Journal of Information Systems and Technology Management – Jistem USP
Vol. 15, 2018, e201815002
ISSN online: 1807-1775
DOI: 10.4301/S1807-1775201815002

A INFLUÊNCIA DA INJUSTIÇA ORGANIZACIONAL NA MOTIVAÇÃO PARA A PRÁTICA DE CRIMES CIBERNÉTICOS

THE INFLUENCE OF ORGANIZATIONAL INJUSTICE IN THE MOTIVATION FOR THE PRACTICE OF CYBERCRIMES

Plínio Silva de Garcia http://orcid.org/0000-0002-0584-0434
Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, RS, Brasil

Marie Anne Macadar http://orcid.org/0000-0003-2744-5352
Fundação Getúlio Vargas, São Paulo, SP, Brasil

Edimara Mezzomo Luciano http://orcid.org/0000-0002-2847-8845
Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, RS, Brasil

RESUMO

Esta pesquisa analisou como a percepção de injustiça organizacional motiva a prática de crimes cibernéticos no local de trabalho. Em uma investigação qualitativa e exploratória, foram realizadas entrevistas com 16 especialistas em segurança cibernética. Os dados foram analisados através da técnica de análise de conteúdo categorial. Os resultados sugerem que a percepção de injustiça produz sentimentos negativos como a baixa-estima, a frustração e a ausência de culpa, e que essas emoções motivam a prática de crimes cibernéticos. Diferentes percepções identificadas entre os entrevistados deste estudo, associadas à revisão da literatura referente ao tema, permitiram a proposição de um modelo conceitual.

Palavras-chave: Justiça organizacional, Motivação criminal, Crime cibernético, Segurança cibernética, *Insiders*.

ABSTRACT

This research analyzes how the perception of organizational injustice motivates the practice of cybercrimes in the workplace. In a qualitative and exploratory investigation, interviews have been carried out for 16 specialists in cybernetic security. Data were analyzed through the categorical content analysis technique. The results obtained suggest that the perception of injustice produces negative feelings, such as low self-esteem, frustration, and lack of guilt, and these emotions, in turn, motivate the practice of cybercrimes. Different perceptions have been identified among the interviewees of this study, which are associated with the literature review related to the theme, allowed the proposition of a conceptual model.

Keywords: Organizational justice, Criminal motivation, Cybercrime, Cybersecurity, Insiders.

Manuscript first received: 2017/Jul/20. Manuscript accepted: 2018/04/11
Address for correspondence:
Plínio Silva de Garcia, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, RS, Brasil.
E-mail: plinio@wwworking.com.br
Marie Anne Macadar, Fundação Getúlio Vargas, São Paulo, SP, Brasil. E-mail: marie.moron@fgv.edu.br
Edimara Mezzomo Luciano, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, RS, Brasil.
E-mail: eluciano@pucrs.br

CC BY

INTRODUÇÃO

Ataques cibernéticos originados por pessoas internas à organização (*insiders*) representam um grande risco para as empresas (Siponen, Mahmood & Pahnila, 2014). O *insider* é alguém que recebeu privilégios que autorizam o acesso e a utilização de sistemas ou instalações na respectiva organização, e que pode ser qualquer pessoa com privilégios e conhecimento sobre os sistemas de informação (Safa, Maple, Watson & Von Solms, 2018). É possível encontrar estudos sobre o comportamento do *insider* antes e durante a perpetração de um crime cibernético. Todavia, ainda é necessário desenvolver pesquisas que melhorem a compreensão sobre a influência de fatores relacionados ao local de trabalho (Willison &, Warketin, 2013). Assim, este artigo tem como objetivo geral analisar como as percepções de injustiça organizacional motivam *insiders* a cometer crimes cibernéticos nas organizações onde trabalham.

O contexto onde o indivíduo está inserido, exerce uma força reconhecidamente relevante, não existindo "... relações sociais entre os indivíduos e os grupos nem entre estes e os objetos sociais que se deem sem referência a um tempo e a um espaço" (Freitas, 2000, p. 4). Assim, a busca perpétua pelo bem-estar no trabalho ocorre subordinada a diferentes variáveis de contexto. O sentimento de justiça, por exemplo, oriundo da equidade de recompensas e reconhecimentos, produz satisfação e, consequentemente, um comportamento social positivo dos trabalhadores em prol da organização. O indivíduo retribui à organização como um todo e não somente a pessoas específicas, e a satisfação no trabalho, quando reforçada por relações interpessoais respeitosas, reduziu tendências de retaliação em virtude de uma maior tolerância dos indivíduos às eventuais injustiças organizacionais (Shropshire, Warkentin & Sharma, 2015).

O estudo sobre a influência que o descontentamento dos indivíduos em relação ao local de trabalho exerce sobre a motivação para a prática do crime cibernético ainda necessita atenção dos pesquisadores. A interação entre o invasor e a respectiva dinâmica ambiental está pouco explorada na literatura (Benson, McAlaney & Frumkin, 2018). A compreensão desta relação pode contribuir para a melhoria das práticas de segurança cibernética mediante a identificação de novas áreas relacionadas à salvaguarda da informação, da infraestrutura de tecnologia, das pessoas e seus respectivos interesses. Embora a pesquisa sobre crimes cibernéticos praticados por *insiders* esteja madura, ainda é frágil o entendimento sobre o problema do descontentamento no espaço organizacional e como esta condição, determinada pelo próprio espaço, impacta na motivação das pessoas para o crime (Willison & Warkentin, 2013). No Brasil, estudos sobre o fator humano na temática da segurança cibernética ainda estão mais focados em aspectos técnicos do que em aspectos comportamentais, ao mesmo tempo em que se faz importante entender as particularidades nacionais (Klein & Luciano, 2016).

Em termos práticos, a compreensão da dinâmica e identificação das influências exercidas pela percepção da injustiça organizacional, entre membros internos de uma organização, bem como a forma como estes são motivados para cometer crimes cibernéticos nas suas próprias organizações, possibilitará que gestores possam estabelecer mecanismos preventivos para este tipo de crime.

Considerando este contexto teórico e prático acerca do tema, a pergunta de pesquisa que emerge é: "De que forma as percepções de injustiça organizacional motivam *insiders* a cometer crimes cibernéticos nas organizações onde trabalham?". Para se responder a esta pergunta, especificamente buscou-se (1) analisar os principais aspectos da justiça organizacional; (2) analisar as principais percepções de injustiça manifestadas por *insiders*; e (3) analisar as principais motivações para a prática de crimes cibernéticos.

CC BY

Assim, a seção 2 demonstra os principais elementos trabalhados pela literatura acadêmica até então, seguida pela proposta de um modelo conceitual (seção 3). Aspectos metodológicos são descritos na seção 4. Os dados coletos em campo são analisados e discutidos na seção 5. Por fim, a última seção apresenta as considerações finais deste estudo.

REVISÃO DA LITERATURA

O crime cibernético

Dinâmico e em constante evolução, o crime cibernético é um crime econômico com amplitude global, de complexa identificação e rastreamento, com impactos variados, cujos riscos e recompensas diferem do crime convencional (Benson, McAlaney & Frumkin, 2018). Sua definição não é precisa e definitiva, tampouco sua tipologia e classificação (Gercke, 2014). São atividades ilegais realizadas mediante o uso da tecnologia, com objetivo de acessar ou comprometer sistemas computacionais (Burden & Palmer, 2003). Compreendem atos desonestos ou maliciosos, originados no ambiente virtual ou herdados do mundo real, e que são perpetrados na Internet, onde criminosos tem a sensação de facilidade, anonimidade, velocidade de operação e uma enorme quantidade de alvos (Burden & Palmer, 2003).

