Analysis of Antecedent Factors that Lead to Cyberloafing and Deviant Behavior in Response to the Announcement of Formal Controls

Vanessa Itacaramby Pardim[a]
Luis Hernan Contreras Pinochet[b]
Cesar Alexandre de Souza[a]

[a] University of São Paulo, São Paulo, Brazil
[b] Federal University of São Paulo, Osasco, Brazil

Abstract

This paper analyzes the antecedent factors that lead to cyberloafing and deviant behavior in response to the announcement of formal controls. The research is descriptive, with a quantitative approach. It was developed through a survey of 517 employees from different organizations using a hybrid model in two stages (SEM-ANN). While a multi-analytical approach using exploratory and confirmatory factor analysis with covariance-based structural equation modeling (CB-SEM) validated the model, the SEM results were used as input to an artificial neural network (ANN) model to predict the factors for cyberloafing intention. As a result, we observed that 'peer cyberloafing' results from the influence of co-workers' use of technology. This justifies the behavior as acceptable and harmless and brings a collective view of this practice and helps promote the organization's social capital. The 'self-efficacy' in the use of electronic devices that leads to cyberloafing should not only be seen as a negative phenomenon to be banned, but as something that can stimulate creativity and the generation of ideas. Finally, this research provides clues on how to deal with the practice of cyberloafing in a balanced way, considering the

management style, whether more controlling or flexible, as well as the feelings of employees concerning the topic, as it is valuable for the organization and society to reflect on the limits of this practice. The introduction of this new methodology and the theoretical contribution of the proposed hybrid model open new horizons for the existing knowledge in the literature related to the understanding cyberloafing.

Keywords: cyberloafing; work environment; productivity; innovation.

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 under discussion, with positive and negative results. Unless certain policies regulate the use of the Internet, the control of cyberloafing activities (Agarwal & Avey, 2020) in organizations can become challenging to manage (Dmour et al., 2019; Messarra et al., 2011). Additionally, employees who spent more time surfing the web and checking e-mails reported greater job satisfaction and were less likely to quit than those who did not cyberloaf (Andel et al., 2019; Blanchard & Henle, 2008; Liberman et al., 2011; Pindek et al., 2018; Smith, 2020; Wu, Mei, & Liu, et al., 2020).

Cyberloafing refers to employees accessing the Internet during work hours for personal and non-work-related purposes, such as accessing social networks, checking the news, making purchases, reading personal e-mails, playing games online, reading blogs, visiting chat rooms, listening to music, downloading pirated software, or viewing pornographic videos, etc. (Koay, 2018). Other terms describe the same or similar behavior, such as cyberslacking, cyberbludging, online loafing, Internet deviation, problematic use of the Internet, personal use of the web at work, internet addiction, internet abuse, or cyber-lodging (Kim & Byrne, 2011; Koay et al., 2017; Wu, Mei, & Ugrin, et al., 2020).

Employees accessing the Internet for personal interests and purposes during working hours is called cyberloafing behavior (Lim, 2002; Lim & Chen, 2012; Lim & Teo, 2005), which is a well-established concept in professional life. It is usually considered counterproductive and has organizational leaders looking for ways to prevent employees from engaging in this behavior (Chavan et al., 2021; Metin-Orta & Demirtepe-Saygılı, 2021).

Conversely, Andel et al. (2019) suggest that cyberloafing can help employees cope with an exceptionally stressful work environment, acting as a means of escape, helping them recover, and contributing to creating spaces for innovation (Kessel et al., 2012; Wisse et al., 2015). Organizational researchers are quickly trying to grasp the causes, consequences, and nature of the phenomenon of slacking off at work using a computer (Zoghbi-Manrique-de-Lara, 2012; Zoghbi-Manrique-de-Lara & Sharifiatashgah, 2021).

Cyberloafing, often associated with problematic use of the Internet (Mohammed Abubakar & Al-zyoud, 2021; Yellowlees & Marks, 2007), represents a problem that is present in the organization's discussion plans. It can have negative consequences for both managers, in terms of productivity and safety, and for employees, who can be dismissed for just cause. This highlights the need to find strategies that balance organizational interests and the employees' needs and concerns.

We have proposed a cyberloafing behavior model adapted from Khansa et al. (2017). This study proposes the use of two of the four antecedents: 'perceived risk' (Siponen & Vance, 2010) and 'peer cyberloafing' (Taylor & Todd, 1995). Two other constructs were also included, 'perceived justice' (Khansa et al., 2017) and 'self-efficacy' (Taylor & Todd, 1995), which are often mentioned in the specialized literature related to the theme.

Therefore, we sought to contribute to the latest knowledge on the topic of cyberloafing, understanding that it is a form of deviant behavior in the workplace that is common in different types and structures of organizations, especially among employees, i.e. 'peer cyberloafing' (Saghih & Nosrati, 2021; Suari & Rahyuda, 2022). Employees' actions during working hours for personal purposes (Aladwan et al., 2021), reducing organizational performance (Beri & Anand, 2020) and consequently causing a loss in productivity in the organizations, represent a potential 'perceived risk' of breaches of information security, which often raises a discussion about the 'perceived justice' of the employees' actions (Saddiq et al., 2021).

However, Rahman and Surjanti (2022) showed a positive relationship between innovative work behavior, cyberloafing and person-organization fit, indicating that this effect influences employee performance by providing new insights into the antecedents of cyberloafing (Rahmah, Nurmayanti, & Surati, 2020). Given this, employees can adopt a positive or negative view of cyberloafing based on 'self-efficacy', providing guidance parameters in their organizations. In the same direction, Ratnasari and Tarimin (2021) identified the impact of cyberloafing on the intended goals of companies if there are no changes in management attitudes.

This article advances by discussing the theory systematized by Khansa et al. (2017) for the analysis of the effect of cyberloafing, based on the theoretical pillar of Ajzen's model of the theory of planned behavior (1991), which is an extension of the theory of reasoned action (Ajzen & Fishbein, 1980). A central factor in the theory of planned behavior is the individual's intention to perform a given behavior, and which was expanded by Taylor and Todd (1995). Thus, this research brings a new approach by discussing the constructs observed in the theory constructed by Khansa et al. (2017).

Of the four variables selected by this study to explain 'cyberloafing intention', 'peer cyberloafing' refers to an external individual/extrinsic factor. In comparison, the other three variables, 'perceived justice', 'perceived risk', and 'self-efficacy', are associated with the individual/ intrinsic internal aspects. The constructs were chosen based on the main issues previously discussed in the literature.

We chose to specifically investigate the effect of intention (Cheng et al., 2020; Hensel & Kacprzak, 2021; Venkatesh & Davis, 2000) rather than occurence, because the study focuses on the implementation of control mechanisms in a hypothetical business situation (Agarwal & Avey, 2020). By addressing gaps in the literature, the present study brings the field one step closer to a thorough understanding of the phenomenon (Tandon et al., 2022). This research seeks to fill a gap in the academic understanding of employee cyberloafing behavior, given the dilemma it poses for managers and its impact on companies' productivity and innovation. Ultimately, a solid understanding of cyberloafing should lead to practical implications and guidelines for organizational decision-makers.

Therefore, the purpose of this paper is to analyze the antecedent factors that lead to cyberloafing and deviant behavior in response to the introduction 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 with respect to cyberloafing and, consequently, is expected to affect employees' cyberloafing characteristics.

The following sections of this paper expand on the previous observations, first by providing an overview of the literature on cyberloafing in organizations and the construction of the research hypotheses and research model, and then by outlining the general approach of the research with a description of the study method and data collection. The empirical results and discussions are then presented. Finally, the research implications and conclusions are presented, subdivided into theoretical and practical implications, as well as the limitations and directions for future research.

Literature review and construction of the theoretical model

Directions for studies on cyberloafing

In this study, we searched for scientific articles with the theme of cyberloafing in publications in Web of Science (WoS) and Scopus to identify the leading journals and authors to support the literature review. Archambault et al. (2009) note that while the two databases differ in policy scope and coverage, they can be highly correlated. Sánchez et al. (2017) found a high correlation (R^2=0.78) between WoS and Scopus concerning the number of articles. The search for articles in the databases covered the last 20 years (2002 to 2022). The search string was "cyberloaf*", and the results obtained were 131 in WoS and 176 in Scopus. Out of these articles, 132 duplicate documents were removed and 182 were combined. All the annual publications on cyberloafing indicated a linear growth trend in the databases on the subject (see Figure 1). The R software package and the bliblioshiny for bibliometrix were used for these procedures.
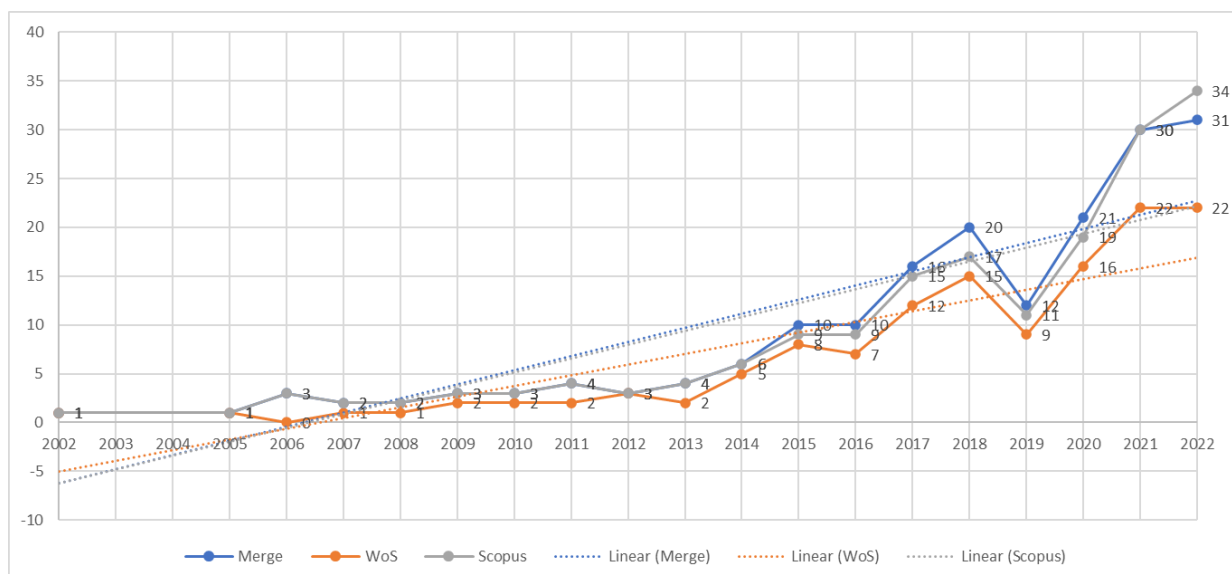

Figure 1. Annual publication of cyberloafing literature in WoS, Scopus, and merged databases

Source: elaborated by the authors.

