Antecedents of Perceived Benefits of Compliance Towards Organizational Data Protection Policies

J. G. Santos, A. Cappellozza and A. L. Albertin

***Abstract*— Personal data protection policies are organizational tools that help to ensure employees´ data privacy. This study analyzed antecedent factors that influence employees´ perception in Brazilian organizations about perceived benefits of compliance towards those policies. The research was conducted through a quantitative approach and structural equation modeling was applied to test our hypothesis. Data were collected through a survey to obtain a sample of 220 respondents. Our results indicate that trust in organization and the risk of privacy loss directly influence perceived benefits of compliance. The results also show that employees who had your data improperly used before, have credibility in organizational controls reduced and perceived risk of privacy loss increased.**

***Keywords*— Personal data, information security, organizational controls, compliance.**

I. INTRODUÇÃO

O PROCESSO de informatização de bases de dados ganha espaço a cada dia nas organizações. A automação de processos organizacionais é vista como sinônimo de eficiência gerencial, redução de custos, maior produtividade, melhor controle sobre as operações desenvolvidas e maior precisão nas atividades fim [29].

A prática da coleta de informações pessoais pelas organizações desenvolveu-se com o advento da estruturação administrativa, estatal e privada. Seja para a gestão de recursos humanos, ou para cumprir requisitos legais, o empregador necessita coletar as infomações pessoais dos seus colaboradores [19]. Com o avanço da tecnologia da informação e comunicação, proteger a privacidade das informações pessoais se tornou um desafio significativo para as organizações [35], uma vez que a ocorrência de vazamento de dados pode gerar consequências desastrosas, incluindo a responsabilidade legal corporativa, a perda de credibilidade, imagem e danos monetários [3].

Somente em 2015, as organizações brasileiras que tiveram seus dados utilizados indevidamente arcaram com um gasto total aproximado a R$ 3,9 milhões de prejuízo, impondo um aumento de 10% nos gastos totais quando comparado ao ano de 2014 [27].

As boas práticas de Governança Corporativa consistem na transparência e padrões éticos em conformidade com normas internas e externas. É papel da Governança Corporativa velar pela integridade organizacional em todos os níveis, sendo fundamental o seu envolvimento ativo no programa de compliance.

Sabe-se que compliance se refere a cumprir, estar em conformidade com leis, diretrizes, regulamentos internos ou externos, buscando mitigar riscos. O cumprimento das normas é indispensável para a equidade nas relações da organização com os stakeholders e para um comportamento responsável da organização e de seus dirigentes [8].

Além disto, o entendimento e cumprimento das políticas e regulamentos de segurança organizacional pelos empregados pode ser fundamental no controle de segurança da informação [2] tendo em vista que os empregados podem expor informações confidenciais pela falta de zelo, distrações ou de forma maliciosa. Desta forma, somente a existência dos mecanismos de controle de dados não se traduz automaticamente em um comportamento individual desejável de adesão às políticas de segurança da informação implantadas, pois os funcionários podem não ser motivados a executar as atividades necessárias para proteger os ativos da informação [32].

Portanto, afim de ampliar o conhecimento sobre as percepções dos colaboradores sobre a segurança de suas informações pessoais nas organizações que atuam, este estudo objetiva analisar os antecedentes individuais aos benefícios percebidos de compliance às políticas organizacionais de proteção de dados pessoais dos empregados.

II. REFERENCIAL TEÓRICO

A violação de dados nas organizações e suas implicações

Um ambiente organizacional com poucas medidas de segurança, como políticas e procedimentos de segurança da informação é mais suscetível à ocorrência de vazamento de informações que pode estar vinculada a venda ou aluguel de nomes de potenciais clientes, endereços, números de telefone, histórico de compras, categorizações, entre outras possibilidades [23].

