a seguir apresenta as considerações finais deste estudo.

5 CONSIDERAÇÕES FINAIS

Neste capítulo são apresentadas as considerações finais acerca do grau de Preocupação de Usuários de Internet do Brasil com a Privacidade dos Dados Pessoais, o qual foi mensurado nessa pesquisa. As principais conclusões deste estudo são apresentadas a seguir.

O primeiro objetivo específico desta pesquisa, qual seja, versionar e validar o instrumento de pesquisa desenvolvido por Hong e Thong (2013) foi atendido, uma vez que as análises de validação do instrumento de coleta de dados traduzido e versionado obtiveram índices satisfatórios. A validação do instrumento de coleta de dados é uma contribuição teórica importante, uma vez que o instrumento pode ser utilizado para pesquisas futuras.

O segundo objetivo específico deste estudo, qual seja, identificar o grau de preocupação com a privacidade dos dados pessoais, relacionado com coleta de dados, uso secundário, erros, acesso não autorizado, controle sobre as informações, consciência com relação à privacidade e sensibilidade das informações foi atendido, uma vez que os resultados desta pesquisa mostram que os usuários de Internet do Brasil possuem alto grau de preocupação com a privacidade dos dados pessoais, conforme apresentado anteriormente.

O terceiro objetivo específico deste estudo, qual seja, identificar quais informações o usuário de Internet julga ser mais sensíveis quanto à perda de privacidade, foi atendido, sendo as médias obtidas mostram que as informações apontadas como mais sensíveis foram senhas, número de cartão de crédito, número de conta corrente e agência, saldo bancário e gastos com cartão de crédito.

O presente estudo fornece um panorama do comportamento do usuário de Internet no contexto brasileiro em relação à preocupação com a privacidade das informações pessoais. 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 preocupações dos usuários.

Uma das questões mais importantes e mais relevantes quanto ao direito à privacidade dos usuários de Internet está relacionada às políticas de privacidade dos serviços oferecidos na Internet. A legislação afirma que as empresas provedoras só podem utilizar as informações com o consentimento dos usuários. O grande problema é que as políticas de privacidade que o usuário aprova para utilizar os serviços delegam poderes muito amplos a tais empresas e o

usuário não tem a possibilidade de opinar sobre o conteúdo de tais políticas. A legislação precisa regular tais políticas para que nãos sejam tão prejudiciais à privacidade dos usuários.

No âmbito empresarial, este estudo contribui para que os provedores de serviços na Internet possam direcionar seus recursos e esforços em busca de atender as reais expectativas e anseios dos usuários. A seguir apresenta-se na Tabela 41 uma comparação dos resultados da presente pesquisa com estudos anteriores realizados utilizando o mesmo instrumento de coleta de dados.

Tabela 41 – Comparação dos resultados com estudos anteriores

Local de aplicação		**Brasil**	**Hong Kong**			
Amostra		1.104	968	961	992	887
Estudos		Presente Pesquisa	Estudo 1	Estudo 2	Estudo 3	Estudo 4
CONSTRUTOS	COLETA	**5,71**	5,63	4,61	5,45	4,27
	USO SECUNDÁRIO	**5,79**	**6,58**	**6,44**	**5,75**	4,28
	ERRO	5,31	5,74	**5,87**	5,17	4,33
	ACESSO INDEVIDO	**5,86**	**6,46**	**6,38**	**5,52**	4,61
	CONTROLE	5,65	**6,01**	5,93	5,3	4,12
	CONSCIÊNCIA	5,65	6,12	**6,01**	**5,62**	4,87

Fonte: O autor (2015)

A Tabela 41 apresenta dados comparativos entre o presente estudo com quatro estudos realizados por Hong e Thong (2013). Percebe-se que os construtos que apresentaram maior preocupação, em quatro dos cinco estudos, são Uso Secundário e Acesso Indevido. Os resultados da presente pesquisa apresentam similaridade com os resultados do Estudo 3, e apresenta menor grau de preocupação com a privacidade quando comparado com os Estudos 1 e 2. Por outro lado, os resultados indicam, com exceção do Estudo 4, um alto grau de preocupação com a privacidade nos estudos.

A divulgação dos 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 as 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 realizadas em outros países.

Uma das maiores limitações deste estudo foi a abrangência da população e da amostra propostas. Na região Sul a quantidade necessária de respostas foi obtida em poucos dias, mas nas demais regiões, após algumas semanas a quantidade de questionários respondidos era muito pequena.

Para que o objetivo de coletar em todas as regiões fosse alcançado, foi necessário contratar uma empresa especializada em coleta de dados para estudos acadêmicos, indicada pelo Programa de Pós-Graduação em Administração da PUCRS, o que tornou o processo de coleta de dados bastante dispendioso.

Como sugestão de pesquisa futura pode-se aprofundar as análises dos estudos apresentados na Tabela 41, para tentar identificar aspectos comuns que possam ter sido determinantes para a semelhança dos resultados.

Outra pesquisa interessante seria realizar um estudo confirmatório para identificar o que influencia a Preocupação com a Privacidade na Internet.

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 Behavior Related to Computer 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 of privacy, 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 of Information 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.

BERGEN, M.; DUTTA, S.; WALKER JR, O.C. Agency relationships in marketing: a review of the implications and applications of agency and related. **Journal of Marketing**. v. 56, n. 3, p. 1 – 24, 1992.

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.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988.

