UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ADMINISTRAÇÃO
DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO

GABRIELA LABRES MALLMANN

DEVIANCE AND ITS FACETS: A MULTI-LEVEL INVESTIGATION OF DEVIANT BEHAVIOR IN IS

Porto Alegre
2020

GABRIELA LABRES MALLMANN

DEVIANCE AND ITS FACETS: A MULTI-LEVEL INVESTIGATION OF DEVIANT BEHAVIOR IN IS

A dissertation submitted to the Postgraduate Program in Administration of the Universidade Federal do Rio Grande do Sul in partial satisfaction of the requirements for the degree Doctor of Philosophy in Management Information Systems.

Advisor: Antonio Carlos Gastaud Maçada

Porto Alegre
2020

CIP – Catalogação na Publicação

GABRIELA LABRES MALLMANN

DEVIANCE AND ITS FACETS: A MULTI-LEVEL INVESTIGATION OF DEVIANT BEHAVIOR IN IS

A dissertation submitted to the Postgraduate Program in Administration of the Universidade Federal do Rio Grande do Sul in partial satisfaction of the requirements for the degree Doctor of Philosophy in Management Information Systems.

Thesis defended and approved in …

Examination Committee:

Prof. Dr. Antonio Carlos Gastaud Maçada, Advisor
UFRGS

Prof. Dr. Andreas Eckhardt, External Advisor
GGS

Prof. Dra. Míriam Oliveira
PUCRS

Prof. Dr. Pietro Cunha Dolci
UNISC

To my family, with gratitude.

ACKNOWLEDGMENTS

I am grateful for all the support and opportunities I have been receiving, in all dimensions of my life, everywhere I go. There is a whole universe of possibilities out there. You do not need to let your rational mind limit you or let your fears hold you back; the universe is vast and abundant. Only for believing in this, I am already grateful.

To my family: *Aos meus pais, Rejane e José Paulo, obrigada por me incentivarem a ser a melhor pessoa que posso ser. Aprendi valores do bem e responsabilidade com vocês. Valores que servem de base para tudo mais na minha existência. Sou incrivelmente grata a sabedoria, amor e apoio de toda minha família. Meus irmãos Paula e Paulo Gabriel, minha família de Porto Alegre (dinda Geci e Thaís), dinda Rose que é meu destino de férias preferido, e meus avós Célia e Antônio. A todos meu muito obrigada por todo o amor e apoio. Não seria quem sou sem o suporte de vocês.*

I would like to say a special thank you for my advisor Professor Antonio Maçada, for the partnership since 2010. It has been a long road, full of challenges, achievements, advice, motivational words, ideas, and support. Thank you for believing in my potential since I was an undergraduate student. If today I can fly higher, it is because you motivated me to go further than I ever thought.

I thank the Universidade Federal do Rio Grande do Sul and everybody that makes this a great university with tradition and excellence in teaching and research. Studying abroad, I could realize how well the university has prepared me for the challenges of academic life. I am thankful also for all the colleagues I have met during my time at UFRGS, with whom I have exchanged so much. Especially, thank you Gustavo Montesdioca, and Cláudinha for all help and support. I thank also CNPq, CAPES, and DAAD for financially support my research projects.

I am extremely thankful for everybody that Germany has brought to my life. Especially, my German advisor, Professor Andreas Eckhardt, who has devoted his time to help and teach me since I arrived in Germany. Thank you so much, Andreas, for giving me this opportunity, for all the long discussions that allow me to learn so much and grown as an academic and a person. I thank my colleagues and friends Lennart, Ines, Victoria, Gregor, and Daniel for being the best Germans I could ever meet, with whom I shared amazing and challenging moments. Also, all the Brazilian girls, especially Renata and Karol, whom Germany gave me as a gift to make me feel less homesick. And I would never forget my best friend from school, Laíde, who stayed in Brazil but is always taking part in my life no matter how. Guys, I will keep you in my heart wherever I go.

“The only true wisdom is in knowing you know nothing.”

Socrates

ABSTRACT

The pervasiveness of technology in our private and professional lives is causing relevant changes to individuals, organizations, and society. Technology is widely available nowadays and individuals are able to find new solutions and exploit their functionalities autonomously. As a result, employees are finding ways to use consumer technologies from their personal lives in the workplace, which is challenging the traditional way to manage technology within organizations. Within this context, deviant behaviors such as the use of unauthorized technology in the workplace, called shadow IT, is attracting attention as a relevant and underexplored organizational phenomenon. Few studies have addressed shadow IT usage at the individual level, but none addresses shadow IT usage from a group-level perspective. The general objective of this dissertation is to investigate the antecedents and consequences of shadow IT usage considering a multi-level perspective (individual and collective). This research aims to investigate deviant behavior in IS taking shadow IT usage as an instance and examining it from different perspectives and methods. This dissertation provides theoretical implications to individual and collective workplace deviance in the IS domain. It contributes also to the emerging body of knowledge regarding shadow IT usage by investigating the phenomenon from a multi-level perspective. Moreover, this dissertation provides implications for IS police violation and security research by addressing shadow IT as collective deviance. A better understanding of the collective deviant behavior of employees within organizations can aid to cope with IS norms violations, providing new insights about policy development and strategies to mitigate such behaviors and increase information security.

Keywords: Workplace Deviant Behavior, Collective Deviance, Shadow IT, Collective IS Deviance, IT Management.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

MIS – Management Information Systems

IS – Information Systems

IT – Information Technology

SIT – Shadow IT

ITD – Information Technology Department

BYOD – Bring-Your-Own-Device

ERP – Enterprise Resource Planning

SPT – Social Presence Theory

SUMMARY

1 INTRODUCTION

The pervasiveness of technology in our private and professional lives is causing relevant changes to individuals, organizations, and society. Not only technology is widely available nowadays, but also individuals are able to find new solutions and exploit their functionalities autonomously (Carter & Grover, 2015; Haag, Eckhardt & Schwarz, 2019). These two factors together are bringing several changes to society and challenges to manage technology within organizations.

One of the challenges that emerge from this scenario is employees' deviant behavior. Broadly, deviance, or deviant behavior, has been defined as any behavior that violates norms regarding appropriate conduct (Wells, 1978; Younts, 2008; Heerdink et al., 2013). The dependence on technology to perform daily tasks also has brought opportunities for deviant behaviors (Rogers, Smoak & Liu, 2006). People are finding ways to use consumer technologies from their personal lives in the workplace, sometimes deviating from IS organizational policies (e.g., Harris, Ives & Junglas, 2012; Haag et al., 2019; Karjalainen, Sarker & Siponen, 2019; Sillic, 2019). In that sense, the traditional IT adoption logics have been completely reversed in the last years because, instead of IT departments deciding which solution their employees should use, employees autonomously adopt and use solution that meets their needs at work (Haag & Eckhardt, 2017).

Cases of deviance like the mentioned IS policy violation above are increasingly common in contemporary digital organizations (e.g., Zhang et al., 2015). Especially, the deviant behavior of using unauthorized technology in the workplace, called shadow IT usage, is attracting attention as an organizational phenomenon that challenges the traditional attitude towards using and managing technology (e.g., Sillic, 2019; Haag et al., 2019). Shadow IT can be defined as any hardware, software, or services built, introduced, and/or used to work without explicit approval or even knowledge of the organization (Haag & Eckhardt, 2017). The term shadow IT refers, then, to the unauthorized information technology (e.g., system, device, application…) and the individual behavior of using such technologies has been referred as shadow IT usage. This research follows the definition of individual shadow IT usage provided by Haag and Eckhardt (2014), which states that shadow IT usage is "the voluntary usage of any IT resource violating injunctive IT norms at the workplace as a reaction to perceived situational constraints with the intent to enhance the work performance, but not to harm the organization". Thus, this perspective addresses the use of shadow IT from a normative view, classifying shadow IT usage as deviant behavior and pointing out its norm-violating characteristic. Thereby, this dissertation uses shadow IT usage as an instance of deviant behavior to investigate the phenomenon in the IS domain.

Individuals and business units can implement a wide range of unauthorized solutions to meet their demands at work. The literature posits that shadow IT emerges at the employees' level (e.g., Györy et al., 2012; Haag, Eckhardt, & Bozoyan, 2015) and can be implemented by individuals, workgroups or whole business units (e.g., Furstenau, Rothe, & Sandner, 2017; Haag & Eckhardt, 2017). This statement suggests that the adoption and use of shadow IT may disseminate among employees within a company, emerging a collective level of use of shadow IT in addition to the individual level. Thereby, taking a multi-level perspective could aid to answer questions such as how and under what conditions several individuals deviate by using shadow IT and how this usage spread across a complete workgroup, as well as how these group actions collectively support and/or challenge organizational goals (Haag & Eckhardt, 2017).

While there are many studies in the IS field on why people comply or violate IS policies at the individual level (e.g., Siponen & Vance, 2010; Ifinedo, 2014; Moody et al., 2018), that are designed for protecting organizational IT assets, few studies examine why people deviate or violate security policies at the collective level. In contrast, the topic has gathered more interest and exploration by researchers from social psychology and criminology field, who frequently consider crime and other forms of deviance as collective behavior and, consequently, as a group-based phenomenon. They refer to this group act of non-compliant behavior as collective deviance or co-offending (e.g., McGloin & Stickle, 2011; McGloin & Thomas, 2016; Akkeren & Buckby, 2017).

Similar to social psychology and criminology that consider deviance as a group-phenomenon (e.g., Gardner & Steinberg 2005; McGloin & Thomas 2016), management scholars have noted the effects of workgroups on individuals. Robinson and O'Leary-Kelly's (1998) findings already provide preliminary evidence that a group-level focus is appropriate and essential for understanding deviant behavior in the workplace. There are recent calls for research on additional insights by examining noncompliance behavior in IS within the social context of workgroups, suggesting the collective-level as a supplement to individual-level explanations (e.g., Warkentin & Willison 2009; Haag & Eckhardt, 2017; Johnston et al., 2019; Yoo, Goo & Rao, 2020). This dissertation aims to fill this void and break new ground in workplace deviance at the collective level, in addition to the individual level. Thereby, this research relies on social psychology and criminology perspectives to address collective deviance and to explain its importance for IS research on non-compliance and policy violation.