Diversos escândalos envolvendo os dados pessoais ocorreram ao redor do mundo: em fevereiro de 2005, a ChoicePoint que é uma empresa Americana responsável por credenciamento, triagem e autenticação de registros públicos para organizações sem fins lucrativos e agências governamentais enviou cartas a 145 mil clientes notificando-

J. G. Santos, Universidade Metodista de São Paulo (UMESP), São Bernardo do Campo, São Paulo, Brasil, julysb1@hotmail.com

A. Cappellozza, Universidade Metodista de São Paulo (UMESP), São Bernardo do Campo, São Paulo, Brasil, alexandre.cappellozza@metodista.br

A. L. Albertin, Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas, São Paulo, Brasil, albertin@fgv.br

os de que, em 2004, suas informações tinham sido de forma fraudulenta acessadas e usadas para cometerem delitos. A violação foi resultado de falhas no processo de credenciamento de novos clientes e monitoramento dos clientes já credenciados que permitiu a negociação de contratos com empresas que buscavam com o credenciamento somente o acesso a informações pessoais [11].

A existência de procedimentos que regulamentam o comportamento dos empregados dentro da organização é o que faz a manutenção da rotina de cada companhia. A aplicação de penalidades pelo ferimento das regras é a prova de que o código de ética da empresa não é uma mera formalidade, mas que existe para ser seguido à risca.

As políticas de segurança da informação consistem na formalização dos anseios da organização quanto à proteção de suas informações a fim de minimizar os riscos da perda dessas informações [38]. Deste modo, cumprir os requisitos de segurança, regras e procedimentos pode estar relacionado com os riscos de perda de privacidade [2].

Riscos de perda de privacidade

A privacidade das informações é um assunto que preocupa os profissionais em diversos contextos organizacionais, pois está se tornando componente de perda organizacional devido às diversas fragilidades relacionadas a segurança das informações [33].

Nas transações de consumo, o cliente quase sempre detalha o seu comportamento e preferências de modo que seus hábitos de compras são facilmente projetados e podem ser compartilhados com terceiros, caso os meios de proteção de dados pessoais das organizações sejam. Esta fragilidade impacta diretamente na preocupação dos titulares da informação e como consequência, poderão deixar de divulgar suas informações em futuras relações de consumo [12].

A atitude pessoal pode ser um dos fatores que norteia os efeitos dos benefícios de compliance e leva em consideração os benefícios e o custo do não cumprimento das políticas de segurança da informação [2]. A pessoa que apresenta preocupação com suas informações pessoais tende a se comportar de modo a manter seus dados em segurança [13]. Portanto, elabora-se a primeira hipótese deste estudo.

Hipótese 1 (H1): A percepção do risco de perda de privacidade influencia positivamente os benefícios percebidos de compliance.

Credibilidade nos controles organizacionais

A privacidade é uma questão organizacional, a ausência de políticas e controles que regem o uso adequado de informações pessoais nas organizações pode gerar o risco de utilização inadequada dessas informações por um único funcionário trazendo consequências negativas para a empresa [12]. Os titulares das informações pessoais estão aptos a revelar suas informações pessoais se as suas preocupações sobre privacidade são amparadas por controles pautados em políticas e procedimentos justos [12].

A credibilidade no controle pode ser o primeiro passo para aliviar as preocupações com a privacidade entre os proprietários das informações pessoais [13]. Nesse sentido, desenvolve-se a segunda hipótese do estudo.

Hipótese 2 (H2): A credibilidade nos controles organizacionais influencia negativamente a percepção do risco de perda de privacidade

Os proprietários das informações pessoais podem passar por experiências positivas ou negativas na disponibilização de suas informações pessoais, entretanto, mesmo que o indivíduo possua mais experiências positivas, um único evento negativo aumentará a sua preocupação com relação aos seus dados pessoais [25]. Algumas pessoas podem desenvolver atitudes sobre a percepção do risco de perda de privacidade somente após terem tido alguma experiência negativa com o uso inadequado de suas informações por terceiros [10].

Experiência negativa de perda de privacidade

Nos Estados Unidos, somente em 2014, estima-se que aproximadamente 110 milhões de americanos, o equivalente a cerca de 50% dos adultos dos EUA tiveram seus dados pessoais expostos nos diversos meios eletrônicos [20].

