III Simpósio Internacional de Gestão de Projetos (III SINGEP)
II Simpósio Internacional de Inovação e Sustentabilidade (II S2IS)
ISSN:2317-8302

AMEAÇAS POTENCIAIS À PRIVACIDADE DAS ORGANIZAÇÕES CAUSADAS PELO COMPORTAMENTO INSEGURO DE USUÁRIOS: UMA ANÁLISE SEGUNDO O FAIR INFORMATION PRINCIPLES

VERGILIO RICARDO BRITTO DA SILVA
Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
vrbritto@gmail.com

EDIMARA MEZZOMO LUCIANO
Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
eluciano@pucrs.br

GUILHERME COSTA WIEDENHÖFT
Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
guilherme.wiedenhoft@pucrs.br

AMEAÇAS POTENCIAIS À PRIVACIDADE DAS ORGANIZAÇÕES CAUSADAS PELO COMPORTAMENTO INSEGURO DE USUÁRIOS: UMA ANÁLISE SEGUNDO O FAIR INFORMATION PRINCIPLES

Resumo

Para utilizar serviços disponíveis na internet o usuário fornece uma quantidade considerável de informações pessoais, colocando em risco sua privacidade. Entende-se que o comportamento do usuário corporativo é um reflexo do comportamento do usuário doméstico. Neste sentido, este estudo buscou identificar potenciais ameaças à privacidade das organizações, por meio do comportamento dos usuários em relação suas próprias informações. Foram analisadas as Políticas de Privacidade de serviços gratuitos de redes sócias e e-mail, concluindo-se que as empresas provedoras não estão garantindo a privacidade das informações pessoais e não atendem aos Princípios de Proteção de Dados Pessoais expondo assim usuários e empresas.

Palavras-chave: Privacidade; Ameaças; Comportamento Inseguro; Redes Sociais; Internet.

Abstract

Users of electronic devices provide an extensive amount of personal information in exchange for the use of services available on the Internet, putting in risk their privacy. Considering that the behavior of the corporate user is a reflection of the domestic user's behavior, the goal of this study is to identify potential threats to the privacy of organizations through users behavior, regarding their own information. Free services and e-mails privacy policies were analyzed, showing that the service providers are not guaranteeing the privacy of personal information and do not meet the principles of Personal Data Protection, thereby exposing users and companies.

Keywords: Privacy; Threats; Unsafe Behavior; Social Media; Internet.

1 Introdução

Antes dos computadores, da internet e da enorme quantidade de informação a que se tem acesso sobre quase qualquer coisa e qualquer um, privacidade já era um assunto de discussão. As origens da preocupação com privacidade estão na filosofia, quando Aristóteles começou a considerar sobre a diferença entre a esfera pública (atividade política) e a esfera privada (vida doméstica). O trabalho do juiz americano Thomas Cooley, "The Elements of Torts", de 1873, deu uma conotação clássica à palavra privacidade, de que privacidade é 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. É a liberdade que uma pessoa tem de não ser observada sem autorização. Mais contemporaneamente, os estudos de Westin (1967) contribuíram para a noção de privacidade como uma reivindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como e em que medida suas informações são comunicadas a outros.

Na área de TI, quando se fala em privacidade, é frequente a discussão sobre o balanço entre os riscos do fornecimento de informações e a conveniência gerada pelo compartilhamento dessa informação. A preocupação é se as organizações têm cuidado suficiente com a informação dos clientes durante a coleta, processamento, uso e armazenamento, e mesmo se a informação não está virando parte de um produto.

A expansão da Internet e dos dispositivos de acesso permitiu a oferta os mais variados serviços, muitos de forma gratuita, os quais podem ser utilizados facilmente pelos usuários corporativos. As redes sociais (Facebook, Twitter, Linkedin, Foursquare, etc.) e os e-mails gratuitos (Gmail, Hotmail, etc) são serviços gratuitos bastante utilizados por usuários domésticos e corporativos. Para utilizar estes serviços gratuitos, o usuário precisa fornecer informações pessoais e profissionais, tais como nome, endereço, telefone, local de trabalho entre outras para que seja possível fazer o cadastro nos serviços. Todos os serviços citados possuem Políticas de Privacidade, as quais precisam obrigatoriamente ser aceitas pelo usuário para que ele possa usufruir destes serviços. Estas Políticas de Privacidade informam aos usuários os objetivos da coleta das informações, como e para qual objetivo poderão ser utilizadas, e como estas informações podem ser compartilhadas pela empresa provedora destes serviços com seus parceiros.

Percebe-se que uma significativa parte dos usuários destes serviços não lê a Política de Privacidade correspondente, e acaba aceitando os termos impostos, uma vez que não aceitar tal política implica em não poder utilizar o serviço pretendido. Entre os fatores que fazem com que estes documentos não sejam lidos está o fato de que estes são muito extensos, requerendo dispêndio de tempo para leitura, o que acaba não acontecendo. A confiança que os usuários têm em relação à empresa fornecedora do serviço é outro fator determinante para a redução do risco percebido relacionado ao fato de aprovar algo que não foi lido. Ao aceitar a Política de Privacidade do serviço que pretende utilizar, o usuário concede poderes às empresas provedoras deste serviço para a utilização da informação para si ou para terceiros, para que sejam utilizadas, vendidas, trocadas, enfim, diversas operações que podem colocar em risco a privacidade do usuário. Em muitas destas Políticas de Privacidade as empresas provedoras destes serviços comunicam que as informações pessoais coletadas podem ser divulgadas como parte de uma transação empresarial, como uma fusão ou venda de ativos. A confiança que os usuários têm nas empresas provedoras faz com que o risco a sua privacidade seja desconsiderado ou não percebido.

Neste contexto, este estudo tem por objetivo identificar potenciais ameaças à privacidade dos usuários (Domésticos e Corporativos) de serviços de e-mails gratuitos e de redes sociais na internet, bem como verificar se as empresas provedoras dos serviços de redes

sociais e e-mails gratuitos podem garantir a privacidade das informações destes serviços e se essas empresas atendem a princípios que devem ser seguidos para garantir a privacidade dos dados pessoais coletados. Como princípios, utilizou-se os *Fair Information Principles*, idealizada pelo Departamento de Segurança Interna dos Estados Unidos no ano de 2008, compostos por princípios que devem ser seguidos para garantir a privacidade dos dados pessoais coletados pelas empresas.