The most relevant authors on cyberloafing report that it is a prevalent practice among employees (Lim, 2002; Lim & Chen, 2012; Lim & Teo, 2005) and has been called a hidden epidemic (Koay et al., 2017), killing business productivity, reducing performance (Wu, Mei, Liu, et al., 2020), and arising as a result of the scarcity of physical resources and agglomeration (Zoghbi-Manrique-de-Lara & Sharifiatashgah, 2021). It is often related to the culture of each country (Ugrin et al., 2018), as well as to the type of generation (S. Kim, 2018) or even to its effects on the mental health of employees (Wu, Mei, Liu, et al., 2020). These authors also stand out for their local impact in terms of h-index.

When analyzing the top authors' production over time, it is noticed that Lim (2002) stands out for being a pioneer and the most cited in cyberloafing studies, and Zoghbi-Manrique-de-Lara and Sharifiatashgah (2021) on the theme in recent years.

We sought to target articles specifically regarding the 'cyberloafing intention' effect (Cheng et al., 2020; Hensel & Kacprzak, 2021; Khansa et al., 2017), rather than stated use, because the study focuses on a hypothetical business situation of implementing control mechanisms and we understand that it would be difficult for people to manifest this type of behavior.

When does cyberloafing occur?

Cyberloafing is common in organizations and estimates of the frequency of its use are usually given as a percentage of work time or in hours per week or day (Aladwan et al., 2021). Estimates vary depending on the source of the study and the sample population. Some are as low as three hours a week, while others are as much as two and a half hours a day (Greenfield & Davis, 2002). The highest estimates tend to be found by software companies that provide monitoring and control services (Agarwal & Avey, 2020). Regardless of the exact prevalence rate of cyberloafing, the implication is that it is prevalent enough to be a major concern for organizations if it is affecting productivity.

This issue, known in the literature as cyberloafing (Tandon et al., 2022), is discussed from the individual's point of view related to dependence on information and communication technologies (ICTs). This brings together work-related and non-work-related applications and platforms. Therefore, the line between work-related and non-work-related activities is increasingly blurred, at both the conscious and the subconscious levels (Lim & Chen, 2012). Cyberloafing can negatively influence employees' and organizations' productivity and performance (Chavan et al., 2021; Metin-Orta & Demirtepe-Saygılı, 2021; Wisse et al., 2015), in addition to exposing organizations to the risk of legal proceedings and ethical responsibilities (Huma et al., 2017; Khansa et al., 2017; Koay, 2018; Usman et al., 2019; Vitak et al., 2011). For this reason, companies are adopting cyberveillance to monitor cyberloafers with software, preventing access to specific websites and allowing managers to verify whether uses are considered appropriate by the organization's policies (Dmour et al., 2019).

Those organizations that keep up with changes in environmental conditions are the ones that innovate. Innovation is accepted as one of the most important driving forces of development, change, and differentiation. One of the most effective methods of developing organizations' innovation capacity is to develop employees' creativity and capacity to produce new ideas. Human capital is the basis of innovation, and evaluating employees is a fundamental strategy for

managers to deal with global competition and environmental uncertainties, and consequently achieve their goals and the expected performance level (Chavan et al., 2021; Metin-Orta & Demirtepe-Saygılı, 2021; Wisse et al., 2015).

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 solutions to problems. The main skill is employees' creativity (Kessel et al., 2012). In this context, workplace behavior driven by cyberloafing can create spaces for innovation that goes beyond creativity, because creativity is only the ability to develop new ideas. Innovative behavior can also include a proposal to implement ideas resulting from the practice of cyberloafing.

In the literature, it is often observed that sex and age are related to cyberloafing, with men practicing more cyberloafing than women and younger employees practicing more cyberloafing than older employees (Garrett & Danziger, 2008; Henle et al., 2009; Zoghbi-Manrique-de-Lara, 2012; Zoghbi-Manrique-de-Lara & Sharifiatashgah, 2021). Finally, the variables that showed the most robust and significant correlations with cyberloafing were relationship norms (Restubog et al., 2011).

Antecedents of cyberloafing behavior

Khansa et al. (2017) identified an opportunity for research that analyzed announcements of formal organizational controls (Agarwal & Avey, 2020) and how these would affect the motivators of cyberloafing behavior (Kaptangil et al., 2021). Therefore, these authors sought insights into cyberloafing behavior before and after the announcement of formal controls to build a complete picture of cyberloafing behavior and help managers design the correct countermeasures in their companies. We propose to use the antecedents 'perceived risk' (Siponen & Vance, 2010) and 'peer cyberloafing' (Taylor & Todd, 1995), which represent important facets in the definition of the individual as a social learner in his/her interaction with the market.

Figure 2 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' (Khansa et al., 2017) and 'self-efficacy' (Taylor & Todd, 1995), which are often mentioned in the specialized literature for their relevance to the theme. Furthermore, it includes the dependent variable 'cyberloafing intention' (Cheng et al., 2020; Hensel & Kacprzak, 2021; Venkatesh & Davis, 2000), as this is a survey that involves a stimulus to provide a hypothetical situation in which an announcement about formal controls is displayed at the time of the survey.
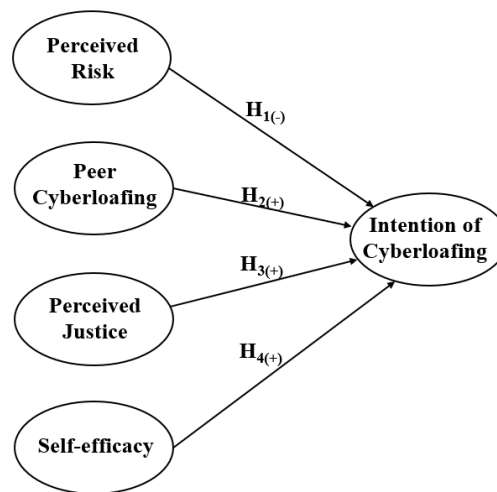
Figure 2. Proposed Model

Sources: elaborated by the authors.

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. The perception of risk sometimes tends to underestimate or fragment the 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 (Kobbeltvedt & Wolff, 2009). Likewise, before the announcement of formal controls, the perceived risk may be too low to affect the 'cyberloafing intention'. 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), perceived risk becomes a significant impediment to 'cyberloafing intention'. Therefore, it is expected that perceived risk is associated with a reduction in 'cyberloafing intention' only after the announcement of formal controls (Agarwal & Avey, 2020; Khansa et al., 2017; Siponen & Vance, 2010; Saddiq et al., 2021). Therefore, the following hypothesis is formulated:

Hypothesis 1: Perceived risk is negatively related to cyberloafing intention after the announcement of formal controls.

Peer cyberloafing (PC)

While most 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. Furthermore, this perspective could also explain why the ability to hide cyberloafing activity - the perception of how easy it is to practice cyberloafing without co-workers 'catching you' - is a strong predictor of cyberloafing (Askew et al., 2014). The spread of cyberloafing results in the expansion of cyberloafing practices (Liberman et al., 2011; Lim & Teo, 2005; Pee et al., 2008). 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. They are expected to slow down the contagion effect among peers, but not eliminate it. Therefore, the relationship between 'peer cyberloafing' and 'cyberloafing intention' is expected to be significant before and after the announcement of formal controls, but to weaken when there are formal controls (Agarwal & Avey, 2020; Cao et al., 2016; Khansa et al., 2017; Taylor & Todd, 1995; Saghih & Nosrati, 2021; Suari & Rahyuda, 2022). Therefore, the following hypothesis is suggested:

Hypothesis 2: Peer cyberloafing is positively related to cyberloafing intention after the announcement of formal controls.

Perceived justice (PJ)

Managers may perceive fairness in existing procedures and processes, while subordinates may perceive them as unfair (Lambert & Hogan, 2013). In this sense, Rahaei and Salehzadeh (2020) analyzed the impact of psychological law and perceived organizational justice on cyberloafing; the consequences of lack of justice in an organization can cause aggressive behaviors, slacking, and low commitment. 'Perceived justice' also refers to the perception of how the employee is treated by the company, based on performance evaluations and reward systems - and this will activate a type of conscious behavioral trait, which is low cyberloafing or not (Kim et al., 2016). The research conducted by Khansa et al. (2017) indicated that 'cyberloafing intention' might have as an antecedent a critical assessment from a cognitive point of view ('perceived justice') only after the announcement of formal controls. These authors also related perceived justice to deterrence theory and its extensions, mostly defending formal controls as an effective deterrent of deviant behaviors, demonstrating empirically that the announcement of formal controls can backfire (Agarwal & Avey, 2020; D'Arcy et al., 2009). This occurs through transforming factors that were previously not determinants into significant antecedents of 'cyberloafing intention' (for example, 'perceived justice'). In addition to being significant in determining 'cyberloafing intention' after the announcement of formal controls, these factors are also known to negatively affect employees' organizational citizenship behavior, prosocial behavior, and job satisfaction. In this study, the 'perceived justice' construct was seen as an independent variable and not a control variable as in the SLT model (D'Arcy et al., 2014; Saddiq et al., 2021). Thus, the corresponding hypothesis is presented:

Hypothesis 3: Perceived justice is positively related to cyberloafing intention after the announcement of formal controls.