In addition to the multi-level perspective to investigate the antecedents of deviant behavior in IS (e.g., shadow IT usage), it would be valuable to include investigations of some consequences (e.g., Haag & Eckhardt, 2017). Despite the intrinsic negative connotation of the term, deviance is a multifaceted phenomenon that can provide positive outcomes such as enhance creativity and innovation (Warren, 2003; Mainemelis, 2010; Jetten & Hornsey, 2014; Mertens et al. 2016). However, there is a larger focus on the negative side, leaving the functional nature of deviance underexplored (e.g., Spreitzer & Sonenshein 2004; Galperin 2012).

Considering that shadow IT may encompass a wide range of technologies, such as software, hardware, self-developed or purchased, cloud services, which can either complement or substitute the mandatory IT (e.g., Haag & Eckhardt, 2014; Silic & Back, 2014), many and occasionally unknown consequences can arise from its use. There is a consensus among researches and managers that shadow IT has potential benefits and drawbacks, although the name itself carries an intrinsic negative connotation (e.g., Haag et al., 2015; Furstenau et al., 2017). The consequences of shadow IT usage remains unclear (e.g., Haag et al., 2019), leaving unanswered the question about the implications of shadow IT usage. Therefore, consider only negative consequences of deviant behavior can represent a limitation to study the phenomenon. In this regard, this dissertation performed empirical studies also to examine positive consequences of using unauthorized technology at work.

1.1 Research Question and General Objective

Considering the above arguments, the general questions that guide this dissertation is: *what are the antecedents and consequences of the deviant behavior shadow IT at the individual and collective level*?

Instead of following previous studies on shadow IT, which mainly investigated the organizational level such as IT governance issues to control shadow IT (e.g., Györy et al., 2012; Zimmermann, Rentrop & Felden, 2016; Zimmermann, Rentrop & Felden, 2017), this dissertation adopts a multi-level perspective. Therefore, the current study aims to explore the individual and collective antecedents that drive employees and workgroups to deviate from IS rules by using shadow IT, as well as some positive consequences of this deviant behavior.

On that basis, this research differs from prior studies in two aspects. First, this study focus on analyzing shadow IT (antecedents and consequences) from a multi-level perspective, including group-level analysis instead of individual perception only. A meso or multilevel research perspective is a suitable way of capturing the complexity of organizational behavior, allowing a better understanding of the relations among units at different levels of analysis in the organizational context (House et al. 1995; Klein & Kozlowski 2000). Second, the study relies on social psychology and criminology literature, to investigate shadow IT as a form of collective IS deviance. In doing so, this dissertation investigates why employees use shadow IT and some consequences of its use. Moreover, it provides insights about what drives the diffusion of shadow IT usage among individuals and workgroups, which aids understanding of noncompliance behavior at the collective level (e.g., Haag & Eckhardt, 2017; Johnston et al., 2019).

Therefore, based on the general questions stated above, the general objective of this dissertation is to *investigate the antecedents and consequences of the deviant behavior of using shadow IT considering a multi-level perspective and its different facets.*

1.2 Specific Objectives

The dissertation was elaborated with four articles presented in the next sections. Thus, the specific objectives of the dissertation represent the objectives of each article, which are presented by level of analysis (individual, cumulative individual level, and collective level). The specific objectives are:

- Perform a literature review on shadow IT usage, which is the instance of deviant behavior used in this dissertation, elucidating its definition, types, and consequences.

- Develop a quantitative study to examine some positive consequences of shadow IT usage at the individual level based on social presence theory.
- Perform a quantitative study to investigate the antecedents of shadow IT usage at the cumulative individual level based on social influence perspective.
- Develop a qualitative and exploratory study to investigate the group-level of deviant behavior in IS to uncover why and how shadow IT usage disseminate among individuals as collective IS deviance.

1.3 Motivation

Deviance is a common phenomenon within organizations, with nearly 95% of all companies reporting various forms of deviance-related behaviors (Zhang et al. 2015). Studies on security and IS policy violation discuss a wide range of deviances, such as using another person's password without authorization, using or writing a virus, sending confidential information unencrypted, using laptops carelessly outside of the company, among others (e.g., Siponen & Vance, 2010; Crossler et al., 2013). However, it is not only dishonest employees that engage in deviant behaviors (e.g., Warkentin & Willison, 2009) because the reasons and motivations behind deviance can be more complex, mainly when we consider a group of people acting together.

Within the current context of society, where the pervasiveness of technology in people's lives is more and more predominant, deviant practices related to the use of technology is emerging as a phenomenon that demands further attention (e.g., Haag et al., 2019). Among the deviant behaviors related to using technology in the workplace, shadow IT is one receiving great attention from managers and researchers. Shadow IT is not a new phenomenon, however, it can be considered an underexplored topic in IS literature (e.g., Silic, Barlow & Back, 2017; Haag et al., 2019), demanding further studies from new perspectives to reveal, explain, and control its challenges, as well as to exploit its opportunities (Haag & Eckhardt, 2017). Furthermore, investigating individual behavior related to the use of technology is central to manage shadow IT since it emerges from the employee's level (Györy et al., 2012; Haag et al., 2015; Furstenau et al., 2017; Silic, 2019).

In addition to the individual level, include group-level investigations of shadow IT usage would be valuable to understand the phenomenon (Haag & Eckhardt, 2017).

Several studies (e.g., Györy et al., 2012; Zimmermann et al. 2016) investigate shadow IT from an organizational level perspective with the purpose to suggest IT governance mechanisms to control the use of unauthorized technology. Moreover, some studies (e.g., Haag et al., 2015; Silic et al., 2017) have addressed shadow IT at the individual level investigating the drivers of shadow IT usage within organizations from the employees' perspective. However, no study was found that investigate the use of shadow IT from a collective level of analysis and a multi-level perspective.

Although collective deviant behavior has been widely explored in social psychology and criminology, there are calls for further studies on the topic, mainly in the IS domain. For example, McGloin and Nguyen (2012) argue for the necessity of clarity about the factors that predict or explain the instigation of group deviance since it is a productive way for intervention and sanctioning policy. In a similar vein, understanding employees' behavior toward noncompliance in groups can add new insights into IS policy development and strategies to cope with IS policy violations (Warkentin & Willison, 2009; Yoo et al., 2020). Therefore, this research is in line with recent calls for group-level research on IS police violation and compliance (e.g., Johnston et al., 2019).

In management, less has been done to examine collective deviance since the study of Robinson and O'Leary-Kelly (1998). Particularly in the IS field, studies that investigate deviance at the group-level of analysis are scarce (Zhang et al. 2015; Yoo et al., 2020). Hence, further research is needed to reveal the underlying mechanisms of deviance in workgroups, which can be rooted in social elements such as peer pressure, information processing, social learning, norm transmission, reinforcement, etc. (e.g. Brown & Treviño, 2006; Younts, 2008; Aguilera & Vadera, 2008; Heerdink et al. 2013; Zhang et al., 2015; Haag & Eckhardt, 2017). This dissertation takes this gap as a motivation to investigate deviant behavior, focusing on shadow IT usage, from a multi-level perspective, including a collective level as a complementary perspective to the individual level findings (Robinson & O'Leary-Kelly 1998; Yoo et al., 2020).

Regarding the consequences of using shadow IT, practical and academic literature discuss different perspectives of shadow IT usage, such shadow IT as an organizational threat for information security (e.g., Walters, 2013; Silic & Back, 2014; Silic, 2019), but also a chance for driving innovation and enhance individual performance (e.g., Furstenau & Rothe 2014; Haag et al., 2015). Hence, the consequences of shadow IT usage remain unclear (Haag et al., 2019). In this regard, Haag and Eckhardt (2017) argue that it is important to examine the contrasting positive and negative consequences of shadow IT for individuals and organizations.

Investigate employees' behavior and their motives to use shadow IT is a manner to find out potential solutions to that complex issue. Research from Cisco Systems pointed out that 80% of end-users use software not formally authorized by organizational IT departments (Starke, 2016). Moreover, recent reports on shadow IT from Gartner and Everest Group have suggested that shadow IT is 30 to 50 percent of IT spending in large companies (Levit, 2018). Thus, organizations also can profit from the insights provided by this dissertation because understanding the mechanisms underlying shadow IT can allow managers to deal with this challenge within organizations (Haag & Eckhardt, 2017).

2 DISSERTATION STRUCTURE

The dissertation is structured as illustrated in Table 1. Chapter 3 is a general literature review that provides an overview of the main concepts of this dissertation. From Chapter 4, the papers that compose this dissertation are presented. As mentioned in the last section, the dissertation was elaborated based on four articles that are presented by level of analysis (individual, cumulative individual level, and collective level).