Este artigo aborda, no seu item 1, o tema e problema de pesquisa, bem como o objetivo e a justificativa da pesquisa. O item 2 discorre acerca do referencial teórico que embasou o estudo. Os itens 3 e 4 mostram, respectivamente, o método de pesquisa e os resultados obtidos. O artigo encerra com as conclusões de estudo, limites e recomendações.

2 Referencial Teórico

A privacidade das informações foi definida por Smith et al. (1996) como uma das questões éticas mais importantes da era da informação. Segundo Westin (1967), pesquisador pioneiro da privacidade nos seus contornos contemporâneos, 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.

Moor (1997) afirma que a privacidade é um dos problemas éticos mais paradigmáticos que envolvem 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 pode ser invadida, e que informações prejudiciais sobre estes indivíduos podem ser reveladas.

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

Hong e Thong (2013) afirma que o aumento da digitalização das informações pessoais e o avanço das tecnologias da informação 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.

Moor (1997) afirma que 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. 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. Os autores afirmam ainda que o processo de decisão individual no que diz respeito à privacidade é afetado e prejudicado por vários fatores, entre os quais está informação incompleta, quando outras pessoas compartilham informações sobre um usuário, sem que este faça parte da transação, e racionalidade limitada, onde mesmo que os indivíduos tivessem acesso a informação completa, eles não seriam capazes de processar e agir da forma mais adequada com grandes quantidades de dados.

Atualmente a privacidade dos usuários de redes sociais e e-mails gratuitos está cada vez mais exposta. Segundo Shin (2010) privacidade nas Redes Sociais 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. Shin (2010) afirma que os dados pessoais dos usuários de 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.

Em 2011 o Departamento de Proteção e Defesa do Consumidor (DPDC) do Ministério da Justiça do Brasil, através da Escola Nacional de Defesa do Consumidor, lançou a segunda edição do Caderno de Investigações Científicas "Proteção de Dados Pessoais: Para Além da Informação Creditícia", com o objetivo de subsidiar a reflexão sobre a titularidade do consumidor sobre seus próprios dados pessoais. O capítulo "Princípio de Proteção de Dados Pessoais" cita a publicação mais recente dos *Fair Information Principles*, realizada pelo Departamento de Segurança Interna dos Estados Unidos no ano de 2008, compostos por princípios que devem ser seguidos para garantir a privacidade dos dados coletados pelas empresas.

Os cinco princípios que serão transcritos a seguir serão utilizados como base para analisar as Políticas de Privacidade e Termos de Uso dos serviços objetos deste estudo.

a) **Princípio da transparência**, pelo qual o tratamento de dados não pode ser realizado sem o conhecimento do titular dos dados, que deve ser informado especificamente sobre todas as informações relevantes concernentes a este tratamento.
b) **Princípio da qualidade**, pelo qual os dados armazenados devem ser fieis à realidade, atualizados, completos e relevantes, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade.
c) **Princípio da finalidade**, pelo qual qualquer utilização dos dados deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados a terceiros, além do que pode-se, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade).
d) **Princípio do livre acesso**, pelo qual o usuário de qualquer natureza deve ter acesso às suas informações armazenadas em um banco de dados, podendo obter cópias destes registros; após este acesso e de acordo com o princípio da qualidade, as informações incorretas poderão ser corrigidas, aquelas registradas indevidamente poderão ser canceladas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos.
e) **Princípio da segurança física e lógica**, pelo qual os dados devem ser protegidos por meios técnicos e administrativos adequados contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Para Hameed et al. (2013), os problemas de segurança e privacidade aumentaram com as recentes aplicações da internet, nas quais os usuários têm a expectativa de um nível de privacidade e controle sobre a rede. É possível verificar a relevância e o impacto em estudos como os de Almeida (2012); Parris e Henderson (2012); Kim (2012); e Turel e Serenko (2012), que apontam temas como: os riscos enfrentados por empresas com redes sociais; o impacto de ameaças de privacidade implícitas em redes sociais; critérios e alternativas para questões de segurança no que tange à confidencialidade, integridade e disponibilidade de informações; a dualidade do prazer e os riscos no uso das redes sociais nos níveis individual, organizacional e social.

A preocupação com a segurança nas redes sociais é contextualizada por Verma et al. (2013), que justificam esta preocupação a mencionar que "o surgimento das redes sociais online trouxe uma era que mudou todo o cenário do compartilhamento de informações online". A quantidade e o tamanho das informações, antes restrita por infraestrutura e serviços limitados (como, por exemplo, o e-mail, o compartilhamento de arquivos, os comunicadores instantâneos), foi amplificada com a grande variedade de serviços oferecidos pelas redes sociais como os chats de texto e de vídeo; o compartilhamento de imagens, vídeos, músicas, notícias; o contato constante com amigos, familiares, conhecidos (VERMA et al., 2013) e todos estes serviços podendo ser acessados de dentro das organizações, gerando um risco potencial para as organizações .

3 Método de Pesquisa

Esta pesquisa caracteriza-se como uma pesquisa exploratória que utilizou como estratégia a análise de conteúdo. A coleta de dados foi realizada através da análise das políticas de privacidade das empresas provedoras dos serviços objetos deste estudo. Estas políticas são de acesso público e estão disponíveis nos sites das redes sociais e e-mails gratuitos, e podem ser acessadas a qualquer momento, sem a necessidade de cadastro prévio.

Foram analisadas as Políticas de Privacidade do Facebook, Twitter, Linkedin, Foursquare, Gmail e Hotmail. A escolha destas redes sociais e serviços de e-mails gratuitos teve como critério o fato de que estes serviços são os mais utilizados no mundo, conforme Banks (2012).

O protocolo seguido para realizar a coleta dos documentos foi o seguinte:

a) Acessar o site dos serviços e realizar a impressão das Políticas de Privacidades;
b) Realizar o cadastramento em cada um dos serviços objetos deste estudo, para identificar os dados solicitados para tal, bem como verificar quais são os dados que devem ser informados de forma obrigatória;
c) Realizar *logon* em cada serviço e acessar as configurações da conta para identificar quais os dados adicionais (não obrigatórios) podem ser inseridos após o cadastro;
d) Definir itens de avaliação com o objetivo de descrever em que nível as políticas de privacidade atendem cada um dos princípios descritos no *Fair Information Principles*. A escala criada foi a seguinte: Não Atende (NA), Atende Parcialmente (AP) e Atende (A);
e) Definir itens de avaliação de risco à privacidade para avaliar as políticas de privacidade. Foram utilizados os seguintes critérios: 1 – Atende (Baixo Risco), 2 – Atende Parcialmente (Médio Risco) e 3 – Não Atende (Alto Risco).
f) Realizar a leitura minuciosa dos documentos.
g) Para cada serviço de rede social e de e-mail gratuito, evidenciar os dados solicitados no momento do cadastro e os dados que podem ser inseridos durante a utilização dos serviços;
h) A cada serviço analisado foi necessário olhar a tabela para conferir se existiam dados novos dados a serem inseridos, e, em caso positivo, retornar aos serviços analisados e complementar a análise.