Self-efficacy (SE)

Self-efficacy is the central component of social cognitive theory (SCT) that encourages individuals to fulfill their responsibilities and achieve their expectations (Bandura, 2001). Self-efficacy is considered a very specific quality of the individual, being observed with greater attention in common activities, for example, in the performance of activities in the company (Drnovšek et al., 2014). It also adds to people's judgments about their ability to perform specific tasks and is a central self-regulation mechanism. People's belief in their efficacy influences their

choices, their aspirations, how much effort they mobilize in an activity, and how much stress they experience when dealing with environmental demands (Bandura, 2001). The existing literature establishes that self-efficacy is necessary for creativity (Mumtaz & Parohoo, 2019). Employees who feel they identify with the company's activities and seek new opportunities to collaborate may have a high level of self-efficacy in their behavioral intentions (Jarvis, 2016). Thus, employees may often see challenges as obstacles, but may be increasingly eager to overcome them by developing innovative ideas and practical alternatives. Consequently, companies can leverage their employees' expertise by tracking self-efficacy, which tends to be a significant criterion for behavioral intentions (e.g., cyberloafing). In addition, new ideas lead individuals to rethink their ability to get involved and collaborate with new ideas, or even to foster innovation with their co-workers, as it has a constructive effect, as well as being able to explore behavioral aspects (Li et al., 2020).

Self-efficacy refers to the belief in what employees can do with their capabilities or skills (Hsu et al., 2011) or in their ability to perform a specific behavior (Lai, 2008) in companies. The nature and scope of perceived 'self-efficacy' undergo 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, such as measures of self-efficacy in the use of electronic equipment, including the computer, the Internet, and smartphones (Duane et al., 2014). In this study, 'self-efficacy' represents the perception of being focused with clearly defined objectives. It has been found that self-efficacy reduces the effectiveness of organizational anti-cyberloafing controls (Derin & Gökçe, 2016; Khansa et al., 2017; Pee et al., 2008; Taylor & Todd, 1995; Ratnasari & Tarimin, 2021). Therefore, the final hypothesis is presented:

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

Cyberloafing intention (CI)

The misuse of the Internet in the workplace has increased, indicating the need to study a wide range of individual and organizational factors concerning the cyberloafing intention behavior, including demographic profile variables such as age, gender, income, education, among others (Metin-Orta & Demirutku, 2020). Intention is defined as a person's conscious or self-instructed plan to perform a behavior (Triandis, 1980). It includes a subjective probability dimension that links the individual to the behavior and indicates how much effort the individual is willing to invest in it. Intention is cognitively related to the observation of the behavior. Thus, the higher the level of cyberloafing intention, the more likely a person is to engage in cyberloafing (Askew et al., 2014; Betts et al., 2014).

In the absence of formal controls that prohibit cyberloafing and explicitly specify sanctions for offenders, cyberloafing is expected to be perpetuated like any other routine activity. Thus, the more employees who have engaged in cyberloafing in the past, the stronger their future intentions. However, the announcement of new formal controls that prohibit cyberloafing breaks the routine as it motivates employees to reconsider engaging in their habit 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 security at work (Cheng et al., 2020; Hensel & Kacprzak, 2021; Khansa et al.,

2017; Lim & Teo, 2005; Moody & Siponen, 2013; Pee et al., 2008; Venkatesh & Davis, 2000; Vitak et al., 2011).

Method

Data collection and sample

We collected the sample of students-workers in the business administration course of a private higher education institution located in the city of São Paulo, Brazil, in 2020. The selection criteria were students-workers at the beginning of their careers in organizations of different sectors and sizes. There was no direct incentive, but rather an indirect one, since the students benefited from understanding the concept within the learning process. Participation in the study was voluntary, and all respondents were assured of confidentiality and anonymity. We believe that this sample is relevant to observing how students at the beginning of their careers behave when using smartphones in a simulated situation (see Figure 3).

For this study, a pre-test was performed with 60 individuals to understand the research instrument (Hair et al., 2009). The questionnaire was made available through the QuestionPro tool to facilitate the professionals' access from the companies that participated in this research. The control of missing data was carried out through the electronic questionnaire. The completion of all items of the scales was mandatory. Then, the Mahalanobis distance (D^2) was used to remove 21 outliers, resulting in a final sample of n=517 respondents (employees from different organizations).

Survey measures and implementation

We chose the scales below to measure the study constructs because they have been widely used in the extant literature and their reliability and validity are well established (see Appendix). The questionnaires were pre-tested with three academic experts (judges) with relevant publications in the scientific field. Their feedback was that all the scale items were clear and easy to understand. So, the authors administered the questionnaires without any changes. The questionnaires were tabulated in an electronic spreadsheet, and the data were analyzed using exploratory factor analysis to validate the scale within the context of the sample and subsequent analysis.

The research was descriptive in nature, with a quantitative approach, and was carried out by applying an online questionnaire (survey), with closed-ended questions, to employees of companies. The data collection method was convenience sampling, technical and not probabilistic, limiting the generalizability of the research results. The authors developed the instrument by operationalizing the constructs in items according to the reference present in the literature, as indicated in the Appendix. The questionnaire was validated and revised by three judges trained by renowned experts in the research area. The instrument was back-translated and validated by three experts in the field. To measure each item of the constructs, the Likert-type scale was used, with endpoints anchored in 'totally disagree' (1) and 'totally agree' (7) for all 15 statements that comprised the model. For aspects characterizing the demographic profile and organizations, specific objective questions were elaborated. At the beginning of the questionnaire, the situation

was presented (Figure 3), which states that the company has recently announced by e-mail a new policy to solve the problem of cyberloafing.
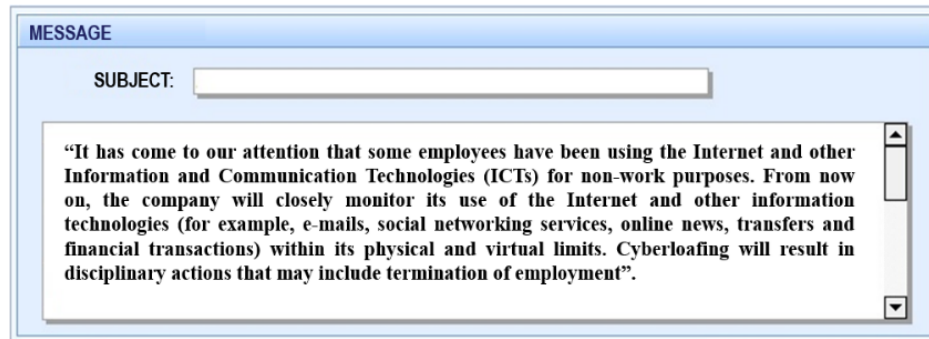
```
┌─────────────────────────────────────────────────────────────┐
│ MESSAGE                                                       │
│                                                               │
│        SUBJECT: [                                    ]        │
│                                                               │
│   ┌──────────────────────────────────────────────────┐ ▲    │
│   │ "It has come to our attention that some employees │ │    │
│   │ have been using the Internet and other            │      │
│   │ Information and Communication Technologies (ICTs)  │      │
│   │ for non-work purposes. From now on, the company   │      │
│   │ will closely monitor its use of the Internet and  │      │
│   │ other information technologies (for example,       │      │
│   │ e-mails, social networking services, online news,  │      │
│   │ transfers and financial transactions) within its  │      │
│   │ physical and virtual limits. Cyberloafing will     │      │
│   │ result in disciplinary actions that may include    │      │
│   │ termination of employment".                        │ ▼    │
│   └──────────────────────────────────────────────────┘      │
└─────────────────────────────────────────────────────────────┘
```

Figure 3. Anti-cyberloafing policy

Sources: elaborated by the authors.

The choice of methods

Covariance-based structural equation modeling (CB-SEM) was applied to examine the data and test the model structure and hypotheses (Gefen et al., 2000). CB-SEM is designed for theory building, confirmation and rejection, along with stringent multivariate assumptions. CB-SEM has been mainly used to confirm (or reject) theories, in this case part of the Khansa et al. (2017) model with adjustments. This method develops a theoretical covariance matrix based on specific equations, focusing on estimating the model to minimize the difference between the theoretical covariance matrix and the estimated covariance matrix. CB-SEM was used in this research because it is the best option to use the overall measure of the model's goodness of fit and the measurement model invariance test. PLS-SEM is used for complex structural models (with many constructs) that seek to develop new theories in exploratory research, which is not the case in this research (Hair et al., 2011).

The methods used in this research were: (1) covariance-based structural equation modeling (CB-SEM) verified the data and tested the structure and hypotheses of the model (Gefen et al., 2000). CB-SEM is designed for theory building, confirmation, and rejection along with rigorous multivariate assumptions; (2) the SEM approach measures linear interrelationships. At the same time, the artificial neural network (ANN) does so for linear and non-linear relationships between the identified factors influencing the variable of interest. Therefore, for the analysis, we employed an integrated SEM-ANN approach (Alam et al., 2020; Liébana-Cabanillas et al., 2017; Raut et al., 2018). For both methods employed, we used the IBM SPSS v.25 and AMOS v.24 software.

Results

Common method bias, non-response bias and collinearity

As primary data were used, it was necessary to ensure that no systematic bias was influencing the information collected. We checked common method variance (CMV) by applying

Harman's one-factor test (Podsakoff & Organ, 1986) to the 15 items, and we extracted five components with an eigenvalue greater than 1.0. The variance extracted by the first component was 23.91%, which is lower than the minimum of 50%. In addition, the analysis of non-response bias was performed according to Armstrong and Overton (1977). When carrying out these tests, it was found that both the common method bias and the non-response bias were not a significant problem. As the sample was considered large, two random subsamples were created and the multigroup effect of latent variables was analyzed (t-test). As a result, both subsamples showed equivalent behavior, so the full sample was kept. Late response bias was also examined, by comparing early (first month) and late (last month) responses, and no statistical differences were found between the groups. When analyzing the collinearity, it was discovered that all the variance inflation factors (VIFs) of the constructs were around 1 (PR=1.057, PC=1.214, CI=1.183, SE=1.158, and PJ=1.101). This indicates that there is no multicollinearity among the constructs. Therefore, we can assume that the regression coefficients are well estimated and suitable for the model.

