XXIII SEMEAD
Seminários em Administração

novembro de 2020
ISSN 2177-3866

BEHAVIORAL INTENTION OF CYBERLOAFING AFTER THE ANNOUNCEMENT OF FORMAL CONTROLS IN THE LIGHT OF THE CONTROLLING AND FLEXIBLE COMPANIES

LUIS HERNAN CONTRERAS PINOCHET
ESCOLA PAULISTA DE POLÍTICA, ECONOMIA E NEGÓCIOS - UNIVERSIDADE FEDERAL DE SÃO PAULO - EPPEN/UNIFESP

VANESSA ITACARAMBY PARDIM
UNIVERSIDADE NOVE DE JULHO (UNINOVE)

CESAR ALEXANDRE DE SOUZA
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO E CONTABILIDADE DA UNIVERSIDADE DE SÃO PAULO - FEA

BEHAVIORAL INTENTION OF CYBERLOAFING AFTER THE ANNOUNCEMENT OF FORMAL CONTROLS IN THE LIGHT OF THE CONTROLLING AND FLEXIBLE COMPANIES

1. INTRODUCTION

The effective participation of technology in social and professional life and the use of tools and services related to production, marketing, communication and management, are constantly being discussed in terms of positive and negative results. Unless the use of the internet is governed by certain policies, the control of cyberloafing activities in organizations can become difficult to manage (Messarra, Karkoulian & McCarthy, 2011).

While some estimates place the value of lost productivity at around US $85 billion a year in American companies, a little bit of cyberloafing can be beneficial to business as it positively impacts employee engagement and satisfaction. On average, American employees spend up to 10% of their workday browsing the Internet, sending e-mails to friends or shopping online. Additionally, employees who spent more time surfing the web and checking emails reported greater job satisfaction and were less likely to want to quit than those who did not cyberloaf (Smith, 2020). In Brazil, as well as in the United States, recent studies on the subject have identified empirical evidence and negative and positive consequences of cyberloafing behavior (Cappellozza, Moraes & Muniz, 2017; Cezar & Corso, 2019).

Cyberloafing refers to employees' accessing the Internet during work for personal and non-work related purposes, such as accessing social networks, checking news, making purchases, reading personal emails, playing any type of game online, reading blogs, visiting chat rooms, listening to music, downloading pirated software, or viewing pornographic videos, etc. (Koay, 2018; Lim, 2002). In addition to cyberloafing, there are other terms that explain the same or similar behavior, such as: cyberslacking, cyberbludging, online loafing, deviation from the internet, problematic use of the internet, personal use of the web at work, internet addiction, internet abuse, or cyber-lodging (Kim & Byrne, 2011).

Conversely, Andel, Kessler, Pindek, Kleinman, and Spector (2019) suggests that cyberloafing can help employees cope with an exceptionally stressful work environment, acting as a kind of escape; helping them to recover and also contributes to creating spaces for innovation (Kessel, Hannemann-Weber, & Kratzer, 2015). The concern has led to a recent explosion of research on the topic and organizational researchers are quickly trying to grasp the causes, consequences, and nature of the phenomenon of slacking off at work through a computer (Zoghbi-Manrique-de-Lara, 2011).

The objective of this article is to identify the impact of each antecedent proposed on the behavioral intention of cyberloafing, on employees of companies with controlling or flexible characteristics after the announcement of formal controls. Regardless of the types of controls that could have been implemented earlier, this announcement generally indicates a more serious posture by the company in relation to cyberloafing and, therefore, is expected to affect the characteristics of employee cyberloafing.

To achieve this goal, the authors proposed a cyberloafing behavior model based on Akers' Social Learning Theory (SLT) adapted from Khansa, Kuem, Siponen, and Kim (2017). This research proposes, based on the SLT model, to use two of the four antecedents - Perceived Risk and Peer Cyberloafing. Two other constructs where also included "Perceived Justice" and "Self-efficacy" that are often mentioned in the specialized literature for being related to the theme. This research seeks to fill a gap in academic understanding in relation to employees' cyberloafing behavior given the dilemma of their management and impact on productivity and innovation in companies.

By addressing gaps in the literature, the present study brings the field one step closer to a thorough understanding of the phenomenon. Eventually, a solid understanding of

cyberloafing should lead to practical implications and guidelines that can be given to organizational decision makers.

2. LITERATURE REVIEW AND CONSTRUCTION OF THE THEORETICAL MODEL

2.1. When does cyberloafing occur?

Cyberloafing is common in organizations, given that estimates for the frequency of its use are usually given as a percentage of working time or in hours per week or day. Estimates vary depending on the source of the study and the sample population. Some are as low as three hours a week (Greenfield & Davis, 2002), others as much as two and a half hours a day (Mills, Hu, Beldona, & Clay, 2001). The highest estimates tend to be found by software companies that provide monitoring and control services. Regardless of the exact prevalence rate of cyberloaf, the implication is that cyberloafing is prevalent enough to be a major concern for organizations, if it does harm productivity.

This issue, known in the literature as cyberloafing, is discussed from the point of view of the individual related to the dependence on the use of information and communications technology (ICT). This puts work-related and unrelated applications and platforms in one place. Therefore, the line between work-related and unrelated activities is increasingly blurring, both at the conscious and the subconscious level (Lim & Chen, 2012). Cyberloafing can negatively influence employee and organizations' productivity and performance, in addition to exposing organizations to the risk of legal processes and ethical responsibilities (Vitak, Crouse & LaRose, 2011; Huma, Hussain, Thurasamy, & Malik, 2017; Khansa et al., 2017; Koay, 2018; Usman, Javed, Shoukat, & Bashir, 2019). For this reason, companies are adopting cyberveillance to accompany cyberloafers with software, preventing access to specific websites and allowing managers to verify the use considered appropriate by the organization's policies.

Many companies allow the use of the BYOD (Bring Your Own Device) model in their organizations, a movement initiated by the worker and often unknown by the IT department. This can cause security and support problems, however, managers at many companies adopt BYOD to reduce costs and increase productivity and employee satisfaction. Although it is believed that the use of technological tools in business contributes to the development of employees, there are studies that have indicated that employee performance is negatively affected by the loss of time or creating conditions for idleness in professional activities. If the agreement based on the mutual expectations of employees and the employer has been violated, employees may be reluctant to perform their activities at work. This could result in employees exhibiting behaviors such as: frequent breaks and late return to work after breaks to create free time (Betts et al., 2014; Kim, Triana, Chung, & Oh, 2015).