Uma vez que o Brasil não possuía legislação específica sobre privacidade na internet na época da realização da pesquisa, os documentos foram analisados sob a ótica dos *Fair Information Principles* publicados pelo Departamento de Segurança Interna dos Estados Unidos e citados pelo Ministério da Justiça do Brasil na segunda edição do Caderno de Investigações Científicas, Proteção de Dados Pessoais: para Além da Informação Creditícia (2010), compostos por cinco princípios que devem ser seguidos para garantir a privacidade dos dados pessoais coletados pelas empresas. Os princípios foram detalhados no referencial

teórico.

Realizou-se leituras minuciosas das políticas de privacidade dos serviços de redes sociais e e-mail gratuitos objetos deste estudo, com o intuito de codificar as possíveis ameaças à privacidade dos usuários e classificar em que grau estas políticas atendem os princípios que buscam garantir a privacidade dos dados coletados. A partir das análises realizadas foi possível a criação da livro de códigos, no qual são listados todos os dados solicitados no momento do cadastro, os dados que podem ser inseridos posteriormente, sendo também indicados os dados obrigatórios e não obrigatórios. As análises possibilitaram ainda a criação dos quadros resumo das análises de cada uma das políticas de privacidade.

4 Análise de Resultados

Este item mostra os dois tipos de análises realizadas, quais sejam, a análise das políticas de privacidade praticadas pelos serviços de redes sociais e de e-mails gratuitos (4.1), seguido da análise das políticas de privacidade.

4.1 INFORMAÇÕES SOLICITADAS NO CADASTRO EM SERVIÇOS DE REDES SOCIAIS E DE E-MAILS GRATUITOS

Identificaou-seOs serviço que coletam a maior quantidade de informações são o Facebook (30) e o Linkedin (30), seguidos de Foursquare (18), Gmail (16), Hotmail (14) e Twitter (13). Fica claro também que os tipos de dados mais coletados pelos serviços de redes sociais são os dados Não Obrigatórios, enquanto que nos serviços de e-mail gratuitos os dados mais coletados são os Obrigatórios. O tipo de dado coletado em maior quantidade de forma obrigatória são os Dados Pessoais, enquanto que o tipo de dado coletado em maior quantidade de forma não obrigatória são os Dados de Localização. Como pode ser observado por meio do Quadro 1 a seguir.

Quadro 1 – Quantidade de dados solicitados em cada serviço

Tipos de Dados	**FACEBOOK**		**TWITTER**		**LINKEDIN**		**FOURSQUARE**		**GMAIL**		**HOTMAIL**	
	Obr	NObr	Obr	NObr	Obr	NObr	Obr	NObr	Obr	NObr	Obr	NObr
ACADÊMICO		3			1	1						
FAMÍLIA		1								1		1
HÁBITOS		1				1						
LOCALIZAÇÃO		7		2	2	4		6	2	3	2	2
PESSOAL	7	3	4	1	4	8	4	2	7		7	
TÉCNICOS	6			6		6		6		1		
TRABALHO		2			2	1				2		2
SUB TOTAL	**13**	**17**	**04**	**09**	**09**	**21**	**04**	**14**	**09**	**07**	**09**	**05**
TOTAL	30		13		30		18		16		14	

Legenda: OBR (Obrigatórios); NObr (Não obrigatórios)

O Quadro 1 mostra ainda que o serviço que coleta a maior quantidade de dados de forma obrigatória é o Facebook (13), seguido por Gmail (09), Hotmail (09), Linkedin (09), Foursquare (04) e Twitter (04). Os dados técnicos indicam as informações coletadas de forma automática no momento em que os usuários acessam o site dos serviços, quais sejam IP do equipamento utilizado para acesso, sistema operacional, configurações de *hardware* e informações sobre o *browser* utilizado. A coleta destes dados é transparente para os usuários, que não percebem que os mesmos estão sendo coletados.

4.2 ANÁLISE DAS POLÍTICAS DE PRIVACIDADE

Para que os usuários de redes sociais da internet, bem como de serviços de e-mail gratuito possam utilizar os serviços oferecidos pelas empresas provedoras, devem obrigatoriamente aprovar as Políticas de Privacidade ou Termos de Uso destes serviços. Caso não concordem e não aprovem estas políticas e termos, não poderão utilizar estes serviços. Isso faz com que muitas vezes os usuários aprovem as condições de uso propostas mesmo sem estar de acordo, ou mesmo sem ler o que está aprovando. Esta situação faz com que seja de grande relevância a análise destas políticas e termos, para que seja possível identificar os riscos à privacidade dos usuários destes serviços.

4.2.1 POLÍTICA DE PRIVACIDADE DO TWITTER

A Política de Privacidade do Twitter descreve as políticas e os procedimentos a respeito da coleta, uso e divulgação das informações coletadas dos usuários que enviam informações para o Twitter quando postam um *tweet* através do site, via SMS, aplicativos e APIs. Ao utilizar qualquer um dos serviços do Twitter, o usuário concorda automaticamente com a coleta, transferência, adaptação ou alteração, armazenamento, divulgação e outros usos de suas informações. Ao realizar o cadastro para a utilização desta rede social o usuário deverá informar obrigatoriamente nome, e-mail, senha e usuário. Posteriormente ele poderá ainda fornecer informações adicionais tais como número e operadora de celular, localização (país, região), catálogo de endereços e foto. Por padrão o perfil do usuário permite que qualquer outro usuário possa visualizar as informações postadas, e as informações públicas dos usuários são divulgadas amplamente de forma imediata.