Originalmente, os crimes cibernéticos foram separados em dois grupos (Burden & Palmer, 2003): 1) atos criminosos já conhecidos no mundo real e que foram viabilizados no ciberespaço, tais como fraudes, roubos de informação, difamação, chantagem, pornografia, lavagem de dinheiro, violação da propriedade intelectual e terrorismo; 2) crimes cibernéticos puros, que compreendem atos desonestos ou mal-intencionados que não existiriam fora do ambiente virtual. Neste grupo, é possível citar vandalismo virtual, disseminação de vírus ou softwares maliciosos, ataques de negação de serviço, falsificação de endereços na Internet e envio de spam ou mensagens eletrônicas indesejadas (Burden & Palmer, 2003). Os meios utilizados para o crime, os danos provocados, a natureza das ações e suas motivações são fatores adicionais para classificação do crime cibernético (Safa, Maple, Watson & Von Solms, 2018).

O fator humano é considerado o elo mais fraco na cadeia da segurança cibernética (Shropshire, Warkentin & Sharma, 2015). Violações ou erros operacionais provocados pelos indivíduos contribuem para criar ou ampliar vulnerabilidades, as quais definem-se como a probabilidade de ocorrer um incidente indesejável quando não são tomadas medidas preventivas (Vance, Siponen, & Pahnila, 2012). Roratto e Dias (2014) definem vulnerabilidade como uma fraqueza dos sistemas de informação e do ambiente no qual estes estão inseridos, e esta fraqueza pode se tornar um risco de segurança. Neste sentido, a falta de consciência sobre ameaças eminentes denota um comportamento desalinhado com preceitos da segurança cibernética (Safa, Maple, Watson & Von Solms, 2018). A gestão da segurança cibernética, portanto, deve focar neste comportamento, considerando causas e consequências, pois o sucesso ou insucesso da organização depende daquilo que seus membros fazem ou deixam de fazer.

A ameaça interna é complexa devido a uma variedade de fatores que a tornam de difícil detecção até que provoque danos indesejados (Klein & Luciano, 2016). Tais ameaças podem ser analisadas sob três perspectivas comportamentais (Willison & Warkentin, 2013): 1) passivo e não volitivo, quando um *insider* está negligente, descuidado, desmotivado ou mal treinado, e age de forma não deliberada contra as normas e políticas de segurança da organização; 2) volitivo, porém sem motivação maliciosa, quando esse *insider* quebra regras de segurança em benefício próprio sem a intenção de produzir graves danos organizacionais; 3) maliciosamente intencional, quando o *insider* realiza ações imorais ou ilegais com objetivo de destruir, roubar,

CC BY

fraudar, prejudicar ou revelar informações sensíveis em benefício próprio ou de terceiros. Os *insiders* têm vantagens que vão além da capacidade de acesso à infraestrutura de TI. Eles estão cientes sobre as vulnerabilidades e as informações sensíveis: quais são, onde estão, quanto valem, como e quando acessá-las (Safa, Maple, Watson & Von Solms, 2018). Possuem tempo para atingir seus objetivos; e, não raro, conseguem ocultar rastros. Embora o fator humano demande atenção, a gestão da segurança cibernética ainda focaliza medidas de proteção puramente tecnológicas (Siponen, Mahmood & Pahnila, 2014).

Justiça organizacional

Profundas mudanças sociais e organizacionais que ocorreram nas últimas décadas (competitividade, globalização, incerteza, cenários de crise, indicadores econômicos e redução do emprego) contribuíram para a ampliação de conflitos sociais. Fatores organizacionais, tais como comunicação, cultura de segurança, política e estrutura organizacional, estão entre os motivos mais proeminentes para o comprometimento da segurança cibernética (Soomro, Shah & Ahmed, 2016). A vivência de situações de injustiça e sofrimento nas relações de trabalho intensificou a ocorrência de comportamentos negativos nas organizações (Mendonça & Mendes, 2005). Frente a uma injustiça vivenciada ou testemunhada, indivíduos utilizam estratégias comportamentais para restaurar a justiça (Kelloway, Francis, Prosser, & Cameron, 2010). E quanto maior é a percepção de injustiça, maior é a prevalência da retaliação organizacional (Mendonça & Tamayo, 2008). Diferentes opções de comportamento contraproducente podem ocorrer na tentativa de restaurar algum senso de equidade ou justiça (Kelloway et al., 2010).

Um ato de retaliação, represália, desforra ou desagravo objetiva, de maneira explícita ou sutil, provocar dano igual ou maior àquele recebido, e consiste em uma resposta à injustiça (Korsgaard, Meglino & Call, 2015). No ambiente de trabalho, percebe-se que a retaliação pode ser considerada uma estratégia do *insider* diante das situações de injustiça que, uma vez assim percebidas, geram sofrimento e sentimentos negativos. Mediante ações contraproducentes, membros da organização protestam contra injustiças que estejam no cerne de suas insatisfações (Kelloway et al., 2010).

A retaliação também pode ser um desdobramento de relações problemáticas e imprevisíveis em nível interpessoal e organizacional, merecendo atenção e esforços de pesquisa sobre suas causas e consequências. A qualidade de vida das pessoas no local de trabalho está relacionada com as características da estrutura física da organização, com a natureza das atividades realizadas, com as relações interpessoais desenvolvidas e com a percepção dos funcionários sobre a dinâmica sistêmica da organização (Mendonça & Tamayo, 2008). Decisões tomadas em relação a distribuição de recursos ou recompensas influenciam vivências de prazer ou sofrimento psíquico e, consequentemente, a própria qualidade de vida na empresa. Esse sofrimento está definido como um conjunto de experiências dolorosas (angústia, medo, insegurança) vividas com frequência por um ou mais indivíduos em um cenário de conflito entre as necessidades de gratificação e as respectivas restrições impostas pelas situações de trabalho (Mendonça & Tamayo, 2008).

Em diversos cenários organizacionais, busca-se compreender, em estudos de campo, as percepções e reações dos *insiders* sobre justiça e injustiça. Para analisar esse sentimento negativo adquirido por determinados *insiders*, a linha de pesquisa que estuda a questão da equidade ou justiça (*fairness*) é utilizada como referencial teórico. Neste sentido, quatro conceitos relacionados

CC BY

à percepção de equidade entre os *insiders* são agrupados sob a designação de Justiça Organizacional (Willison & Warkentin, 2013): 1) justiça distributiva, 2) justiça procedimental, 3) justiça interpessoal e 4) justiça informacional. Na literatura, as duas últimas agrupam-se, eventualmente, em uma dimensão única denominada justiça internacional.

O conceito de distribuição corresponde a um evento unilateral de alocação (destinação, designação ou divisão de elementos). É realizado por quem está além dos indivíduos envolvidos numa situação, com impacto direto na vida das pessoas, diferenciando-se de uma relação de troca, uma vez que esta última é um processo bilateral (Kazemi & Törnblom, 2014). Estudos sobre a teoria da equidade analisam quão equitativamente os distribuidores alocam recursos aos beneficiários. A equidade percebida está no cerne da justiça distributiva . As pessoas querem resultados equitativos para si mesmos e demandam que os outros, de forma equivalente, recebem recompensas e punições conforme suas contribuições ou infrações (Kazemi & Törnblom, 2014). O processo de distribuição deve apresentar equidade, igualdade ou equivalência; do contrário, é injusto.

A justiça procedimental estabelece procedimentos para regular as trocas e minimizar conflitos em um grupo social, assumindo que procedimentos considerados justos facilitam que o indivíduo assuma e aceite responsabilidades (Mendonça & Tamayo, 2008). A teoria da justiça processual (Leventhal, Karuza, & Fry, 1980) analisa os julgamentos sobre o processo ou o meio através do qual as decisões de alocação de recursos, bens ou benefícios são realizadas, estabelecendo que a equidade das políticas e práticas durante o processo de tomada de decisão têm grande relevância para as pessoas envolvidas (Simons & Roberson, 2003). Ao perceberem que os processos são justos, os trabalhadores tendem a demonstrar mais lealdade e disposição para agir em conformidade com os interesses e objetivos da organização; e, consequentemente, estarão menos propensos a trair a instituição e seus líderes (Jesus & Rowe, 2014). O reconhecimento intelectual e emocional de justiça motiva a cooperação para com a estratégia organizacional.