Additionally, cyberloafing may be a natural response to boredom in the workplace, as it differs from other, many more harmful, forms of behavior considered countervailing. In the literature, cyberloafing is observed when the workload is low, but in many cases, it does not harm the work. When analyzing prevalence rates, some researchers concluded that cyberloafing is reducing productivity. While others have concluded that this practice can provide a break, increasing productivity and employee satisfaction (Belanger & Van Slyke, 2002; Block, 2001). One reason why cyberloafing is limited is due the company's cyber security. Conversely, it is possible to understand cyberloafing as a way to reduce stress in the workplace (Pindek, Krajcevska & Spector, 2018).

Innovative behavior at work is understood as the conscious creation, promotion and implementation of new ideas to benefit a specific group or the entire organization. This behavior is a process for creating new problem solutions. To implement this behavior, the main skill is employees' creativity (Kessel et al., 2015). In this context, behavior at work, driven by

cyberloafing, can create spaces for innovation, and has a broader meaning than creativity, because creativity is only the ability to develop new ideas, but innovative behavior can include an implementation proposal of those ideas.

In the literature it is often observed that sex and age are related to cyberloafing with men who practice more cyberloafing than women, and younger employees who practice more cyberloafing than older employees (De Lara, 2007; Garrett & Danziger, 2008; Henle & Blanchard, 2008). Finally, the variables that showed the most robust and significant correlations with cyberloafing have been relationship norms (Carmeli et al., 2008; Restubog et al., 2011).

2.2. Antecedents in Cyberloafing Behavior

Khansa et al. (2017) identified the absence of research that analyzed ads for formal organizational controls, and how these would affect the motivators of cyberloafing behavior. Therefore, these authors sought insights into the aspects of cyberloafing behavior, before and after the announcement of formal controls, to create a complete picture of cyberloafing behavior and help managers design the correct countermeasures in their companies. This research proposes, based on the SLT model, to use two of the four antecedents - Perceived Risk and Peer Cyberloafing - which represent important facets in the definition of the individual as a social learner in his interaction with the market. The construct "Neutralization" was not used in this research due to the need for companies to present to employees, in a recurring and repeated way, the practices adopted, from the historical point of view, related to cyberloafing - which was not possible to precisely identify in this search.

Figure 1 shows the theoretical model proposed in this research, which was adapted from the study by Khansa et al. (2017) with the inclusion of two constructs "Perceived Justice" and "Self-efficacy" that are often mentioned in the specialized literature for being related to the theme. Furthermore, it includes the dependent variable identified by the "Intention of Cyberloafing" as it is a survey that involves an incentive to provide a hypothetical situation in which an ad about formal controls is displayed at the time of the survey.

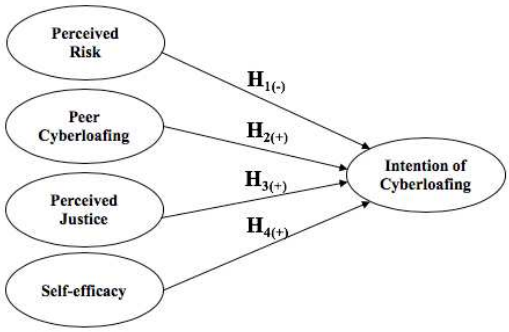


Figure 1: Proposed Model

2.2.1. Perceived Risk (PR)

Perceived risk can be defined as the feeling of insecurity and vulnerability within a given context on which the individual's general assessment is based (Alcántara-Pilaret al., 2015). This construct is also an essential determinant in the intention to use or make a decision, as well as in a relationship between individuals. After the announcement of formal controls in companies, the atmosphere of uncertainty in decisions is accentuated. The perception of risk sometimes tends to underestimate or fragment an understanding of how an employee may react when making decisions, due to risk or uncertainty, as there are studies that indicate that, in many cases, the emotional reaction exceeds the cognitive assessment (Kobbeltved & Wolff, 2009). Therefore, even if an organization has formal controls, users may not be aware of them or pay little attention to them, as they do not consider them to be real or an imminent risk (Kim &

Malhotra, 2005; Lowry, Zhang, Wang, & Siponen, 2016). If people do not consider the perceived risk substantial, they are unlikely to change their behavior. Likewise, before the announcement of formal controls, the perceived risk may be too low to affect the Intention of Cyberloafing. However, the announcement of formal controls activates the perceived risk, increasing future losses for the employee. Since people tend to adjust their behavior when faced with real threats (Barnett & Breakwell, 2001), the perceived risk becomes a significant impediment to Intention of Cyberloafing. Taken together, it is expected that the perceived risk is associated with a reduction in the Intention of Cyberloafing only after the announcement of formal controls (Khansa et al., 2017). Therefore, the following hypothesis is formulated:

Hypothesis 1: Perceived Risk is negatively related to Intention of Cyberloafing after the announcement of formal controls.

2.2.2. Peer Cyberloafing (PC)

While the majority of withdrawal behaviors are motivated by the desire to escape or avoid an unpleasant situation, cyberloafing can be motivated, for example, by a moment of idleness. So, people report that they practice cyberloafing because they find it enjoyable. The perspective of this approach could also explain why the ability to hide cyberloaf activity - perceiving how easy it is to practice cyberloaf without coworkers "catching you" - is a strong predictor of cyberloafing (Askew, Buckner, Taing, Bauer & Coovert, 2014). The spread of cyberloafing results in the expansion of cyberloafing practice (Liberman, Seidman, McKenna, & Buffardi, 2011; Lim & Teo, 2005; Pee, Woon & Kankanhalli, 2008). The immediate supervisor is the best person to judge what constitutes a non-work related activity because the supervisor presumably (a) has at least basic knowledge of the subordinate's job area, and (b) is less likely to be biased than the subordinate or his or her coworkers in judging what constitutes cyberloafing. This second aspect clarifies how borderline behaviors such as how an individual who commits something involuntary could be classified by his peers and the direct leadership. For this reason, it is necessary to announce formal controls, since before the announcement, non-cyberloafers may feel left out or at a disadvantage because their colleagues' cyberloafing went unpunished. If the organization makes no formal attempt to contain employees' cyberloafing, it will likely become the new standard and spread throughout the organization. Thus, the announcement of formal controls marks a turning point, because it signals the organization's position when dealing with cyberloafers. The newly imposed monitoring and sanctions for typified cases are likely to reduce the perceived rewards of cyberloafing and are expected to slow down the contagion effect between peers, but it will not eliminate it. Therefore, the relationship between Peer Cyberloafing and Intention to Cyberloafing will be significant before and after the announcement of formal controls but is expected to weaken when there are formal controls (Taylor & Todd, 1995; Cao, Guo, Vogel, & Zhang, 2016; Khansa et al., 2017). Therefore, the following hypothesis is suggested:

Hypothesis 2: Peer Cyberloafing is positively related to Intention of Cyberloafing after the announcement of formal controls.