Os serviços do Twitter são projetados para compartilhar as informações dos usuários com o mundo, e o usuário autoriza que a maioria das informações fornecidas sejam tornadas públicas. Por padrão o Twitter sempre torna públicas as informações que o usuário fornece, e segundo o que está descrito na Política de Privacidade, em diversas situações o Twitter oferece configurações de conta que permitem que o usuário torne as suas informações mais privadas, o que inclui não somente os *tweets* enviados e favoritos, mas também listas criadas pelo usuário, as pessoas que segue e muitas outras informações resultantes do uso deste serviço.

Os servidores do Twitter registram automaticamente informações dos usuários a partir do uso dos serviços. Estas informações podem conter o endereço IP, sistema operacional, tipo de navegador, páginas visitadas e operadora do dispositivo móvel.

O site do Twitter utiliza *cookies* para coletar informações referentes aos sites acessados pelos seus usuários. São utilizados *cookies* de sessão, os quais são armazenados na memória do dispositivo eletrônico, perdendo as informações no momento em que o usuário fecha o navegador web, e também são utilizados *cookies* persistentes, que são aqueles que são gravados no disco rígido da máquina. As informações coletadas através dos *cookies* podem ser compartilhadas indevidamente com outros sites, o que pode acabar colocando em risco a privacidade dos usuários.

Segundo o que está descrito em sua Política de Privacidade, para ajudar a fornecer os serviços propostos, a empresa utiliza alguns serviços de terceiros, como por exemplo, para hospedar blogs e wikis. Estas empresas também podem coletar informações dos usuários através do Twitter, que pode ainda compartilhar com suas empresas fornecedoras as informações pessoais de seus usuários, para que estas empresas possam prover os serviços para os quais foram contratadas. Ao aceitar a Política de Privacidade do Twitter, além de autorizar todos os procedimentos detalhados acima, o usuário concorda ainda que, caso a empresa seja envolvida em fusão, falência ou aquisição, poderá vender ou transferir as

informações de seus usuários como parte destas transações. O Quadro 2 traz a análise da Política de Privacidade do Twitter.

Quadro 2 – Resumo da Análise da Política de Privacidade do Twitter

Princípio	Análise Quanto ao Princípio	Motivo
Transparência	Não atende	Não informa especificamente como os dados serão tratados
Qualidade	Atende parcialmente	A Política diz que os dados podem ser manipulados, com isso corre-se o risco de que as informações deixem de ser fiéis à realidade
Finalidade	Não atende	Os dados dos usuários podem ser coletados pelas empresas parceiras
Livre Acesso	Atende parcialmente	O usuário não tem acesso aos dados coletados pelas empresas parceiras
Segurança física e lógica	Atende parcialmente	Ao compartilhar os dados com empresas parceiras, o provedor perde o controle sobre os riscos a privacidade dos usuários

A análise realizada e resumida no quadro acima mostra que a Política de Privacidade do Twitter atende parcialmente três princípios e não atende os outros dois.

4.2.2 POLÍTICA DE PRIVACIDADE DO LINKEDIN

Quando o usuário registra uma conta para se tornar usuário dos serviços oferecidos pelo Linkedin, deve fornecer obrigatoriamente nome, sobrenome, e-mail e senha. Após a validação do usuário, para que este possa utilizar o serviço oferecido por esta rede social, deverá informar, obrigatoriamente, país onde mora, código postal, empresa onde trabalha e cargo que ocupa. Outras informações complementares podem ser adicionadas ao perfil do usuário do Linkedin, entre elas formação acadêmica, telefone, endereço e estado civil.

O site do Linkedin utiliza *cookies* e arquivos de *log* para rastrear a utilização do site com o objetivo de, segundo a Política de Privacidade, melhorar a qualidade do serviço oferecido, e apresentar publicidade do Linkedin e de terceiros aos usuários, dentro e fora do site do Linkedin. Ao exibir anúncios ou aperfeiçoar os serviços aos usuários, o Linkedin poderá permitir que empresas parceiras insiram ou reconheçam *cookies* no navegador dos usuários, para que possam coletar informações.

Quando o usuário visita o site do Linkedin, o provedor deste serviço recebe automaticamente a URL do site do qual o usuário veio e do site para o qual irá quando sair do site do Linkedin. Além disso, os anunciantes recebem a URL da página em que o usuário estava ao clicar em um anúncio veiculado pelo Linkedin, que também recebe o endereço IP e o sistema operacional do computador do usuário, o tipo de navegador utilizado, padrões de e-mail, tipo de aparelho celular e sistema operacional do aparelho (caso o usuário esteja acessando o Linkedin por celular), assim como o nome do provedor de internet ou da operadora de celular. O Linkedin também poderá receber dados referentes à localização do usuário que possam ter sido transmitidos pelos serviços de terceiros ou dispositivos com GPS ativado.

Segundo a Política de Privacidade do Linkedin, o usuário concede a este provedor direito não exclusivo, irrevogável, mundial, perpétuo, ilimitado e transferível, totalmente pago e isento de *royalties*, de copiar, preparar trabalhos derivativos, melhorar, distribuir, publicar, excluir, guardar, acrescentar, processar, analisar, utilizar e comercializar, de qualquer maneira atualmente conhecida ou descoberta no futuro, quaisquer informações fornecidas pelo usuário, direta ou indiretamente, ao Linkedin, incluindo, entre outros, qualquer conteúdo gerado por usuário, ideias, conceitos, técnicas ou dados relacionados aos serviços que o

usuário apresentar ao Linkedin, sem nenhum outro consentimento, aviso e/ou remuneração ao usuário nem a nenhum terceiro.

Quadro 3 – Resumo da Análise da Política de Privacidade do Linkedin

Princípio	Análise Quanto ao Princípio	Motivo
Transparência	Não atende	Conforme descrito na Política, o Linkedin pode realizar quaisquer operações com as informações coletadas, não especificando o que será feito
Qualidade	Não atende	Como as informações podem ser vendidas, não é possível garantir que após a venda permaneçam fiéis ao que fora publicado pelo usuário
Finalidade	Não atende	A Política informa que as informações podem ser comercializadas
Livre Acesso	Atende parcialmente	Não é possível ter acesso às informações comercializadas com terceiros
Segurança física e lógica	Não atende	Ao comercializar as informações, não é possível protegê-las dos riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado

A análise realizada e resumida no quadro acima mostra que a Política de Privacidade do Linkedin atende parcialmente um dos princípios e não atende os outros quatro.