Table 1 – Structure of the Cumulative Dissertation

Workplace Deviant Behavior in IS – Shadow IT Usage
1. Introduction • Research Question • General and Specific Objectives • Motivation
2. Dissertation Structure • Overall Structure • Papers • General Framework
3. General Literature Review • Deviant Behavior • Shadow IT • Collective Deviance in IS
Literature Review on Shadow IT **4. Paper 1:** Shedding Light on Shadow IT: Definition, Related Concepts and Consequences. **Mallmann**, G. L., Pinto, A. V. & Maçada, A.C.G. (2018). Shedding Light on Shadow IT: Definition, Related Concepts, and Consequences. Proceedings of the 18.ª Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI'2018), Santarém, Portugal. **Mallmann**, G. L., de Vargas Pinto, A., & Maçada, A. C. G. (2019). Shedding Light on Shadow IT: Definition, Related Concepts, and Consequences. In Information Systems for Industry 4.0 (pp. 63-79). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-14850-8_5
Individual Level Study **5. Paper 2:** Social Presence on the Relationship between Shadow IT Usage and Individual Performance. **Mallmann**, G. L. & Maçada, A.C.G. (2017). The Mediating Role of Social Presence in the Relationship between Shadow IT Usage and Individual Performance: A Social Presence Theory Perspective. In Proceedings of the VI Encontro de Administração da Informação (EnaDI), Curitiba, Brazil. ***Winner of the Best Paper Award **Mallmann**, G. L. & Maçada, A.C.G. (2019). Social Presence in the Relationship between Shadow IT Usage and Individual Performance. Behaviour & Information Technology. DOI: 10.1080/0144929X.2019.1702100

Cumulative-Individual Level Study **6. Paper 3:** We are Social: a Social Influence Perspective to Investigate Shadow IT Usage. **Mallmann**, G. L., Maçada, A.C.G. & Eckhardt, A. (2018). We are social: a social influence perspective to investigate shadow IT usage. Proceedings of the Twenty-Sixth European Conference on Information Systems (ECIS2018), Portsmouth, UK.
Collective Level (Meso Level) Study **7. Paper 4:** Toward a Theory of Collective IS Deviance: a Grounded Theory Approach. **Mallmann**, G. L., Eckhardt, A. & Maçada, A.C.G. (2018). Collective Deviance in IS. Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy, San Francisco, the USA. **Mallmann**, G. L., Eckhardt, A. & Maçada, A.C.G. (2020). "From one of us to us": Developing a Theoretical Model of Collective Deviance in IS. In the 80th Annual Meeting of the Academy of Management (AOM2020). **Mallmann**, G. L., Eckhardt, A. & Maçada, A.C.G. (XXXX). Toward a Theory of Collective IS Deviance: a Grounded Theory Approach. To be submitted to an AIS basket-of-eight journal.
9. Conclusion • General Discussion • Theoretical and Practical Implications • Limitations and Future Work

Source: Prepared by the author

Chapter 4 presents the first article that is a literature review on shadow IT. To investigate deviant behavior in the IS domain, this dissertation focus on shadow IT usage as an instance of IS deviant behavior in the workplace. Paper 1 aims to gather the knowledge on shadow IT from previous studies, following the Webster and Watson (2002) guidelines for structure literature review. This study provides a conceptual discussion about shadow IT and its instances, as well as the differences between shadow IT and related concepts. Moreover, the paper discusses the consequences of using shadow IT, suggesting that it has not only the potential to provide negative outcomes (e.g., security risks) but also positive ones, such as productivity and innovation.

Chapter 5 presents Paper 2, which has the general purpose of examining the mediating role of social presence on the relationship between shadow IT usage and individual performance. Therefore, this study takes an individual-level perspective to investigate some positive consequences of shadow IT usage. It was performed a survey among 286 employees from three large companies in Brazil. The results show a positive relationship between shadow IT usage and social presence. Also, the results provide empirical evidence to show social presence has a mediating role in the relationship between shadow IT usage and individual performance, which aid to explain the impact of using shadow IT on employee’s performance to execute work tasks.

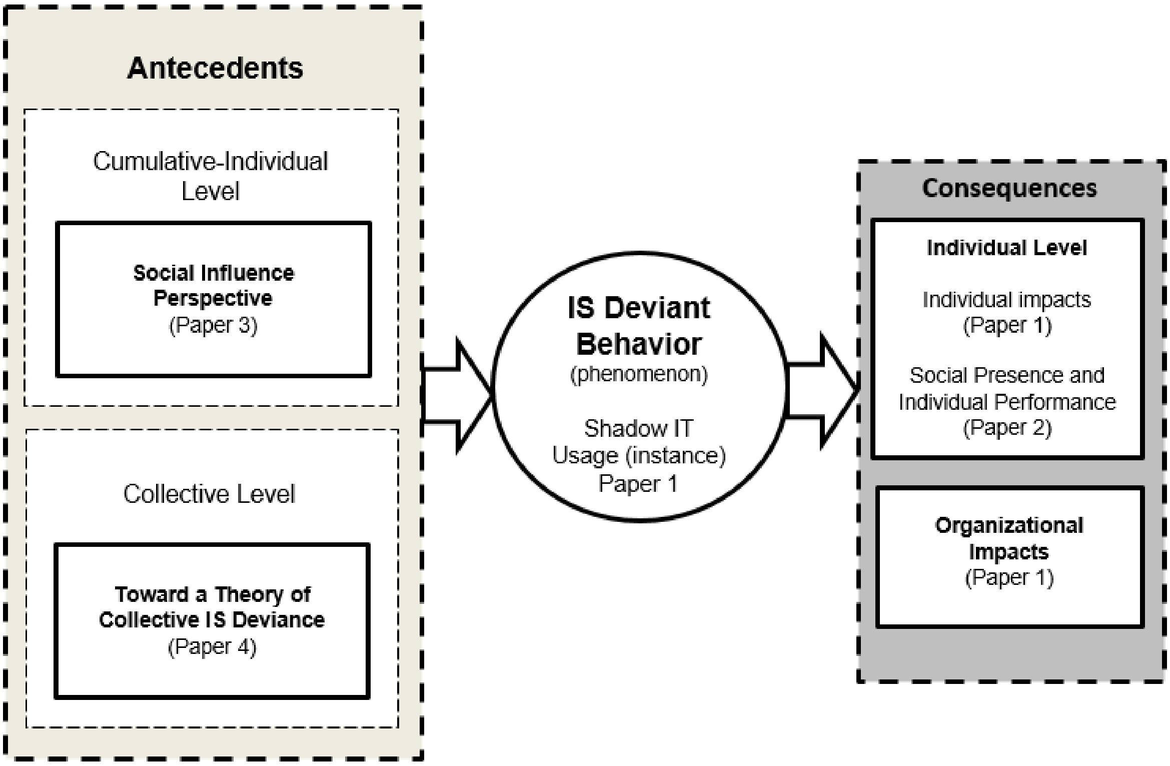
Chapter 6 presents Paper 3. Paper 3 takes a social influence perspective to investigate why shadow IT usage diffuses from one individual to another, spreading to a whole group of people. It was used social influence perspective to capture the cumulative individual effect of these influences on individual behavior (e.g., Karahanna, Straub & Chervany, 1999). A survey was performed among 148 employees of four organizations. The results show that social influence varies depending on the group of reference in question (peer, superior, mass influence). The study found that employees are strongly influenced by their peers and by a mass of people to use shadow IT, such as co-workers, professional workmates, and employees from other departments, suggesting a broader range of social influence that can affect the diffusion of shadow IT among employees.

Chapter 7 presents the study at the collective level or meso level of analysis. The main paper of this study is Paper 4 that aims to investigate the mechanisms behind deviant behavior among workgroup members, uncovering reasons for the occurrence of collective deviance within organizations, and offering a theoretical model that explains the phenomenon. It was developed a qualitative study with an exploratory perspective following the guidelines by Corbin and Strauss (2015). The data was collected among five workgroups, gathering a total of 21 interviews with members (superiors and peers). This study shows that the proliferation of the deviant act continues indefinitely overtime and, ultimately, the deviance becomes normalized. It is developed a process model describing the mechanisms and components that allow the normalization of the deviant behavior within workgroups.

In order to receive feedback from the IS community, a short paper version of this study was published in the Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy, San Francisco, the USA. A previous version of this paper was accepted in the 80th Annual Meeting of the Academy of Management (AOM2020) and a complete version of this study is planned to be submitted to an AIS basket-of-eight journal. Besides, this study was presented as a project in the Doctoral Consortium of the International Conference on Information Systems (ICIS2019) in Munich, Germany.

To summarize the objectives of this proposal, a general framework was developed. Figure 1 shows the general framework of this cumulative dissertation proposal, which presents the different perspectives and levels of analysis to investigate the antecedents and consequences of the deviant behavior of using shadow TI.

Figure 1 – Framework of the Cumulative Dissertation



Source: Prepared by the author

Finally, Chapter 8 presents the general discussion and conclusions of the dissertation. At the end of the document, it is displayed the appendixes. Appendix A contains the English version of the survey items developed to perform study 3, and the Portuguese version is presented in Appendix B. Appendix C provides the qualitative study protocol used to interview members of workgroups in study 4.

3 GENERAL LITERATURE REVIEW

3.1 The Concept of Deviance: Individuals as part of a Collective

In a general way, deviance refers to behavior that violates norms related to appropriate conduct (Younts, 2008). The definition of deviant behavior, thus, is always related to a norm that is transgressed, becoming important to identify who creates and enforces those norms. In addition, deviance can be performed by an individual that violates a norm, or by a collective of individuals, which is named collective deviance or co-offending (e.g., Brown & Treviño, 2006; McGloin & Nguyen, 2012; Lantz & Hutchiso, 2015; McGloin & Thomas, 2016). Thereby, the definition of deviant behavior requires the identification of the source of norms, as well as the level of analysis. At the collective level, it is also important to specify the group because the content and contexts of a group where the deviance is expressed may influence the perception of the deviant act (Jetten & Hornsey, 2014).

Literature suggests a tight relationship between the levels of analysis of deviance, whether individual or collective. Robinson and O'Leary-Kelly (1998) have argued that deviant behavior has predominately been examined at the individual level, which is reasonable because the decision of deviating is made by individuals. However, only focus on deviance as an individual phenomenon has limitations because, although deviance originates from the behaviors of individuals, it also may disseminate and converge into a common behavior among people and members of a group (Brown & Treviño, 2006). In this regard, research on social psychology and criminology has long argued that deviance can be a collective attribute once the behavior of others can influence one's decision to engage in deviance (McGloin & Thomas, 2016; Schabram et al., 2018). This perspective has motivated research on deviance at the collective level as a complement to individual-level studies (Robinson & O'Leary-Kelly, 1998).

Regarding the source of norms, the literature presents different perspectives of who creates and/or enforces the norms (Yount, 2008), which is a crucial aspect to understand deviance. Moreover, to align the individual and collective perspectives, it is suggested considering collective deviance as a behavior that emerges from individuals as part of a collective, such as friends, classmates, workgroups, gangs, political parties, cities, etc. Overall, the analysis of literature suggests three different sources of norms that will determine the content and context in which deviance is being examined. Table 2 presents an overview of those perspectives, which we detailed below.