2.2.3. Perceived Justice (PJ)

Perceived Justice refers to the perception of how the employee is treated by the company (Schmidt, Houston, Bettencourt, & Boughton, 2003), based on performance evaluations and reward systems - and this will activate a type of conscious behavior trait which is low cyberloafing or not (Kim et al., 2015). The research performed by Khansa et al. (2017) indicated that the Intention of Cyberloafing may have as a predecessor an important assessment from a cognitive point of view (Perceived Justice), only after the announcement of formal controls. These authors also related Perceived Justice to the theory of deterrence and its extensions (D'Arcy, Hovan & Galleta, 2009), who mostly defend formal controls as an effective deterrent

to deviant behaviors, demonstrating empirically that the announcement of formal controls can backfire (D'Arcy, Herath & Shoss, 2014; Salinas & Farfán, 2017). This happens by transforming factors that previously were not determinants into significant ones of the Intention of Cyberloafing (for example: Perceived Justice) in significant precursors of the Intention of Cyberloafing. In addition to being significant in determining the Intention of Cyberloafing after the announcement of formal controls, these factors are also known to have negative repercussions on employees' organizational citizenship behavior, prosocial behavior and job satisfaction. In this study, the Perceived Justice construct was seen as an independent variable and not of control like the SLT model. Thus, the corresponding hypothesis is presented:

Hypothesis 3: Perceived Justice is positivity related to Intention of Cyberloafing after the announcement of formal controls.

2.2.4. Self-efficacy (SE)

Self-efficacy refers to the belief in what employees can do with the capacity or skills they have (Hsu, Chang, & Yen, 2011) or in their ability to perform specific behavior (Lai, 2008) in companies. The nature and scope of perceived self-efficacy undergoes several changes as a new competence emerges, which requires further development of self-efficacy to function successfully. There is evidence of this in the literature as measures for self-efficacy in the use of electronic equipment, including the computer, the Internet and smartphones (Duane, O'Reilly & Andreev, 2014). In this study, self-efficacy represents the perception of being focused with clearly defined objectives. It was found that self-efficacy decreases the effectiveness of organizational anti-cyberloafing controls (Taylor and Todd, 1995; Pee et al., 2008; Derin & Gökçe, 2016; Khansa et al., 2017). Finally, the formulated hypothesis is presented:

Hypothesis 4: Self-efficacy is positively related to Intention of Cyberloafing after the announcement of formal controls.

2.2.5. Intention of Cyberloafing (IC)

In the absence of formal controls that prohibit cyberloafing and explicitly specify sanctions against offenders, cyberloafing is expected to be perpetuated like any other routine activity (Lim, 2005; Moody & Siponen, 2013; Pee et al., 2008; Vitak et al., 2011). Thus, the more employees who participated in cyberloafing in the past, the stronger their intention in the future. However, the announcement of new formal controls that prohibit cyberloafing breaks the routine as it motivates employees to reconsider engaging in their habits and to make a rational choice that would ultimately be in their best interest - one that would benefit them or at least not harm or affect their safety at work.

3. METHOD

The research was descriptive in nature, with a quantitative approach and was carried out through the application of an online questionnaire (survey), with closed-ended questions, for employees of companies. The method of data collection was convenience sampling, technical and not probabilistic, a fact that limits the generalization of research results. To measure each item of the constructs, the Likert-type scale was used with end points anchored in "totally disagree" (1) and "totally agree" (7) for all 15 statements that comprised the model. For aspects of the characterization of the demographic profile and organizations, specific objective questions were elaborated. At the beginning of the questionnaire, the situation, Figure 2, was presented, which states that the company had recently announced by e-mail a new policy to solve the problem associated with cyberloafing.

Pearson's bivariate correlation and analysis of variance (ANOVA) measured the independent variables Perceived Risk, Peer Cyberloafing, Perceived Justice, Self-efficacy and

Intention of Cyberloafing and variables of control sex, type of management, and frequency of use (cyberloafing), about the consequences on people management strategies regarding the control of cyberloafing in the workplace.

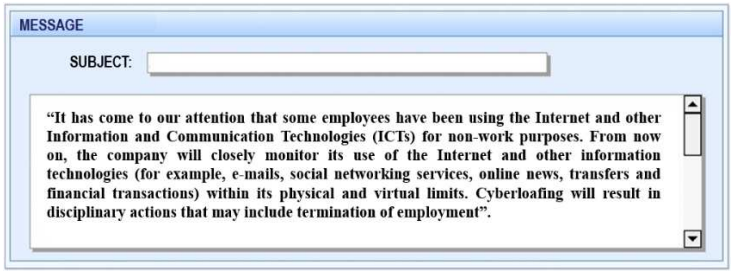


Figure 2: Anti-cyberloafing policy
Source: own elaboration.

For this study, a pre-test was performed with 60 individuals to check for an understanding of the research instrument (Hair, Black, Babin, & Anderson, 2010). The questionnaire was made available by the QuestionPro tool, to facilitate the access of professionals from the companies that participated in this research. Around 1,112 employees were contacted via social networks, and 538 valid questionnaires were obtained in total, which were tabulated in Microsoft Excel and analyzed by means of exploratory factor analysis to validate the scale within the context of the sample, and subsequently, the analysis. The confirmatory method was used using structural equation modeling based on covariance using the IBM SPSS v.25 and AMOS v.25 software. In this research, G*Power 3.1.9 software was used to calculate a priori the number of questionnaires needed to validate the test that should be maintained at least 80% of the observed power to guarantee the validity of the applied model. In this case, the test power (1-b err prob) observed was equal to 99.99%.