Profile of respondents and organizations

The survey respondents' profile is presented in this section to characterize the sample of 517 people, 305 (59%) males and 212 (41%) females. Table 1 shows that the sample has a homogeneous profile composed of a young university and early career population, representing 86.7% (n=387). Regarding the average time in the company, the respondents have been there for just over two years (=25.56 months).

Table 1

Demographic characteristics of respondents

Characteristic	Total (n=517)	Characteristic	Total (n=517)
Age		*Hierarchical position*	
Up to 20	188 (36.4%)	Director/Manager	20 (3.9%)
From 21 to 30	286 (55.3%)	Coordinator/Supervisor	15 (2.9%)
From 31 to 40	36 (7%)	Analyst	53 (10.3%)
Over 41	7 (1.4%)	Assistant	125 (24.2%)
		Operational/Technical	159 (30.8%)
		Trainee/Apprentice	145 (28%)
Company sector		*Company size*	
Industry	43 (8.3%)	Micro	38 (7.4%)
Commerce	127 (24.6%)	Small	91 (17.6%)
Services	293 (56.7%)	Medium	121 (23.4%)
Public services	54 (10.4%)	Large	267 (51.6%)

Sources: elaborated by the authors.

Analysis of means

As shown in Table 2, Hotelling's T2 and multivariate analysis of variance (MANOVA) tests were developed for the predictive variables of the proposed model.

Table 2

Hotelling's T2 and MANOVA of the analyzed variables from the proposed model

Variables analyzed in the model	Sex - Male - Female	Management type - Parent - Flexible	Frequency of use (a few times a week/about once a day/less than once a week/several times an hour/a few times a day/once an hour)
Perceived risk	There is no effect on the groups.	There is no effect on the groups.	There is no effect on the groups.
Peer cyberloafing	There is no effect on the groups.	There is no effect on the groups.	There is an effect of frequency of use on peer cyberloafing [$F_{(1, 511)}$=8.207; p<.001]. Tukey's test indicates that the difference in means is in the 123 individuals (22.86%) who engage in cyberloafing between a few times a day and once an hour.
Perceived justice	There is no effect on the groups.	There is an effect of the group on self-efficacy [$F_{(1. 515)}$=12.773; p<.001]. This difference in means indicates that individuals who work in flexible ($\bar{x}$=4.73) companies have a greater sense of perceived justice.	There is no effect on the groups.
Self-efficacy	There is no effect on the groups.	There is no effect on the groups.	There is an effect of frequency of use on self-efficacy [$F_{(1, 511)}$=4.093; p=.001]. Tukey's test indicates that the difference in means is in the 123 individuals (22.86%) who have self-efficacy between a few times a day and once an hour.
Cyberloafing intention	There is an effect of the group on cyberloafing intention [$F_{(1, 515)}$=5.916; p=.015]. This difference in means indicates that females ($\bar{x}$=4.71) have a greater cyberloafing intention than males ($\bar{x}$=4.35).	There is an effect of the group on cyberloafing intention [$F_{(1, 515)}$=4.556; p=.033]. This difference in means indicates that individuals who work in flexible ($\bar{x}$=4.62) companies have a greater inclination toward cyberloafing intention.	There is an effect of frequency of use on cyberloafing intention [$F_{(1,.511)}$=34.354; p<.001]. Tukey's test indicates that the difference in means is in the 65 individuals (12.08%) who have a cyberloafing intention several times an hour.

Sources: elaborated by the authors.

Exploratory factor analysis

Regardless of the existing theoretical background, it is necessary to perform an exploratory factor analysis (EFA) to identify a potential structure or ensure that the measurements reflect accuracy (Fabrigar & Wegener, 2011). The first analysis of the scales - 'perceived risk' (PR), 'peer cyberloafing' (PC), 'self-efficacy' (SE), 'perceived justice' (PJ), and 'cyberloafing intention' (CI) -

occurred through the commonality matrix. For this analysis, the Kaiser-Meyer-Olkin (KMO) criterion, 0.745, and Bartlett's sphericity test, p<0.001, were used. After this procedure, the cross-loading was observed. There was no need to exclude any variable since all variables had a commonality score - the proportion of each variable's variability that is explained by the factors - greater than 0.5. The Cronbach's alpha results confirmed the reliability of the measurement items, as can be seen in the Appendix. The EFA test in SPSS software, with varimax rotation and an autovalue equal to 1.0, indicated the existence of the five components, as predicted in the research model, for a total variation explained by 74.39%, confirming all the dimensions predicted in the model. In fact, it is unnecessary to present this procedure because they are totally independent scales. Even so, we took the liberty of doing this test to demonstrate that it was possible to distinguish the scales using EFA and that each scale has distinct characteristics (Bido, Mantovani, & Cohen, 2018).

Confirmatory factor analysis

The confirmatory factor analysis (CFA), a covariance-based study (CB-SEM), was conducted to verify the fit of the measurement model with the support of SPSS and AMOS v.24, which has specific characteristics in the construction of the model that were not present in the simplified diagram of the theoretical model (Figure 2). Among them, there is a need to indicate the correlations between exogenous variables (in a path analysis), as well as the endogenous (dependent) variable receiving an error attribution (Figure 4). In order to test the convergent and discriminant validity, the strategy of correlating all exogenous and endogenous variables with each other was used. Maximum likelihood (ML) is the most widely used fitting function for structural equation models and was the method used to estimate the parameters for this study.

The judgment of the fit of the model should reflect the analysis of several criteria. The coefficients considered, the ratio between the chi-square ($\chi 2$) and degrees of freedom (df), and the CFI, TLI, GFI, IFI, PGFI, RMSEA, and SRMR goodness-of-fit indexes were used. The $\chi 2$ 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 fit. However, it is more common to consider its ratio concerning the degrees of freedom ($\chi 2$/df), whose values must be between 1 and 3 (Kline, 2015).

The CFI (comparative fit index), TLI (Tucker-Lewis index), GFI (goodness of fit of index), and IFI (incremental fit index) calculate the relative fit of the observed model, whose values above 0.95 indicate optimal fit and those above 0.90 indicate adequate fit. The PGFI (parsimony goodness of fit index) is recommended to have a value above 0.50. In turn, the RMSEA (root mean square error of approximation) is also a measure of a discrepancy, with results expected to be less than 0.05, but acceptable up to 0.08, despite such a coefficient penalizing a complex model. Finally, the SRMR (standardized root mean square residual) reports the standardized average of the residuals (discrepancies between the observed and modeled matrix), with indexes less than 0.10 indicative of a good fit (J. F. Hair et al., 2017; Kline, 2015; Schumacker & Lomax, 2010).

The details of the model fit are as follows: $\chi 2$=178.738 and df=80.00, resulting in a model fit; ($\chi 2$/df)=2.234, TLI=0.962, CFI=0.971, GFI=0.960, IFI=0.980, PGFI=0.640, SRMR=0.042, and RMSEA=0.049, indicating that all items meet the model and fit criteria.

The reliability analysis results, in Table 3, are as follows: the value of the AVE (average variance extracted) ranged from 0.577 to 0.651, indicating that all variables meet the criteria of 0.5 (Bagozzi & Yi, 1988). The internal consistency of the CR (composite reliability) was considered adequate, ranging from 0.776 to 0.880, with all variables above 0.7 or more (J. F. Hair et al., 2017). Jöreskog (1969) analyzed the MaxR(H) (maximum reliability) of the five factors, and the values were higher than 0.813. These values are considered quite satisfactory since the indexes must be greater than 0.7. The standard factor load of all items was above the recommended level (0.50), and based on the analysis results, the measurement model was acceptable, accepted, and reliable.
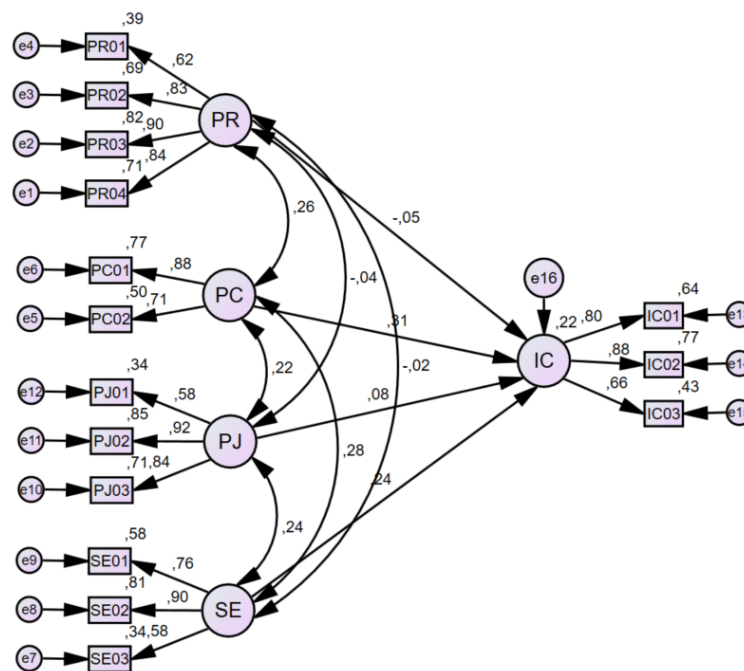

Figure 4. Structural equation model results

Sources: elaborated by the authors.

Discriminant validity is assessed by examining the loadings of the indicator construct and the correlations between the constructs. This is done by first comparing the square root of the AVE of each construct with all the correlations between it and other constructs (Fornell & Larcker, 1981), where the total square root of the AVEs must be greater than any of the correlations between the corresponding construct and another construct.

The maximum shared variance (MSV) and the average squared variance (ASV) were used to test the discriminant validity of the measurement model. The MSV and the ASV results need to be less than the AVE for discriminant validity (Hair et al., 2017). Table 3 shows that the MSV (the square of the highest correlation coefficient between latent constructs) and the ASV (the mean of the squared correlation coefficients between latent constructs) results are less than the AVE values, which means that the discriminant values are valid. Furthermore, the measurement model is under the initial assumptions noted in the structural equation model results in Table 4.