A qualidade do tratamento interpessoal que ocorre nos relacionamentos sociais entre indivíduos apresenta aspectos que determinam sentimentos de justiça ou injustiça, a partir da capacidade de julgamento dos indivíduos sobre a maneira que a comunicação e os procedimentos relacionados a tomada de decisão são encaminhados (Simons & Roberson, 2003). A justiça interacional refere-se ao tratamento interpessoal (Bies & Moag, 1986). A noção de justiça, nesta perspectiva, está fundamentada em valores, crenças e sentimentos em relação às ações humanas consideradas justas ou injustas. O comportamento das pessoas, durante as suas interações sociais, sofre influência de julgamentos sobre o que é certo ou errado, merecido ou não merecido e sobre direitos e deveres em geral. Quando um trabalhador percebe algum grau de injustiça nas relações interpessoais com seu interlocutor (um chefe ou colega que participa da interação social por meio da linguagem), ele pode reagir negativamente considerando aspectos cognitivos, afetivos e comportamentais (Korsgaard, Meglino & Call, 2015).

A justiça informacional, por sua vez, aborda a justificativa para decisões tomadas e de que maneira essas decisões foram comunicadas (Rego & Souto, 2004). Segundo os autores, trabalhadores esperam que seus líderes forneçam explicações lógicas, sinceras e adequadas sobre as decisões que são tomadas em âmbito organizacional; especialmente, quando produzem efeitos desfavoráveis. Ao fornecer justificativas aceitáveis, as reações negativas frente a percepção de injustiça informacional são reduzidas.

CC BY

Sentimentos humanos

Sentimentos surgem por estímulos ao sistema sensorial humano, produzindo sensações ou percepções. Atividades neurais relacionadas ao processamento e armazenamento de informações produzem efeitos periféricos no organismo humano. Alterações neurais e hormonais decorrentes geram condições psicológicas que são denominadas como as emoções das pessoas (Feelings, 1998). Conforme este autor, sentimentos podem produzir efeitos observáveis: a felicidade pode produzir o riso; todavia, o riso não explica a felicidade. Eles são reconhecidos pelo indivíduo quando ocorrem. São positivos ou negativos, promovendo uma condição de aproximação ou rejeição.

Os sentimentos parecem ter surgido para retratar situações fisiológicas, facilitando a aprendizagem das condições de desequilíbrio, antecipando futuros estados favoráveis ou adversos (Damasio & Carvalho, 2013). O tema é pesquisado com profundidade na Psicologia e na Psiquiatria, e com razoável atenção no campo da Sociologia e Antropologia. No âmbito do interesse desta pesquisa, a literatura prévia considerada trata dos sentimentos humanos sob a perspectiva da Psicologia orientada para o campo da gestão das organizações. Partindo dessa abordagem teórica, os sentimentos humanos são reflexos de uma representação mental da realidade, e não uma cópia da realidade tal como ela pretensamente seja de fato.

Sentimentos são sensações corporais, próprias da espécie humana, derivadas das contingências, e a sua denominação é determinada pela aprendizagem e tem origem social (Skinner, 1974): O sentimento pode ser uma sensação oriunda do tato ou pode ser fruto de uma relação com o ambiente, o qual é percebido mediante a capacidade de o indivíduo responder ao mundo conforme sua percepção e disposição analítica. O sentimento ocorre em virtude de um acontecimento (Skinner, 1995). "Não choramos porque estamos tristes, ou sentimos tristeza porque choramos; choramos e sentimos tristeza porque alguma coisa aconteceu" (Skinner, 1995, p. 2). Ao observar e discriminar os próprios sentimentos, pode-se inferir o sentimento de outra pessoa diante das situações que ocorreram em seu ambiente social.

Experiências emocionais, sejam positivas ou negativas, sua frequência e eventualmente intensidade, demarcam noções sobre o bem-estar individual, fundamental para a concepção de saúde (Siqueira & Padovam, 2008). As emoções ruins são reações de eventos específicos, e indicam o grau de importância que tal evento adquire para o indivíduo (Schwarz & Clore, 1996). A reação é consequência de uma avaliação do evento conforme objetivos pessoais relacionados ao bem-estar. Aversão, raiva ou medo são exemplos de uma reação a circunstâncias que refletem danos, perdas ou ameaças.

Elementos inerentes ao meio ambiente determinam um entendimento sobre a qualidade de vida, um julgamento sobre níveis de satisfação e o desenvolvimento de aspirações versus realidade (Siqueira & Padovam, 2008). O espaço onde situa-se o indivíduo aumenta ou reduz o bem-estar. O surgimento de emoções negativas está relacionado à discordância com decisões gerenciais, ao desconforto gerado pelo comportamento dos colegas, ao desgaste físico e mental causado pelo excesso de trabalho, bem com ao estresse derivado dos níveis de exigência e desempenho que estão no âmbito das expectativas e políticas da empresa (Siponen, Mahmood & Pahnila, 2014). Sentimentos ruins desdobram-se de um estado emocional negativo prévio, frequentemente oriundo de experiências malévolas anteriores (ameaças, brigas, abusos, rejeições), as quais tornam o indivíduo propenso a intenções hostis (Korsgaard, Meglino & Call, 2015). Portanto, ao sentir-se ameaçado, o indivíduo desenvolve um conjunto de emoções ruins que estimulam algum grau de agressividade.

CC BY

Motivações para o crime cibernético

A palavra motivo origina-se do latim "*moveres*" ou "*motum*", que significa aquilo que faz mover. Motivar significa provocar movimento, atividade no indivíduo, e diz respeito à energia, direção, persistência e equifinalidade, direcionando o indivíduo a fazer alguma coisa. A motivação refere-se a um processo voluntário e guia as decisões sobre o engajamento em atividades particulares (Deci & Ryan, 2008).

As pessoas motivam-se conforme um senso particular de comprometimento, ou pelo medo de estarem sendo vigiadas (Deci & Ryan, 2008). Viabilizam suas ações a partir de aspirações, pretensões ou interesses pessoais legítimos. Alternativamente, movimentam-se por estímulos externos, como ameaças, chantagens, culpas, subornos ou gratificações ilícitas. Apenas um desejo não é suficiente. É preciso ter as capacidades, habilidades e ferramentas para atingir metas, levando em consideração oportunidades e custos inerentes (Shropshire, Warkentin & Sharma, 2015). A ponderação entre capacidades, oportunidades e interesses subjacentes estabelece uma intenção criminal.

Com origem nos estudos sobre agressividade humana, a ideia de atos contraproducentes no âmbito das organizações vem sendo investigada a partir de diferentes abordagens comportamentais: abusos contra outrem, desvios de produção ou sabotagem, roubo ou furto, afastamentos ou algum tipo de ausência do trabalho (Benson, McAlaney & Frumkin, 2018). Em determinadas circunstâncias, aspectos organizacionais estimulam a violação das regras estabelecidas e a frustração de expectativas. Tal motivação pode ser autônoma ou controlada (Deci & Ryan, 2008). O primeiro tipo compreende motivações intrínsecas e extrínsecas do ser humano, quando as pessoas correlacionam ações aos seus valores fundamentais. A motivação na forma autônoma oferece a experiência de volição (vontade, não acidental, inerente a um processo cognitivo de querer pelo qual se decide praticar uma ação) e de auto aprovação das realizações. O segundo tipo possui regulação externa, mediante um esquema de recompensas ou punições. Trata-se de um controle internalizado e impulsionado por fatores como aprovação, vergonha, ego e autoestima (Deci & Ryan, 2008). Neste caso, existe um sentimento de pressão para pensar, sentir ou proceder de acordo com determinada orientação.

Frustração, estresse, raiva ou descontentamento, envolvendo elementos psicológicos, financeiros e sociais, motivam pessoas a tomar o caminho da criminalidade cibernética, utilizando habilidades e conhecimentos em prejuízo de terceiros (Arpad, 2013). Violações de políticas de segurança podem ser realizadas por indivíduos com status de confiança (Dhillon, 2001). Segundo o autor, essas pessoas praticam o crime cibernético em virtude de fatores pessoais e profissionais, aproveitando oportunidades específicas.