4. ANALYSIS OF RESULTS

This section presents and analyzes the profile of respondents and companies, analysis of difference in group means, and of the structural model.

4.1. Profile of respondents and organizations

The profile of the survey respondents is presented in this section to characterize the sample, which is comprised of 538 people, 317 (58.9%) male and 221 (41.1%) female. In addition, as can be seen in Table 1, the sample has a homogeneous profile composed of a young, university and early career audience, representing 83.8% (n=451). Regarding the average company time, the respondents are just over two years ($\bar{x}$=25.56 months).

Table 1: Demographic Characteristics of Respondents

Characteristic	**Total (N=538)**	**Characteristic**	**Total (N=538)**
Age		*Hierarchical position*	
Up to 20	191 (35.5%)	Director/Managing	21 (3.9%)
From 21 to 30	303 (56.3%)	Coordinator/Supervisor	16 (3.0%)
From 31 to 40	37 (6.9%)	Analyst	57 (10.6%)
Above 41	7 (1.3%)	Assistant	134 (24.9%)
		Operational/Technical	163 (30.3%)
		Trainee/Apprentice	147 (27.3%)
Company sector		*Company size*	
Industry	46 (8.6%)	Micro	39 (7.2%)
Trade	133 (24.7%)	Small	94 (17.5%)
Service	303 (56.3%)	Medium	125 (23.2%)
Public services	56 (10.4%)	Large	280 (52.0%)

Source: own elaboration.

As shown in Table 2, ANOVA tests were developed for the predictive variables of the proposed model. Of the main results, it is observed that the female sex has a greater intention of practicing cyberloafing, which contradicts the findings of the De Lara (2007), Garrett and Danziger (2008); Henle and Blanchard (2008) studies. Regarding the type of management, it is observed that the variables Perceived Justice and Intention of Cyberloafing have similar influence in relation to the flexible company. Finally, the frequency of use observed identified exactly the constructs that were significant in this study - Peer Cyberloafing, Self-efficacy and Intention of Cyberloafing -, the first two having similar characteristics, and the Intention of Cyberloafing with individuals who intend to practice it on several times an hour.

Table 2: Analysis of Variance (ANOVA) of variables analyzed from the Proposed Model

Variables analyzed in the model	**Sex** - Male - Female	**Management Type** - Parent - Flexible	**Frequency of Use**
Perceived Risk	There is no effect on groups.	There is no effect on groups.	There is no effect on groups.
Peer Cyberloafing	There is no effect on groups.	There is no effect on groups.	There is an effect of frequency of use on peer cyberloafing [$F_{(1.532)}$=4.233; p<.001] This difference indicates that 123 individuals (22,86%) have peer cyberloafing between a few times a day and once an hour.
Perceived Justice	There is no effect on groups.	There is an effect of the group on self-efficacy [$F_{(1.536)}$=12.873; p<.0001] This difference indicates that individuals who work in flexible ($\bar{x}$=4,72) companies have a greater sense of perceived justice.	There is no effect on groups.
Self-efficacy	There is no effect on groups.	There is no effect on groups.	There is an effect of frequency of use on self-efficacy [$F_{(1.532)}$=4.233; p<.001] This difference indicates that 123 individuals (22,86%) have self-efficacy between a few times a day and once an hour.
Intention of Cyberloafing	There is an effect of the group on intention of cyberloafing [$F_{(1.536)}$=4.492; p=.035]. This difference indicates that female ($\bar{x}$=4,72) have a greater intention of cyberloafing than male ($\bar{x}$=4,34).	There is an effect of the group on intention of cyberloafing [$F_{(1.536)}$=6.839; p=.009] This difference indicates that individuals who work in flexible ($\bar{x}$=4,62) companies have a greater sense of intention of cyberloafing.	There is an effect of frequency of use on intention of cyberloafing [$F_{(1.532)}$=4.233; p<.001] This difference indicates that 65 individuals (12.08%) have the intention of cyberloafing several times an hour.

Source: own elaboration.

When asked about the average frequency with which they access the Internet available at work for private purposes within the past month, it was observed that 22.5% access it a few

times a week. Regarding the profile of companies, there is a concentration in the services area, 56.3% (n=303), of which 244 (80.5%) are national companies and 59 (19.5%) international companies.

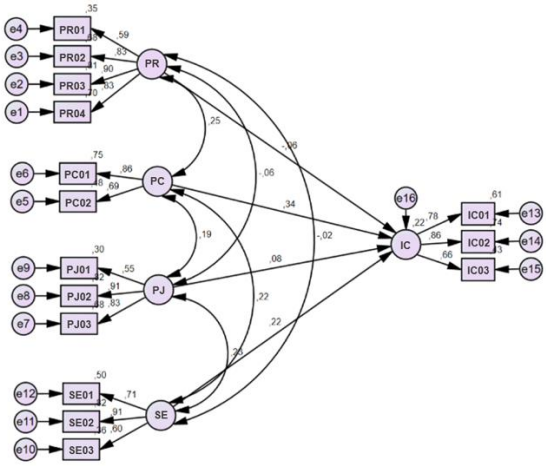
4.2. Exploratory Factor Analysis

Performing an exploratory factor analysis, regardless of the existing theoretical background, is necessary to identify a potential structure or ensure that the measurements reflect accuracy (Fabrigar & Wegener, 2012). The first analysis of the scales - Perceived Risk (PR), Peer Cyberloafing (PC), Self-efficacy (SE), Perceived Justice (PJ) and Intention to Cyberloafing (IC) - occurred through the commonality matrix. For this analysis, the Kaiser-Meyer-Olkin (KMO) criterion, 0.734, and Bartlett's Sphericity Test, $p < 0.001$, were used. After this procedure, the cross-loading was observed and there was no need to exclude any variable, since all variables had a commonality score - proportion of variability of each variable that is explained by the factors - greater than 0.5. The results of Cronbach's Alpha confirmed the reliability of the measurement items, as can be seen in Table 3.