Table 3

Convergent and discriminant validity test

Construct	CR	MaxR(H)	AVE	MSV	ASV	PR	PC	PJ	SE	CI
PR	.880	.907	.651	.065	.017	**.807**				
PC	.776	.813	.637	.147	.091	.256***	**.798**			
PJ	.799	.861	.577	.123	.091	-.024	.279***	**.759**		
SE	.833	.895	.632	.059	.043	-.043	.219***	.244***	**.795**	
CI	.826	.856	.617	.147	.281	.016	.383***	.351***	.208***	**.785**

Note: ***p<.001

Sources: elaborated by the authors.

Table 4

Structural equation results

	Estimate (ß)	S.E.	t-test	p-value	Results
H_1	-.055	.041	-1.125	.260	Rejected
H_2	.312	.065	5.394	.000	Supported
H_3	.078	.047	1.583	.113	Rejected
H_4	.243	.086	4.476	.000	Supported

Sources: elaborated by the authors.

Artificial Neural Network (ANN)

The SEM likely oversimplifies the complexity of decisions since it can only detect linear relationships. Therefore, this study adopted an SEM-ANN approach to address this gap, as ANN does not require multivariate assumptions (e.g., linearity, normality, or homoscedasticity) and can identify linear and non-linear relationships (Lee et al., 2013). The variables determined by the SEM as input units for the ANN to overcome this limitation, providing greater predictive accuracy than linear models (Tan et al., 2014). Therefore, these methods can be complementary in a data analysis process. In this study, we proposed a multilayer perceptron (MLP) with the feed-forward back-propagation (FFBP) algorithm (Chong et al., 2015). The MLP had four input layers (independent variables), PR, PC, SE, PJ, and automatically calculated the hidden layers, which resulted in three depending on the complexity of the problem to be solved, and an output layer (the dependent variable), CI. From the means of the items of each variable ($\bar{V}_i$), the items were normalized [0, 1] by the following expression:

$$\bar{X}_i = \frac{\bar{V}_i - 1}{6} \tag{1}$$

This research process used the sigmoid function to activate neurons for hidden and output layers (Leong et al., 2013). The basic ANN model uses a supervised learning process in which the outputs are known and used in training (with a descending gradient optimization algorithm). The FFBP algorithm for prediction and classification was assumed to be an advanced multiple regression analysis (MRA) capable of dealing with complex and nonlinear relationships. We performed cross-validation with 90:10 data partition for training and testing, respectively. The number of hidden units was automatically generated, and the root mean square error (RMSE) was

calculated along with the normalized importance in the sensitivity analysis. The RMSE of the training and testing datasets for all ten neural networks and the means and standard deviations were calculated and presented in Table 5.

Table 5
RMSE values for the neural networks

| Network | Training | | | Testing | | | RMSE(Training)-RMSE |
	n	SSE	RMSE	n	SSE	RMSE	(Testing)
1	456	13.776	0.174	61	2.022	0.182	0.008
2	454	14.093	0.176	63	2.206	0.187	0.011
3	456	13.776	0.174	61	2.022	0.182	0.008
4	464	14.372	0.176	53	1.376	0.161	0.015
5	459	13.775	0.173	58	1.802	0.176	0.003
6	467	15.023	0.179	50	1.409	0.168	0.011
7	459	13.825	0.174	58	2.075	0.189	0.016
8	463	14.028	0.174	54	1.978	0.191	0.017
9	463	14.419	0.176	54	1.416	0.162	0.015
10	454	14.378	0.178	63	1.57	0.158	0.020
	mean	14.147	0.175	mean	1.788	0.176	0.012
	sd	0.405	0.002	sd	0.317	0.013	0.005

Note: SSE= sum of squared errors, RMSE=root mean square error, sd=standard deviation.

Sources: elaborated by the authors.

Definitions of these criteria are given below:

$$\text{SSE} = \sum_{t=1}^{n}(Q_t - \widehat{Q}_t) \tag{2}$$

$$\text{RMSE} = \sqrt{\frac{\text{SSE}}{n}} \tag{3}$$

Q_t is the observed data (Q) at time t, $\widehat{Q}_t$ is the predicted value at time t.

Validating the ANN model

In this study, an artificial neural network (ANN) model contains four input neurons, three hidden neurons (automatically calculated by SPSS software - usually, the number of hidden neurons is around 2/3 of the size of the input layer), and one output neuron. In addition, bias is a cell that issues a fixed value to contemplate 'starting values' that are ≠0 when all inputs are 0. Based on the RMSE values of the neural network (Table 5), we conclude that the ANN model has precision in the means for training ($\bar{x}_{training} = 0.175$) and testing ($\bar{x}_{testing} = 0.176$), respectively. Training determines weights and values for each bias to minimize forecast error and is used to estimate the network parameters. Testing feeds the already trained network with different data to verify if the network 'understands' the phenomenon and is used to prevent overtraining. Therefore, the models can provide an accurate prediction based on the RMSE values, indicating a fairly accurate prediction (Leong et al., 2013; Tan et al., 2014).

Sensitivity analysis

We conducted the sensitivity analysis to measure the strength of the weight resistances by calculating the normalized importance of the resistances from the ten ANN simulations. Normalized importance is the ratio of the relative importance to the greatest relative importance and is expressed as a percentage. Table 6 shows that the PC and SE are the most significant predictors in the sensitivity analysis, showing 100% normalized importance and 38.8% and 38.5%, respectively, of the average overall importance among the predictors of cyberloafing intention. Next, we have PJ ($\bar{x}_{PJ} = 17.7\%$) and PR ($\bar{x}_{PR} = 5\%$), according to the degree of importance. It is possible to observe the behavior of all predictors when analyzed through the importance value.

Table 6
Sensitivity analysis

	Relative importance			
Neural network (NN)	PR	PC	SE	PJ
NN (i)	0.069	0.358	0.359	0.214
NN (ii)	0.054	0.504	0.357	0.085
NN (iii)	0.069	0.358	0.359	0.214
NN (iv)	0.059	0.439	0.366	0.136
NN (v)	0.056	0.403	0.413	0.128
NN (vi)	0.041	0.338	0.429	0.192
NN (vii)	0.062	0.353	0.356	0.229
NN (viii)	0.028	0.365	0.426	0.181
NN (ix)	0.014	0.404	0.419	0.163
NN (x)	0.049	0.361	0.363	0.226
Average importance	0.050	0.388	0.385	0.177
Normalized importance (%)	13.3	100	99.8	47.1

Sources: elaborated by the authors.

Discussion

We achieved the objective of this research by proposing the development of a hybrid model in two stages (SEM-ANN) that allows for identifying the determining factors that were selected for this research to analyze the phenomenon of cyberloafing intention in response to the announcement of formal controls.

The sample was characterized as an early career population (86.5%) occupying an initial hierarchical position, such as assistant, operational, technical, trainee or apprentice. Most respondents belong to the services sector (56.7%) and work in medium and large companies. The analysis of means for the constructs that had an effect on 'cyberloafing intention' indicated that 'peer cyberloafing' and 'self-efficacy' occur a few times a day and once an hour. When we look at 'cyberloafing intention', the female group has a greater intention to practice cyberloafing than the male group. Furthermore, individuals belonging to flexible companies are more likely to practice cyberloafing, probably due to the autonomy granted. Finally, the analysis shows that a small group represented by 12.08% intends to engage in cyberloafing several times an hour.

The MANOVA results show that the female sex has a greater intention to practice cyberloafing, which contradicts the findings of the literature (Garrett & Danziger, 2008; Henle et

al., 2009; Zoghbi-Manrique-de-Lara, 2012; Zoghbi-Manrique-de-Lara & Sharifiatashgah, 2021). Regarding the type of management, it is observed that the variables 'perceived justice' and 'cyberloafing intention' have a similar influence on the flexible company. Finally, the observed frequency of use identified exactly the significant constructs in this study - 'peer cyberloafing', 'self-efficacy', and 'cyberloafing intention' - with the first two having similar characteristics, and 'cyberloafing intention' with individuals who intend to practice it several times an hour.

The research yielded interesting data that revealed that the measure of model fit - the coefficient of determination - of the dependent variable 'cyberloafing intention' was $R^2=0.22$ (22%). This explains employees' concern about engaging in cyberloafing at work, only a few times a week, based on the four constructs selected for this research ('perceived risk', 'peer cyberloafing', 'perceived justice', and 'self-efficacy'). Despite being a quality indicator, the coefficient of determination does not necessarily indicate whether a regressive model is adequate since it can have a low R^2 value for a good model (Kvalseth, 1985). Therefore, it is important to note what R^2 is evaluating. This case indicates what was already foreseen: after the announcement of formal controls, employees would be more likely not to engage in cyberloafing or even refrain from it.

Given the result, H_1 was rejected ($\beta=-0.055$; $t=-1.125$; $p=0.260$), as it did not negatively affect the construct 'perceived risk related to cyberloafing intention'. Although a non-significant result was obtained, the effect remained negative as expected. This is likely because employees are not concerned about being directly reprimanded or leaving a bad impression that affects their professional reputation. Also, this lack of a professional relationship can lead to a discussion that employees pay little attention to the risks or disregard them as 'real', and this, according to Barnett and Breakwell (2001), is understood as a behavior that is difficult to change, even after a formal control announcement (Khansa et al., 2017).

H_2 , regarding the causal relationship 'peer cyberloafing is positively related to cyberloafing intention', was supported ($\beta=0.312$; $t=5.394$; $p<0.001$) due to the respondents considering the influence of cyberloafing by their co-workers as acceptable and harmless, to justify their actions, especially in cases where it is used to minimize boredom, when there is a low workload, as corroborated by the results obtained by Pindek et al. (2018), Saghih and Nosrati (2021), and Suari and Rahyuda (2022). Additionally, there was an awareness of this effect with greater intensity among the female respondents. Thus, 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 network bonds among teams in terms of trust, enriching the professionals' performance and, as a result, the dynamics of work (Beri & Anand, 2020; Cao et al., 2016; Chavan et al., 2021; Metin-Orta & Demirtepe-Saygılı, 2021).