Table 2 – Deviant Behavior concerning the Source of Norms

	Norms	Perspective	Description	Examples
Collective Deviance Individuals as part of a collective	**Hyper norms or societal norms**	Individuals as part of a larger collective in society (e.g., neighborhood, city, …)	Deviant behavior related to non-conformity to societal norms such as laws and policies (e.g., theft, vandalism, fighting, sexual assault, drug use and sales).	Weerman (2003); Younts (2008); Hochstetler (2001); D'Alessio and Stolzenberg (2010); Andresen and Felson (2010); Bastomski et al. (2017); Charette and Papachristos (2017)
	Organizational norms	Individuals as part of an organization	Deviant behavior related to non-conformity to managerial norms.	Robinson and O'Leary-Kelly (1998); Dunlop and Lee (2004); Gunia and Kim (2016)
	Group norms	Individuals as part of specific groups (e.g., workgroup, classmates, friends …). Intragroup and intergroup dynamics.	Deviant behavior related to non-conformity to prescriptive group norms.	Abrams et al. (2000); Bown and Abrams (2003); Heerdink et al. (2013); Camiera and Ribeiro (2014); Kim and Choi (2017)

Source: Prepared by the author

The first perspective is deviance concerning hyper norms or societal norms. It refers to individuals as part of a larger collective in society (e.g., neighborhood or city-level) who deviate from societal norms such as laws and policies. These studies are mainly from criminology and use the term co-offending to embrace actual collective execution of an offense, which refers to crimes such as theft, vandalism, fighting, sexual assault, drug use and sales (e.g., Weerman, 2003; D'Alessio & Stolzenberg, 2010; McGloin & Nguyen, 2012; Charette & Papachristos, 2017). The idea of deviate from societal norms rises the discussion about ethics because it refers to "behavior that is right or wrong when judged in terms of justice, law, or other societal guidelines determining the morality of behavior" (Robinson & Bennett, 1995).

The second perspective refers to deviant behavior concerning managerial norms. In this case, individuals are part of an organization subjected to norms created and enforced by the organizational structure. The literature presents different terms to this perspective, such as antisocial behavior, workplace deviance, organizational interpersonal deviance or counterproductive workplace behavior (e.g., Robinson & O'Leary-Kelly, 1998; Brown & Treviño, 2006; Arthur, 2011; Gunia & Kim, 2016). Many of those studies (e.g., Dunlop & Lee, 2004; Gunia & Kim, 2016; Schabram et al., 2018) adopt the deviant workplace behavior concept suggested by Robinson and Bennett (1995), who define employee deviance as "voluntary behavior that violates significant organizational norms and in so doing threatens the well-being of an organization, its members, or both".

Gunia and Kim (2016), for example, use the term organizational deviance, which is also called "counterproductive workplace behavior," to describe employees' misbehavior or failure to meet minimum requirements and, consequently, violating significant organizational norms (e.g., competence and integrity). Dunlop and Lee (2004) suggest that workplace deviant behavior may take different forms from minor acts to serious acts, such as spreading rumors and mocking co-workers to theft and sabotage. This raises the idea that deviance in the workplace not only involves acts that violate organizational norms, but also societal norms, including serious interpersonal and organizational misconduct, such as misusing organizational resources, sexual harassment, stealing, or aggression (Robinson & O'Leary-Kelly, 1998; Brown & Treviño, 2006; Arthur, 2011).

It can be observed, then, that literature on deviance concerning organizational norms encompasses a wide range of deviances, which can bring some consequences when investigating deviant behavior in the workplace once not all deviants in this context have the intention of violating laws and commit crimes (e.g., Kim & Choi, 2017). There is an overlap between societal perspective and organizational perspective because some acts that are regulated by societal norms, such as laws, might also be considered deviant by organizational norms (Treviño et al., 2006). However, deviation from organizational norms not necessarily means deviation from societal norms. In this regard, it can be helpful to revisit Robinson and Bennett (1995) definition. First, the authors mentioned that the definition of workplace deviance excludes minor infractions of social norms, focusing only on violations of norms that threaten the well-being of an organization. Second, Robinson and Bennett (1995) point out that the research on workplace deviance is distinct from research on ethics because workplace deviance refers to nonconformity with organizational norms, suggesting that although some behaviors may be both deviant and unethical, the two qualities are not necessarily linked.

The third perspective refers to deviant behavior concerning group norms. Individuals here are part of a specific collective, such as workgroups, classmates, or friends who share similar thoughts, opinions, and standards. Heerdink et al. (2013) broadly define deviance “as any behavior or expression of an opinion or idea that is intentionally or unintentionally different from other group members’ behaviors or opinions”. Jetten and Hornsey (2014) argue that deviance as violation of group norms is determined in relation to (a) prominent content of a group in relation to norms and (b) the contexts in which deviance is expressed. In that sense, the perception of certain behavior as deviant or not can vary depending on the group norm and context (Jetten & Hornsey, 2014; Chang et al., 2015).

This perspective is based on intragroup and intergroup dynamics. Group norms determine the behaviors and attitudes that are accepted and expected of group members, consequently, the perception of an act as deviant or normative rely on behaviors, opinions and standards of the members within the group, as well as the group in comparison with other groups (Chang et al., 2015). Abrams et al. (2000) define it as subjective group dynamics, which is a process members use to “maximize and sustain descriptive intergroup differentiation while simultaneously maximizing and sustaining the relative validity of prescriptive in-group norms through intragroup differentiation”. In sum, within this perspective, deviants are those that do not comply with norms prescribed by the group.

3.2 Shadow IT as an Instance of Workplace Deviant Behavior

Shadow IT can be defined as any hardware, software, or services built, introduced, and used to work without explicit approval or even knowledge of the organization (Haag & Eckhardt, 2017). The term shadow IT refers, then, to the unauthorized information technology used by employees to perform their work tasks. Employees can use shadow IT in a variety of ways. Shadow IT may encompass software or hardware, on-premise or on-demand, self-developed or purchased, subject to or free of charge, and whether complementing or substituting the organizational IT infrastructure (Silic & Back, 2014; Haag & Eckhardt, 2014).

The thematic of shadow IT studies has been evolving. The first studies discuss the emergence of shadow IT after the adoption of ERPs. For instance, the use of Excel spreadsheets to perform the work tasks instead of the official ERP system implemented (e.g., Jones et al. 2004; Behrens & Sedara, 2004; Raden, 2005). From 2012, several studies approached shadow IT at the organizational level of analysis, having the focus on IT governance mechanisms to cope with shadow IT and minimize security risk (e.g., Györy et al., 2012, Furstenau et al., 2017; Zimmermann et al., 2017).

Recent research has addressed shadow IT from an individual level perspective, investigating the behavioral aspects related to the use of shadow IT. From 2014, the studies have investigated the behavioral aspects (e.g., motivations or antecedents) from the employee's perspective, as well as the relationship between shadow IT usage and individual performance (e.g., Haag & Eckhardt, 2014; Haag et al., 2015). The main contribution of those studies was the definition of shadow IT usage, which states that shadow IT usage is "the voluntary usage of any IT resource violating injunctive IT norms at the workplace as a reaction to perceived situational constraints with the intent to enhance the work performance, but not to harm the organization" (Haag & Eckhardt, 2014). Thus, this perspective addresses the use of shadow IT from a normative view, classifying shadow IT usage as deviant behavior and pointing out its norm-violating characteristic.

It is also important to mention that shadow IT differs from related concepts, such as workaround and BYOD. Haag and Eckhardt (2017) highlight that shadow IT distinguishes from closely related concepts such as workaround, bring-your-own-device (BYOD), and IT consumerization. Although those concepts carry some similarities, there are crucial differences that "characterize and justify shadow IT as a unique and relevant concept worthy of future investigation" (Haag & Eckhardt, 2017).

Workarounds are, in a broader way, conscious adaptations of work activities that include also non-IT-based workarounds without using any IT, such as paper to collect and process information (Laumer, Maier & Weitzel, 2017; Haag & Eckhardt, 2017). Therefore, workaround is a broader concept that encompasses other instances, including shadow IT, and both terms can be classified as deviant work behavior.

In turn, IT consumerization and BYOD are not deviant behaviors itself. BYOD may not be considered a deviant behavior because it is defined as a policy that allows employees to bring and use personal devices at work (e.g., French, Guo & Shim, 2014). Finally, IT consumerization is the adoption of consumer devices and applications by employees (Harris et al., 2012). That is a broader concept related to all the prior ones (e.g., Haag & Eckhardt, 2017) because consumer IT can be related to the IT-supported solution, to the personal IT (e.g., BYOD) or the unapproved consumer IT (e.g., shadow IT or workaround). Thus, although IT consumerization and BYOD can facilitate or drive shadow IT usage because employees can inappropriately use their devices, they are not the same phenomenon.

3.3 Collective Deviance: from the Individual to the Collective level of Shadow IT

The act of committing the deviance in groups has been called collective deviance or co-offending. Collective deviance or co-offending embraces the actual collective execution of an offense, that is, a violation of a law or rule, an illegal act (e.g., Weerman 2003). Studies have shown that being in a group can produce significant changes in behavior, including a tendency for people to demonstrate a shift toward risky or deviant behavior when in the presence of others (e.g., Gardner & Steinberg 2005; McGloin & Thomas 2016).

According to a model of collective behavior proposed by Granovetter’s (1978), an individual’s belief about whether an act will maximize his utility is conditional on the behavior of others, that is, others’ actions serve as situational contingencies affecting decision-making. The subjective perceptions regarding rewards, informal social costs, and sanction risks vary under group conditions (McGloin & Thomas 2016). Moreover, an individual’s decision to engage in a collective action depends in part on how many others participate in that action (Granovetter 1978; McGloin & Thomas 2016). Thus, the decision to participate in collective deviance may be conditional on the behavior of others because the anticipated experience of formal sanctions, social costs, and rewards are conditional on the individuals’ behavior engaged in that deviant act (Gardner & Steinberg 2005; McGloin & Thomas 2016). Thereby, researchers in social psychology and criminology have used group processes to understand and explain crime and other forms of deviance.