4.2.3 POLÍTICA DE PRIVACIDADE DO FACEBOOK

Ao realizar o cadastro no site do Facebook o usuário deverá informar nome, endereço de e-mail, data de nascimento e sexo. Informações adicionais podem ser inseridas pelo usuário, entre elas telefone, endereço, cidade natal, cidade onde mora, religião, empresa onde trabalha, cargo ocupado, formação acadêmica, foto, interesses, etc. Por padrão o perfil do usuário do Facebook é criado como público, sendo possível que qualquer usuário desta rede social possa visualizar as informações inseridas.

O Facebook, além das informações inseridas diretamente pelos usuários, recebe informações quando os usuários interagem com a rede social, quando olha a linha do tempo de outra pessoa, envia ou recebe mensagens, procura por um amigo ou uma página, usa um aplicativo móvel do Facebook. Quando o usuário publica fotos ou vídeos, dados relacionados são recebidos pelo Facebook, como hora, data e local em que a foto ou vídeo foram postados. Dados do computador, do telefone celular e de outros dispositivos que o usuário utiliza para acessar o Facebook são coletados. Essas informações podem incluir IP, servidor de internet, localização, tipo de navegador, páginas que são visitadas. Quando o usuário acessa algum jogo, aplicativo ou site que utilize a plataforma do Facebook, através de *cookies* as informações são recebidas pelo Facebook, podendo incluir data e hora em que o site foi acessado, sistema operacional e, caso o usuário esteja conectado ao Facebook, sua identificação de usuário.

O Facebook recebe informações sobre o usuário através de seus amigos, quando estes carregam informações de contato deste usuário, publicam uma foto, marcam o usuário em uma foto ou atualizações de *status*, ou quando o adicionam a um grupo. Além disso, as informações que um usuário compartilha podes ser recompartilhadas. Isso significa que se um usuário compartilha uma informação no Facebook, qualquer pessoa que puder vê-la, poderá compartilhá-la com outros usuários. Através de anunciantes parceiros, clientes e outras fontes que ajudam a fornecer anúncios, o Facebook pode receber informações de seus usuários. Um anunciante pode informar como um usuário respondeu a um anúncio no Facebook ou em outro site. O Facebook pode usar as informações que recebe sobre seus usuários da seguinte

forma: a) Como parte dos esforços para manter os produtos, serviços e integrações do Facebook seguros e protegidos; b) Para proteger os direitos ou propriedades do Facebook e de outros; c) Para fornecer recursos e serviços de localização, como informar o usuário e seus amigos quando algo está acontecendo nas redondezas; d) Avaliar ou saber a eficiência dos anúncios que os usuários veem, incluindo fornecer anúncios relevantes para estes usuários; e) Para fazer sugestões aos usuários do Facebook, como sugerir que outros usuários adicionem alguém como amigo porque este importou o mesmo endereço de e-mail ou sugerir que um usuário marque um amigo em uma foto que ele carregou e que este amigo esteja presente; f) Para operações internas, que incluem correção de erros, análise de dados, testes, pesquisa, desenvolvimento e melhoria do serviço.

A Política de Privacidade do Facebook informa ainda que os jogos, aplicativos e sites são criados e mantidos por outras empresas e desenvolvedores que não fazem parte do Facebook, e por esta razão os usuários devem ler os Termos de Serviço e as Políticas de Privacidade destas empresas.

Quadro 4 – Resumo da Análise da Política de Privacidade do Facebook

Princípio	**Análise Quanto ao Princípio**	**Motivo**
Transparência	Atende parcialmente	Um aplicativo instalado por um amigo da lista do usuário pode ter acesso aos seus dados deste usuário, mesmo que ele não o tenha instalado
Qualidade	Atende parcialmente	A Política não informa que tipo de tratamento de informações as empresas parceiras podem realizar
Finalidade	Não atende	O Facebook compartilha informações dos usuários com empresas de marketing para realizar publicidade dirigida
Livre Acesso	Não atende	O Facebook não possibilita que os usuários corrijam informações incorretas a seu respeito quando estas são publicadas por outros usuários
Segurança física e lógica	Não atende	Uma vez que informações dos usuários são compartilhadas com empresas parceiras, o Facebook não tem como garantir a privacidade dos dados

A análise realizada e resumida no quadro acima mostra que a Política de Privacidade do Facebook atende parcialmente dois princípios e não atende os outros três.

4.2.4 POLÍTICA DE PRIVACIDADE DO FOURSQUARE

Para criar um perfil no Foursquare o usuário deverá fornecer seu nome, e-mail, senha, cidade, sexo e data de nascimento. Logo após o site oferece a possibilidade de localizar amigos no Twitter, no Facebook, no Gmail e no Yahoo, sendo possível importar as informações destes contatos para o perfil no Foursquare. Finalizada esta etapa inicial, o usuário poderá inserir mais informações pessoais ao seu perfil e, caso o usuário tenha um perfil no Twitter, poderá permitir que o Foursquare tenha acesso a suas informações, podendo ler o histórico de tweets, ver quem o usuário segue e por quem é seguido, além de poder enviar tweets para o usuário.

Quando o usuário usa o serviço do Twitter, o Foursquare automaticamente recebe e registra informações sobre o navegador ou plataforma móvel utilizado, incluindo a localização, endereço IP, informações de *cookies* e a página solicitada. Estas informações são tratadas como não pessoais. Utilizando a funcionalidade do Foursquare de realizar *check-in* nos locais frequentados pelo usuário, como restaurantes, cinemas, bares e shoppings, os amigos do usuário poderão conhecer seus hábitos, bem como ver a localização e a hora de

cada *chech-in* realizado, ter acesso a informações de nome, e-mail, telefone, fotografia, cidade natal e link para as contas do Twitter e do Facebook.

Segundo sua Política de Privacidade, o Foursquare contrata outras empresas e pessoas para realizar tarefas em seu nome, entre elas para realizar campanhas de marketing. Para isto, precisa compartilhar as informações pessoais de seus usuários com estes terceiros, que também utilizam *cookies* para obter informações sobre os usuários.