BRASIL. Lei 12.965 – Marco Civil da Internet. Brasília, DF: Senado Federal, 2014.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. **Mis Quarterly**, v. 34, n. 3, p. 523 – 548, 2010.

CGI.br. Resolução CGI.br/RES/2009/003/P. Disponível em: <http://www.cgi.br/resolucoes/documento/2009/003>. Acesso em: 26/10/2014.

_____. Lei do Marco Civil da Internet no Brasil . Disponível em: <http://www.cgi.br/pagina/lei-do-marco-civil-da-Internet-no-brasil/177>. Acesso em: 26/10/2014.

CHAI, S. et al.. Internet and *online* information privacy: an exploratory study of preteens and early teens. **IEEE Transactions on Professional Communication**, v. 52, n. 2, p. 167 – 182, 2009.

CORBITT, B. J.; THANASANKIT, T.; YI, H. Trust and e-commerce: A study of consumer perceptions. **Electronic Commerce Research and Applications**, v. 2, n. 3, p. 203 – 215, 2003.

CRONBACH, L.J; MEEHL, P.E. Construct Validity in Psychological Tests. **Psychological Bulletin**. vol. 52, n. 4, p. 281-302, 1955.

CULNAN, M.J. ARMSTRONG, P.K., Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. **Organization Science**, v. 10, n. 1, p. 104 – 115, 1999.

DEGIRMENCI, K.; GUHR, N.; BREITNER, M. H. Mobile applications and access to personal 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.

DHS. The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security Resolução. USA, 2008.

DINEV, T.; HU, Q. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. **Journal of the Association for Information Systems.** v. 8, n. 7, p. 386 – 408, 2007.

EARP, J. B.; ANTON, A. I.; SMITH, L. A.; STUFFLEBEAM, W. H. Examining Internet privacy policies within the context of user privacy values. **IEEE Transactions on Engineering Management.** v. 52, n. 2, p. 227 – 236, 2004.

EISENHARDT, K.M. Agency theory: an assessment and review. **The Academy of Management Review**. v.14, n. 1, p. 57 – 74, 1989.

FAJA, S.; TRIMI, S. Influence of the web vendor's interventions on privacy-related behaviors in e-commerce. **Communications of AIS**. v. 17, p. 2 – 68, 2006.

FEATHERMAN, M.S.; MIYAZAKI, A.D.; SPROTT, D.E. Reducing *online* privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility. **The Journal of Services Marketing**, v. 24, n. 3, p. 219-229, 2010.

FRA. European Union Agency for Fundamental Rights. Information society, privacy and data protection. Disponível em: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection. Acesso em: 07/01/2014.

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.; BABIN, B.; MONEY, A.; SAMOUEL. **Fundamentos de Métodos de Pesquisa em Administração**. 7 ed. Porto Alegre: Bookman, cap. 5 e 7, 2007.

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.

HANN, I; HUI, K.; LEE, S.T.; PNG, I.P.L. Overcoming *online* information privacy concerns: an information-processing theory approach. **Journal of Management Information Systems.** v. 24, n. 2, p. 13 – 42, 2007.

HINKIN, T. R. A brief tutorial on the development of measures for use in *survey* questionnaires. Organizational Research Methods. v. 1, n. 1, p. 104–121, 2008.

HOFFMAN, D.L.; NOVAK, T.P.; PERALTA, M.A. Information privacy in the marketspace: implications for the commercial uses of anonymity on the web. **The Information Society**. v. 15, n. 2, p. 129 – 139, 1999.

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.

HOPPEN, N., LAPOINTE, L.; MOREAU, E. Um guia para a avaliação de artigos de pesquisa em Sistemas de Informação. Revista Eletrônica de Administração (REAd), Edição 3, set/out. 1996, 34p.

HUI, K.L.; TEO, H.H.; LEE, S.Y.T. The Value of Privacy Assurance: An Exploratory Field Experiment. **MIS Quarterly**. v. 31, n. 1, p. 19 – 33, 2007.

JOHNSTON, A. C.; WARKENTIN, M. Fear appeals and information s ecurity behaviors: An empirical study. **MIS Quarterly**. v. 34, n. 3, p. 549 – 566, 2010.

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

KANKANHALLI, A.; TEO, H. H.; TAN, B. C. Y.; WEI, K. K. An integrative study of information systems security effectiveness. **International Journal of Information Management**. v. 23, n. 2, p. 139 – 154, 2003.

KLEIN, R.H. Ameaças, Controle, Esforço e Descontentamento do Usuário no Comportamento Seguro em Relação à Segurança da Informação. 2014. 103p. **Dissertação** (Mestrado em Administração) – PPGAd PUCRS, Porto Alegre, 2014.

KLINE, R. B. Principals and Practice of Structural Equation Modeling. 3a ed. New York: Guilford, 2011.

LI, Y.; Theories in *online* information privacy research: A critical review and an integrated framework. **Decision Support Systems**. v. 54, p. 471 – 481, 2012.

LIGINLAL, D.; SIM, I.; KHANSA, L. How Significant is Human Error as a Cause of Privacy Breaches? An Empirical Study and a Framework for Error Management. **Computers & Security**. doi:10.1016/j.cose.2008.11.003, 2009

LUCIANO, E. M.; MAÇADA, A.C.G.; MAHMOOD, M. A. The influence of human factors on vulnerability to information security breaches. **Americas Conference on Information Systems**, 2010, Lima/Peru.