Crimes cibernéticos envolvem intenções antecedentes ao ato criminoso (Rasmi & Jantan, 2013). A motivação para o crime é definida como um desejo de se envolver em comportamentos indesejáveis e condenáveis relativos ao crime, sobrepondo eventuais condições restritivas (Soomro, Shah & Ahmed, 2016). Intenções são equivalentes a planos orientados para alcançar um objetivo específico.

O impulso para o crime cibernético advém de demandas pessoais, que se ativam na direção da prática ilegal e imoral, conforme a influência de visões, anseios, ambições, expectativas, vivências e experiências passadas. As pessoas são atraídas para o desvio, pois é gratificante. Em sentido oposto, o autocontrole explica qual seria a probabilidade de engajamento nesse tipo de ato (Soomro, Shah

CC BY

& Ahmed, 2016). O ato que viola considera dois fatores importantes: a recompensa final e o risco envolvido. Diferenças individuais na atitude frente ao risco influenciam a intenção de transgredir.

As motivações que levam pessoas a cometer crimes cibernéticos podem agrupar-se em categorias conforme suas características (Rogers, 2006). Estas categorias compreendem habilidades e motivações de acordo com o Quadro 1.

Quadro 1. Habilidades e Motivações de Criminosos Cibernéticos

Tipo, Características e Motivações dos Criminosos Cibernéticos
[1] Novatos: Indivíduos sem muita experiência na computação e no desenvolvimento de sistemas. Buscam emoções e satisfação do ego. Querem ser aceitos em grupos sociais, provando seu valor e competência. Desejam aceitação como membros de gangues urbanas.
[2] Punks cibernéticos: Possuem conhecimentos de computação e linguagens de programação. Envolvem-se em vandalismos virtuais, tais como desfiguração de *websites*, envio de *spam*, roubo de dados de cartão de crédito e fraudes nas telecomunicações (violação de privacidade e ligações gratuitas). Desejam atenção da mídia para obter fama e notoriedade. Em alguns casos, ganho monetário. Quando são capturados, almejam sucesso posterior prestando consultoria na área da segurança cibernética.
[3] *Insiders* (colaboradores internos à organização): Trata de uma categoria menos publicitada que representam alto risco. São funcionários descontentes ou ex-funcionários (alguns da área de TI) que violam as regras e a confiança que lhes foi atribuída, usando privilégios de acesso para realizar ataques contra a sua organização. Possuem algum nível de habilidade. A motivação mais citada é a vingança ou a revanche.
[4] Pequenos Ladrões: A pirataria é um dos métodos de promover atividades criminosas. Estas pessoas não estão interessadas em notoriedade pública. Ao contrário, a fama seria perigosa. Este grupo foi atraído à tecnologia e à Internet, pois os alvos potenciais migraram para o ciberespaço (bancos, operadoras de cartões de crédito, pessoas ingênuas). Exibem boas habilidades técnicas. A necessidade de ganhos fáceis é a principal motivação. É típico desse grupo o desejo de enriquecer, a ganância e, em alguns casos, a vingança.
[5] *Hacker da Velha Guarda*: Eles não demonstram intenção criminosa, embora desrespeitem a propriedade pessoal e/ou intelectual. São amantes da ideologia dos primeiros hackers, orientados para uma diferenciação intelectual. Este grupo tem habilidades técnicas profundas e, muitas vezes, escrevem os códigos que são usados por criminosos menos qualificados. As principais motivações são curiosidade e desafio intelectual.
[6] Criminosos profissionais: São profissionais que orientam suas capacidades e habilidades em prol do crime. Tem alto grau de perspicácia técnica e preparo psicológico. Integram organizações criminosas. São especializados em espionagem corporativa, são bem treinados, e tem acesso ao estado-da-arte da tecnologia. Motivam-se por dinheiro e ganhos financeiros. Não estão interessados na fama ou publicidade. Buscam uma espécie distorcida de orgulho profissional.
[7] Guerreiros da Informação: Pessoas especializadas em defesa ou ataques para a perturbação e desestabilização social de comunidades ou países, focando em organismos ou instituições de controle e tomada de decisão. O grupo envolve-se em guerras cibernéticas patrocinadas por Estados ou nações. São altamente treinados e qualificados, possuindo acesso ao estado-da-arte da tecnologia. Essas pessoas normalmente são motivadas pelo espírito de patriotismo.

Fonte: Adaptado de Rogers (2006).

PROPOSTA DE UM MODELO CONCEITUAL

Os elementos, as relações e os significados contidos (implícita ou explicitamente) nesta pesquisa são ilustrados na Figura 1. Eles emergiram a partir da análise detalhada da literatura e das reflexões realizadas pelos pesquisadores e, consequentemente, foram estudados em profundidade para um melhor entendimento do fenômeno.

CC BY

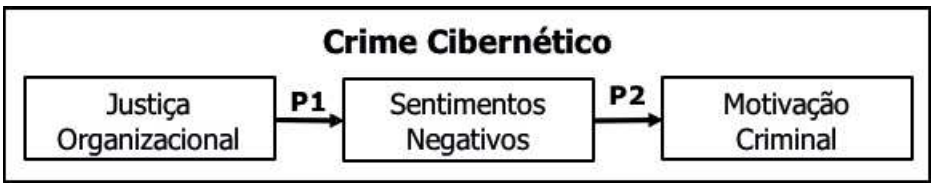

Figura 1. Modelo Conceitual

Estudos relacionados à qualidade de vida no local de trabalho constataram que o descontentamento dos trabalhadores impacta diretamente nas atitudes e no comportamento destes indivíduos em relação a organização (Willison & Warkentin, 2013). Através da percepção sensorial, utilizando seus sentidos e sua inteligência, um indivíduo é capaz de reconhecer, interpretar e compreender informações oriundas do meio (Feelings, 1998). Ao receber e decodificar sinais exteriores, o indivíduo atribui significados aos dados analisados e organizados conforme suas crenças, valores éticos e princípios morais (Schwarz & Clore, 1996). Essas percepções sofrem influências das características culturais presentes em um determinado grupo social.

Com base nisso, a seguinte proposição foi elaborada:

Proposição 1 (P1): A percepção de injustiça, no contexto organizacional, produz sentimentos negativos no indivíduo.

Sentimentos negativos gerados pela percepção de injustiça no contexto organizacional podem levar a condutas indesejadas contra a empresa e seus gestores (Benson, McAlaney & Frumkin, 2018). A percepção de injustiça na distribuição de recompensas e reconhecimentos, na vivência ou participação em processos organizacionais, na relação interpessoal com superiores e colegas, ou mesmo na qualidade da comunicação produz diferentes intensidades emocionais de dor, mal-estar, desconforto, ansiedade, aflição frustração, culpa, raiva, entre outros estados psíquicos de sofrimento (Willison & Warkentin, 2013). Conforme as características psicossociais de cada indivíduo, esses sentimentos negativos podem adquirir maior ou menor importância na motivação para a prática de atos ilegais ou imorais, como é o caso do crime cibernético.

O modelo conceitual proposto neste trabalho apresenta o crime cibernético praticado por *insiders* tendo relação indireta com a percepção de injustiças no contexto organizacional. Esse entendimento é defendido nas pesquisas de Willison e Siponen (2009) e Willison e Warkentin (2013) sobre descontentamento das pessoas em seu local de trabalho. A redução dos incidentes de segurança cibernética, então, dependeria de estratégias de gestão que minimizassem a ocorrência de injustiças distributivas, procedimentais, interpessoais ou informativas.

Quando o gestor desconhece as motivações que levaram pessoas da sua própria organização a praticar crimes cibernéticos, sua capacidade de interferência ou influência diminui. Quando ele compreende os fatores estimuladores que extrapolam as características e patologias individuais, mudanças no local de trabalho podem ser encaminhadas para que os sentimentos negativos não evoluam facilmente. Entender o comportamento potencialmente nocivo das pessoas oferece melhores condições para gerenciar os riscos pertinentes ao crime cibernético no âmbito organizacional (Klein & Luciano, 2016).

Com base nisso, a seguinte proposição foi elaborada:

Proposição 2 (P2): Os sentimentos negativos do indivíduo influenciam a sua motivação criminal.