Quadro 5 – Resumo da Análise da Política de Privacidade do Foursquare

Princípio	Análise Quanto ao Princípio	Motivo
Transparência	Não atende	A Política não informa como as empresas parceiras utilizam as informações coletadas
Qualidade	Atende parcialmente	Ao compartilhar as informações com terceiros, torna-se impossível garantir que as informações continuem fiéis a realidade
Finalidade	Não atende	Não especifica como os parceiros utilizam as informações compartilhadas
Livre Acesso	Atende parcialmente	Os usuários não tem acesso às informações armazenadas pelas empresas parceiras
Segurança física e lógica	Não atende	Não é possível atender a este princípio ao compartilhar as informações dos usuários com empresas parceiras

4.2.5 POLÍTICA DE PRIVACIDADE DO GMAIL

Ao criar uma nova conta no Gmail, o usuário deverá informar, obrigatoriamente, nome de usuário, senha, nome, sobrenome, e-mail alternativo, sexo, data de nascimento, telefone celular, país onde está localizado. Após a confirmação de cadastro, o usuário poderá a seu critério informar endereço, telefone comercial e residencial, cidade e país onde mora, estado civil, escola ou faculdade onde estudou, empresa onde trabalha e cargo. Por padrão estas informações são públicas, sendo visíveis através de buscas mesmo para quem não tem conta no Gmail.

Além das informações inseridas pelo próprio usuário, o Gmail coleta dados a partir da utilização do seu serviço. São coletadas informações sobre o *hardware* utilizado, detalhes de como o usuário usou os serviços do Google, como sites visitados e pesquisas realizadas. Com a utilização dos serviços através de dispositivos moveis, são coletadas informações de telefonia como número de telefone, números chamados, horário e data das chamadas. *Cookies* também são utilizados para coleta de informações.

Quadro 6 – Resumo da Análise da Política de Privacidade do Google

Princípio	Análise Quanto ao Princípio	Motivo
Transparência	Não atende	Não é informado como as empresas parceiras tratam as informações dos usuários
Qualidade	Não atende	Não é possível atender a este princípio ao compartilhar as informações com outras empresas
Finalidade	Atende parcialmente	Não atende a restrição de transferência de dados pessoais a terceiros
Livre Acesso	Atende parcialmente	O usuário não tem acesso às informações armazenadas por empresas parceiras
Segurança física e lógica	Não atende	Ao compartilhar as informações com empresas terceiras, não é possível atender este princípio

Segundo a Política de Privacidade do Gmail, as informações dos usuários são compartilhadas com empresas, organizações ou indivíduos externos ao Google, além de administradores de domínios, os quais têm acesso às informações da conta dos usuários,

inclusive dados de e-mails. Caso o Google seja envolvido em uma fusão, aquisição ou venda de ativos, as informações pessoais de seus usuários poderão ser transferidas ou submetidas a uma nova Política de Privacidade.

A análise realizada e resumida no quadro acima mostra que a Política de Privacidade do Google atende parcialmente dois princípios e não atende a outros três.

4.2.6 POLÍTICA DE PRIVACIDADE DO HOTMAIL

Para realizar o cadastro de uma conta de usuário no Hotmail, deve-se inserir informações obrigatórias, tais como: usuário, senha, nome/sobrenome, e-mail, sexo, data de nascimento, código postal, país onde mora, e informações adicionais podem ser inseridas após a criação da como, tais como: telefone comercial e residencial, empresa onde trabalha, cargo que ocupa, tipo de relacionamento em que está envolvido e país da localização atual.

Segundo a Declaração de Privacidade *online* da Microsoft, provedora do serviço de e-mail do Hotmail, as informações coletadas podem ser combinadas a informações obtidas de outros serviços da Microsoft e de outras empresas. O Hotmail utiliza *cookies* para controlar as interações com outros sites e serviços, além disso, fornece informações de seus usuários para empresas que trabalham em seu nome.

Quadro 7 – Resumo da Análise da Política de Privacidade do Hotmail

Princípio	**Análise Quanto ao Princípio**	**Motivo**
Transparência	Atende parcialmente	A forma como as empresas parceiras manipulam os dados dos usuários não é informada
Qualidade	Não atende	Não pode garantir que as informações sejam fiéis a realidade ao compartilhá-las com outras empresas
Finalidade	Não atende	Por compartilhar as informações com empresas terceiras
Livre Acesso	Atende parcialmente	O usuário não tem acesso às informações que estão em posse das empresas parcerias
Segurança física e lógica	Não atende	Não pode garantir o cumprimento deste princípio uma vez que as informações são compartilhadas com outras empresas

A análise realizada e resumida no quadro acima mostra que a Política de Privacidade do Hotmail atende parcialmente dois princípios e não atende os outros três.

4.3 IDENTIFICAÇÃO DE POTENCIAIS AMEAÇAS À PRIVACIDADE

A análise dos documentos realizada no item anterior, que identifica a forma como as empresas provedoras dos serviços de rede social e e-mail gratuito manipulam as informações dos usuários, mostra também que nenhuma destas empresas atende totalmente os Princípios de Proteção de Dados Pessoais que compõem o *Fair Information Principles*. Com isso conclui-se que a privacidade dos usuários destes serviços está exposta às seguintes ameaças:

a) Coleta de informações sem conhecimento dos usuários: todos os provedores dos serviços de redes sociais e e-mail gratuito utilizam *cookies* para coleta de dados. Estes *cookies* coletam informações além das necessárias para utilização destes serviços. A partir destas informações podem-se conhecer as preferências dos usuários, as quais podem ser utilizadas, por exemplo, para direcionar publicidade indesejada e sites de comércio eletrônico ferecendo produtos que atendam ao perfil do usuário;

b) Uso indevido de informações: as informações divulgadas podem ser utilizadas para ataques de força bruta, que consiste em utilizar um algoritmo para analisar as informações com o objetivo, por exemplo, de descobrir as senhas, criação de perfil falso de usuário, golpes de engenharia social e responder questões de segurança para recuperação de senhas.

Quando as ameaças listadas acima encontram uma brecha, gerando uma vulnerabilidade, trazem como conseqüência mais algumas ameaças, quais sejam:

a) Ataques de engenharia social: através das informações que podem ser obtidas nas redes sociais é possível criar perfis de usuários, com características que podem ser exploradas em ataques de Engenharia Social, que normalmente são realizadas enviando e-mails com mensagens que despertem o interesse dos usuários, fazendo com que executem arquivos anexos que podem ter como objetivo coletar contas e senhas de banco;

b) Invasão de privacidade: é impossível controlar as informações que os usuários repassam sobre seus contatos. Quando maior a rede de contatos dos usuários, maior o número de pessoas que terão acesso às informações publicadas;

c) Disponibilização de informações para criminosos: através das informações disponíveis nas redes sociais é possível conhecer os hábitos do usuário, locais que costuma frequentar, tais como restaurantes, bares e casas noturnas. Estas informações podem ser usadas para roubo de bens e tentativas de sequestro;

d) Perda de controle sobre as informações: todas as empresas provedoras dos serviços objetos deste estudo compartilham as informações de seus usuários com empresas terceiras. Os usuários não têm acesso às informações armazenadas pelas empresas parceiras, não sendo possível removê-las ou controlar o uso futuro destas informações;

e) Furto de identidade: através da grande quantidade de informações que podem ser obtidas nas redes sociais pode-se criar um perfil falso para que alguém se passe por outra pessoa, o que muitas vezes tem por objetivo obter informações sobre os amigos deste usuário ou fazer operações como se fosse um determinado usuário e outras ações que podem denegrir a imagem desse usuário.