LUCIANO, E. M.; TESTA, M. G.; BRAGANÇA, C. E. B. A. Percebendo os benefícios e dificuldades da adoção da gestão de serviços de tecnologia da informação. Revista de Gestão, v. 19, n. 1, p. 143-162, 2012.

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.

MALHOTRA, N. K. Pesquisa de Marketing - Uma Orientação Aplicada. 6 ed. Porto Alegre: Bookman, 2010.

MIYAZAKI, A. D.; FERNANDEZ, A. Consumer perceptions of privacy and security risks for *online* shopping. **The Journal of Consumer Affairs**, v. 35, n. 1, p. 27 – 44, 2001.

MILNE, G.R.; ROHM, A.J; BAHL, S. Consumers' protection of *online* privacy and identity. **Journal of Consumer Affairs**. v. 38, p. 217 – 232, 2004.

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

Ng, B. Y.; RAHIM, M. A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security. PACIS, 2004.

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

PAVLOU, P.A.; LIANG, H.; XUE, Y. Understanding and mitigating uncertainty in *online* exchange relationships: a principal-agent perspective. **MIS Quarterly**. v. 31, n. 1, p. 105 – 136, 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.

PRESIDÊNCIA DA REPÚBLICA. Decreto nº 4.729. Brasília, 03 de setembro de 2003. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm>. Acesso em: 26/10/2014.

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

RENSEL, A.D.; ABBAS, J.M.; RAO, H.R. Private transactions in public places: an exploration of the impact of the computer environment on public transactional web site Use. **Journal of the Association for Information Systems**. v.7, n. 1, p. 19 – 51, 2006.

ROSE, E. A.; An examination of the concern for information privacy in the New Zealand regulatory context. **Information & management**, v. 43, n. 3, p. 322 – 335, 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.

SOLOVE, D. J. A Taxonomy of Privacy. **University of Pennsylvania Law Review**. v. 154, n. 3, p. 477 - 560, 2006.

SOM, J.; KIM, S.S. Internet Users' Information Privacy-Protective Responses: 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.

VERMA et al. Privacy and security: *Online* social networking. **International Journal of Advanced Computer Research**. v. 3, n. 8, p. 310, 2013.

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

YAO, M. Z.; RICE, R. E.; WALLIS, K. Predicting user concerns about *online* privacy. **Journal of the American Society for Information Science and Technology**, v. 58, n. 5, p. 710 – 722, 2007.

ZHANG, L.; MC DOWELL, W.C. Am I really at risk? Determinants of *online* users' intentions to use strong passwords. **Journal of Internet Commerce**. v. 8, n. 3 e 4, p. 180 – 197, 2009.

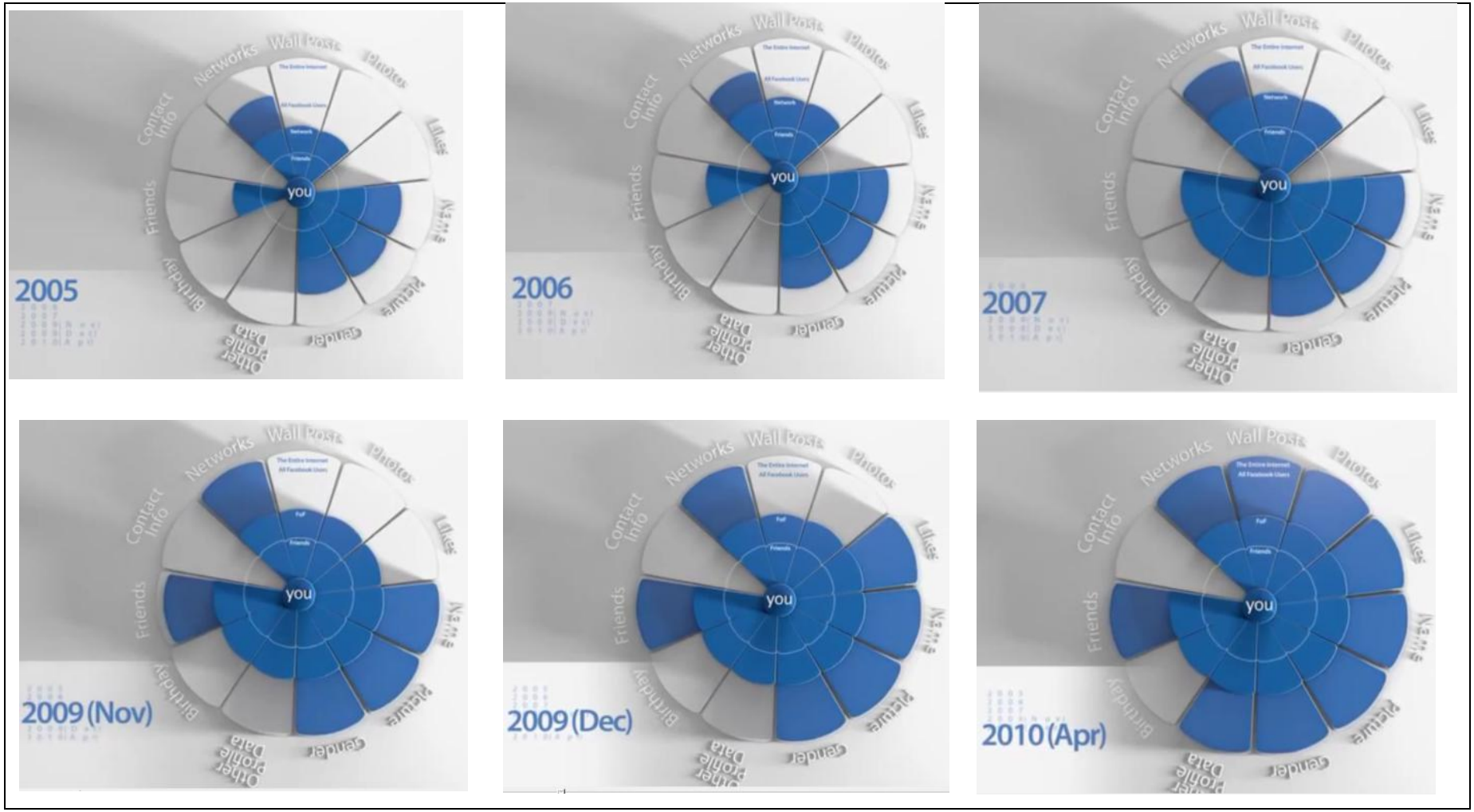
ZIMMER, J.C. et al.. Knowing your customers: using a reciprocal relationship to enhance voluntary information disclosure. **Decision Support Systems**. v. 48, n. 2, p. 395 – 406, 2010.