CC BY

A coleta e a análise de dados foram pensadas com base nesta proposta de modelo conceitual, sem negligenciar o contexto em que se situam as variáveis estudadas.

PROCEDIMENTOS METODOLÓGICOS

Este trabalho foi desenvolvido com base em uma pesquisa qualitativa, de caráter exploratório, atitudinal, com corte transversal. Foi utilizada a técnica de entrevista individual aberta com apoio de um roteiro semiestruturado. Especialistas em segurança cibernética foram entrevistados. A seleção dos participantes da pesquisa foi não probabilística e intencional, de modo a possibilitar uma seleção apurada de entrevistados dentre a população de interesse. Por se tratar de um assunto delicado, e muitas vezes tratado com confidencialidade em muitas organizações, a escolha dos depoentes foi baseada na confiança depositada nos entrevistadores e dos contatos que estes tinham com membros do universo pesquisado. Para tanto, um dos pesquisadores participou de eventos relacionados ao tema, de forma a estabelecer ou estreitar contatos com aqueles que viriam a ser os respondentes. Igualmente, foi utilizada a técnica denominada de bola de neve de modo a se criar uma maior proximidade entre a equipe de pesquisa e os entrevistados. Outro cuidado metodológico que os autores deste estudo tiveram refere-se à validação prévia do roteiro de entrevista junto à especialistas na área. Consequentemente, ajustes necessários foram incorporados à versão final do instrumento utilizado na coleta de dados.

No que se refere ao perfil dos participantes, todos foram selecionados conforme seu nível de conhecimento, experiência e capacidade. Os entrevistados tinham mais de cinco anos de experiência na área de segurança cibernética e mais de dez anos de experiência na área de TI. Metade dos entrevistados trabalhavam na área há mais de 10 anos, atuando como consultores, gerentes, instrutores, professores, analistas ou investigadores ligados a área, possuindo certificações e títulos acadêmicos que atestavam algum grau de excelência no campo da segurança cibernética. Com vasta bagagem de conhecimento, experiência e capacidade, os entrevistados foram percebidos, e por isso selecionados pela equipe de pesquisa como potenciais contribuintes desta investigação.

Dezesseis entrevistas foram realizadas, sendo utilizado o critério de saturação dos dados para a compreensão do fenômeno estudado. O grupo de entrevistados possui uma bagagem de histórias profissionais que ajudaram a aprofundar a compreensão sobre questões humanas, tecnológicas e operacionais que se relacionam no campo da segurança cibernética. Cada entrevistado assinou um termo de confidencialidade que garante o sigilo dos dados coletados e sua finalidade exclusivamente acadêmica.

Os encontros foram presenciais (reuniões previamente agendadas) e virtuais (via conferência utilizando o aplicativo Microsoft Skype). As reuniões presenciais ocorreram na cidade de Porto Alegre (RS). As entrevistas virtuais foram feitas com participantes de São Paulo (SP). Todas as entrevistas foram realizadas durante o mês de fevereiro de 2016, totalizando aproximadamente 12 horas de gravação, transcritas em 170 páginas de conteúdo.

A Figura 2 apresenta as principais etapas desenvolvidas durante o andamento desta pesquisa.

CC BY

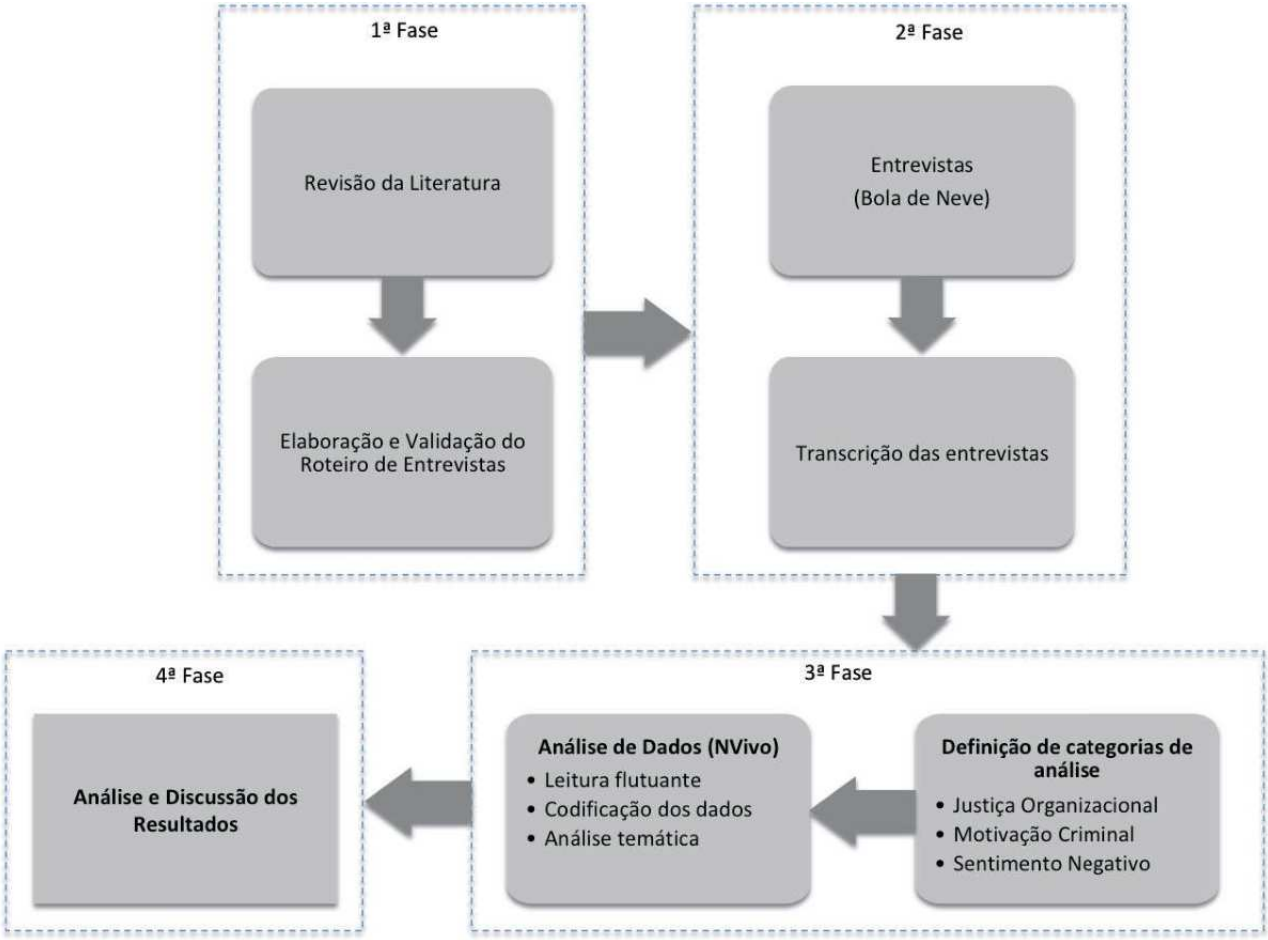

Figura 2. Desenho de Pesquisa

As entrevistas gravadas foram transcritas, e seu conteúdo analisado em três fases (Bardin, Reto, & Pinheiro, 1979). Uma leitura flutuante (1) do material foi realizada, bem como um tratamento preliminar de resultados. Em seguida (2) os dados foram codificados a partir do conteúdo registrado. Por fim, (3) uma análise temática foi efetuada, na qual categorias emergiram a partir da sensibilidade dos pesquisadores, contribuindo para a produção de significados acerca do conteúdo analisado (Bardin, 2011). Também buscou-se explicar e relacionar conceitos subjacentes ao tema para que fosse possível compreender o fenômeno de maneira precisa e aprofundada.

O trabalho de exploração e categorização do conteúdo das entrevistas foi realizado com auxílio do software NVIVO. Nas dezesseis transcrições analisadas, foram identificadas e codificadas, com apoio da revisão de literatura, diferentes categorias: três para o constructo de Justiça Organizacional, vinte e cinco para o constructo Motivação Criminal (com seis subcategorias adicionais), e vinte e nove para o constructo denominado Sentimentos Negativos.