O Quadro 8 traz um resumo das análises realizadas nas políticas de privacidade, indicando o nível de atendimento de cada princípio, onde se pode perceber que nenhum dos princípios é atendido na totalidade pelos serviços de redes sociais e e-mail gratuitos.

Quadro 8 – Resumo das Análises realizadas

PRINCÍPIOS	**SERVIÇOS**					
	Twitter	Linkedin	Facebook	Foursquare	Gmail	Hotmail
Transparência	NA	NA	AP	NA	NA	AP
Qualidade	AP	NA	AP	AP	NA	NA
Finalidade	NA	NA	NA	NA	AP	NA
Livre acesso	AP	AP	NA	AP	AP	AP
Segurança física e lógica	AP	NA	NA	NA	NA	NA

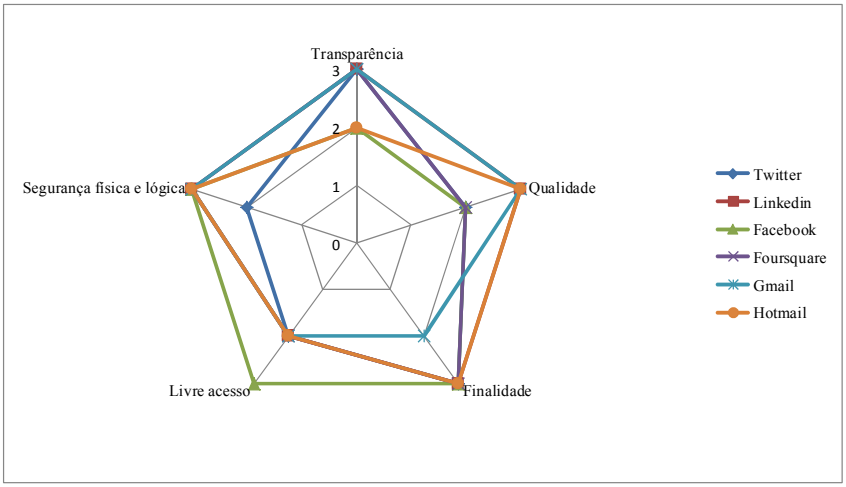
Legenda: NA – Não Atende; AP – Atende Parcialmente; AT - Atende

O Quadro 8 mostra que nenhum dos serviços atende (plenamente) a nenhum princípio. Os atendimentos parciais são em número de 12, e 18 são as células com itens não atendidos. O Quadro 8 ainda que a rede social Linkedin atende apenas de forma parcial somente o princípio Livre Acesso, e o serviço com melhor nível de atendimento é o Twitter, que atende parcialmente três princípios. Com base nestes resultados fica evidente o alto grau de risco a que está exposta a privacidade dos usuários destes serviços.

Atribuindo-se valores aos resultados obtidos, através do Gráfico 1 é possível identificar o nível de risco à privacidade causado pelas empresas provedoras dos serviços de redes sociais e e-mails gratuitos em cada princípio. Quanto mais próximo de 1 mais os serviços atendem os princípios.

O Gráfico 1 mostra que o risco à privacidade dos usuários dos serviços objetos deste estudo varia de Médio a Alto Risco, sendo que a maior ocorrência é de Alto Risco. Quanto menor o número, melhor os princípios são atendidos.

Gráfico 1 – Nível de Risco à Privacidade



Legenda: 1 – Atende (Baixo Risco), 2 – Atende Parcialmente (Médio Risco) e 3 – Não Atende (Alto Risco)

A Figura 1 mostra a grande quantidade e variedade de informações sobre os usuários dos serviços de redes sociais e e-mails gratuitos que estão disponíveis nas bases de dados dos provedores destes serviços, e que estão expostas a este Alto Risco.

Informações Pessoais	Usuário, Senha, Nome, Sobrenome, Telefones, Foto, E-mail, Sexo, Data de nascimento, Local de nascimento, Operadora de celular, Nacionalidade, Religião, Etnia, Orientação sexual,
Informações Acadêmicas	Escola onde estudou, Faculdade, Ano de conclusão/período,
Trabalho	Empresa onde trabalha, Perfil profissional, Cargo, Profissão, Salário,
Localização	Endereço, CEP, Cidade onde mora, País onde mora, Localização, Check-in,
Dados Técnicos	Localização de contatos em outros serviços, Coleta IP, Browser, Sistema Operacional, Provedor de internet,
Família	Filhos, Relacionamento, Com quem mora,
Hábitos	Fumar, Beber, Animal de estimação, Check-in em festas, restaurantes, cinemas, Livros, Filmes, Músicas,

Figura 1 – O que se pode saber sobre os usuários

A partir das análises realizadas é possível concluir que a privacidade dos usuários de redes sociais e e-mails gratuitos não pode ser garantida pelas empresas provedores destes serviços, fazendo com que a privacidade destes usuários esteja exposta a muitas ameaças. Conforme descrito nas políticas de privacidade analisadas, os provedores destes serviços compartilham com empresas parceiras as informações dos usuários, seja para que estas empresas prestem serviços para os provedores, seja como parte de alguma negociação comercial. Uma vez que as informações são compartilhadas não é possível garantir que estas não sejam utilizadas para fins indevidos. Da mesma forma não é possível garantir que, caso o usuário exclua seu perfil ou sua conta, suas informações sejam totalmente eliminadas. Tanto os provedores dos serviços quanto seus parceiros mantêm cópias de segurança das informações armazenadas em seus bancos de dados, e não se pode garantir que estas cópias não serão utilizadas mesmo após a exclusão do perfil ou conta.