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.

WILLIAMS, P. A. Information Security Governance. **Information Security Technical Report**. vol. 6, n. 3 p. 60 – 70, 2001.

ANEXO A – DADOS CONFIGURADOS COMO PÚBLICOS NO FACEBOOK

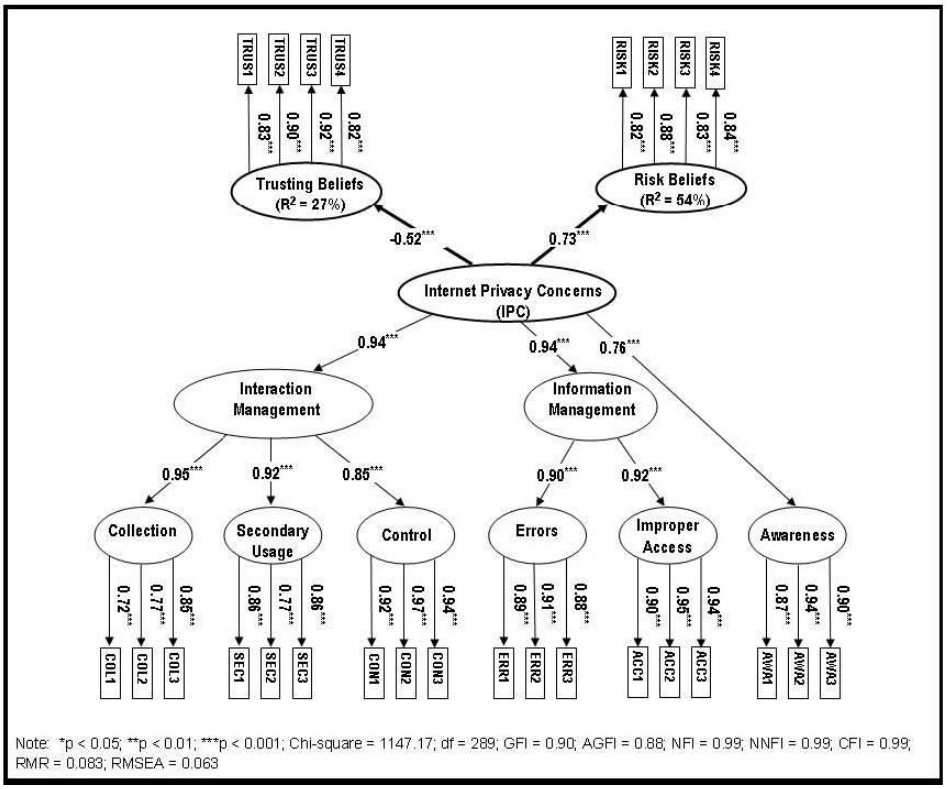


ANEXO B –LEGISLAÇÃO DOS EUA COM IMPLICAÇÕES NA PRIVACIDADE

Legislation	Privacy focus	Specific provisions
Health Insurance Portability and Accountability Act (HIPAA)	Specifies how protected health information (PHI) should be managed by covered entities.	• Organizations may only release PHI with the prior written consent of the individuals. • Organizations should take reasonable steps to ensure the confidentiality of PHI and maintain proper records. • Individuals maintain the right to request to retrieve their PHI and to correct any inaccurate information.
Gramm-Leach-Bliley Act (GLBA)	Governs the collection and disclosure of customers' personal financial information by financial institutions.	• Organizations must provide a consumer with a privacy notice when the consumer relationship is established and annually thereafter. • The privacy notice must describe which information is collected, where and how that information is used, and how that information is protected. • It must identify the consumer's right to opt-out of the sharing of information with unaffiliated parties. • If the privacy policy changes, the consumer's consent must be obtained.
Family Educational Rights and Privacy Act (FERPA)	Regulates the rights and restrictions of parents, employees, and state agencies to access student educational records.	• Organizations must allow students to inspect and review their education records within 45 days of a request. • Students maintain the right to request the amendment of their education records that they believe is inaccurate, misleading, or otherwise in violation of their privacy rights. • Schools must obtain the student or parent's permission before allowing student records to be shared with a third party.
U.S.A. Patriot Act	Requires all U.S. businesses to provide access to customer information for law enforcement.	• Companies should establish a document management system to ensure ready access to documents and retention of documents relevant in litigation or other government investigation. • Financial institutions must ensure they have procedures for identifying customer account information and the ability to verify customer identity and maintain records of information used to verify identity.
The Fair and Accurate Credit Transactions Act	Requires proper disposal of consumer report information and records.	• Any person or company who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.
The Identity Theft Penalty Enhancement Act	Establishes a new federal crime, i.e., aggravated identity theft.	• Any U.S. resident, knowingly transfers, possesses, or uses, without lawful authority a means of identification of another person or a false identification document will face punishment.
California SB 1386[a] (See note about other state legislation)	Defines and specifies the notification requirements, procedures, and timelines of customers' 'personal information.'	• Specifies what type of data is subject to breach law (an individual's name, social security number, identification card number, account or credit card number, date of birth, biometric data). • Any person or business who reasonably believes that personal information has been acquired by an unauthorized person is required to notify the affected party. • Notice must be provided to affected individuals using either written notice, electronic notice with customer's consent, or a substitute notice.