Considering the literature on shadow IT, previous studies have suggested that shadow IT emerges at the employee’s level (e.g., Győry et al., 2012; Furstenau et al., 2017) and can be used by one individual, a team or a whole department. The adoption and use of shadow IT may disseminate, then, among employees within a company, emerging a collective level of use of shadow IT.

As mentioned above, shadow IT usage is a deviant work behavior because it is a voluntary use of technology that violates injunctive IT norms at the workplace (Haag & Eckhardt, 2014). Whether shadow IT usage can spread among employees as the literature suggests, it can be identified as collective deviant behavior. To explain that dynamic, it is proposed two paths of diffusion of shadow IT usage among employees.

Path 1 represents the situations when an individual uses a shadow IT to perform his/her work tasks and, after some time, other employees from the same team or department adopt and use the same shadow IT. In turn, Path 2 represents the situation when a group of individuals (e.g., team or department) adopt and use the shadow IT as their work solution and, as new individuals join this group, they consequently adopt and use the same shadow IT as others in the group. Therefore, some mechanisms underlie the adoption and diffusion process of use shadow IT among employees, configuring then a collective deviant behavior.

It is well documented that most misbehavior, deviance or even crime has been conducted in groups. In line with previous research in the social psychology field, mainly criminology studies (e.g., McGloin & Thomas 2016), this dissertation integrates group deviance, collective behavior and shadow IT literature to investigate how group processes affect behavior as a way to explain IS deviant behavior such as shadow IT usage within organizations at different levels of analysis.

4 ARTICLE 1: SHEDDING LIGHT ON SHADOW IT: DEFINITION, RELATED CONCEPTS, AND CONSEQUENCES

Abstract[1]

The use of Information Technology (IT) without formal approval and support of the IT department, called shadow IT, has challenged organizations to rethink ways of managing IT resources in order to cope with the use of unauthorized technologies in the workplace. We review the literature on shadow IT to shed light on this phenomenon, discussing the conceptual definition and types, the related concepts, and its consequences. This study, then, is an effort to better understand the phenomenon based on the existing literature. We provide contributions by enhancing the emerging body of knowledge on shadow IT, as well as by suggesting research gaps to be addressed in future research in order to advance on the topic.

Keywords: Shadow IT, Workarounds, IT consumerization, BYOD, Literature review.

4.1 INTRODUCTION

The organizational IT department is no longer the only provider of information technology (IT) used by employees in the business processes. Many individuals and workgroups have autonomously implemented and used technological solutions not provided by the IT department to perform work tasks. These unauthorized or unknown information technologies to the IT department used by employees to perform their work tasks have been called shadow IT (e.g., Haag and Eckhardt 2017).

The magnitude of the phenomenon shadow IT is increasing over the last years because people are more familiar with technologies, which are readily available nowadays and, sometimes, free of charge. Thereby, it is easier for employees to adopt and use technologies beyond the ones provided by the organization. Consequently, it has been increasingly difficult for IT managers to administrate the growing variety of systems and the risks arising from it (Fürstenau and Rothe 2014). The Ponemon

[1] A previous version of this paper was published in CAPSI 2018. The updated version was published in the Lecture Notes in Information Systems and Organisation of Springer.

Institute, for example, argues that the average data breach in 2015 costs to businesses an average of $4 million, being 70% of unauthorized data access committed by the organization's employees (Globalscape 2016).

However, when an employee's action puts the organization at risk, there may be no malicious intent, but rather a need to be productive (e.g., Zimmermann et al. 2017; Mallmann et al. 2018a, b). Moreover, in some cases, employees are not aware of or do not understand the organization's information security policies (e.g., Haag and Eckhardt 2014; Silic et al. 2017).

Shadow IT is, then, gaining relevance in practice and attracting the attention of managers and researchers. Shadow systems and related concepts, such as workarounds, have received wide attention due to the popularization of cloud computing services (Müller et al. 2015), bring your own device policies (BOYD) (Miller et al. 2012), IT workarounds (Alter 2014), and other important trends in the IT consumerization scenario (Harris et al. 2012). Motivated by this context, this study aims to shed light on the shadow IT phenomenon, presenting and discussing its definition and types, related concepts and consequences of use. In that sense, this work contributes by answering, through a literature review, the following research questions:

RQ1: What is the conceptual definition of shadow IT and how can the different instances of shadow IT be classified?

RQ2: Which concepts are relevant when investigating shadow IT and how are these concepts related?

RQ3: Which are the positive and negative consequences of using shadow IT?

Although shadow IT is not a new phenomenon, it can be considered relatively unexplored and the current knowledge is still limited and scarce (e.g., Silic et al. 2017; Haag and Eckhartd 2017). The academic literature on shadow IT is focused on exploratory studies, which mainly discuss the benefits and drawbacks of these technologies for companies (e.g., Fürstenau and Rothe 2014; Silic and Back 2014), as well as governance mechanisms to control these unauthorized technologies (e.g., Györy et al. 2012; Zimmermann et al. 2014). Thus, the need for a literature review on shadow IT is justified by the scarcity of theoretical-conceptual approaches in studying the subject (e.g., Haag and Eckhartd 2017).

We aim, thus, to gather the findings on shadow IT to contribute to the understanding of the phenomenon, which is crucial to advance the knowledge on the subject (Webster and Watson 2002). Another contribution of this study is to present the relation of shadow IT with related concepts. Haag and Eckhardt (2017) state that some concepts studied in the IS field share attributes with shadow IT, such as BYOD, IT consumerization and workaround, but it is important to recognize the aspects that differentiate them, allowing the characterization of shadow IT as unique and relevant concept. Finally, this study also may contribute to discuss some consequences that arise from the use of shadow IT once knowing the unauthorized technologies and its possible consequences can help mitigate risks by effectively redesigning existing workflows and/or technological systems (Vogus and Hilligoss 2016).

This article is organized in sections. Section 2 presents the literature review on the topic. Section 3 describes the method used. The analysis of the results is presented in Sect. 4. Next, the results are discussed, identifying research gaps and providing theoretical and practical contributions.

4.2 RELATED WORK

The literature on shadow IT has gained relevance over the last few years. Since 2012, the number of published academic papers on the subject has increased considerably. The vast majority of studies on shadow IT are recent, being more than 70% of publications dated from the last four years (2014–2017). In this sense, the subject can be considered little explored yet, although it has gained notoriety in academia over the years. The first articles on the subject discuss the emergence of shadow IT after the adoption of ERPs (Enterprise Resource Planning), for example, the creation and use of Excel spreadsheets to perform the work tasks instead of using the official ERP system implemented by organizations (e.g., Jones et al. 2004; Behrens and Sedara 2004; Raden 2005).

From 2012, the studies have approached shadow IT at the organizational level, focusing on IT governance mechanisms to cope with the use of shadow IT in organizations, minimizing security risks (e.g., Györy et al. 2012; Zimmermann and Rentrop 2014; Fürstenau et al. 2017; Zimmermann et al. 2017). From 2014, studies have investigated shadow IT as a behavior that deviates from organizational policies, for example, by investigating motivations and antecedents that drive the use of shadow IT from the employee perspective, as well as the relationship between the use of shadow IT and individual performance (e.g., Haag and Eckhardt 2014; Haag et al. 2015).

The term shadow IT, although not recent, still lacks a widely accepted definition and a better understanding of what the phenomenon is and how it occurs inside organizations. The topic can then be considered relatively unexplored and the current knowledge is still limited (e.g., Silic et al. 2017; Haag and Eckhartd 2017). In addition, previous studies (e.g., Silic and Back 2014; Huber et al. 2017; Zimmermann et al. 2017) have proposed that there are many instances of shadow IT within organizations once shadow IT can be hardware, software or any other solution such as a spreadsheet, cloud services, or an employee-developed application. Thereby, the topic lacks a conceptual discussion, being necessary also to clarify the differences among related concepts and the consequences of shadow IT usage (Haag and Eckhardt 2017).

4.2.1 Related Concepts

4.2.1.1 IT Consumerization

IT consumerization (ITC) represents the impact exerted by market technologies on organizations. Harris et al. (2012) argue that the popularization of devices and applications originating in the consumer sector is causing a second individual-oriented IT revolution. The presence of innovations from the consumerization sector is increasing within companies this tendency, called IT consumerization, has changed the way companies manage technology and continuously bringing new challenges for IT managers (Weiss and Leimeister 2012).

Weiss and Leimeister (2012) present a model of individual expectations changes to explain the origin of the consumerization trend. According to these authors, what drives employees to use market technologies is an expectation of high-level user experience and their expectation of new application options by the organizational IT department. However, it is not always possible to the IT department to provide new and many technological options to satisfy users, and whether the solution offered by the IT department failed in meeting employees’ expectations, they tend to find and adopt consumer market technologies by their-selves. This tendency is more prominent among higher positions, such as managers and supervisors (Weiss and Leimeister 2012), and among a new generation of technology users, called in the literature as tech-savvy or digital natives (Harris et al. 2012; Silic and Back 2014; Weiss and Leimeister 2012).

According to Harris et al. (2012), the ITC may have different definitions depending on the stakeholder. From the employee's perspective, ITC is related to individual use and familiarity with devices and applications of the user's personal life, which are seen as useful when used at work. From the perspective of the company's IT department, ITC is a vast amount of devices and applications used within the organization that may not be part of the sanctioned solutions list or that have not been formally approved by the IT department and can be seen either as a threat or as an opportunity. From the market perspective, ITC can be considered as any device or application that originates in the consumer market, and it is not, at least in the beginning, the target of the organization as a solution to be used together or replace the current information technology used by the company.