ANÁLISE E DISCUSSÃO

Poucos são os estudos acerca do crime cibernético que consideram aspectos relacionados ao local de trabalho e às respectivas percepções de injustiça que possam emergir. Willison e Warkentin

CC BY

(2013) reconhecem esta lacuna e buscaram enfatizar a relevância dos fatores contextuais na produção de sentimentos negativos. É nesse sentido que emergem relações importantes entre os crimes cibernéticos motivados por sentimentos negativos e as percepções de justiça distributiva, justiça procedimental, justiça interacional e informacional.

Com o avanço do conhecimento neste campo, observou-se que elementos relacionados aos sentimentos negativos adquiridos no local de trabalho também exerciam impacto (positivo ou negativo) na motivação das pessoas. Nesta pesquisa, colocações relevantes relacionadas aos conceitos de justiça distributiva, justiça procedimental, justiças interacional e informacional emergiram quase que naturalmente. Os informantes referiram-se a questão da injustiça percebida pelos indivíduos no contexto organizacional, e como essa percepção fornecia energia para o engajamento em atos de retaliação. A percepção de injustiça como elemento motivador de um comportamento indesejado no âmbito organizacional está em sintonia com as análises e proposições de Kelloway et al. (2010).

Sentimentos de raiva, ultraje ou ressentimento que surgem em consequência de decisões organizacionais ou ações gerenciais julgadas injustas fornecem o estimulo para a retaliação. Na visão de vários informantes, a vingança tem participação decisiva na motivação para o crime cibernético. Focando especificamente na falta de equidade sobre rendimentos financeiros no âmbito da justiça distributiva, o Entrevistado 16 relata:

> Tem gente que não entende que o cara do lado, por algum motivo, ganha mais do que ele.

No que tange às percepções de injustiça procedimental, os dados analisados sugerem que sentimentos negativos capazes de motivar o crime cibernético igualmente são gerados em eventos onde o indivíduo percebe que foi injustiçado em processos organizacionais. Conflitos nas relações interpessoais produzem intensos sentimentos negativos. Raiva é o principal deles, quando relações conflitosas se encaminham para a demissão de funcionários ou para o desligamento de prestadores de serviços internos. E com raiva, as pessoas tendem a buscar alguma vingança, retaliando as organizações onde vivenciaram desavenças, desrespeito ou desconsideração de superiores ou colegas de trabalho. O Entrevistado 4 relata que:

> É bastante comum a questão de revolta no sentido de vingança, relativo à alguma situação anterior, algum mal-entendido [...]. E aí envolve também a questão do crime contra a honra, injúria, calúnia e difamação.

Sentimentos negativos adquiridos pelos indivíduos podem motivar a perpetração do crime cibernético contra organizações, especialmente nos casos em que tais sentimentos foram adquiridos em circunstâncias organizacionais apreendidas, avaliadas subjetivamente e declaradas como injustas (Willison & Warkentin, 2013). Raiva, frustração, mal-estar ou algum tipo de sofrimento emergem na experiência de uma injustiça distributiva, procedimental ou interpessoal. A literatura prévia elenca sentimentos negativos, os quais foram destacados pelos participantes da pesquisa. Feelings (1998), cita exemplos e estabelece cinco principais atributos relacionados aos sentimentos humanos. Damasio e Carvalho (2013), por sua vez, declaram o impacto que essas emoções produzem no comportamento das pessoas.

A baixa-estima, que denota uma avaliação ruim de si mesmo, está presente em trechos de alguns dos entrevistados. O Entrevistado 2, por exemplo, cita problemas relacionados a autoestima originados em relações conflituosas no trabalho:

CC BY

> Situações onde a pessoa quer se afirmar pessoalmente ou profissionalmente, ela quer mostrar que tem mais conhecimento que o outro, então ela pega e... ah, eu tenho acesso a essa tabela da base de dados [...], ah, eu consigo autenticar naquele servidor [...]. E baseada nessa falta de conteúdo, de formação e de educação queriam se autopromover.

Outra emoção que emergiu na coleta de dados, refere-se à frustração que emerge quando algo esperado não ocorreu e/ou quando um objetivo não é atingido, ou ainda, quando demandas, necessidades ou desejos não são realizados e/ou impedidos por circunstâncias específicas. O Entrevistado 5 relata que situações relacionadas ao local de trabalho com frequência produzem o sentimento de frustração. O tamanho dessas sensações, dependendo das características do indivíduo podem levar a consequências indesejadas, como é o caso do crime cibernético. Explicitado pelo Entrevistado 16, o impacto do local de trabalho no sentimento de frustração que é experimentado por alguns *insiders* é ilustrado na sua fala:

> O ambiente de trabalho influencia? Sim, quando o ambiente não dá o retorno que a pessoa espera – só que isso é uma percepção pessoal- a pessoa passa o sentimento de que você também não merece nada meu.

A culpa é uma emoção que produz desdobramentos imprevisíveis, especialmente no escopo desta pesquisa. Ela integra a relação de sentimentos ruins que atuam sobre o bem-estar do indivíduo (Siqueira & Padovam, 2008), e pode aparecer em seu repertório de experiências emocionais vividas no local de trabalho. Guilhardi (2002) destaca o papel desse sentimento com profundos desdobramentos sociais. Trata-se de uma consciência penosa de ter descumprido um compromisso social, religioso, afetivo, moral ou institucional. O indivíduo reavalia um comportamento passado e considera-o reprovável. Na visão do Entrevistado 16, ao invés da presença desse sentimento, exatamente a sua ausência pode fornecer energia para uma motivação criminal no contexto organizacional:

> Se uma pessoa não tem medo das consequências e ela não tem sentimento de culpa nenhum, ela vai fazer.

Se a organização fornece elementos que desagradam o indivíduo (injustiças distributivas, procedimentais ou interpessoais), somados ao fato de que a pessoa não possui gratidão ou reconhecimento de valor perante a empresa, o chefe ou colegas de trabalho, a prática de crimes cibernéticos pode evoluir sem qualquer remorso ou arrependimento. Sem culpa e pessoa realiza o crime cibernético, conforme ainda pondera o Entrevistado 16.

Nesta pesquisa, foram levantadas diversas motivações analisadas pela literatura. Após a coleta de dados, os pesquisadores analisaram as entrevistas buscando identificar essas e outras motivações que pudessem emergir. A vingança foi a motivação que apareceu com mais frequência nas falas dos informantes. Para vários participantes, sentimentos ligados a raiva e frustração, oriundos da percepção de injustiça nas relações interpessoais, motiva intensamente trabalhadores a retaliarem a sua organização mediante um crime cibernético. Brigas com o chefe, demissões ou mesmo disputas de poder aparecem como principais fatores estimuladores da vingança. As passagens abaixo atestam essa visão:

> A gente já pegou casos, por exemplo, onde era um cara se vingando, ou um cara que sabia que ia ser demitido (Entrevistado 1).

CC BY

> Saiu mordido, não recebeu o que tinha que receber, o cara se sentiu excluído ou se sentiu injustiçado. E ele, de uma forma ou de outra, disse [...]. Ah, os meus acessos na empresa ainda não foram cortados, vou lá e vou detonar (Entrevistado 5).

A segunda motivação para o crime cibernético que mais foi lembrada pelos informantes é a oportunidade. Willison e Warkentin (2013) apresenta um modelo denominado Estrutura do Crime Específico de Oportunidade, o qual mapeia elementos formadores da oportunidade para o crime. Ele analisa potenciais infratores em um ambiente de trabalho, considerando que existe uma tomada racional de decisão para o crime, influenciada pelas oportunidades e a respectiva relação de custo e benefício que o contexto oferece num dado momento. Na fala de alguns informantes, um *insider* que eventualmente já adquiriu sentimentos negativos, aproveitando o surgimento de uma oportunidade específica ou explorando uma condição especial relativa ao seu cargo, promove um crime cibernético:

> O cara da TI normalmente tem acesso a tudo, ou no mínimo ele tem acesso a um conjunto de ativos importantes naquele ambiente; e ele se sente com o poder de fazer o que ele bem entender na empresa (Entrevistado 6).