a California SB 1386 has influenced data breach legislation in most other states in the U.S.A. and is also a model for federal privacy legislation (see http://www.ncsl.org/programs/lis/privacy/idt-legis.htm).

ANEXO C – REDE NOMOLÓGICA DE IPC



Fonte: Hong e Thong (2013)

ANEXO D – INSTRUMENTO DE PESQUISA - IPC

IPC (Collection)
COL1: It usually bothers me when commercial/government web*sites* ask me for personal information. COL2: When commercial/government web*sites* ask me for personal information, I sometimes think twice before providing it. COL3: I am concerned that commercial/government web*sites* are collecting too much personal information about me.
IPC (Secondary Usage)
SEC1: I am concerned that when I give personal information to a commercial/government website for some reason, the website would use the information for other reasons. SEC2: I am concerned that commercial/government web*sites* would sell my personal information in their computer databases to other companies. SEC3: I am concerned that commercial/government web*sites* would share my personal information with other companies without my authorization.
IPC (Errors)
ACC1: I am concerned that commercial/government website databases that contain my personal information are not protected from unauthorized access. ACC2: I am concerned that commercial/government web*sites* do not devote enough time and effort to preventing unauthorized access to my personal information. ACC3: I am concerned that commercial/government web*sites* do not take enough steps to make sure that unauthorized people cannot access my personal information in their computers.
IPC (Improper Access)
ACC1: I am concerned that commercial/government website databases that contain my personal information are not protected from unauthorized access. ACC2: I am concerned that commercial/government web*sites* do not devote enough time and effort to preventing unauthorized access to my personal information. ACC3: I am concerned that commercial/government web*sites* do not take enough steps to make sure that unauthorized people cannot access my personal information in their computers.
IPC (Control)
CON1: It usually bothers me when I do not have control of personal information that I provide to commercial/government web*sites*. CON2: It usually bothers me when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by commercial/government web*sites*. CON3: I am concerned when control is lost or unwillingly reduced as a result of a marketing transaction with commercial/government web*sites*.
IPC (Awareness)
AWA1: I am concerned when a clear and conspicuous disclosure is not included in *online* privacy policies of commercial/government web*sites*. AWA2: It usually bothers me when I am not aware or knowledgeable about how my personal information will be used by commercial/ government web*sites*. AWA3: It usually bothers me when commercial/government web*sites* seeking my information *online* do not disclose the way the data are collected, processed, and used.
Trusting Beliefs
TRUS1: Commercial/Government web*sites* in general would be trustworthy in handling my personal information. TRUS2: Commercial/Government web*sites* would keep my best interests in mind when dealing with my personal information. TRUS3: Commercial/Government web*sites* would fulfill their promises related to my personal information. TRUS4: Commercial/Government web*sites* are in general predictable and consistent regarding the usage of my personal information.
Risk Beliefs
RISK1: In general, it would be risky to give my personal information to commercial/government web*sites*. RISK2: There would be high potential for loss associated with giving my personal information to commercial/government web*sites*. RISK3: There would be too much uncertainty associated with giving my personal information to commercial/government web*sites*. RISK4: Providing commercial/government web*sites* with my personal information would involve many unexpected problems. 298 MIS

ANEXO E – MARCO CIVIL DA INTERNET NO BRASIL

Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Art. 2º A disciplina do uso da Internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

I - o reconhecimento da escala mundial da rede;

II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VI - a finalidade social da rede.

Art. 3º A disciplina do uso da Internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na Internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 4º A disciplina do uso da Internet no Brasil tem por objetivo a promoção:

I - do direito de acesso à Internet a todos;

II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Art. 5º Para os efeitos desta Lei, considera-se:

I - Internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II - terminal: o computador ou qualquer dispositivo que se conecte à Internet;

III - endereço de protocolo de Internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

V - conexão à Internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela Internet, mediante a atribuição ou autenticação de um endereço IP;

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de Internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet; e

VIII - registros de acesso a aplicações de Internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP.

Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da Internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

CAPÍTULO II
DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à Internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela Internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - não suspensão da conexão à Internet, salvo por débito diretamente decorrente de sua utilização;

V - manutenção da qualidade contratada da conexão à Internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de

acesso a aplicações de Internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de Internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de Internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de Internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à Internet e de aplicações de Internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na Internet.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela Internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

CAPÍTULO III
DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET
Seção I
Da Neutralidade de Rede

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:

I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II - priorização de serviços de emergência.

§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1o, o responsável mencionado no caput deve:

I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei no 10.406, de 10 de janeiro de 2002 - Código Civil;

II - agir com proporcionalidade, transparência e isonomia;

III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

§ 3º Na provisão de conexão à Internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Seção II
Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7o.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7o.

§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de Internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

Subseção I
Da Guarda de Registros de Conexão

Art. 13. Na provisão de conexão à Internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.

§ 3º Na hipótese do § 2o, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2o, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3o.

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Subseção II
Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão

Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de Internet.

Subseção III
Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações

Art. 14. O provedor de aplicações de Internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de Internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de Internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de Internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de Internet que os registros de acesso a aplicações de Internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3o e 4o do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Art. 16. Na provisão de aplicações de Internet, onerosa ou gratuita, é vedada a guarda:

I - dos registros de acesso a outras aplicações de Internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7o; ou

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de Internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

Seção III
Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

Art. 18. O provedor de conexão à Internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de Internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

§ 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5o da Constituição Federal.

§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na Internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de Internet, poderão ser apresentadas perante os juizados especiais.

§ 4º O juiz, inclusive no procedimento previsto no § 3o, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na Internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de Internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de Internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização.

Art. 21. O provedor de aplicações de Internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Seção IV
Da Requisição Judicial de Registros

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de Internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

CAPÍTULO IV
DA ATUAÇÃO DO PODER PÚBLICO

Art. 24. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da Internet no Brasil:

I - estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica;

II - promoção da racionalização da gestão, expansão e uso da Internet, com participação do Comitê Gestor da Internet no Brasil;

III - promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos;

IV - promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade;

V - adoção preferencial de tecnologias, padrões e formatos abertos e livres;

VI - publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;

VII - otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de Internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

VIII - desenvolvimento de ações e programas de capacitação para uso da Internet;

IX - promoção da cultura e da cidadania; e

X - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos.

Art. 24. As aplicações de Internet de entes do poder público devem buscar:

I - compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;

II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;

IV - facilidade de uso dos serviços de governo eletrônico; e

V - fortalecimento da participação social nas políticas públicas.

Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da Internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da Internet como ferramenta social devem:

I - promover a inclusão digital;

II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e

III - fomentar a produção e circulação de conteúdo nacional.

Art. 28. O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da Internet no País.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente.

Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de Internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no caput, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.

Art. 30. A defesa dos interesses e dos direitos estabelecidos nesta Lei poderá ser exercida em juízo, individual ou coletivamente, na forma da lei.

Art. 31. Até a entrada em vigor da lei específica prevista no § 2o do art. 19, a responsabilidade do provedor de aplicações de Internet por danos decorrentes de conteúdo gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, continuará a ser disciplinada pela legislação autoral vigente aplicável na data da entrada em vigor desta Lei.

Art. 32. Esta Lei entra em vigor após decorridos 60 (sessenta) dias de sua publicação oficial.

Brasília, 23 de abril de 2014; 193º da Independência e 126º da República.

DILMA ROUSSEFF
José Eduardo Cardozo
Miriam Belchior
Paulo Bernardo Silva
Clélio Campolina Diniz

APÊNDICE A – INSTRUMENTO DE COLETA DE DADOS FINAL

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA
MESTRADO EM ADMINISTRAÇÃO E NEGÓCIOS

Este questionário é parte integrante da pesquisa acadêmica realizada por Vergilio Ricardo Britto da Silva (vergílio.britto@pucrs.br), no âmbito do Programa de Pós-Graduação em Administração, sob a orientação da Prof. Dr. Edimara Mezzomo Luciano (eluciano@pucrs.br). Os dados serão usados apenas de forma consolidada, não permitindo a sua identificação. Não há respostas certas ou erradas, responda de acordo com sua percepção.

Objetivo da Pesquisa: Identificar o grau de preocupação com a privacidade dos dados pessoais de usuários de Internet no Brasil.

Por favor, leia com atenção todas as instruções abaixo antes de começar a responder a pesquisa. Elas não serão mostradas novamente e são importantes para o entendimento das questões:

Instruções: Marque opção que melhor corresponder à sua resposta, sendo que a **opção 1 corresponde à "Discordo totalmente" e a opção 7 à "Concordo totalmente".** Após avançar para a próxima questão, não será permitido retornar às questões anteriores.