The cognitive relationship 'perceived justice is positively related to cyberloafing intention', as presented in H_3, was rejected ($\beta=0.078$; $t=1.583$; $p=0.113$). Although a non-significant result was obtained, the effect remained positive as expected. This is probably because employees do not have the opportunity to participate in performance reviews and reward systems (Beri & Anand, 2020). In this sense, employees can ignore formal controls and, as noted in this research, there are no repercussions. There are concerns regarding illegal practices in the use of ICTs by professionals in the workplace, as the organization may be obliged to involve employees legally for any

deviation. In addition, cyberloafing practices that violate organizational norms can legally lead to dismissal (Restubog et al., 2011).

Finally, H$_4$ was supported (ß=0.243; t=4.476; p<0.001), indicating that the path 'self-efficacy is positively related to cyberloafing intention' made employees develop, within the limits imposed under the conditions of specific skills, abilities, and capabilities 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 through the use of ICTs, the deviation of concentration and focus that can cause leisure and boredom can also make employees more confident in performing their activities and thus increase the quality of the activities performed (Pindek et al., 2018; Tandon et al., 2022). Announcements of formal controls probably stimulated individuals' reflection on fulfilling their responsibilities and meeting their expectations, as observed by Bandura (2001), and on the performance of the company's activities, as observed by Drnovšek et al. (2014). Mumtaz and Parohoo (2019) state that the existing literature establishes that self-efficacy is necessary for creativity. It was observed as one of the main factors employed in behavioral intentions, specifically cyberloafing intention. Self-efficacy was considered one of the main constructs when analyzing issues that rethink the ability to get involved and collaborate with new ideas or even foster innovation with co-workers and the organization.

Using the SEM-ANN approach made it possible to test the sample in a predictive way, allowing the algorithm to simulate ten different learning scenarios. In this sense, the ANN obtained an adequate performance based on the data obtained in the sample. Both SEM and ANN approaches obtained similar and, at the same time, complementary results, validating the results of the hypotheses. Therefore, with the use of these approaches together, it is possible to affirm that future studies that use these factors will likely obtain results very similar to this research.

This research can provide senior executives and managers with information on how they can deal with cyberloafing within organizations in a balanced way, depending on the management style employed, whether 'more controlling' or 'flexible'. The present study shows that employees' feelings about cyberloafing are valuable for the organization and society to reflect on the limits of these activities. Therefore, executives and managers should focus their efforts on improving employees' perceptions of meaningful work, clearly communicating the value of employees' contributions to their personal lives, organizations, and society (Agarwal & Avey, 2020; Usman et al., 2019).

Supervisors can also improve employees' perceptions 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 holds for others (e.g., implications for colleagues, organization, and society). In doing so, supervisors can restrict employee involvement in cyberloafing with the support of expository methods that include formal control announcements.

Both popular media and academic research negatively portray cyberloafing as a problem and support monitoring and restricting personal use of technology. However, organizations must attract and retain new generations, and it is crucial to understand their characteristics and what

drives them (S. Kim, 2018). Based on research on generational differences and organizational control, it is possible to explain how the unique characteristics of millennials lead them to engage in the personal use of technology at work and how organizations can deal with any problems that may occur. These solutions include establishing a technology use policy in the workplace based on a common understanding among all.

In addition, this is a competitive era in which executives and managers emphasize economic values, which is conducive to creating a significant labor crisis, resulting in dysfunctional behaviors, e.g., cyberloafing. Therefore, it is suggested that companies' top management may play a central role in creating a balance between connecting social and economic values for employees to combat the labor crisis (Tandon et al., 2022). Managers can do this by providing employees with autonomy, improving their self-esteem, establishing a sense of responsibility, facilitating easier access to resources, and developing trust-based relationships. This would help senior management deter employees' involvement in cyberloafing and other dysfunctional behaviors, making them more determined to complete their work.

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

Conclusions

Given the results obtained in this study, it can be concluded that the purpose of this paper, which was to analyze the antecedent factors that lead to cyberloafing and deviant behavior in response to the announcement of formal controls, was achieved. In addition, applying two-stage CB-SEM based on deep learning and ANN analysis proves to be a robust methodological approach, detecting linear and non-linear associations between the factors.

The research addressed a theme that involves a paradoxical relationship (positive and negative) in the use of ICTs for personal purposes in organizations (Hu et al., 2021; Zhu et al., 2021). H_4 indicated that, by adopting a permissive position and giving employees greater freedom in using ICTs, organizations exempt themselves from restrictions and expect employees' attitudes to be sensible, thus avoiding negative consequences and creating innovation spaces (Kessel et al., 2012; Rahmah, Nurmayanti, & Surati, 2020; Rahman & Surjanti, 2022). The H_2 result raises the discussion of productivity. For example, scientific literature indicates that cyberloafing can help with boredom, fatigue, psychological disorders (anxiety, stress, depression, loneliness, among others), and the balance between the personal and professional spheres. However, it can also lead to loss of productivity and performance (Beri & Anand, 2020; Chavan et al., 2021; Metin-Orta & Demirtepe-Saygılı, 2021; Wisse et al., 2015). Thus, both positive and negative effects coexist and affect employee productivity and innovation in different organizations (Rahmah, Nurmayanti, & Surati, 2020; Rahman & Surjanti, 2022).

The study showed that, on average, women engage in cyberloafing more than men, and that those who work in flexible companies are more likely to engage in cyberloafing than those who work in parent companies. The respondents who work in flexible companies have a better

perception of fairness. In addition, the reported frequency of practicing cyberloafing is one hour per day, which is lower than the two hours per day of engagement observed by Andel et al. (2019).

This study corroborates the results of recent research, which found that the interviewees perceived the opposing side in terms of loss of time and concentration when they practice cyberloafing, even after the company announcement. The employees also perceived that they can use technologies for personal purposes in the workplace in times of boredom (Pindek et al., 2018), as an 'escape valve' to recover before returning to their tasks.

This research indicated that a tendency for cyberloafing could lead to inefficiency and generate costs for companies, even in a situational way. While some organizations try to eliminate these behaviors by installing security options, such as firewalls, others are still alarmed because they cannot prevent this behavior. For cyberloafing to occur, all it takes is a mobile device and Internet access. Internet use in the workplace is growing and raising much attention to the adverse 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.

Among the main lessons learned from the study and that can stimulate the interest of other researchers, we can highlight that: (1) the control mechanisms do not eliminate the problem, so it is necessary to create people management policies that foster a creative spirit and innovation so that these tools are part of the solution and not part of the problem; (2) it is a topic that deserves more attention and in-depth study of the antecedent and consequent variables of 'cyberloafing intention'; (3) there is a natural tendency for professionals to increasingly use personal devices, due to the effect of Bring Your Own Device (BYOD), in their organizations, which can favor the practice of cyberloafing; and (4) there is an infinite number of possible analyses to be carried out based on behavioral and psychological constructs that can provide theoretical contributions.

The results emphasize the importance of evaluating cyberloafing as part of the well-being of students in the labor market, rather than as a variable merely related to professional performance (Chavan et al., 2021; Metin-Orta & Demirtepe-Saygılı, 2021). The study results may also help to enlighten researchers and managers in developing appropriate policies and interventions to manage Internet misuse in the workplace.

Limitations and future research directions

This research examined a sample of 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, we propose analyzing the behavior of employees according to the size of the institution (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 can overload ICTs with improper use (here adapted to 'cyberloafing'), affecting productivity. Also, issues of labor costs and waste of activities could be analyzed. Finally, we also suggest studies involving problematic Internet usage as an antecedent factor for cyberloafing.

References

Alam, M. Z., Hu, W., Kaium, M. A., Hoque, M. R., & Alam, M. M. D. (2020). Understanding the determinants of mHealth apps adoption in Bangladesh: A SEM-Neural network approach. Technology in Society, 61, 101255. https://doi.org/10.1016/j.techsoc.2020.101255

Agarwal, U. A., & Avey, J. B. (2020). Abusive supervisors and employees who cyberloaf: Examining the roles of psychological capital and contract breach. *Internet Research*, *30*(3), 789–809. https://doi.org/10.1108/INTR-05-2019-0208

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Aladwan, M., Muala, I. dan Salleh, H. (2021). Cyberloafing as a mediating variable in the relationship between workload and organizational commitment. *Management Science Letters*, *11*(3), 1013-1022. http://dx.doi.org/10.5267/j.msl.2020.9.041

Andel, S. A., 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. https://doi.org/10.1016/j.chb.2019.07.013

Archambault, É., Campbell, D., Gingras, Y., & Larivière, V. (2009). Comparing bibliometric statistics obtained from the Web of Science and Scopus. *Journal of the American Society for Information Science and Technology*, *60*(7), 1320–1326. https://doi.org/10.1002/asi.21062

Armstrong, J. S., & Overton, T. S. (1977). Estimating Nonresponse Bias in Mail Surveys. *Journal of Marketing Research*, *14*(3), 396–402. https://doi.org/10.1177/002224377701400320

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. https://doi.org/10.1016/j.chb.2014.04.006

Bandura, A. (2001). Social cognitive theory: An agentic perspective. *Annual Review of Psychology*, *52*(1), 1–26. https://doi.org/10.1146/annurev.psych.52.1.1.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74–94. https://doi.org/10.1007/BF02723327

Barnett, J., & Breakwell, G. M. (2001). Risk Perception and Experience: Hazard Personality Profiles and Individual Differences. *Risk Analysis*, *21*(1), 171–178. https://doi.org/10.1111/0272-4332.211099

Beri, D.N. & Anand, S. (2020). Consequences Of Cyberloafing –A Literature Review. *European Journal of Molecular & Clinical Medicine*, *7*(6), 434–440.