4.3. Confirmatory Factor Analysis

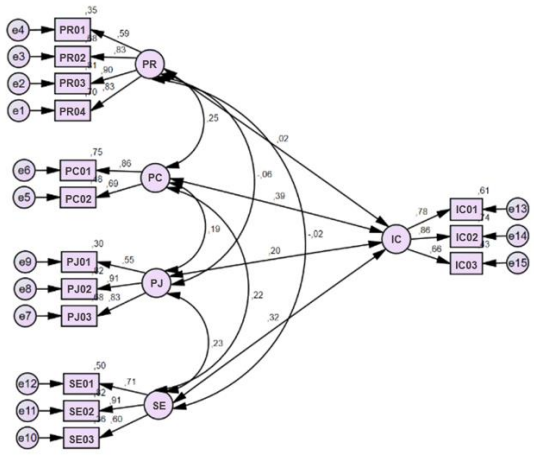
Confirmatory factor analysis (CFA), a covariance-based study (CB-SEM) was conducted to verify the fit of the measurement model with the support of the SPSS and AMOS v.25 that has specific characteristics in the construction of the model that were not present in the simplified diagram of the theoretical model (Figure 1). Among them, there is a need to indicate the correlations between exogenous variables (in path analysis), as well as the endogenous (dependent) variable receiving an error attribution (Figure 3). To test the convergent and discriminant validity (following the precepts of Fornell & Larcker, 1981), the strategy of correlating all exogenous and endogenous variables with each other was used (Figure 4).

Figure 3: Final Model



Source: AMOS output.

Figure 4: Validity Test



Source: AMOS output.

Table 3: Result of the Exploratory Factor Analysis

Item	Assertive	Factor Loadings					Communality (h^2)	Cronbach α	Authors
		1	2	3	4	5			
PR01	I consider cyberloafing dangerous.	.720					.524	.866 (good)**	Siponen and Vance (2010) Khansa *et al*. (2017)
PR02	Cyberloafing would put me in danger.	.888					.791		
PR03	It is risky for me to be involved in cyberloafing.	.902					.816		
PR04	Cyberloafing could cause problems for me.	.849					.754		
PC01	I believe that most people occasionally get involved in cyberloafing.					.855	.798	.747 (acceptable)**	Taylor and Todd*** (1995) Khansa *et al*. (2017)
PC02	I am convinced that my co-workers occasionally get involved in cyberloafing.					.869	.788		
IC01	I predict that I would use the Internet at work for non-work purposes at some point.		.794				.723	.804 (good)**	Venkatesh and Davis (2000) Khansa *et al*. (2017)
IC02	I am sure that I will use the Internet at work for non-work purposes at some point.		.877				.798		
IC03	I plan to use the Internet at work for non-work purposes next month.		.821				.69		
SE01	It is easy for me to use information technology in general (for example, computers, smartphones, among others).				.797		.682	.768 (acceptable)**	Taylor and Todd (1995) Khansa *et al*. (2017)
SE02	I have the ability to use information technology in general (for example: computers, smartphones, among others).				.868		.786		
SE03	I am technically trained to use information technologies in general (for example, computers, smartphones, among others).				.781		.624		
PJ01	I believe that my company is fair in dealing with cyberloafing.			.708			.541	.797 (acceptable)**	Schmidt *et al*. (2003) Khansa *et al*. (2017)
PJ02	My company's cyberloafing policy is reasonable.			.892			.816		
PJ03	In general, cyberloafing is treated reasonably in my company.			.891			.799		
Eigenvalue		3.408	2.991	1.78	1.569	1.182			
Variance (%)		22.718	19.94	11.869	10.459	7.882	72.868		

* Dimension reduction: analysis of the main components by Varimax rotation.

** George and Mallery (2003) criteria.

*** The authors Taylor and Todd (1995) adapted Ajzen's model of Planned Behavior Theory (1991) indicating only 2 items as they are sufficient for the "Peer Influence" scale.

The judgment of the fit of the model should reflect the analysis of several criteria. Regarding the coefficients considered, the ratio between the chi-square (χ^2) and degrees of freedom (gl), and the CFI, TLI, GFI, RMSEA and SRMR adjustment indexes were used. The χ^2 indicates the magnitude of the discrepancy between the observed and modeled covariance matrix, testing the probability of the theoretical model fitting the data. The higher the value, the worse the adjustment. However, it is more common to consider its reason in relation to the degrees of freedom (χ^2/gl) whose values must be between 1 and 3 (Kline, 2015).

The CFI (Comparative Fit Index), TLI (Tucker-Lewis Index) and GoF (Goodness of Fit of Index) indexes calculate the relative adjustment of the observed model, whose values above 0.95 indicate optimal adjustment and those above 0.90 indicate adequate adjustment (Hu & Bentler, 1999). In turn, the RMSEA (Root of Mean Square Error of Approximation) is also a measure of discrepancy, with results expected to be less than 0.05, but acceptable up to 0.08, despite such a coefficient penalizing complex model. Finally, the SRMR (Standardized Root Mean Square Residual) reports the standardized average of the residues (discrepancies between the observed and modeled matrix), with indexes less than 0.10 indicative of good fit (Hair et al., 2010; Kline, 2015). For the effectiveness of the analyzes, the maximum likelihood estimator (ML) was used.

The details of the model adjustment are as follows. The value of χ^2=180.20 and gl=80.00, resulting in model adjustment (χ^2/gl)=2.250, TLI=.960, CFI=.969, GFI=.959 SRMR=.042, and RMSEA=.048, indicating that all items meet the model and adjustment criteria.

The results of the reliability analysis, Table 4, are as follows: the value of the AVE (Average Variance Extracted) ranged from 0.561 to 0.633, indicating that all variables meet the criteria of 0.5 (Bagozzi & Yi, 1988). The internal consistency of CR (Composite Reliability) was considered adequate, ranging from 0.758 to 0.871, with all variables above 0.7 or more (Hair et al., 2010). The reliability of the six factors was analyzed by Jöreskog's rho and the values were higher than 0.795. According to Chin (1998), these values are considered quite satisfactory, since the Jöreskog indices must be greater than 0.7. The standard factor load of all items was above the recommended level (0.50) and, from the results of the analysis, the measurement model was acceptable accepted and reliable.