Após uma experiência negativa relacionada à perda de informações pessoais, os proprietários das informações ressentem em fornecer suas informações novamente devido ao risco de novo incidente, assim serão menos propensos a confiar nas organizações. Experiências negativas de privacidade podem aumentar a percepção de risco dos consumidores quanto a divulgação de suas informações pessoais [1] e afetar a confiança nas empresas [37]. Neste sentido, propõe-se a seguinte hipótese:

Hipótese 3 (H3): Experiência negativa de privacidade influencia positivamente a percepção do risco de perda de privacidade.

Uma vez que o titular da informação pessoal tenha vivenciado uma experiência negativa com a violação de seus dados, eles serão mais sensíveis à questão da privacidade, aumentando o seu nível de preocupação com os seus dados.

Caso o proprietário da informação pessoal não acredite nos controles internos da organização possuidora de seus dados pessoais ou perceba o mau uso dos seus dados, ele tende a solicitar a remoção de seus dados dessa companhia. [13]. Deste modo, elabora-se a quarta hipótese:

Hipótese 4 (H4): Experiência negativa de privacidade influencia negativamente a credibilidade nos controles organizacionais.

Confiança na organização

A confiança pode ser representada pela vontade de assumir o risco [22; 29]. A confiança entre proprietário das informações pessoais e organização é direcionada aos atributos utilizados pela organização para maximizar a proteção de privacidade e ao poder dado às organizações no gerenciamento e divulgação dos seus dados privados. Se uma organização possui políticas de privacidade robustas, os titulares das informações podem sentir maior controle sobre seus dados [4].

Do mesmo modo que a confiança é um antecedente direto das intenções de transação ele atua como um antecedente indireto através do risco percebido sobre o fornecimento de dados pessoais a um sistema de informação [26].

A redução de risco nas transações contribui para a relação de confiança [30], uma vez que um indivíduo estabelece a confiança em uma entidade por meio da percepção de segurança de que seus dados pessoais estão armazenados de maneira segura, ele provavelmente apresenta níveis reduzidos de preocupação com o risco de privacidade porque vê a probabilidade de resultado negativo reduzida [24]. Portanto, elabora-se a seguinte hipótese:

Hipótese 5 (H5): A confiança na organização influencia negativamente a percepção do risco de perda de privacidade.

A confiança consiste nas expectativas mantidas pelo proprietário das informações pessoais de que a empresa em que trabalha cumprirá suas responsabilidades organizacionais de forma adequada [36].

Partindo da confiança na organização, empregados podem agir em compliance com as políticas de proteção de dados pessoais, pois acreditam no benefício nesta relação [12].

O tratamento adequado das informações pessoais é essencial para a construção da relação de confiança entre o proprietário das informações pessoais e a organização com a qual possui algum tipo de relacionamento [12].

Os mecanismos de controle das informações pessoais podem ser percebidos positivamente pelos empregados como benefício e favorecer o cumprimento das políticas de segurança da informação [2]. Deste modo, elabora-se a hipótese seis e sete deste estudo.

Hipótese 6 (H6): A Confiança na organização influencia positivamente os benefícios percebidos de compliance.

Hipótese 7 (H7): A Confiança na organização influencia positivamente a credibilidade nos controles organizacionais.

III. PROCEDIMENTOS METODOLÓGICOS

Esta é uma pesquisa de abordagem quantitativa que buscou compreender a realidade por meio da coleta de dados com profissionais a respeito da proteção de dados pessoais. Nesta pesquisa, para a coleta dos dados brutos foi utilizado um questionário com escalas validadas com o objetivo de testar as hipóteses propostas no referencial teórico. Para os cálculos e validações dos testes estatísticos foi utilizado o software SmartPLS 3.0.M3 [28].