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*, *26*(4), 23–42. doi:10.4018/joeuc.2014100102

Bido, D. S., Mantovani, D. M. N., & Cohen, E. D. Destruição de escalas de mensuração por meio da análise fatorial exploratória nas pesquisas da área de produção e operações. *Gestão & Produção*, *25*(2), 384-397. http://dx.doi.org/10.1590/0104-530x3391-16

Blanchard, A. L., & Henle, C. A. (2008). Correlates of different forms of cyberloafing: The role of norms and external locus of control. *Computers in Human Behavior*, *24*(3), 1067–1084. https://doi.org/10.1016/j.chb.2007.03.008

Cao, X., Guo, X., Vogel, D., & Zhang, X. (2016). Exploring the influence of social media on employee work performance. *Internet Research*, *26*(2), 529–545. https://doi.org/10.1108/IntR-11-2014-0299

Chavan, M., Galperin, B. L., Ostle, A., & Behl, A. (2021). Millennial's perception on cyberloafing: Workplace deviance or cultural norm? *Behaviour & Information Technology*, 1–18. https://doi.org/10.1080/0144929X.2021.1956588

Cheng, B., Zhou, X., Guo, G., & Yang, K. (2020). Perceived Overqualification and Cyberloafing: A Moderated-Mediation Model Based on Equity Theory. *Journal of Business Ethics*, *164*(3), 565–577. https://doi.org/10.1007/s10551-018-4026-8

Chong, A., Y-L., Liu, M. J., Luo, J., & Keng-Boon, O. (2015). Predicting RFID adoption in healthcare supply chain from the perspectives of users. *International Journal of Production Economics*, 159(C), 66–75. https://doi.org/10.1016/j.ijpe.2014.09.034

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. https://doi.org/10.2753/MIS0742-1222310210

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. https://doi.org/10.1287/isre.1070.0160

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. https://doi.org/10.1016/j.sbspro.2016.11.070

Dmour, M. M., Bakar, H. S., & Hamzah, M. R. (2019). Antecedent, Consequences, and Policies View of Cyberloafing among the Employees. *Journal of Physics*, 1–12. https://doi.org/10.1088/1742-6596/1529/2/022016

Drnovšek, M., Slavec, A., and Cardon, M. S. (2014). "Cultural context, passion and self-efficacy: do entrepreneurs operate on different 'planets'?," in *Handbookof Entrepreneurial Cognition*, eds B. Randolph-Seng, R. K. Mitchell, and J. R. Mitchell (Cheltenham: Edward Elgar Publishing).

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. https://doi.org/10.1080/0144929X.2012.745608

Fabrigar, L. R., & Wegener, D. T. (2011). *Exploratory Factor Analysis* (1 edition). Oxford University Press, Usa.

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18*(1), 39–50. JSTOR. https://doi.org/10.2307/3151312

Garrett, R. K., & Danziger, J. N. (2008). On Cyberslacking: Workplace Status and Personal Internet Use at Work. *CyberPsychology & Behavior*, *11*(3), 287–292. https://doi.org/10.1089/cpb.2007.0146

Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural Equation Modeling and Regression: Guidelines for Research Practice. *Communications of the Association for Information Systems*, 4, 1–77. https://doi.org/10.17705/1CAIS.00407

George, D., & Mallery, P. (2002). *SPSS for Windows Step by Step: A Simple Guide and Reference*, 11.0 Update (4o ed). Allyn & Bacon.

Greenfield, D. N., & Davis, R. A. (2002). Lost in cyberspace: The Web @ work. *CyberPsychology & Behavior*, *5*(4), 347–353. https://doi.org/10.1089/109493102760275590

Hair, J., Anderson, R., & Babin, B. (2009). *Multivariate Data Analysis* (7th Edition). Prentice Hall.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). A primer on partial least squares structural equation modeling (PLS-SEM). SAGE. http://www.vlebooks.com/vleweb/product/openreader?id=Liverpool&isbn=9781483377438

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152. doi:10.2753/mtp1069-6679190202

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. https://doi.org/10.1016/j.chb.2009.03.005

Hensel, P. G., & Kacprzak, A. (2021). Curbing cyberloafing: Studying general and specific deterrence effects with field evidence. *European Journal of Information Systems*, *30*(2), 219–235. https://doi.org/10.1080/0960085X.2020.1756701

Hsu, M.-H., Chang, C.-M., & Yen, C.-H. (2011). Exploring the antecedents of trust in virtual communities. *Behaviour & Information Technology*, *30*(5), 587–601. https://doi.org/10.1080/0144929X.2010.549513

Hu, Y., Chen, Y., & Ye, M. (2021). Eager to belong: Social cyberloafing as a coping response to workplace ostracism. *Current Psychology*. https://doi.org/10.1007/s12144-021-01690-y

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.

Jarvis, L. C. (2016). Identification, intentions and entrepreneurial opportunities: an integrative process model. *International Journal of Entreprise Behavior & Research*, 22, 182–198. doi: 10.1108/ijebr-02-2015-0041

Jöreskog, K. G. (1969). A general approach to confirmatory maximum likelihood factor analysis. *Psychometrika*, *34*(2), 183–202. https://doi.org/10.1007/BF02289343

Kaptangil, K., Aşan, K., & gargacı, A. (2021). The effect of the cyberloafing behaviors of tourism business employees on business motivations and organizational identification. *Tourism & Management Studies*, 17, 31–43. https://doi.org/10.18089/tms.2021.170103

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*(2–3), 146–153. https://doi.org/10.1016/j.healthpol.2012.02.010

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. https://doi.org/10.1080/07421222.2017.1297173

Kim, K., del Carmen Triana, M., Chung, K., & Oh, N. (2016). When Do Employees Cyberloaf? An Interactionist Perspective Examining Personality, Justice, and Empowerment. *Human Resource Management*, *55*(6), 1041–1058. https://doi.org/10.1002/hrm.21699

Kim, S. (2018). Managing millennials' personal use of technology at work. *Business Horizons*, *61*(2), 261–270. https://doi.org/10.1016/j.bushor.2017.11.007

Kim, S. J., & Byrne, S. (2011). Conceptualizing personal web usage in work contexts: A preliminary framework. *Computers in Human Behavior*, *27*(6), 2271–2283. https://doi.org/10.1016/j.chb.2011.07.006

Kline, R. B. (2015). *Principles and Practice of Structural Equation Modeling*, Fourth Edition (Edição: Fourth). The Guilford Press.

Koay, K. Y. (2018). Workplace ostracism and cyberloafing: A moderated–mediation model. *Internet Research*, 28(4), 1122–1141. https://doi.org/10.1108/IntR-07-2017-0268

Koay, K. Y., Soh, P. C.-H., & Chew, K. W. (2017). Do employees' private demands lead to cyberloafing? The mediating role of job stress. *Management Research Review*, *40*(9), 1025–1038. https://doi.org/10.1108/MRR-11-2016-0252

Kobbeltvedt, T., & Wolff, K. (2009). The risk-as-feelings hypothesis in a theory-of-planned-behaviour perspective. *Judgment and Decision Making*, *4*(7), 567–586. https://doi.org/10.1017/S1930297500001145

Kvalseth, T. O. (1985). Cautionary Note about R^2. *The American Statistician*, *39*(4), 279–285. https://doi.org/10.2307/2683704

Lai, M. (2008). Technology readiness, internet self-efficacy and computing experience of professional accounting students. *Campus-Wide Information Systems*, *25*(1), 18–29. https://doi.org/10.1108/10650740810849061

Lambert, E. G., & Hogan, N. L. (2013). The Association of Distributive and Procedural Justice With Organizational Citizenship Behavior. *The Prison Journal*, *93*(3), 313–334. https://doi.org/10.1177/0032885513490491

Lee, V.-H., Leong, L.-Y., Hew, T.-S., & Ooi, K.-B. (2013). Knowledge management: A key determinant in advancing technological innovation? *Journal of Knowledge Management*, *17*(6), 848–872. https://doi.org/10.1108/JKM-08-2013-0315

Leong, L.-Y., Hew, T.-S., Tan, G. W.-H., & Ooi, K.-B. (2013). Predicting the determinants of the NFC-enabled mobile credit card acceptance: A neural networks approach. *Expert Systems with Applications*, *40*(14), 5604–5620. https://doi.org/10.1016/j.eswa.2013.04.018

Li, C., Murad, M., Shahzad, F., Khan, M. A. S., Ashraf, S. F., & Dogbe, C. S. K. (2020). Entrepreneurial Passion to Entrepreneurial Behavior: Role of Entrepreneurial Alertness, Entrepreneurial Self-Efficacy and Proactive Personality. *Frontiers in Psychology*, 11. https://doi.org/10.3389/fpsyg.2020.01611

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. https://doi.org/10.1016/j.chb.2011.06.015

Liébana-Cabanillas, F., Marinković, V., & Kalinić, Z. (2017). A SEM-neural network approach for predicting antecedents of m-commerce acceptance. *International Journal of Information Management*, *37*(2), 14–24. https://doi.org/10.1016/j.ijinfomgt.2016.10.008

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. https://doi.org/10.1002/job.161

Lim, V. K. G., & Chen, D. J. Q. (2012). Cyberloafing at the workplace: Gain or drain on work? *Behaviour & Information Technology*, *31*(4), 343–353. https://doi.org/10.1080/01449290903353054

Lim, V. K. G., & Teo, T. S. H. (2005). Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore. *Information & Management*, *42*(8), 1081–1093. https://doi.org/10.1016/j.im.2004.12.002

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. https://doi.org/10.1108/17537981111190042

Metin-Orta, I., & Demirutku, K. (2020). Cyberloafing behaviors among university students and its relation to Hedonistic-Stimulation value orientation, cyberloafing attitudes, and time spent on the Internet. *Current Psychology*. https://doi.org/10.1007/s12144-020-00932-9

Metin-Orta, I., & Demirtepe-Saygılı, D. (2021). Cyberloafing behaviors among university students: Their relationships with positive and negative affect. *Current Psychology* (New Brunswick, N.J.), 1–14. https://doi.org/10.1007/s12144-021-02374-3

Mohammed Abubakar, A., & Al-zyoud, M. F. (2021). Problematic Internet usage and safety behavior: Does time autonomy matter? *Telematics and Informatics*, 56, 101501. https://doi.org/10.1016/j.tele.2020.101501