Cod.	Questões	Discordo totalmente						Concordo totalmente
	IPC (Coleta)	**1**	**2**	**3**	**4**	**5**	**6**	**7**
COL1	Geralmente me incomoda quando *sites* me pedem informações pessoais							
COL2	Quando *sites* me pedem informações pessoais, às vezes penso duas vezes antes de fornecê-las.							
COL3	Estou preocupado que os *sites* estejam recolhendo muita informação pessoal sobre mim.							
	IPC (Uso Secundário)							
USEC1	Eu estou preocupado que quando eu dou informações pessoais a um site por algum motivo, o site use as informações para outros objetivos.							
USEC2	Estou preocupado que os *sites* vendam as minhas informações pessoais em seus bancos de dados para outras empresas.							
USEC3	Estou preocupado que os *sites* compartilhem minhas informações pessoais com outras empresas sem a minha autorização.							
	IPC (Erros)							
ERR1	Estou preocupado que os *sites* não tomem medidas suficientes para se							

	certificar de que as minhas informações pessoais em seus arquivos estejam corretas.							
ERR2	Estou preocupado que os *sites* não tenham procedimentos adequados para corrigir erros em minhas informações pessoais.							
ERR3	Estou preocupado que os *sites* não dediquem tempo e esforço suficiente para verificar a exatidão de minhas informações pessoais em seus bancos de dados.							
	IPC (acesso indevido)							
ACI1	Estou preocupado que os bancos de dados de *sites* que contenham as minhas informações pessoais não sejam protegidos contra o acesso não autorizado.							
ACI2	Estou preocupado que os *sites* não dediquem tempo e esforço suficiente para impedir o acesso não autorizado a minhas informações pessoais.							
ACI3	Estou preocupado que os *sites* não tomem medidas suficientes para se certificar de que pessoas não autorizadas possam acessar minhas informações pessoais em seus computadores.							
	IPC (CONTROLE)							
CTRL1	Geralmente me incomoda quando eu não tenho controle sobre as informações pessoais que eu forneço aos *sites*.							
CTRL2	Geralmente me incomoda quando eu não tenho controle ou autonomia sobre as decisões de como as minhas informações pessoais são coletadas, utilizadas e compartilhadas por *sites*.							
CTRL3	Estou preocupado em perder ou ter reduzido o controle sobre as minhas informações pessoais como resultado de uma transação de marketing entre *sites*.							
	IPC (consciência)							
CONS1	Estou preocupado quando uma divulgação clara e visível não está incluída na política de privacidade on-line dos *sites*.							
CONS2	Geralmente me incomoda quando eu não estou ciente ou bem informado sobre como as minhas informações pessoais serão utilizadas por *sites*.							
CONS3	Geralmente me incomoda quando *sites* que buscam a minha informação on-line não divulgam a forma como os dados são recolhidos, processados e utilizados.							
	Crenças de confiança							

CONF1	*Sites*, em geral, são dignos de confiança para lidar com as minhas informações pessoais.							
CONF2	*Sites* mantêm meus melhores interesses em mente ao lidar com as minhas informações pessoais.							
CONF3	*Sites* cumprem suas promessas relacionadas com as minhas informações pessoais.							
CONF4	*Sites* são, em geral, previsíveis e consistentes em relação ao uso das minhas informações pessoais.							
	Crenças de Risco							
RISC1	Em geral, é arriscado fornecer os meus dados pessoais para *sites*.							
RISC2	Existe alto potencial de perda associado a fornecer os meus dados pessoais para *sites*.							
RISC3	Existe muita incerteza associada a fornecer os meus dados pessoais para *sites*.							
RISC4	Abastecer *sites* com as minhas informações pessoais envolve muitos problemas inesperados.							

Qual a sua preocupação com a privacidade em relação aos dados abaixo?

Instruções: Marque com um X a opção que melhor corresponder à sua resposta, sendo que a **opção 1 corresponde à "Nenhuma preocupação" e a opção 5 à "Muita preocupação".**

Cod.	**Dados**	**Nada preocupado**				**Muitíssimo preocupado**
	Informações	**1**	**2**	**3**	**4**	**5**
SENS1	Escola onde estuda/estudou					
SENS2	Notas					
SENS3	Empresa onde trabalha					
SENS4	Cargo					
SENS5	Salário					
SENS6	Endereço residencial					
SENS7	Localização pelo celular					
SENS8	Senha					
SENS9	Telefones					
SENS10	Fotos					
SENS11	Data de nascimento					

SENS12	Orientação sexual					
SENS13	Vícios					
SENS14	Número de conta corrente / agência					
SENS15	Saldo					
SENS16	Limite do cheque especial					
SENS17	Número de cartão de crédito					
SENS18	Limite de cartão de crédito					

Dados sociodemográficos

1. Informe seu gênero ( ) Feminino ( ) Masculino
2. Qual a sua idade em anos? _____ anos
3. Qual a sua situação profissional?
   ( ) Empregado(a)
   ( ) Empresário(a)
   ( ) Profissional Liberal
   ( ) Estudante (Sem atividade profissional)
   ( ) Servidor(a) Público(a)
   ( ) Outro
4. Qual o seu grau de escolaridade?
   ( ) Ensino Médio Completo
   ( ) Graduação em Andamento
   ( ) Graduação Completa
   ( ) Pós-graduação em Andamento (Especialização/MBA)
   ( ) Pós-graduação Completa (Especialização/MBA)
   ( ) Mestrado em Andamento
   ( ) Mestrado Completo
   ( ) Doutorado em Andamento
   ( ) Doutorado Completo
5. Qual a sua renda familiar mensal?
   ( ) Até R$ 1.449,99
   ( ) De R$ 1.450,00 a R$ 2.899,99
   ( ) De R$ 2.900,00 a R$ 7.249,99
   ( ) De R$ 7.250,00 a R$ 14.499,99
   ( ) R$ 14.500,00 ou mais
6. Por quantas horas por semana você navega na Internet?