4.2.1.2 Workaround

Workaround is conceptualized by Alter (2014) as adaptations of the systems and resources provided by the company with the purpose to overcome constraints that make impossible or harder the completion of tasks in an effective way (Malaurent and Avison 2015). Workaround can be a strategy of using a system in a way that is not expected to be used or using alternative methods to solve an immediate and urgent problem (Azad and King 2008). Typical examples of workaround are the adjustment or manipulation of data to arrive at desired results (Alojairi 2017). Many organizations consider that workaround is composed of temporary practices implemented to deal with uncertainties, for example, after a system's implementation, with the understanding that workarounds may decrease over time. However, pieces of evidence suggest that these practices actually evolve over time rather than disappear and may lead to the use of alternative technologies (Azad and King 2012). Many alternative solutions occur because the mandatory technology does not fit the work needs (Alter 2014). Consequently, an alternative solution may be necessary for employees to support their daily activities (Azad and King 2012) and facilitate user interaction when the official system is not well planned (Ferneley and Sobreperez 2006).

4.2.1.3 BYOx

The concept of Bring Your Own Anything (BYOx) can be related to the concepts discussed here since it concerns the adoption and use of technologies brought by the employee to the workplace. BYOx is a term that encompasses various BYO trends in organizations such as Bring Your Own Device (BYOD) and Bring Your Own Cloud (BYOC), etc. (e.g., French et al. 2014; Haag 2015).

The term BYOD is the most widely known and, therefore, the most discussed in the academic literature. BYOD is conceptualized as a policy that allows users to access work applications from their personal mobile devices (Dang-pham and Pittayachawan 2015). BYOD allows employees to bring their own computing devices to work and incorporate them into the organization’s network rather than using company-owned devices (French et al. 2014). This can be considered policy and strategy developed by organizations to deal with the tendency of employees to adopt and use their own solutions in the workplace.

4.2.1.4 Cloud Computing

By definition, cloud computing is a model that allows ubiquitous and convenient access over the Internet to a shared pool of configurable computing resources that can be quickly provisioned and released with minimal management effort or interaction with service providers (Mell and Grance 2011). The primary feature of cloud computing is the ability to acquire and manage data whenever the user requests (Lis and Paula 2015). Among the driving forces behind the use of cloud computing, we highlight the possibility of accessing application services without the need for any detailed or specific knowledge of the infrastructure used to deliver the features. Moreover, the services can be accessed virtually from anywhere using any device because applications are web-based (Shin 2015), allowing users to share information and knowledge more easily (Park and Ryoo 2013). The cloud services have brought revolutionary changes in the way solutions are designed, built, delivered, and managed. Therefore, given the facilities to access and use cloud resources, it enables a favorable scenario for users to adopt and use cloud services without the organizational IT department approval or support (Khalil et al. 2017).

4.3 METHOD

The research method of this paper is a literature review based on the guidelines proposed by Webster and Watson (2002). As shadow IT is still underexplored, a literature review can corroborate by creating a solid foundation for knowledge advance (Webster and Watson 2002). Thus, gathering knowledge from existing studies is essential for the evolution of the topic understanding.

Overall, we divided the research into two steps to achieve the objectives proposed by this study. First, we selected articles from several databases, considering the criteria of inclusion and exclusion. Second, the data collection and the analysis were performed based on three main categories. These steps are detailed below. The articles search was carried out based on a research protocol. First, as suggested by Webster and Watson (2002), we performed a search in the leading journals of the IS field ('AIS basket eight'). Next, we searched in scientific databases such as ScienceDirect, Web of Knowledge, Google Scholar, and EBSCO. We also searched in the databases of the Association for Information System—AIS Electronic Library (AISeL), which contains papers from the most significant conferences of Information Systems, such as the International Conference on Information Systems (ICIS) and the European Conference on Information Systems (ECIS). A broader source of articles is justified because most of the literature on shadow IT comes from international conferences, being necessary to expand the search to conferences as well. The number of publications on the topic has been increasing over the years. However, it still can be considered an emerging topic.

The following keywords were used to find the relevant articles: shadow IT and shadow systems, which should appear in the title, abstract or keywords. The following words served as exclusion criteria: workarounds, end-user-computing, and bring your own device (BYOD), because although they share similarities, they are different from the term shadow IT (Rentrop and Zimmermann 2012; French et al. 2014; Haag and Eckhardt 2017). Those concepts were used later, in the analysis, to identify the differences between shadow IT and related concepts. Considering the research protocol, 50 relevant articles were selected that bring shadow IT as the central theme. The search was carried out between March and May 2018. Table 3 presents the articles selected according to the inclusion and exclusion criteria of articles.

Table 3 – Selected Articles

SOURCE		NUMBER OF ARTICLES
Journal	Network Security	2
	Computer & Security	1
	Information & Management	1
	Others (Computer Fraud & Security, CAIS, Journal of Information Systems, etc.)	9
	Total	13
Conference	AMCIS	8
	ECIS	7
	ICIS	5
	PACIS	5
	Others (ACIS, ICDS, BLED, ECKM, Conf-irm …)	12
	Total	37
Total		50

Source: Prepared by the author

We used Excel to tabulate and analyze data, dividing the analysis into three main categories. First, the definition and types, where we collected the definitions and approaches from previous studies, as well as instances of shadow IT. Second, the relationship among shadow IT and related concepts, where we gathered the characteristics of shadow IT that differentiate it from the other concepts. Third and last, we identified the most prolific consequences of shadow IT in the literature, gathering positive and negative outcomes to organizations. Below we present our findings based on these three main categories.

4.4 RESULTS

4.4.1 Conceptualizing Shadow IT

According to previous studies, shadow IT is defined as any hardware, software or services created, introduced and used by employees without explicit approval or even without the knowledge of the organization (Silic and Back 2014; Haag and Eckhardt 2017). Users implement shadow systems autonomously within the business units; consequently, these technologies have no technical or strategic relationship with the organization's IT service management (Zimmermann et al. 2014). Thereby, shadow IT represents the unauthorized or, sometimes, unknown technologies used by employees at work.

Another important point to define shadow IT is the user's intention to adopt unauthorized technology, defined by Györy et al. (2012) as well-intentioned, although it does not comply with organizational policies. The term "shadow" implies an illicit and malicious behavior. However, most shadow IT cases occur by convenience (Walters 2013). Thus, shadow IT is intentionally implemented by employees to perform and complete work tasks as a support solution to the business process, and not with malicious intentions such as to cause economic harm to the organization (e.g., Györy et al. 2012; Silic and Back 2014; Haag and Eckhardt 2014).

Differing from previous studies, recent investigations (e.g., Haag et al. 2015; Mallmann et al. 2018a, b) have addressed shadow IT from a behavioral approach. These studies are based on the concept called individual shadow IT usage proposed by Haag and Eckhardt (2014), which defines the use of shadow IT as the voluntary use of any IT resource that violates workplace standards as a reaction to perceived situational constraints with the intention of improving work performance without, however, harming the organization. This definition argues that shadow IT users act on their own with the primary goal of efficiently and productively performing their work tasks, which are adversely affected, for example, due to the malfunctioning of the organizational IT solution or inadequate instructions. These restrictions drive employees to deliberately bypass policies and accept potential security risks and damages to the organization's IT assets (Haag and Eckhardt 2014).

4.4.2 Instances of Shadow IT

First studies on shadow IT discuss the emergence of shadow IT after the implementation of Enterprise Resource Planning (ERP) (e.g., Jones et al. 2004; Behrens and Sedara 2004), mainly regarding the use of Excel spreadsheets instead ERP tools implemented by the company. However, due to technological advances, recent studies (e.g., Silic and Back 2014; Mallmann et al. 2018a, b) have presented other shadow IT occurrences, such as the use of social media and cloud-based services (e.g., Dropbox and Google Apps). Silic and Back (2014), for example, divide the types of shadow software found in their exploratory study into two groups: internal and external. Internal shadow software is software installed on organizational devices, while external shadow software is provided by external services such as cloud-based services.

The existing literature suggests that the occurrences of shadow IT may be applications, spreadsheets, cloud services, mobile devices, or a combination of these instances (e.g., Silic and Back 2014; Huber et al. 2016; Zimmermann et al. 2017). As an effort to clarify how individuals use shadow IT in the workplace, we sought in the literature how these technologies have been occurred in practice according to previous studies. Table 4 summarizes the four types of shadow IT based on the literature.

Table 4 –Types of Shadow IT

Shadow IT Usage Types	Description	Authors
Unapproved cloud services	Use of Internet-based Software and Software as a Service (SaaS) that are not approved or unknown by the IT department. These systems are also called Mobile Shadow IT once it can be accessed outside the workplace (e.g., WhatsApp, Facebook, Skype for Web, Dropbox, Google Apps, etc.).	Rentrop and Zimmermann (2012); Györy et al. (2012); Fürstenau and Rothe (2014); Silic and Back (2014); Haag and Eckhardt (2014); Zimmermann, Retrop and Felden (2014); Huber et al. (2016); Walters (2013); Walterbusch, Fietz and Teuteberg (2017).
Self-made solutions	Use of solutions developed by employees on the company's computers to perform their work tasks. For example, an excel spreadsheet or an application developed by employees.	Jones et al. (2004); Rentrop and Zimmermann (2012); Fürstenau and Rothe (2014); Zimmermann et al. (2014); Huber et al. (2016).
Self-installed applications	Use of software installed by employees to perform their work tasks, on the company's computers. For example, downloading and	Jones et al. (2004); Rentrop and Zimmermann (2012); Fürstenau and Rothe (2014); Zimmermann

	installing software available free of charge on the internet.	et al. (2014); Silic and Back (2014).
Self-acquired devices	Use of devices owned by employees. These devices are purchased directly from retail rather than being ordered through the official catalog of the IT department. It includes the use of applications in the employee’s personal devices at the workplace (smartphones, tablets, notebooks, etc.).	Rentrop and Zimmermann (2012); Silic and Back, (2014); Zimmermann et al. (2014); Gozman and Willcocks (2015), Huber et al. (2016).