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 & Management*, 50(6), 322–335. https://doi.org/10.1016/j.im.2013.04.005

Mumtaz, S., & Parahoo, S. K. (2019). Promoting employee innovation performance: Examining the role of self-efficacy and growth need strength. *International Journal of Productivity and Performance Management*, *69*(4), 704-722. doi: 10.1108/IJPPM-12-2017-0330

Pee, L. G., Woon, I. M. Y., & Kankanhalli, A. (2008). Explaining non-work-related computing in the workplace: A comparison of alternative models. *Information & Management*, *45*(2), 120–130. https://doi.org/10.1016/j.im.2008.01.004

Pindek, S., Krajcevska, A., & Spector, P. E. (2018). Cyberloafing as a coping mechanism: Dealing with workplace boredom. *Computers in Human Behavior*, 86, 147–152. https://doi.org/10.1016/j.chb.2018.04.040

Podsakoff, P. M., & Organ, D. W. (1986). Self-Reports in Organizational Research: Problems and Prospects. *Journal of Management*, *12*(4), 531–544. https://doi.org/10.1177/014920638601200408

Rahaei, A., & Salehzadeh, R. (2020). Evaluating the impact of psychological entitlement on cyberloafing: The mediating role of perceived organizational justice. *Vilakshan - XIMB Journal of Management*, *17*(1/2), 137–152. https://doi.org/10.1108/XJM-06-2020-0003

Rahman, M. F. W., & Surjanti, A. K. (2022) Does cyberloafing and person-organization fit affect employee performance? The mediating role of innovative work behavior. *Global Business and Organizational Excellence*, *41*(5), 44-64.

Rahmah, I. L., Nurmayanti, S. dan Surati. (2020). The Role of Cyberloafing Mediation on The Influence of Role Conflict and Role Ambiguity On Performance, *International Journal of Innovative Science, Engineering & Technology*, *7*(7), 207–220.

Ratnasari, S. D. & Tarimin, T. (2021). Efek Perilaku Individu terhadap Kinerja Karyawan. *Jurnal Administrasi Bisnis*, *10*(2), 165-175.

Raut, R. D., Priyadarshinee, P., Gardas, B. B., & Jha, M. K. (2018). Analyzing the factors influencing cloud computing adoption using three stage hybrid SEM-ANN-ISM (SEANIS) approach. *Technological Forecasting and Social Change*, 134, 98–123. https://doi.org/10.1016/j.techfore.2018.05.020

Restubog, S. L. D., Garcia, P. R. J. M., Toledano, L. S., Amarnani, R. K., Tolentino, L. R., & 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. https://doi.org/10.1016/j.jrp.2011.01.006

Saghih, A. M. F., & Nosrati, S. (2020). The antecedents of job embeddedness and their effects on cyberloafing among employees of public universities in eastern Iran. *International Journal of Islamic and Middle Eastern Finance and Management*, *14*(1), 77-93. https://doi.org/10.1108/IMEFM-11-2019-0489

Sánchez, A. D., de la Cruz Del Río Rama, M., & García, J. Á. (2017). Bibliometric analysis of publications on wine tourism in the databases Scopus and WoS. *European Research on Management and Business Economics*, *23*(1), 8–15. https://doi.org/10.1016/j.iedeen.2016.02.001

Schumacker, R. E., & Lomax, R. G. (2010). *A beginner's guide to structural equation modeling*, 3rd ed (p. xx, 510). Routledge/Taylor & Francis Group.

Shaddiq, S., Haryono, S., Uii, M., & Isfianadewi, D. (2021). 'Antecedents and Consequences of Cyberloafing in Service Provider Industries: Industrial Revolution 4.0 and Society 5.0', *Journal*

of Asian Finance, Economics and Business, 8(1), 157–167. http://dx.doi.org/10.13106/jafeb.2021.vol8.no1.157

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, *34*(3), 487. https://doi.org/10.2307/25750688

Smith, K. (2020, janeiro 21). *The Small Business Daily Rundown: Are You a Cyberloaf?* Workest. https://www.zenefits.com/workest/the-small-business-daily-rundown-are-you-a-cyberloaf/

Suari, G. A. M. S. & Rahyuda, A. G. (2022). The effect of role ambiguity on cyberloafing with work stress as a mediation variable. *International Journal of Health Sciences*, *6*(S4), 2211–2219. https://doi.org/10.53730/ijhs.v6nS4.7145

Tan, G. W.-H., Ooi, K.-B., Leong, L.-Y., & Lin, B. (2014). Predicting the drivers of behavioral intention to use mobile learning: A hybrid SEM-Neural Networks approach. *Computers in Human Behavior*, 36, 198–213. https://doi.org/10.1016/j.chb.2014.03.052

Tandon, A., Kaur, P., Ruparel, N., Islam, J. U., & Dhir, A. (2022). Cyberloafing and cyberslacking in the workplace: Systematic literature review of past achievements and future promises. *Internet Research*, *32*(1), 55–89. https://doi.org/10.1108/INTR-06-2020-0332

Taylor, S., & Todd, P. A. (1995). Understanding Information Technology Usage: A Test of Competing Models. *Information Systems Research*, *6*(2), 144–176. https://doi.org/10.1287/isre.6.2.144

Triandis, H. (1980). Values, attitudes, and interpersonal behavior, Nebraska Symposium on Motivation, 27, 195–259.

Ugrin, J. C., Pearson, J. M., & Nickle, S. M. (2018). An Examination of the Relationship between Culture and Cyberloafing Using the Hofstede Model. *Journal of Internet Commerce*, *17*(1), 46–63. https://doi.org/10.1080/15332861.2018.1424395

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. https://doi.org/10.1080/0144929X.2019.1683607

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, *46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Vitak, J., Crouse, J., & LaRose, R. (2011). Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior*, *27*(5), 1751–1759. https://doi.org/10.1016/j.chb.2011.03.002

Wisse, B., Barelds, D. P. H., & Rietzschel, E. F. (2015). How innovative is your employee? The role of employee and supervisor Dark Triad personality traits in supervisor perceptions of employee innovative behavior. *Personality and Individual Differences*, 82, 158–162. https://doi.org/10.1016/j.paid.2015.03.020

Wu, J., Mei, W., Liu, L., & Ugrin, J. C. (2020). The bright and dark sides of social cyberloafing: Effects on employee mental health in China. *Journal of Business Research*, 112, 56–64. https://doi.org/10.1016/j.jbusres.2020.02.043

Wu, J., Mei, W., Ugrin, J., Liu, L., & Wang, F. (2020). Curvilinear performance effects of social cyberloafing out of class: The mediating role as a recovery experience. *Information Technology & People*, *34*(2), 581–598. https://doi.org/10.1108/ITP-03-2019-0105

Yellowlees, P. M., & Marks, S. (2007). Problematic Internet use or Internet addiction? *Computers in Human Behavior*, *23*(3), 1447–1453. https://doi.org/10.1016/j.chb.2005.05.004

Zhu, J., Wei, H., Li, H., & Osburn, H. (2021). The paradoxical effect of responsible leadership on employee cyberloafing: A moderated mediation model. *Human Resource Development Quarterly*, *32*(4), 597–624. https://doi.org/10.1002/hrdq.21432

Zoghbi-Manrique-de-Lara, P. (2012). Reconsidering the boundaries of the cyberloafing activity: The case of a university. *Behaviour & Information Technology*, *31*(5), 469–479. https://doi.org/10.1080/0144929X.2010.549511

Zoghbi-Manrique-de-Lara, P., & Sharifiatashgah, M. (2021). The relationship between perceived crowding and cyberloafing in open offices at Iranian IT-based companies. *Cognition, Technology & Work*, *23*(2), 331–342. https://doi.org/10.1007/s10111-020-00627-y

Funding

Authorship

Vanessa Itacaramby Pardim

Doctoral student in Administration at the University of São Paulo, Faculty of Economics, Administration, Accounting and Actuarial Science (FEA-USP); Professor of Administration at the Nove de Julho University (UNINOVE).

E-mail: vanessa.itacaramby@usp.br

ORCID: https://orcid.org/0000-0003-0893-7271

Luis Hernan Contreras Pinochet

Professor of the Academic Department of Administration (DAA) of the Paulista School of Politics, Economics and Business (EPPEN) of the Federal University of São Paulo (UNIFESP).

E-mail: luis.hernan@unifesp.br

ORCID: https://orcid.org/0000-0003-2088-5283

Cesar Alexandre de Souza

Professor at the University of São Paulo, Faculty of Economics, Administration, Accounting and Actuarial Science (FEA-USP); Permanent member of the stricto sensu Graduate Program in Administration.

E-mail: calesou@usp.br

ORCID: https://orcid.org/0000-0001-8941-8582

Conflicts of interest

The authors have stated that there are no conflicts of interest.

Inclusive language

The authors use inclusive language that acknowledges diversity, shows respect for all people, is sensitive to differences, and promotes equal opportunities.

Authors' contributions

Vanessa Itacaramby Pardim: conceptualization (equal); data curation (supporting); formal analysis (equal); methodology (equal); project administration (supporting); resources (equal); supervision (equal); validation (equal); visualization (equal); writing - original draft (supporting); writing - review & editing (equal).

Luis Hernan Contreras Pinochet: conceptualization (equal); data curation (supporting); formal analysis (equal); methodology (lead); project administration (lead); resources (equal); supervision (equal); validation (equal); visualization (equal); writing - original draft (supporting); writing - review & editing (equal).

Cesar Alexandre de Souza: conceptualization (equal); data curation (supporting); formal analysis (equal); methodology (equal); project administration (supporting); resources (equal); supervision (equal); validation (equal); visualization (equal); writing - original draft (supporting); writing - review & editing (equal).

Plagiarism check

O&S submit all documents approved for publication to a plagiarism check, using specific tools.

Data availability

O&S encourages data sharing. However, in compliance with ethical principles, it does not demand the disclosure of any means of identifying research participants, preserving fully their privacy. The practice of open data seeks to ensure the transparency of research results, without revealing the identity of research participants.