As escalas utilizadas são de sete pontos nas quais (1) representa que o respondente Discorda totalmente e (7) Concordo totalmente sobre cada afirmativa. A composição dos itens do instrumento de medida foi elaborada a partir de pesquisas que versavam sobre os respectivos temas, tais como, benefícios percebidos de compliance [2], risco de privacidade e credibilidade nos controles organizacionais [24], experiência negativa de privacidade [32] e confiança na organização [36].

A pesquisa foi aplicada de duas maneiras, a primeira forma abordou 180 empregados de diversas organizações e atividades, presencialmente, por meio de questionário impresso, aplicado a uma amostra segmentada de empregados de organizações brasileiras que utilizam meios eletrônicos como sistemas integrados e e-mail em seu cotidiano e que trabalhavam, pelo menos, um ano em sua função atual. Desse total foram validados 172 questionários, oito formulários tiveram que ser excluídos da amostra por estarem incompletos. A coleta de dados também foi realizada por meio de questionário eletrônico criado no ambiente Survey Monkey® com amostra direcionada obtendo um total de 50 respondentes. Nesta amostra apenas dois questionários apresentaram divergências passiveis de eliminação, tendo um total de 48 questionários validados. Considerando as duas maneiras de coleta, 220 foi o total de questionários válidos.

IV. DESCRIÇÃO E ANÁLISE DOS RESULTADOS

A amostra do estudo contou com 50,9% de respondentes do gênero feminino (112 pessoas) e 49,1% dos participantes do gênero masculino (108 pessoas). A idade média dos respondentes é igual a 35 anos. A maioria dos participantes do estudo, 35,9% da amostra, possui ensino superior incompleto e 24,01% dos respondentes possuem especialização completa. O tempo médio de experiência profissional dos respondentes é igual a 14,9 anos.

A análise realizada com os participantes da pesquisa revelou que 55% das organizações permitem o uso de computadores da companhia para fins particulares e 45% já não permitem esse acesso, ainda que, em percentual menor, é possível notar restrição do uso de computadores das companhias para fins particulares.

Um vazamento de dados pode estar relacionado à divulgação de informações que não deveriam ser públicas por um invasor ou mesmo por fragilidades que permitam a exposição desses dados indevidamente com consequências pessoais. O resultado da pesquisa apresentou que 30,5% dos respondentes da pesquisa já tiveram o conhecimento da ocorrência de vazamento de dados pessoais de pessoas próximas. Apenas 30,5% das organizações possuem um canal pelo qual os empregados podem comunicar a ocorrência de vazamento de dados. Apesar da variável Experiência negativa de privacidade continuar um pouco abaixo de 0,70, o indicador de confiabilidade composta do construto dessa variável apresentou valor adequado, e optou-se por manter

essa variável. Os valores da Variância Média Extraída (AVE) e Confiabilidade Composta são adequados para continuidade das análises [17]. A TABELA I apresenta os resultados de validação do modelo de mensuração.

TABELA I.
SÍNTESE DA AVALIAÇÃO DOS MODELOS DE MENSURAÇÃO

	BPC	CNO	ENP	CCO	RPP
BPC	**0,785**				
CNO	0,618	**0,799**			
ENP	-0,009	-0,182	**0,795**		
CCO	0,476	0,706	-0,325	**0,797**	
RPP	-0,085	-0,334	0,378	-0,440	**0,760**
AVE	0,616	0,638	0,633	0,636	0,578
Confiabilidade Composta	0,865	0,841	0,772	0,875	0,873

Na análise das cargas fatoriais cruzadas, todos os indicadores apresentaram cargas fatoriais altas em suas variáveis latentes, superiores a 0,70, e baixa nas demais variáveis latentes. Para analisar as significâncias dos indicadores, foi utilizada a técnica *bootstrapping* [17]. Foi realizada uma reamostragem de 5.000 amostras, com reposição de 220 casos [26]. A TABELA II apresenta os valores dos coeficientes entre os construtos e as respectivas estatísticas t de *Student*. Todos os valores dos relacionamentos apresentaram valores de t de *Student* superiores a 1,96 (nível de significância = 5%), apresentando suporte para as hipóteses do estudo.