Nas palavras do Entrevistado 13:

> Então, eu acho que o risco, principalmente para TI, ocorre quando eu tenho o fator acesso à informação ou aos meios para executar o crime, esse incidente [...]. Teve um caso de uma pessoa de RH que autorizou a si própria um empréstimo que ela não tinha direito. Por quê? Porque ela tinha poder para isso, ela tinha as ferramentas para isso.

Relações pessoais com criminosos influenciam a prática de crimes cibernéticos na visão de alguns participantes. A associação diferencial estabelece que influências para o comportamento criminal advém de relacionamentos sociais iniciados fora do contexto organizacional. O principal constructo dessa abordagem é a Determinação Favorável ao Crime, que pode ser mensurada pelo grau de supervisão familiar; intensidade de coesão nos grupos de amizades; existência de amigos que foram, em algum momento, pegos pela polícia; percepção dos jovens acerca de outros jovens na vizinhança que se envolvem em problemas; e se o jovem mora com os dois pais.

Rebellon et al. (2010) tratam essa questão, inclusive propondo o conceito da Vergonha como inibidor da motivação criminal. Essas interações sociais negativas estão dentro da própria organização. *Insiders* podem ser influenciados por outros *insiders*. Normalmente, variáveis de contexto, tais como a situação da empresa ou as práticas usuais de tratamento interpessoal, estimulam alguns indivíduos a cometer crimes cibernéticos na empresa. Segundo o Entrevistado 3:

> São das pessoas que são suscetíveis, são pessoas que dependendo de quem chega na orelha dela, ela vai pender para um lado ou para o outro. E essas pessoas são um risco ao negócio [...]. Se um mal-intencionado chegar nela, vai conseguir manipular ela e fazer com que essa pessoa seja cúmplice de uma fraude interna.

O Entrevistado 15 reforça:

> Tinha umas falcatruas. Os caras eram bons, tecnicamente eram bons, só que eles queriam proteger a empresa deles de uma maneira, tipo assim, ninguém podia entrar na panela.

CC BY

A impunidade pode ser uma importante motivação para o crime cibernético, na medida em que desperta a sensação de que não haverá a punição ou está será insuficiente, eventual ou branda. Son (2011) corrobora com essa probabilidade ao referenciar a teoria da dissuasão (GTD), que foi desenvolvida para explicar o envolvimento das pessoas com atividades indesejadas mediante um comportamento desviante. A GTD postula que os indivíduos são menos propensos a cometer crimes quando os riscos de serem capturados e punidos aumenta. A certeza das sanções age como inibidor das práticas ilícitas, na medida em que influencia o comportamento do indivíduo e o custo e benefício calculados para tomar a decisão pelo crime.

> A internet tem muito aquele sentimento de terra sem lei, que aquilo que eu vou fazer na internet não dá nada [...]. A legislação brasileira, mesmo com a nova lei [Marco Civil da Internet], que até nem ajuda muito em relação a isso, ela é muito frágil nesse sentido. (Entrevistado 2).

O Entrevistado 8 ainda ressalta:

> A minha experiência aqui dentro da empresa é a sensação de impunidade. A sensação de que não vai acontecer nada. Não existe uma exposição do funcionário, justamente por questões legais.

A partir das entrevistas realizadas e da comparação com a literatura, algumas relações são propostas com base no modelo conceitual apresentado na seção 3. Pode-se pressupor que as percepções e sensações de injustiça no âmbito distributivo, procedimental, interpessoal e informacional produzem baixa-estima, frustração e podem reduzir o sentimento de culpa dos funcionários em relação a organização. Tais sentimentos estimulam a vingança e a ganância, reforçada por oportunidades, costume, associação ou impunidade no local de trabalho.

Com base nos relacionamentos identificados acerca do fenômeno estudado, foi desenvolvido uma nova proposta de modelo conceitual, derivada de um refinamento do modelo original (Figura 1). A principal alteração neste modelo conceitual refinado foi o foco nas variáveis relevantes de cada constructo, conforme ilustra a Figura 3.



Figura 3. – Modelo Conceitual Refinado

As proposições anteriormente sugeridas sofreram então alterações para adequação com a realidade organizacional observada nesta pesquisa.

Proposição 1 (P1): A percepção de injustiça, no contexto organizacional, produz no indivíduo, sentimentos negativos, tais como a baixa-estima, a frustração e a ausência de culpa;

CC BY

Proposição 2 (P2): Sentimentos negativos, tais como a baixa-estima, a frustração e a ausência de culpa, motivam as pessoas a cometer crimes cibernéticos nas organizações onde trabalham.

A capacidade de antecipar um evento, no que tange o crime cibernético perpetrado por *insiders*, se dá mediante a investigação de tendências, a análise de atitudes e comportamentos. Trata-se de construir relacionamentos interpessoais positivos, e colaborar pelo desenvolvimento de processos organizacionais e sistemas de distribuição de recompensas e reconhecimentos baseados na justiça, na transparência, na imparcialidade e no respeito a igualdade de direitos. A ideia principal é diminuir o descontentamento dos *insiders* para que se limite a retaliação contra a organização. Trata-se de trabalhar na reversão de situações desfavoráveis, quando circunstâncias provocam frustrações e decepções. A gestão dos conflitos e das limitações financeiras, materiais e humanas é parte da gestão da informação da mesma forma que a gestão de pessoas na organização deve considerar aspectos mais profundos da relação daquele indivíduo com a organização.

As organizações são espaços complexos assim como o são os indivíduos. Portanto, é necessário entender o indivíduo na organização como parte de uma complexa rede de pessoas, processos, estratégias, tecnologias, mas também de sentimentos e frustrações. A informação da organização, sendo um ativo vital, pode ser utilizada para que um funcionário extravase um descontentamento (Klein & Luciano, 2016) não gerenciado.

Considerando que a TI não é neutra, mas sim política e social, a gestão da informação e do ambiente de TI organizacional deve considerar que a própria TI, suas regras e o impacto que esta gera na identidade do funcionário, pode gerar sentimentos negativos que, em um ciclo vicioso, afetem a segurança cibernética da organização.

CONSIDERAÇÕES FINAIS

Esta pesquisa analisou como as percepções de injustiça organizacional motivam *insiders* a cometer crimes cibernéticos nas organizações onde trabalham. Conforme estudos anteriores (Kelloway et al., 2010; Mendonça & Tamayo, 2008; Willison & Warkentin, 2013), elementos relacionados ao local de trabalho podem desenvolver sentimentos negativos que motivariam a prática do crime cibernético. Esses elementos estão relacionados a percepções de injustiça que indivíduos desenvolvem sobre a falta injustificável de equidade em decisões gerenciais, na correção, lisura e retidão de políticas e práticas gerenciais e na qualidade e respeito do tratamento interpessoal predominante no local de trabalho mediante uma comunicação clara, precisa e transparente.

As diferentes percepções identificadas entre os entrevistados deste estudo, associadas à revisão da literatura referente ao tema, permitiu que se chegasse a um modelo conceitual detalhado o qual deve ser futuramente testado. Nele, foram identificados três grandes constructos (justiça organizacional, sentimentos negativos e motivação criminal), suas inter-relações, e as proposições sugeridas foram estabelecidas com base na pesquisa exploratória realizada.

Nesta pesquisa, a vingança e a ganância foram identificados como sendo os principais fatores motivacionais para o crime cibernético, com uma participação importante e complementar de elementos relacionados à oportunidade, ao costume, à associação e, principalmente, à impunidade. A expectativa de que não haverá punição se um crime for cometido se configura um determinante. Estes fatores são alavancados por sentimentos negativos (baixa-estima, frustração e ausência de culpa) que são produzidos pela percepção de injustiça organizacional.

CC BY

No que se refere às contribuições acadêmicas deste estudo, ressalta-se que a literatura prévia sobre a relação entre as percepções de injustiça no âmbito organizacional e a motivação para o crime cibernético é restrita (e no Brasil é praticamente inexistente). A proposta de relacionar aspectos de justiça organizacional e de motivação criminal apresenta um novo enfoque de pesquisa ainda pouco explorado. Assim, a investigação de um escopo específico sobre a problemática da segurança cibernética, representa um valor agregado para a área de gestão da informação.