Four types of shadow IT have emerged from the literature review. The first one, called unapproved cloud services, represents unauthorized cloud services accessed through the internet (e.g., Fürstenau and Rothe 2014; Haag 2015; Walterbusch et al. 2017) that does not need to be installed on any device to be used. For example, the use of Dropbox to share content with colleagues or Skype for web to communicate with clients without permission from the IT department. The second type is unauthorized solutions developed and used by employees on organizational devices to perform their work tasks (e.g., Zimmermann et al. 2014; Zimmermann et al. 2017), which can vary from a simple Excel worksheet to a more complex application developed by employees to be used by a whole business unit. For example, the use of an Excel spreadsheet developed for controlling, rather than using the company’s official system.

The third type, called self-installed applications, is those unauthorized applications installed and used by employees on enterprise devices, for example, on computers, smartphones, or tablets provided by the organization (e.g., Jones et al. 2004; Silic and Back 2014). This type of shadow IT involves solutions that are generally available free of charge on the Web and need to be downloaded and installed before using, rather than accessed via the Internet. Finally, the fourth type represents the self-acquired devices by employees and represents the hardware layer of shadow IT. These are devices purchased, owned and used at work by employees, instead of company devices, without official permission or BYOD policy. This last type includes the use of applications on personal devices on the company’s network (e.g., Rentrop and Zimmermann 2012; Zimmermann et al. 2017).

4.4.3 Shadow IT and Related Concepts

Haag and Eckhardt (2017) point out that shadow IT distinguishes conceptually from other related terms, such as bring-your-own-device (BYOD) and IT consumerization. While these concepts share similarities, there are crucial differences between them. Bellow, we discuss the relationship between shadow IT and related concepts, emphasizing the differences between them.

IT consumerization is a broader concept that encompasses different phenomena related to the use of consumer technologies in the workplace (Harris et al. 2012). The relationship between IT consumerization and shadow IT is due to the fact that consumerization encompasses both the consumer market technologies approved by organizational IT policies and technologies that are not yet included in these policies, that is unauthorized technologies that were not formally approved by the IT department, as it is the case of shadow IT.

Also under the concept of IT consumerization, the term workaround refers, in a broader way, to conscious adaptations of work activities that are not expected or specified to be altered (Laumer et al. 2017). Haag and Eckhardt (2017) suggest three instances of alternative solutions. First is the non-IT-based workarounds, for example, use of paper to collect and process information. Second, the adaptation of mandatory IT solution and/or approved personal IT, using those solutions in different and unexpected ways, for example, using MS Word to convert and re-edit the content of PDF documents. Third and last, shadow IT, for example, the use of unapproved IT and/or approved IT changed in unapproved ways, for example, by using Dropbox instead of the official cloud-based services to store and share organizational information.

Thus, shadow IT is a type of workaround, although not every workaround is necessarily a shadow IT since workaround encompasses additional features that go beyond shadow IT. Shadow IT is technology-related, as its concept suggests, while workaround may also be related to non-IT devices (e.g., paper). In that sense, workaround is a broader concept that encompasses other instances, including shadow IT, and both terms can be classified as work deviance behavior that deviates or violates organizational policies (e.g., Haag and Eckhardt 2017). Another difference is, according to Lund-Jensen et al. (2016), related to the temporal aspect because workarounds tend to be temporary practices, while shadow IT used to be long-term practices used in daily activities.

In turn, BYOx is a concept often confused with shadow IT. The difference between the two concepts is crucial because it refers to the compliance or not with the IT security policies. In the context of BYOx, the technology brought to the workplace by employees is allowed by the organization through policies developed in conjunction with the IT department (e.g., Dang-pham and Pittayachawan 2015).

For example, BYOD policy allows users to bring and use their own devices in the workplace. In the context of shadow IT, however, the solution used by employees is generally unknown by the IT area, and, therefore, neither approved nor supported by the company's IT department (e.g., Rentrop and Zimmermann 2012).

Silic and Back (2014) argue that in the current technological context, where smartphones are being increasingly used in the workplace as the case of BYOD policies, shadow IT is becoming even more critical at different organizational levels, also motivated by the fact that users believe they are not doing anything wrong. Therefore, the consequence of BYOx policies in the context of shadow IT is to facilitate the emergence of these unauthorized technologies because the adoption of BYOx policies can increase IT complexity in managing the growing number of devices and applications used by employees, allowing numerous occurrences of shadow IT at work.

Finally, cloud computing emerges as a relevant concept in the context of shadow IT. In addition to mobile devices from the consumer market, Haag and Eckhardt (2015) argue that cloud-computing services have made shadow IT accessible also to people without much IT knowledge since the services are quite simple and intuitive to users, and usually it is delivered free of charge via web browsers. For this reason, many studies (e.g., Silic and Back 2014; Mallmann et al. 2018a, b) present cloud-based services as the primary occurrence of shadow IT, often used by employees in the workplace without authorization from the IT department.

4.4.4 Consequences of Shadow IT

Although the term “shadow” implies illicit and malicious behavior that jeopardizes the organizational IT security, most shadow IT cases are caused by convenience (Walters 2013). Previous studies suggest that employees use shadow IT to assist them when they are performing their tasks, but not with malicious intention (e.g., Györy et al. 2012; Haag and Eckhardt 2014). Thus, a broader discussion about the positive and negative consequences of the use of shadow is important to understand the impact on organizations.

Productivity and individual performance stand out in recent research as benefits of using shadow IT to perform work tasks (e.g., Silic and Back 2014; Haag and Eckhardt 2014; Haag 2015; Haag et al. 2015; Fürstenau et al. 2017). Empirical studies (e.g., Haag et al. 2015), suggest that shadow IT leverages individual productivity, improving employee work performance. Also related to employee performance, studies have found that employees often use shadow IT to communicate and collaborate at work (e.g., Shumarova and Swatman 2008; Silic and Back 2014), as well as to share information and knowledge among colleagues, clients and external partners (e.g., Steinhüser et al. 2017; Mallmann et al. 2018a, b). In that sense, improvements in communication and collaboration are some of the elements that can lead to increased productivity and individual performance of shadow IT users.

Shadow IT is also often related to innovation, being considered a legitimate driver of IT solutions and process innovation (Fürstenau and Rothe 2014). Haag et al. (2015) argue that the use of shadow IT question the importance of employees' autonomy for the emergence of innovative behaviors within organizations because the use of shadow IT seems to be a manifestation of creativity and personal innovation. Thus, the literature also suggests an innovative side of shadow IT driven by employees (Fürstenau and Rothe 2014; Györy et al. 2012; Fürstenau et al. 2017; Singh 2015).

The individual performance improvements, in turn, can have impacts on the organization as a whole. Singh (2015) argues that IT managers who manage shadow IT, instead of just trying to avoid it, can see improvements in organizational performance due to the introduction of user innovations since employees are more satisfied with the tools they use to perform work tasks. Similarly, the empirical findings from Haag et al. (2015) show that, at the individual level, shadow IT users can be valuable to organizations because they are more goal-oriented, effective, and try to find long-term solutions. Thus, managers should also take into account the positive outcomes of using shadow IT, such as employees’ productivity improvements and, consequently, organizational performance (Haag and Eckhardt 2015).

The downside of shadow IT, however, persists despite the potential benefits. Many employees are not aware they are deviating from IS policies, jeopardizing the organizational information security (Walters 2013; Silic and Back 2014; Silic et al. 2017). Security risks, therefore, are among the main concerns cited in the literature (e.g., Haag and Eckhardt 2015; Silic and Back 2014). By using shadow IT such as cloud-based applications to upload organizational data without the company's knowledge, it can provide several security issues, such as information leakage, data loss, data privacy, compliance, etc.

4.5 DISCUSSION AND FINAL CONSIDERATIONS

This study aimed to review the literature on shadow IT in order to shed light on the phenomenon, presenting and discussing its definition and instances, related concepts and consequences. This section discusses the results, pointing out research gaps on the topic, as well as providing theoretical and practical contributions.

The literature on shadow IT so far has focused on identifying which unauthorized technologies are being used within companies (e.g., Silic and Back 2014), the investigation about employees motivations to adopt these technologies (e.g., Haag and Eckhardt 2015), and governance forms to control shadow IT (e.g., Fürstenau and Rothe 2014). These studies collaborate, primarily, to define shadow IT and its types. Based on the existing research, the present study discusses the conceptual definition of shadow IT, its types and consequences. In addition, the study discusses the differences between shadow IT and related concepts to clarify the unique characteristics of the phenomenon, as suggested by Haag and Eckhardt (2017).

Results suggest that when employees bring technology from the consumer market to use at work and this technology is not in line with organizational policies it can be characterized as shadow IT. Shadow IT, thus, is part of the IT consumerization phenomenon, which is different from BYOx policies. These policies, such as BYOD, allow employees to use their own solutions to accomplish their job tasks, within a range of predefined options by the IT department. In short, while shadow IT is a deviant behavior, BYOx is a policy that allows employees to bring and use personal devices and solutions at work (e.g., French et al. 2014). Workarounds, in turn, is also a behavior that deviates from IT norms. However, it is broader than shadow IT because it also includes non-technology based solutions. Finally, cloud-based services are not necessarily shadow IT, but it does relate because many shadow IT used by employees are cloud services due to the ease of accessing and using these services and low barrier costs.

Regarding the consequences, the results suggest that there is still a divergence in the literature about the positive and negative outcomes of shadow IT. Information security risks, data leakage and loss, privacy risk, and compliance are among the main concerns cited in the literature (e.g., Haag and Eckhardt 2015; Silic and Back 2014). In this sense, previous studies (e.g., Haag and Eckhardt 2015) point out the need to balance the pros and cons of shadow IT. Therefore, further studies about the impacts of using shadow IT, such as organizational performance, innovative features, and security issues, would aid to clarify the consequences of shadow IT to mitigate the risks arising from its use and enhance its benefits.