TABELA II
COEFICIENTES DO MODELO ESTRUTURAL

Indicadores	Média	Erro Padrão	Valor T	P-valor
Confiança → Benefício percebido de compliance	0,668	0,042	15,754	0,000
Confiança →Credibilidade nos controles organizacionais	0,671	0,045	14,738	0,000
Confiança →Risco de perda de privacidade	-0,073	0,095	0,751	0,453
Experiência Negativa de privacidade → Credibilidade nos controles organizacionais	-0,206	0,051	3,993	0,000
Experiência Negativa de privacidade → Risco de perda de privacidade	0,272	0,061	4,361	0,000

De acordo com as análises, o construto Credibilidade nos Controles Organizacionais (CCO) apresentou um r² de 0,538 considerado alto, o construto Percepção do Risco de Perda de Privacidade (RPP) apresentou um r² de 0,258, considerado alto, e o construto Benefícios Percebidos de Compliance apresentou um r² de 0,399, também considerado alto [7].

Com as validações obtidas com o modelo estrutural, obteve-se a síntese dos testes de hipóteses do estudo na Figura 1.

Hipóteses	Descrição	Resultado
H1	Percepção do risco de perda de privacidade influencia positivamente os benefícios percebidos de compliance	Confirmada
H2	Credibilidade nos controles organizacionais influencia negativamente a percepção do risco de perda da privacidade	Confirmada
H3	Experiência negativa de privacidade influencia positivamente a percepção do risco de perda da privacidade	Confirmada
H4	Experiência negativa de privacidade influencia negativamente a credibilidade nos controles organizacionais	Confirmada
H5	Confiança na organização influencia negativamente a percepção do risco de perda da privacidade	Não Confirmada
H6	Confiança na organização influencia positivamente os benefícios percebidos de compliance	Confirmada
H7	Confiança na organização influencia positivamente a credibilidade nos controles organizacionais	Confirmada

Figura 1. Síntese dos testes de hipóteses do estudo

V. CONCLUSÕES

Este estudo identificou e analisou os antecedentes que influenciam empregados de organizações brasileiras quanto aos benefícios percebidos de compliance às políticas estabelecidas na prevenção e proteção dos dados pessoais. Sete hipóteses foram estabelecidas e apenas uma não foi confirmada.

Como um antecedente do Benefício percebido de compliance, a Credibilidade nos controles organizacionais apresenta o quanto o empregado acredita nos controles de proteção de dados pessoais. De acordo com o resultado, essa dimensão apresentou um r² de 54%, considerado alto [7], ou seja, a credibilidade nos controles organizacionais é explicada em 54% pela Experiência negativa de privacidade e Confiança na organização.

O construto Credibilidade nos controles organizacionais indica que o empregado que acredita nesses controles organizacionais enxerga, de forma reduzida, o risco de vazamento de seus dados pessoais pelas organizações, além disso, nota-se que a confiança na organização apresenta maior influência a percepção do risco de perda de privacidade assim, uma das possibilidades sugeridas aos gestores é a implementação de um processo de governança e gestão de riscos que favoreça a credibilidade nos controles organizacionais por meio de planos que elevem a confiança dos empregados na organização. Adicionalmente, os gestores devem promover campanhas que valorizem a organização e o sucesso alcançado com o auxílio dos empregados.

A Percepção do risco de perda de privacidade é um construto com poder de explicação também considerado alto [7]. E apresentou r² de 26%, ou seja, a Experiência negativa de privacidade e Credibilidade nos controles organizacionais

explica 26% da Percepção do risco de perda de privacidade. Conclui-se, então que o indivíduo que sofreu consequências negativas com a perda de seus dados pessoais é mais sensível ao risco, ou seja, percebe facilmente o risco de perda de privacidade e consequentemente a sua credibilidade com relação aos controles internos organizacionais é diminuída.

O relacionamento entre confiança na organização e a Percepção do risco de perda de privacidade é um ponto que merece atenção neste estudo, pois o resultado não confirmou a existência de relacionamento e difere dos estudos de Culnan e Armstrong (1999) e Miltgen e Smith (2015), deste modo, merece investigação futura.