( ) até 10 horas por semana

( ) entre 10 e 20 horas por semana

( ) entre 21 e 30 horas por semana

( ) mais de 30 horas por semana

7. Você utiliza alguma rede social? ( ) sim ( ) não
8. Quais as Redes Sociais que mais utiliza
   ( ) Instagram ( ) Twitter ( ) Youtube ( ) Facebook

   ( ) Linkedin ( ) Flickr

   ( ) Outra. Qual? _____
9. Por quantas horas por semana você navega nas redes sociais?
   ( ) até 10 horas por semana
   ( ) entre 10 e 20 horas por semana
   ( ) entre 21 e 30 horas por semana
   ( ) mais de 30 horas por semana
10. Quantas vezes por dia você navega nas redes sociais?
    ( ) até 10 vezes por dia
    ( ) entre 11 e 20 vezes por dia
    ( ) entre 21 e 30 vezes por dia
    ( ) mais de 30 vezes por dia

APÊNDICE B – COVARIÂNCIA RESIDUAL PADRONIZADA

	CONF1	CONF2	CONF3	CONF4	CONS3	CONS2	CONS1	RISC4	RISC3	RISC2	RISC1	CTRL1	CTRL2	CTRL3	ACI3	ACI2	ACI1	ERR1	ERR2	ERR3	USEC3	USEC2	USEC1	COL1	COL2	COL3
CONF1	0																									
CONF2	0,72	0																								
CONF3	-0,1	-0,325	0																							
CONF4	-0,63	-0,237	0,527	0																						
CONS3	-0,28	1,484	-0,041	1,701	0																					
CONS2	-1,71	-0,177	-1,336	-0,334	0,206	0																				
CONS1	0,016	1,446	-0,16	0,504	-0,341	0,012	0																			
RISC4	-1,02	1,031	-0,908	0,086	0,25	-0,893	0,421	0																		
RISC3	-3,44	-0,962	-2,057	-0,932	1,335	0,361	0,016	0,456	0																	
RISC2	1,296	3,228	1,685	3,651	-0,602	-2,181	-0,46	0,209	-0,31	0																
RISC1	-1,59	0,878	-0,405	1,359	1,604	0,494	0,053	-1,08	0,006	0,516	0															
CTRL1	-0,78	0,044	-0,276	0,366	-0,635	-0,549	0,144	-0,02	-0,66	-0,92	-0,15	0														
CTRL2	-2,06	0,039	-1,833	-0,722	-0,225	0,257	0,573	-0,39	0,552	-1,82	0,091	-0,34	0													
CTRL3	1,319	2,191	0,688	2,071	-0,787	-0,01	1,455	0,991	0,65	1,266	0,358	-1,61	1,333	0												
ACI3	-1	0,713	-0,443	1,342	0,265	-0,213	-0,54	-0,2	0,561	-0,88	0,815	2,108	-0,65	-0,45	0											
ACI2	-1,23	0,571	-0,283	1,585	0,325	-0,554	-0,47	-0,41	0,411	-0,96	0,716	1,884	-1,26	-0,57	0,204	0										
ACI1	-2,26	-0,071	-0,637	0,68	0,774	0,478	0,24	0,126	0,318	-1,54	1,295	2,095	-0,91	-0,37	-0,13	-0,16	0									
ERR1	-1,5	-0,411	-1,458	-0,303	0,769	-0,165	1,029	-0,07	-0,5	0,728	1,069	0,807	-0,8	0,983	0,148	0,494	0,88	0								
ERR2	-0,69	0,147	-0,838	0,03	-0,78	-0,944	0,393	-0,22	-1,32	-0,59	-0,02	0,908	-1,43	0,4	-0,36	-0,32	0,125	-0,03	0							
ERR3	1,462	2,791	1,81	2,213	0,332	-0,665	1,786	2,075	-0,31	2,303	-0,11	1,097	-1,3	0,879	-0,75	0,082	-0,37	-0,76	0,671	0						
USEC3	-1,52	-0,227	-0,274	1,177	0,476	-0,198	-0,3	-0,26	-0,27	-1,36	0,438	1,158	-0,33	-0,47	-0,39	0,308	0,634	2,177	-0,78	-1,37	0					
USEC2	0,267	0,744	0,675	1,735	-0,25	-1,21	0,119	0,83	0,373	-0,37	1,485	1,573	-0,46	-0,11	-0,43	-0,11	-0,04	2,215	0,111	-0,22	0,47	0				
USEC1	-2,1	-1,006	-0,31	0,765	1,059	0,43	-0,12	-0,38	0,218	-1,17	2,33	0,77	-0,09	-1,18	-0,32	-0,33	0,848	0,496	-1,56	-1,85	-0,17	-0,4	0			
COL1	-2,16	-0,881	-1,418	-0,254	-0,445	0,158	-1,41	-0,39	0,286	-1,48	0,146	0,078	1,357	0,012	-1,34	-1,46	-0,48	0,13	-0,53	-1,74	-1,73	-1,62	0,213	0		
COL2	-1,83	-0,126	-0,746	1,24	0,418	1,294	0,286	-0,82	0,091	-2	1,339	1,759	0,05	-1,69	-0,49	-0,51	0,653	0,114	-0,65	-2,01	-0,61	-0,93	1,274	1,413	0	
COL3	-0,67	0,566	0,453	1,611	-0,252	-0,219	-0,4	-0,13	0,429	-0,42	1,726	1,77	-0,66	-1,04	0,439	0,087	0,932	1,33	0,052	0,276	-0,63	-0,13	2,277	-0,08	-0,36	0