Table 4: Convergent and Discriminant Validity Test

Construct	Number of itens	CR	AVE	rho	RP	PC	PJ	SE	IC
RP	**4**	0.871	0.633	0.902	**0.796**				
PC	**2**	0.758	0.613	0.795	0.246***	**0.783**			
PJ	**3**	0.813	0.602	0.878	-0.058	0.189***	**0.776**		
SE	**3**	0.788	0.561	0.862	-0.025	0.215***	0.234***	**0.749**	
IC	**3**	0.814	0.596	0.839	0.016	0.392	0.204	0.317	**0.772**

Note: *** p < .001
Source: Amos output

In view of the result, **H1** (ß=-.048; $S_{\bar{x}}$=.40; t=-1.189; p=.234) was rejected, as it had no effect on the "Perceived Risk → Intention of Cyberloafing" construct. Although a non-significant result was obtained, the effect remained negative as expected. This is likely due to the fact that employees are not concerned with being reprimanded directly, or with leaving a bad impression that affects their professional reputation. In addition, this lack of professional relationship can lead to a discussion that employees pay little attention to, or they simply disregard risks as "real" and this, according to Barnett

and Breakwell (2001), is understood as a behavior that is difficult to change, even after the formal control announcement (Khansa et al., 2017).

The **H2** (ß=.381; $S_{\bar{x}}$=.064; t=5.923; p<.001) of the causal relationship "Peer Cyberloafing → Intention of Cyberloafing" was accepted due to the respondents considering the influence of cyberloafing by their co-workers as admissible and harmless, to justify their actions, especially in cases where it is used to minimize boredom, when there is a low workload and the practice of BYOD, as corroborated by the results obtained in ANOVA (Table 4). Additionally, there was an awareness of this effect with greater intensity among the female audience. This brings a collective view of employees in which cyberloafing behavior can promote the organization's social capital as it facilitates knowledge sharing among employees. This is because ICTs would have the potential to strengthen the bonds of the network between teams in terms of trust, enriching the performance of professionals and, as a result, the dynamics of work (Cao et al., 2016).

The cognitive relationship "Perceived Justice → Intention of Cyberloafing", as presented in **H3** was rejected (ß=.079; $S_{\bar{x}}$=.046; t=1.694; p=.090). Although a non-significant result was obtained, the effect remained positive as expected. This is probably because employees are not having the opportunity to participate in performance reviews and reward systems. In this sense, formal controls can be ignored by employees and, as noted in this research, have no repercussions. There are concerns regarding illegal practices in the use of ICTs performed by professionals in the workplace, as the organization may be obliged to involve employees legally in the event of any kind of deviation or in extreme case - crime. In addition, cyberloafing practices contrary to organizational norms can legally lead to dismissal (Salinas & Farfán, 2017).

Finally, **H4** (ß=.331; $S_{\bar{x}}$=.078; t=4.261; p<.001) was accepted indicating that the path "Self-efficacy → Intention of Cyberloafing" made employees develop, within the limits imposed under the conditions of specific skills, abilities and skills supported by the use of ICTs. As a result, when using ICTs for personal purposes during working hours, employees can stimulate their creativity and generate ideas that can somehow benefit organizational dynamics (Derin & Gökçe, 2016). Even if one of the reasons for cyberloafing is related to negative effects, as is the case of distraction from the use of ICTs, the deviation of concentration and focus that can cause leisure and boredom, it can make employees more confident to perform their activities and thus increase the quality of the activities performed.

5. CONCLUSIONS

In view of the results obtained in this study, it can be concluded that the proposed general objective, to identify the impact of each of the proposed antecedents on the behavioral intention of cyberloafing in employees of companies with controlling or flexible characteristics after the announcement of formal controls, was reached.

The research addressed a theme that brings a paradoxical relationship (positive and negative) in the use of ICTs for personal purposes in organizations. **H4** indicated that organizations, by adopting a permissive position and giving employees greater freedom in the use of ICTs, exempt themselves from restrictions and expect that the attitudes of the staffs are sensible, thus avoiding negative consequences and creating innovation spaces (Kessel et al., 2015). The **H2** result, brings the discussion of productivity. For example, scientific literature indicates that cyberloafing can help in situations of boredom, fatigue, psychological disorders (anxiety, stress, depression, loneliness, among others), and the balance between personal and professional spheres (Arshad, Aftab & Bukhari, 2016), but it can also lead to loss of productivity and performance (Andreassen,

Torsheim & Pallesen, 2014). Thus, both positive and negative effects coexist and affect employee productivity and innovation in different organizations.

This study corroborates the results of a recent research by Cezar and Corso (2019), in which it was found that despite interviewees perceiving the negative side regarding the loss of time and concentration when they intend to practice cyberloafing, even after the announcement of a company, they also have the perception that they can make use of technologies for personal purposes in the workplace in times of boredom, such as an "escape valve", to recover before returning to their tasks.

The research brought interesting data that revealed that the measure of adjustment of the model - the coefficient of determination - of the dependent variable "Intention in Cyberloafing" was R^2=.22 (22%). This explains the concern of employees to perform cyberloafing at work, only a few times a week to avoid boredom with the use of BYOD, from the four constructs that were selected for this research (Perceived Risk, Peer Cyberloafing, Perceived Justice, and Self-efficacy). The coefficient of determination, despite being a quality indicator, does not necessarily indicate whether a regressive model is adequate, since it is possible to have a low R^2 value for a good model (Kvålseth, 1985). Therefore, it is important to note what R^2 is actually evaluating, and in this case, it is indicating what was already foreseen, which is that after the announcement of formal controls, employees would be more likely to not use cyberloafing, or even to omit their use.

This research indicated, even in a situational way, a trend in cyberloafing that can lead to inefficiency and generate costs for companies. While some organizations try to eliminate these behaviors by installing security options, such as firewalls, some are still alarmed because they cannot prevent this type of behavior, since for cyberloafing to occur, only a mobile device and Internet access are needed. Internet use in the workplace is growing and raising a lot of attention on the negative effects on employees' attitudes. Thus, the necessary measures must be considered to avoid losses in productivity. Vitak et al. (2011) and most studies in the area recommend educating employees about the negative consequences of cyberloafing behavior.

5.1. Managerial implications

This research can provide information to senior executives and managers on how they can deal with cyberloafing within organizations in a balanced way, depending on the management style employed "more controlling" or "more flexible". The present study shows that employees' feelings about the topic of cyberloafing are valuable for the organization and society to reflect the limits of these activities. Therefore, it is suggested that executives and managers focus their efforts on improving employees 'perception of meaningful work, clearly communicating the value of employees' contribution to their personal lives, organizations and society' (Usman et al., 2019).

Supervisors can also improve employees' perception that their work serves a greater good by initiating dialogues with employees and encouraging them to reflect on their perceptions regarding the nature of the work and the values it carries for others (for example: reflexes for colleagues, organization and society). In doing so, supervisors can restrict employee involvement in cyberloafing with the support of expository methods containing formal control announcements.