Acredita-se que o resultado ocorreu devido o efeito da mediação da Credibilidade nos controles organizacionais. Além disso, a dimensão com maior influência nesse relacionamento é a Credibilidade nos controles organizacionais. Portanto, é sugerido aos gestores de organizações mostrarem a eficiência dos controles estratégicos que favoreçam a segurança dos dados dos empregados com o objetivo de aumentar a credibilidade nos controles de proteção de dados pessoais.

O estudo confirma que o empregado que confia na organização em que trabalha tem maior probabilidade de seguir as políticas de proteção de dados pessoais, pois percebe o benefício dessa ação. Evidenciou-se também que o empregado que confia na organização em que trabalha tem a sua credibilidade nos controles organizacionais aumentada.

De acordo com o resultado da pesquisa o benefício percebido de compliance é explicado em 40% pela Confiança na organização e a Percepção do risco de perda de privacidade. Sugere-se então que pesquisas futuras abordem temas que busquem maior poder de explicação do modelo.

Os Benefícios percebidos de compliance sofrem maior influência pela Confiança na organização. Para os gestores, o estudo amplia a compreensão de que a Confiança na organização é um fator determinante no benefício percebido de compliance e credibilidade nos controles organizacionais.

Com o objetivo de aperfeiçoar os processos de gestão de risco de perda de dados, as organizações devem divulgar a seus empregados o quão efetiva são as políticas de proteção de dados e os benefícios gerados quando essas políticas são seguidas. Avaliar a percepção dos empregados com relação aos controles internos existentes e implementar melhorias conforme anseio dos empregados a fim de disseminar a confiança no processo de gestão de riscos e consequentemente na organização.

Entre as contribuições originadas por esta pesquisa, algumas estão relacionadas ao âmbito acadêmico. Os resultados contribuem com os estudos associados a preocupações com a privacidade e confiança conforme as chamadas de pesquisa de Liao; Liu e Chen, (2011) e Okazaki; Li e Hirose, (2009). Adicionalmente o estudo também contribui com as chamadas de pesquisa relacionadas com a privacidade no trabalho por meio de políticas e práticas organizacionais referentes a coleta e uso de informações pessoais [35].

Pesquisas futuras podem agregar ao estudo dimensões que versam o custo e benefício de estar em compliance. Por exemplo, uma possibilidade de estudo futuro é a mensuração da efetividade dos controles internos relacionados a proteção de dados pessoais por meio da percepção dos empregados sobre as ações organizacionais na busca pela manutenção e aperfeiçoamento de controles de proteção de dados.

Outra possibilidade de pesquisa pode ser a condução de diferentes grupos organizacionais com o objetivo de verificar, por exemplo, se o porte da organização influencia no nível de controle de proteção de dados pessoais, como exemplo, a infraestrutura de tecnologia e controles de uma grande organização em comparação com uma organização de menor porte. Outro fator que pode ser considerado como sugestão de pesquisa refere-se a região na qual a organização está inserida para investigar se a cultura regional influencia a proteção de dados pessoais.

Entende-se como limitação desta pesquisa o fato de o estudo poder conter erros de medida através de imprecisão na mensuração dos valores reais das respostas e não pode afirmar que a significância e valores dos testes realizados neste estudo sejam constantes uma vez que a pesquisa foi aplicada em diversas organizações, sem um padrão exclusivo, contidas em uma mesma região geográfica.

REFERÊNCIAS

[1] Bansal, G. e Zahedi, F. Trust violation and repair: The information privacy perspective, *Decision Support Systems*, vol. 71, pp. 62-77, 2015.

[2] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. Information security policy compliance: An empirical study of racionality-based beliefs and information security awareness. *MIS Quarterly,* vol. 34, no. 3, pp. 523-548, 2010.

[3] Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. Economics of IT Security Management: Four Improvements to Current Security Practices, *Communications of the Association for Information Systems*, vol. 14, pp. 65-75, 2004.