Os provedores não informam especificamente como as empresas parceiras tratam, armazenam ou utilizam as informações dos usuários, sendo estas ações realizadas sem o conhecimento do titular dos dados, o que caracteriza uma potencial ameaça à privacidade dos usuários dos serviços de redes sociais e de e-mails gratuitos.

O usuário destes serviços tem acesso somente às informações que estão em seus perfis

e suas contas, mas não consegue identificar ou excluir as informações que foram repassadas às empresas parceiras dos provedores, não sendo possível acessá-las, perdendo-se assim o controle sobre estas informações. Esta prática fere o princípio de livre acesso, uma vez que o usuário não tem livre acesso ao total das suas informações.

O princípio da qualidade não é atendido uma vez que as informações são compartilhadas com empresas terceiras, o que faz com que os provedores não tenham como garantir que estas informações permaneçam fiéis à realidade, completas e relevantes. A própria política de privacidade de uma das redes sociais, o Twitter, informa que a informações poderão ser adaptadas ou alteradas.

Pode-se concluir que o princípio da finalidade, o qual restringe a transferência de dados para terceiros, não é cumprido pelos provedores dos serviços de rede social e e-mails gratuitos, uma vez que compartilham as informações de usuários com empresas parceiras com as quais terceirizam parte de seus serviços.

5 Considerações Finais

Com a grande quantidade de informações que é lançada na rede mundial de computadores diariamente, tem crescido a preocupação com a segurança e com a privacidade das informações dos usuários. Com base na Figura 1 pode-se chegar à conclusão mais importante deste estudo, a qual diz respeito à grande quantidade de informações dos usuários que são coletadas e das grandes ameaças potenciais à privacidade. Atualmente não é possível garantir a privacidade das informações pessoais dos usuários dos serviços de redes sociais e de e-mails gratuitos. A grande quantidade de informações fornecidas por si só já expõe a privacidade dos usuários a um grande risco, e o fato das empresas compartilharem as informações de seus usuários com empresas terceirizadas potencializa estes riscos.

As análises realizadas neste estudo identificaram as ameaças a que está exposta a privacidade dos usuários dos serviços de redes sociais e de e-mails gratuitos. Através do que está descrito na política de privacidade destes serviços, pode-se constatar que atualmente não é possível garantir que as informações de seus usuários não serão utilizadas para fins alheios aos necessários para usufruir destes serviços. Contrariamente a isto, estas políticas de privacidade inclusive informam que as informações fornecidas pelos usuários poderão ser compartilhadas com empresas parceiras, fazer parte de transações comerciais e, em alguns casos, até mesmo alteradas ou adaptadas.

Com base na análise das políticas de privacidade dos serviços de redes sociais e de e-mails gratuitos e da análise dos dados que são coletados de forma obrigatória e de forma espontânea, pode-se concluir que as empresas provedoras destes serviços não podem garantir a privacidade das informações dos usuários. Este resultado atende ao primeiro objetivo específico deste estudo.

A partir da análise minuciosa das políticas de privacidade dos serviços de redes sociais e de e-mail gratuitos conclui-se que estas políticas não atendem aos princípios que compõem os *Fair Information Principles*, publicados pelo Departamento de Segurança Interna dos Estados Unidos, que devem ser seguidos para garantir a privacidade dos dados pessoais coletados. Estes resultados obtidos atendem ao segundo objetivo específico deste estudo.

O objetivo geral deste estudo pode ser atendido a partir das análises realizadas para atender aos objetivos específicos, uma vez que com essas análises pode-se identificar as potenciais ameaças a privacidade dos usuários dos serviços de redes sociais e de e-mails gratuitos. Esta pesquisa tem como limitações o fato de utilizar uma publicação americana para analisar os riscos à privacidade, já que na época da coleta de dados nãohvia uma legislação brasileira com a mesma finalidade. qual seja, *Fair Information Principles*, realizada pelo Departamento de Segurança Interna dos Estados Unidos no ano de 2008, compostos por

princípios que devem ser seguidos para garantir a privacidade dos dados pessoais coletados pelas empresas, para analisar as políticas de privacidade dos serviços objetos deste estudo.

Como sugestões para pesquisas futuras têm-se a proposta de um modelo teórico e survey para que seja possível identificar a percepção de confiança dos usuários dos serviços de redes sociais e de e-mails gratuitos, bem como a percepção de invasão de privacidade, com relação às informações fornecidas às empresas provedoras destes serviços, identificando o *privacy concerns* dos brasileiros.

Referências

BANKS, Alex. **2012 BRAZIL DIGITAL FUTURE IN FOCUS**. Disponível em: <http://www.comscore.com/por/Press_Events/Press_Releases/2012/3/Brazil_s_Social_Networking_Activity_Accelerates_in_the_Past_Year>. Acesso em: 14 de maio de 2012.

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

AZEVEDO, R.. Um sistema autonômico baseado em ontologias e agentes inteligentes para uso em segurança da informação. **Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação.** v. 17, n. 35, 2012.

BÉLANGER, 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.

CHOOBINEH, J; DHILLON, G.; GRIMAILA, M.; REES, J. Management of Information Security: Challenges and Research Directions. **Communications of the Association for Information Systems**. v. 20, Article 57, 2007.

HAIR, J. et al. **Fundamentos de métodos de pesquisa em administração**. Porto Alegre: Bookman, 2005.

HAMEED, S. Priority user access for social network security. **Research Journal of Information Technology**. v. 5, n. 2, p. 45, 2013.

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

HUI, K. et al. The value of privacy assurance: An exploratory field experiment. **MIS Quarterly**, v.31, n.1, p. 19-33, 2007.

Ministério da Justiça do Brasil. Departamento de Defesa e Proteção do Consumidor. **Caderno de Investigações Científicas**: A Proteção de Dados Pessoais nas Relações de Consumo: Para Além da Informação Creditícia. Brasília, 2010. P. 121.

NJENGA, K. Conceptualising improvisation in information systems security. **European journal of information systems**. v. 21, n. 6, p. 592-607, 2012.

PARRIS, I. Privacy-enhanced social-network routing. **Computer communications**. v. 35, n. 1, p. 62-74, 2012.

SCHWAIG, K.; KANE, G.; STOREY, V. Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures?. **Information & Management**, v.43, n. 7, p. 805-820, 2006.

SHIN, D. 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.

TUREL, O. The benefits and dangers of enjoyment with social networking websites. **European journal of information systems**. v. 21, n. 5, p. 512-528, 2012.

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

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