In addition, there is a competitive era in which the emphasis of executives and managers prevails on economic values and this favors the creation of a significant work crisis, which can result in dysfunctional behaviors - for example, cyberloafing (Bailey et al., 2019). Therefore, it is suggested that the top management of companies may play a central role in creating a balance between connecting social and economic values for

employees to combat the labor crisis. Managers can do this by providing employees with autonomy, improving their self-esteem and establishing a sense of responsibility, facilitating easier access to resources and developing trust-based relationships with them. This would help senior management to deter employee involvement in cyberloafing and other dysfunctional behaviors, making them resolute in completing their work.

Finally, it is essential to improve the experience in the workplace so that employees see the potential of this space for learning and competence development, in line with the achievement of organizational objectives. As such, employees are likely to use their time and energy to improve their skills instead of wasting those valuable resources on cyberloafing activities.

5.2. Limitations and future studies

This research brought a sample that involved employees from different organizations, with different natures, types and sectors to evaluate and find common points in employee profiles in different companies. However, it would be appropriate to conduct in-depth studies within the same organization to analyze the perceptions of the phenomenon of cyberloafing, highlighting, for example, the time spent on this practice.

As a suggestion for expanding this research, it is proposed to analyze the behavior of employees by the size of the institutions (micro, small, medium and large) individually, given that in addition to the research by Messarra et al. (2011) the literature shows indications that smaller organizations that have fewer resources, from improper use (here adapted for cyberloafing) can overload ICTs, affecting productivity. In addition, issues of labor cost and waste of activities could be analyzed.

REFERENCES

Ajzen, I (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

Akers, R. L (1977). *Deviant Behavior: A Social Learning Approach*, 2nd ed. Belmont, CA: Wadsworth.

Alcántara-Pilar, J. M., & Del Barrio-García, S. (2015). Antecents of atitudes toward the website. *Cross Cultural Management*, 22(3), 379-404.

Andel, S. A., Kessler, S. R., Pindek, S., Kleinman, G., & Spector, P. E. (2019). Is Cyberloafing More Complex than we Originally Thought? Cyberloafing as a Coping Response to Workplace Aggression Exposure. *Computers in Human Behavior*, 101, 124-130.

Andreassen, C. S., Torsheim, T., & Pallesen, S. (2014). Use of Online Social Network Sites for Personal Purposes at Work: Does it Impair Self-Reported Performance? *Comprehensive Psychology.* 3(18), p. 1-11.

Arshad, M., Aftab, M., & Bukhari, H. (2016). The Impact of Job Characteristics and Role Stressors on Cyberloafing: The Case of Pakistan. *International Journal of Scientific and Research Publications*, 6(12), 244-252.

Askew, K., Buckner, J. E., Taing, M. U., Ilie, A., Bauer, J. A., & Coovert, M. D. (2014). Explaining cyberloafing: The role of the theory of planned behavior. *Computers in Human Behavior*, 36, 510-519.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16(1), 74-94.

Bailey, C., Lips-Wiersma, M., Madden, A., Yeoman, R., Thompson, M., & Chalofsky, N. (2019). The Five Paradoxes of Meaningful Work: Introduction to the Special Issue 'Meaningful Work: Prospects for the 21st Century'. *Journal of Management Studies,* 56 (3): 481–499.

Barnett, J., & Breakwell, G. M. (2001). Risk perception and experience: Hazard personality profiles and individual differences. *Risk Analysis*, 21(1), 171–177.

Belanger, F., & Van Slyke, C. (2002). Abuse or learning? *Communications of the ACM*, 45(1), 64-65.

Betts, T. K., Setterstrom, A. J., Pearson, J. M., & Totty, S. (2014). Explaining cyberloafing through a theoretical integration of theory of interpersonal behavior and theory of organizational justice. *Journal of Organizational and End User Computing (JOEUC)*, *26*(4), 23-42.

Block, W. (2001). Cyberslacking, business ethics and managerial economics. *Journal of Business Ethics*, 33(3), 225-231.

Cao, X., Guo, X., Vogel, D., & Zhang, X. (2016). Exploring the influence of social media on employee work performance. *Internet research: Electronic networking applications and policy*, 26(2), 529-545.

Cappellozza, A., Moraes, G., & Muniz, L. (2017). Uso Pessoal das Tecnologias no Trabalho: Motivadores e Efeitos à Distração Profissional. *Revista de Administração Contemporânea*, 21(5), 605-626.

Carmeli, A., Sternberg, A., & Elizur, D. (2008). Organizational culture, creative behavior, and information and communication technology (ICT) usage: A facet analysis. *CyberPsychology & Behavior*, 11(2), 175-180.

Cezar, B. G. da S., & Corso, K. B. (2019). Os Dois Lados do Cyberloafing: uma Análise Qualitativa das Percepções de Trabalhadores Acerca dos Consequentes Negativos e Positivos do Comportamento de Uso das TICs para Fins Pessoais no Ambiente de Trabalho. *XLIII Encontro da ANPAD – EnANPAD 2019*, São Paulo/SP – 02 a 05 de outubro.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (ed.). *Modern methods for business research. Methodology for business and management* (pp. 295-336). Mahwah, NJ: Lawrence Erlbaum Associates Publishers.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, 31(2), 285–318.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79–98.

Derin, N., & Gökçe, S. G. (2016). Are cyberloafers also innovators? A study on the relationship between cyberloafing and innovative work behavior. *Procedia-Social and Behavioral Sciences*, 235, 694-700.

De Lara, P. Z. M. (2007). Relationship between organizational justice and cyberloafing in the workplace: Has 'anomia' a say in the matter? *CyberPsychology & Behavior*, 10(3), 464-470.

Duane, A. O'Reilly, P., & Andreev, P. (2014). Realising M-Payments: modelling consumers' willingness to M-pay using Smart Phones. *Behaviour & Information Technology*, 33(4), 318-334.

Fabrigar, L. R., & Wegener, D. T. (2012). *Understanding statistics: Exploratory factor analysis.* New York, NY: Oxford University Press.

Fornell, C., & Larcker, D (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 18(1), 39-50.

Garrett, R. K., & Danziger, J. N. (2008). On cyberslacking: Workplace status and personal Internet use at work. *CyberPsychology & Behavior*, 11(3), 287-292.