[4] Chang, Y., Lee, H., & Wong, S. Understanding perceived privacy: a privacy boundary management model, *PACIS 2015 Proceedings*, Art. 78, 16 p, 2015.

[5] Chin, W. *The Partial Least Squares Approach to Structural Equation Modeling*, in Marcoulides, G. A. (Ed.), Modern Methods for Business Research, Lawrence Erlbaum, Mahwah, pp. 295-358, 1998.

[6] Chin, W., & Newsted, P. *Structural equation modeling analysis with small samples using partial least squares*. In Hoyle, R. H. (Ed.), Statistical strategies for small sample research, Sage Publications, Thousand Oaks, pp. 307-341, 1999.

[7] Cohen, J. *Statistical power analysis for the behavioral sciences*, Erlbaum, Hillsdale, 1988.

[8] Coimbra, M. A., & Manzi, V. A. *Manual de Compliance - Preservando a Boa Governança e Integridade das Organizações*, Atlas, São Paulo, 168 p, 2010.

[9] Cooper, C. *Employee data protection policies*, Global Data Hub. Disp. em http://united-kingdom.taylorwessing.com/globaldatahub/article_employee_dp_policies.html, 2013.

[10] Culnan, M. Consumer awareness of name removal procedures: Implications for direct marketing*, Journal of Direct Marketing*, vol. 9, no. 2, pp.10-19, 1995.

[11] Culnan, M., & Williams, C. How ethics can enhance organizational privacy: lessons from the Choicepoint and Tjx data breaches, *MIS Quarterly*, vol. 33, no. 4, pp. 673-687, 2009.

[12] Culnan, M., & Armstrong, P. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, *Organization Sciences*, vol. 10, no. 1, pp. 104-115, 1999.

[13] Dolnicar, S., & Jordaan, Y. Protecting Consumer Privacy in the Company's Best Interest, *Australasian Marketing Journal,* vol. 14. no. 1, pp. 39-61, 2006.