Quanto às contribuições práticas desta pesquisa destaca-se a possibilidade do modelo conceitual proposto oferecer subsídios para a criação de mecanismos preventivos acerca de incidentes de segurança, ou ainda de ataques internos por meio da gestão de pessoas. Da mesma forma, os resultados deste estudo possibilitam que se crie diretrizes para apoiar a manutenção e o equilíbrio no âmbito da justiça distributiva, procedimental, interpessoal e informacional.

Como limitação desta pesquisa, temos o fato da utilização de uma amostra não probabilística, que apesar de ser adequada para um estudo exploratório de cunho qualitativo, não permite a generalização dos resultados alcançados. Contudo, as descobertas realizadas nesta pesquisa podem estimular outros pesquisadores a continuar percorrendo um caminho que ainda necessita ser explorado.

O comportamento humano é complexo, dinâmico e imprevisível, e sofre as mais diferentes influências de ordem educacional, social, ética, moral, cultural e temporal. Neste sentido, os pesquisadores sugerem a realização de estudos futuros que possam contribuir com o conhecimento no campo da segurança cibernética e da gestão da informação, que contemplem os seguintes enfoques de investigação científica: (a) Validar o modelo conceitual proposto, bem como implementação de pesquisa quantitativa com teste de hipóteses que tenham como base as proposições sugeridas; (b) Considerar a natureza da organização e o local de trabalho. Isso se deve ao fato de que diferentes organizações podem apresentar diferentes fatores relacionados à justiça organizacional que, por sua vez, podem gerar sentimentos negativos, os quais motivam o indivíduo à prática de crimes cibernéticos; (c) Definir como unidade de análise o criminoso. Contudo, ressalta-se que para tanto, uma pesquisa multidisciplinar seria mais apropriada, uma vez que são necessários ferramentais e conhecimentos avaliativos provenientes dos campos da psicologia, psiquiatria, sociologia e/ou antropologia.

AGRADECIMENTOS

Os autores agradecem o apoio prestado pela CAPES (Brasil).

REFERÊNCIAS

Arpad, I. (2013). A greater involvement of education in fight against cybercrime. *2nd World Conference on Educational Technology Research, 83*, 371-377.

Bardin, L. *Análise de conteúdo*. São Paulo: Edições 70, 2011.

Benson, V., McAlaney, J., & Frumkin, L. A. (2018). Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape. In Psychological and Behavioral Examinations in Cyber Security (pp. 266-271). IGI Global.

Bies, R. J., & Moag, J. S. (1986). Interactional justice: Communication criteria of fairness. *Research on negotiation in organizations, 1*(1), 43-55.

Burden, K., & Palmer, C. (2003). Internet crime. *Computer Law & Security Review, 19*(3), 222-227.

CC BY

Damasio, A., & Carvalho, G. B. (2013). The nature of feelings: evolutionary and neurobiological origins. *Nat Rev Neurosci, 14*(2), 143-152.

Deci, E. L., & Ryan, R. M. (2000). The 'What' and 'Why' of Goal Pursuits: Human Needs and the Self-Determination of Behavior. *Psychological Inquiry, 11*(4), 227.

Deci, E. L., & Ryan, R. M. (2008). Self-determination theory: A macrotheory of human motivation, development, and health. *Canadian Psychology/Psychologie canadienne, 49*(3), 182-185. doi:10.1037/a0012801

Dhillon, G. (2001). Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers & Security, 20*(2), 165-172. doi:http://dx.doi.org/10.1016/S0167-4048(01)00209-7

Feelings, I. (1998). Welfare, stress, and the evolution of feelings. *Advances in the Study of Behavior: Stress and Behavior, 27*, 371.

Freitas, M. E. d. (2000). Contexto social e imaginário organizacional moderno. *Revista de Administração de Empresas, 40*(2), 6-15.

Gercke, M. (2014). Understanding cybercrime: Phenomena, challenges and legal response. *ITU Telecommunication Development Sector*, 380.

Guilhardi, H. J. (2002). Análise comportamental do sentimento de culpa. *Ciência do comportamento: conhecer e avançar, 1*, 173-200.

Jesus, R. G. D., & Rowe, D. E. O. (2014). Organizational Justice Perceived by Teachers of Basic, Technical anda Technological Education. *Revista de administração Mackenzie, 15*(6), 172-200.

Kazemi, A., & Törnblom, K. (2014). Third-Party Allocation of Rewards The Effects of Categorization and Request for Justice. *Small Group Research, 45*(4), 435-450.

Kelloway, E. K., Francis, L., Prosser, M., & Cameron, J. E. (2010). Counterproductive work behavior as protest. *Human Resource Management Review, 20*(1), 18-25.

Klein, R. H., & Luciano, E. M. (2016). What influences information security behavior? A study with Brazilian users. *JISTEM-Journal of Information Systems and Technology Management, 13*(3), 479-496.

Korsgaard, M. A., Meglino, B. M., & Call, M. L. (2015). The Role of Concern for Others in Reactions to Justice: Integrating the Theory of Other Orientation with Organizational Justice. The Oxford Handbook of Justice in the Workplace, 387.

Leventhal, G., Karuza, J., & Fry, W. (1980). Beyond fairness: A theory of allocation preferences. In G. Mikula (Ed.), Justice and social interaction: 167-218. New York: Springer-Verlag.

Mendonça, H., & Tamayo, Á. (2008). Valores pessoais e retaliação organizacional: estudo em uma organização pública organização pública. *RAC-Eletrônica, Curitiba, 2*(2), 189-200.

Rasmi, M., & Jantan, A. (2013). A New Algorithm to Estimate the Similarity between the Intentions of the Cyber Crimes for Network Forensics. *4th International Conference on Electrical Engineering and Informatics (Iceei 2013), 11*, 540-547.

Rebellon, C. J., Piquero, N. L., Piquero, A. R., & Tibbetts, S. G. (2010). Anticipated shaming and criminal offending. *Journal of Criminal Justice, 38*(5), 988-997. doi:10.1016/j.jcrimjus.2010.06.016

Rego, A., & Souto, S. (2004). A percepção de justiça como antecedente do comprometimento organizacional: um estudo luso-brasileiro. *Revista de administração contemporânea, 8*(1), 151-177.

Richardson, R. (2008). CSI computer crime and security survey. *Computer Security Institute, 1*, 1-30.

CC BY

Robinson, S. L., & Bennett, R. J. (1995). A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of Management Journal, 38*(2), 555-572.

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation, 3*(2), 97-102. doi:10.1016/j.diin.2006.03.001

Roratto, R., & Dias, E. D. (2014). Security information in production and operations: a study on audit trails in database systems. *JISTEM-Journal of Information Systems and Technology Management, 11*(3), 717-734.

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications*, doi.org/10.1016/j.jisa.2017.11.001

Schwarz, N., & Clore, G. L. (1996). Feelings and phenomenal experiences. *Social psychology: Handbook of basic principles, 2*, 385-407.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers & Security, 49, 177-191.

Simons, T., & Roberson, Q. (2003). Why managers should care about fairness: the effects of aggregate justice perceptions on organizational outcomes. *Journal of Applied Psychology, 88*(3), 432-443.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & management, 51(2), 217-224.

Siqueira, M. M. M., & Padovam, V. A. R. (2008). Bases teóricas de bem-estar subjetivo, bem-estar psicológico e bem-estar no trabalho. *Psicologia: teoria e pesquisa, 24*(2), 201-209.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.

Skinner, B. (1995). O lugar do sentimento na análise do comportamento. *AL Néri (Trad.), Questões recentes na análise do comportamento*, 13-24.

Skinner, B. (1974). Sobre o Behaviorismo. Trad. Maria da Penha Villalobos: São Paulo: Cultrix/EDUSP.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296-302. doi:10.1016/j.im.2011.07.002

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management, 49*(3), 190-198.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *Mis Quarterly, 37*(1), 1-20.

CC BY