George, D., & Mallery, P. (2003). *SPSS for Windows step by step: A simple guide and reference.* 11.0 update (4th ed.). Boston: Allyn & Bacon.

Greenfield, D. N., & Davis, R. A. (2002). Lost in cyberspace: The web @ work. *CyberPsychology and Behavior*, 5, 347–353.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis: A Global Perspective.* New Jersey, Pearson Prentice Hall.

Henle, C. A., Kohut, G., & Booth, R. (2009). Designing electronic use policies to enhance employee perceptions of fairness and to reduce cyberloafing: An empirical test of justice theory. *Computers in Human Behavior*, 25(4), 902-910.

Hsu, M. H., Chang, C. M., & Yen, C. H. (2011). Exploring the antecedents of trust in virtual communities. *Behaviour and Information Technology*, 30(5), 587–601.

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives. *Structural Equation Modeling*, 6(1),1-55.

Huma, Z. E., Hussain, S, Thurasamy, R, & Malik, M. I. (2017). Determinants of Cyberloafing: A Comparative Study of a Public and Private Sector Organization. *Internet Research,* 27(1), 97–117.

Kessel, M., Hannemann-Weber, H., & Kratzer, J., (2012). Innovative work behavior in healthcare: The benefit of operational guidelines in the treatment of rare diseases. *Health Policy*, 105, 146-153.

Khansa, L., Kuem, J., Siponen, M., & Kim, S. S. (2017). To Cyberloaf or Not to Cyberloaf: The Impact of the Announcement of Formal Organizational Controls. *Journal of Management Information Systems*, 34(1), 141-176.

Kim, S. J., & Byrne, S. (2011). Conceptualizing personal web usage in work contexts: A preliminary framework. *Computers in Human Behavior.* 27(6), 2271-2283.

Kim, K., Triana, M. del C., Chung, K., & Oh, N. (2015). When Do Employees Cyberloaf? An Interactionist Perspective Examining Personality, Justice, and Empowerment. *Human Resource Management,* 55(6), 1041–1058.

Kim, S. S., & Malhotra, N. K. (2005). A longitudinal model of continued IS use: An integrative view of four mechanisms underlying postadoption phenomena. *Management Science*, 51(5), 741–755.

Kline, R. B. (2015). *Principles and Practice of Structural Equation Modeling*. Fourth Edition. The Guildford Press: New York and London.

Koay, K. Y. (2018). Workplace Ostracism and Cyberloafing: a Moderated–Mediation Model. *Internet Research*, 28(4), 1122–1141.

Kobbeltvedt, T., & Wolff, K. (2009). Risk-as-fellings and theory-of-planned-behavior. *Judgment and Decision Making*, 4(7), 567-586.

Kvålseth, T. O. (1985). Cautionary note about R^2. *The American Statistician*, 39(4), 279-285.

Lai, M. L. (2008). Technology readiness, internet self-efficacy and computing experience of professional accounting students. *Campus-Wide Information Systems*, 25(1), 18–29.

Liberman, B., Seidman, G., McKenna, K. Y. A., & Buffardi, L. E. (2011). Employee job attitudes and organizational characteristics as predictors of cyberloafing. *Computers in Human Behavior*, 27(6), 2192–2199.

Lim, V. K. G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing, and organizational justice. *Journal of Organizational Behavior*, 23(5), 675–694.

Lim, V. K. G., & Chen, D. J. (2012). Cyberloafing at the Workplace: Gain or Drain on Work? *Behaviour & Information Technology,* 31(4), 343-353.

Lim, V. K. G., & Teo, T. S. H. (2005). Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: An exploratory study. *Information and Management*, 42(8), 1081–1093.

Lowry, P. B., Zhang, J., Wang, C., & Siponen, M. (2016). Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model. *Information Systems Research*, 27(4), 962–986.

Messarra, L. C., Karkoulian, S., & McCarthy, R. (2011). To restrict or not to restrict personal internet usage on the job. *Education, Business and Society: Contemporary Middle Eastern Issues*, 4(4), 253-266.

Mills, J. E., Hu, B., Beldona, S., & Clay, J. (2001). Cyberslacking! A liability issue for wired workplaces. *Cornell Hotel and Restaurant Administration Quarterly*, 42, 34–47.

Moody, G. D., & Siponen, M. (2013). Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. *Information and Management*, 50(6), 322–335.

Pee, L. G., Woon, I. M. Y., & Kankanhalli, A. (2008). Explaining non-work-related computing in the workplace: A comparison of alternative models. *Information and Management*, 45(2), 120–130.

Pindek, S., Krajcevska, A., & Spector, P. E. (2018). Cyberloafing as a coping mechanism: Dealing with workplace boredom. *Computers in Human Behavior*, 86, 147–152.

Restubog, S. L. D., Garcia, P. R. J. M., Toledano, L., Amarnani, R., Tolentino, L., & Tang, R. L. (2011). Yielding to (cyber)-temptation: Exploring the buffering role of self-control in the relationship between organizational justice and cyberloafing behavior in the workplace. *Journal of Research in Personality*, 45(2), 247-251.

Salinas, E. & Farfán, G. R. (2017). Análisis e impacto del ocio cibernético en las organizaciones. *Espirales revista multidisciplinaria de investigación científica*, 7(1), 47-56.

Schmidt, T. A., Houston, M. B., Bettencourt, L. A., & Boughton, P. D. (2003). The impact of voice and justification on students' perceptions of professors' fairness. *Journal of Marketing Education*, 25(2), 177–186.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487–502.

Smith, K. (2020). The Small Business Daily Rundown: Are You a Cyberloaf? *The daily run down*. Disponível em: https://www.zenefits.com/workest/the-small-business-daily-rundown-are-you-a-cyberloaf/. Acesso em 23/05/2020.

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, 6(2), 144–176.

Usman, M., Javed, U., Shoukat, A., & Bashir, N. A. (2019). Does meaningful work reduce cyberloafing? Important roles of affective commitment and leader-member exchange. *Behaviour & Information Technology,* 1–15.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186–204.

Vitak, J., Crouse, J., & LaRose, R. (2011). Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior*, 27(5), 1751–1759.

Zoghbi Manrique de Lara, P. (2011). Reconsidering the boundaries of the cyberloafing activity: The case of a university. *Behaviour & Information Technology*, 37(1), 1- 1.