[14] Fontes, E. *Segurança da informação, o usuário faz a diferença*, Saraiva, São Paulo, 172 p, 2006.
[15] Fornell, C., & Larcker, D. F. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, vol. 18, no. 1, pp. 39-50, 1981.
[16] Hair, J. F., Jr., Anderson, R., Tatham, R., & Black, W. *Análise multivariada de dados*, Bookman, Porto Alegre, 2005.
[17] Hair, J. F., Jr., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. *Primer on Partial Least Squares Structural Equation Modeling* (PLS-SEM). SAGE Publications, Thousand Oaks, 2014.
[18] Hair, J. F., Jr., Ringle, C. M., & Sarstedt, M. PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*, vol. 19, no. 2, pp. 139-151. 2011.
[19] Hassan, K. Personal data protection in employment: New legal challenges for Malaysia, *Journal Computer Law and Security Review*, vol. 28, no. 6, pp. 696-703, 2012.
[20] Kelly, E. *Officials warn 500 million financial records hacked*, USA Today, Washington. Disponível em http://www.usatoday.com/story/news/politics/2014/10/20/secret-service-fbi-hack-cybersecuurity/17615029, 2014.
[21] Liao, C., Liu, C., & Chen, K. Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model, *Electronic Commerce Research and Applications*, vol. 10, no. 6, pp.702–715, 2011.
[22] Mayer, R., Davis, J., & Schoorman, F. An integrative model of organizational trust. *Academy of Management Review*, vol. 20, no. 3, pp.709–734, 1995.
[23] Milberg, S., Smith, H., & Burke, S. Information Privacy: Corporate Management and National Regulation. *Organization Sciences*, vol. 11, no. 1, pp. 35–57, 2000.
[24] Miltgen, C., & Smith, H. Exploring information privacy regulation, risks, trust, and behavior. *Information Management*, vol. 52, no. 6, pp.741-759, 2015.
[25] Okazaki, S., Li, H., & Hirose, M. Consumer Privacy Concerns and Preference for Degree of Regulatory Control, *Journal of Advertising*, vol. 38, no. 4, pp. 63–77, 2009.
[26] Pavlou, P. A. Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model, *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 101-134, 2003.
[27] *Ponemon Institute. Cost of Data Breach Study*. Michigan, USA, p.1-30, May /2015. Disponível em < http://www-03.ibm.com/security/data-breach>, 2015.
[28] Ringle, Christian M., Wende, Sven, & Becker, Jan-Michael. *SmartPLS 3*. Bönningstedt: SmartPLS. Retrieved from http://www.smartpls.com, 2015.
[29] Rousseau, D. M., Sitkin, S., Burt, R. S., & Camerer, C. F. Not so different after all: a crossdiscipline view of trust. *Academy of Management Review*, vol. 23, no. 3, pp.393-404, 1998.
[30] Santos, C. P., & Fernandes, D. V. H. A recuperação de serviços como ferramenta de relacionamento: seu impacto na confiança e lealdade dos clientes. *EnANPAD 2005 - XXIX Encontro da ANPAD*. Brasília, 2005.
[31] Sardeto, P. E. R. *A proteção de dados pessoais em debate no Brasil*, Âmbito Jurídico, Rio Grande, vol. 14, no. 88, 2011.
[32] Smith, H., Milberg, J., & Burke, J. Information Privacy: Measuring Individuals: Concerns about Organizational Practices, *MIS Quarterly*, vol. 20, no. 2, pp. 167-196, 1996.
[33] Stanton, J M., Stam, K. R., Mastrangelo, P., & Jolton, J. Analysis of end user security behaviors, *Computers & Security*, vol. 24, no. 2, pp. 124-133, 2005.
[34] Stone, E. F., & Stone, D. L. Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms, in Ferris, G. e Rowland, K. (eds.), *Research in Personnel and Human Resources Management*, vol. 8, pp. 349-411, 1990.
[35] Stone-Romero E. F., Stone, D. L., & Hyatt, D. Personnel Selection Procedures and Invasion of Privacy, *Journal of Social Issues*, vol. 59, no. 2, pp. 343-368, 2003.
[36] Terres, M., Koetz, C., Santos, C., & Caten, C. O papel da confiança na marca na intenção de adoção de novas tecnologias. *Revista de administração e inovação*, vol. 7, no. 4, pp.162-185, 2009.
[37] Xu, H., Dinev, T., Smith, J., & Hart, P. Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View, *Twenty Ninth International Conference on Information Systems, Association for Information Systems* AIS Electronic Library (AISeL), Paris, pp. 1-166, 2008.
[38] Yang, H., & Liu, H. Prior negative experience of online disclosure, privacy concerns, and regulatory support in Chinese social media. *Chinese Journal of Communication*, vol. 7, no. 1, pp. 40-59, 2013.
[39] Zanon, S. B. Gestão e segurança da informação eletrônica: Exigências para uma gestão documental eficaz no Brasil, *Biblios,* no. 56, pp. 69-79, 2014.

Juliana Graciela dos Santos é Mestre em Administração de Empresas pela Universidade Metodista de São Paulo. Possui experiência na área de Administração e Auditoria Interna com ênfase na avaliação de controles internos e gerenciamento de riscos.

Alexandre Cappellozza é Doutor em Administração de Empresas pela Fundação Getulio Vargas. Professor Titular dos Programas de Pós-Graduação em Comunicação Social e Psicologia da Universidade Metodista de São Paulo. Seus interesses de pesquisa envolvem Tecnologia de Informação e suas implicações nos níveis individuais, organizacionais e sociais.

Alberto Luiz Albertin é Doutor em Administração pela Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo (FEA-USP). Professor Titular da Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas (FGV-EAESP). Coordenador do Centro de Tecnologia de Informação Aplicada (FGVcia) da FGV EAESP. Consultor na área de Administração de Tecnologia de Informação, Transformação Digital, Negócios na Era Digital e Gerência de Projetos, tendo realizado vários projetos, pesquisas, estudos e publicações nestas áreas.