4.5.1 Research Gaps by Level of Analysis

Previous studies have suggested that shadow IT emerges at the employee level (e.g., Györy et al. 2012; Fürstenau et al. 2017), but can be used by an individual or a group of individuals, emerging an individual and/or collective level of shadow IT usage. However, this perspective at different levels needs further research, including a group-level approach, in addition to the individual level, to understand how the working groups collectively support the use of shadow IT and what are the consequences for the group (Haag and Eckhardt 2017). Studies on shadow IT at the individual level have been developed since 2014 (e.g., Haag and Eckhardt 2014; Haag et al. 2015). Those studies have been analyzing shadow IT as a behavior, called shadow IT usage, as a manner to understand what drives individuals to deviate from IT policies and use shadow IT at work. In line with Haag and Eckhardt (2017), we could not find studies at the collective level of analysis, which suggests the necessity for further studies at group-level to understand the use of shadow IT among workgroups, for example, the widespread of shadow IT usage among teams and departments.

The literature also provides evidence for a relationship between the use of shadow IT and age or generation. The dependence on technology for social interaction is increasing, especially among digital natives (Turkle 2011), changing the way we socially interact and bringing many consequences to individuals, organizations, and society. Previous studies have suggested that the use of consumer-based technologies is more prominent among younger generations, called tech-savvy, millennials or generation Y (e.g., Weiss and Leimeister 2012; Turner 2015). Thus, age can be a potential factor in understanding user behavior regarding technology. A generational study on the use of shadow IT can add valuable information about individual behavior in a postmodern society.

At the organizational level, issues such as IT governance should be associated with shadow IT. Studies at this level can seek management practices to deal with the use of unauthorized technologies in the workplace through IT governance approaches, for example, to reduce information security gaps and reduce the risks of overhead in IT infrastructure of the company by users (e.g., Györy et al. 2012).

4.5.2 Theoretical and Practical Contributions

This study provides theoretical and practical implications for the emerging knowledge on shadow IT. Although not recent, shadow IT is still understudied in the IS literature. This study contributes, in this sense, by providing a conceptual discussion about shadow IT and its use. The article also provides conceptual contributions by discussing the differences between shadow IT and related concepts, clarifying the characteristics of shadow IT. In addition, the article discusses the consequences of using shadow IT that are still few explored and unknown.

We also provide some practical contributions. Managers should pay attention to the fact that the main reason for the emergence of shadow IT is the complete or partial absence of appropriate IT solutions that meet employee requirements (Walterbusch et al. 2017). Thereby, knowing the types of shadow IT and its consequences is also a good opportunity for IT managers to understand users' expectations and their technological needs to provide suitable technologies to perform their tasks. Moreover, shadow IT literature discusses a wide range of consequences, from performance improvements and innovative solutions to security and compliance risks. Thus, organizations must find ways to balance the positive and negative outcomes of shadow IT according to the context of each organization.

Finally, this study is an effort to better understand the phenomenon through a literature review and suggest research gaps to advance the knowledge on the topic.

As a limitation of this research, we point out the limited number of articles in journals that bring shadow IT as a central topic. Most of the studies on shadow IT are from conferences, showing the necessity of theoretical and conceptual advances on the phenomenon.

REFERENCES

Alter, S. (2014). Theory of workarounds. *Communications of the association for information systems*. 34(55), 1041–1066.

Alojairi, A. (2017). The dynamics of IT workaround practices a theoretical concept and an empirical assessment. *International Journal of Advanced Computer Science and Applications*, 8(7), 527–534.

Azad, B., & King, N. (2008). Enacting computer workaround practices within a medication dispensing system. *European Journal of Information Systems*, 17(3), 264–278.

Azad, B., & King, N. (2012). Institutionalized computer workaround practices in a Mediterranean country: an examination of two organizations. *European Journal of Information Systems*, 21 (4), 358–372.

Behrens, S., & Sedera, W. (2004). Why do shadow systems exist after an ERP implementation? Lessons from a case study. In Pacific Asia conference on information systems (PACIS).

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers & Security*, 48, 281–297.

Ferneley, E. H., & Sobreperez, P. (2006). Resist, comply or workaround? An examination of different facets of user engagement with information systems. *European Journal of Information Systems*, 15(4), 345–356.

French, A. M., Guo, C., & Shim, J. P. (2014). Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems*, 35(10), 191–197.

Fürstenau, D., & Rothe, H. (2014). Shadow IT systems: discerning the good and the evil. In Twenty-second European conference on information systems, Tel Aviv.

Fürstenau, D., Rothe, H., & Sandner, M. (2017). Shadow systems, risk, and shifting power relations in organizations. *Communications of the Association for Information Systems*, 41, 43–61.

Globalscape. (2016). Be afraid of your shadow: What is “shadow IT” and how to reduce it. Disponível em: https://www.globalscape.com/resources/whitepapers/shadow-it-guide. Acesso em: 05 março 2018.

Gozman, D., & Willcocks, L. (2015). Crocodiles in the regulatory swamp: Navigating the dangers of outsourcing, SaaS and Shadow IT. In Proceedings of the thirty-sixth international conference on information systems, Fort Worth.

Györy, A. A. B., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the shadows: IT governance approaches to user-driven innovation. In Proceedings of european conference on information systems. Paper 222.

Haag, S., & Eckhardt, A. (2014). Normalizing the shadows–The role of symbolic models for individuals’ shadow IT usage. In Proceedings of the thirty-fifth international conference on information systems, Auckland.

Haag, S. (2015). Appearance of dark clouds?-an empirical analysis of users’ shadow sourcing of cloud services. In Proceedings of the Wirtschaftsinformatik (pp. 1438–1452).

Haag, S., & Eckhardt, A. (2015). Justifying shadow IT usage. In Proceedings of the 19th Pacific Asia conference on information systems, Singapore.

Haag, S., Eckhardt, A., & Bozoyan, C. (2015). Are shadow system users the better IS users?–Insights of a lab experiment. In Proceedings of the thirty-sixth international conference on information systems, Fort Worth.

Haag, S.,& Eckhardt, A. (2017). Shadow IT. *Business & Information Systems Engineering* (pp. 1–5).

Harris, J., Ives, B., & Junglas, I. (2012). IT consumerization: When gadgets turn into enterprise IT tools. *MIS Quarterly Executive*, 11(3).

Huber, M., Zimmermann, S., Rentrop, C., & Felden, C. (2016). The relation of shadow systems and ERP systems—Insights from a multiple-case study. *Systems*, 4(1), 11. https://doi.org/10.3390/systems4010011.

Huber, M., Zimmermann, S., Rentrop, C., & Felden, C. (2017). Integration of shadow IT systems with enterprise systems—a literature review. In Proceedings of the twenty-first Pacific Asia conference on information systems, Langkawi.

Jones, D., Behrens, S., Jamieson, K., & Tansley, E. (2004). The rise and fall of a shadow system: Lessons for enterprise system implementation. In ACIS 2004 Proceedings (p. 96).

Khalil, S., Winkler, T. J., & Xiao, X. (2017). Two Tales of Technology: Business and IT Managers' Technological Frames Related to Cloud Computing.

Laumer, S., Maier, C., & Weitzel, T. (2017). Information quality, user satisfaction, and the manifestation of workarounds: a qualitative and quantitative study of enterprise content management system users. *European Journal of Information Systems*, 26(4), 333–360.

Lis, T., & Paula, B. (2015). The use of cloud computing by students from technical university-The current state and perspectives. *Procedia Computer Science*, 65, 1075–1084.

Lund-Jensen, R., Azaria, C., Permien, F. H., Sawari, J., & Bækgaard, L. (2016). Feral information systems, shadow systems, and workarounds–A drift in IS terminology. *Procedia Computer Science*, 100, 1056–1063.

Mallmann, G. L., Maçada, A. C. G., & Oliveira, M. (2018a). The influence of shadow IT usage on knowledge sharing: An exploratory study with IT users. *Business Information Review*, 35(1), 17–28.

Mallmann, G. L., Maçada, A. C. G., Eckhardt, A. (2018b). We are Social: a social influence perspective to investigate shadow IT usage. In Proceedings of European conference on information systems, Portsmouth, UK.

Malaurent, J., & Avison, D. (2015). From an apparent failure to a success story: ERP in China— Post implementation. *International Journal of Information Management*, 35(5), 643–646.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. Disponível em http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf.

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. It Professional, 14(5), 53–55.

Müller, S. D., Holm, S. R., & Søndergaard, J. (2015). Benefits of cloud computing: Literature review in a maturity model perspective. *CAIS*, 37, 42.

Park, S. C., & Ryoo, S. Y. (2013). An empirical investigation of end-users' switching toward cloud computing: A two factor theory perspective. *Computers in Human Behavior*, 29(1), 160–170.

Raden, N. (2005). Shedding light on shadow IT: Is excel running your business. DSSResources. com, 26.

Rentrop, C., & Zimmermann, S. (2012). Shadow IT-management and control of unofficial IT. In Proceedings of the 6th international conference on digital society (pp. 98–102).

Silic, M., & Back, A. (2014). Shadow IT–A view from behind the curtain. *Computers & Security*, 45, 274–283.

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & management*, (in press), 1–15. http://dx.doi.org/10.1016/j.im.2017.02.007.

Singh, H. (2015). Emergence and consequences of drift in organizational information systems. In Proceedings of the Asia conference on information systems (PACIS). Paper 202.

Shin, D. (2015). Beyond user experience of cloud service: Implication for value sensitive approach. *Telematics and Informatics*, 32(1), 33–44.

Shumarova, E., & Swatman, P. A. (2008). Informal ecollaboration channels: Shedding light on “shadow cit”. In Proceedings of LED 2008, Bled, Slovenia.

Steinhüser, M., Waizenegger, L., Vodanovich, V. & Richter, A. (2017). Knowledge management without management—Shadow IT in knowledge-intense manufacturing practices. In Proceedings of the 25th European conference on information systems, Guimarães, Portugal.

Turner, A. (2015). Generation Z: Technology and social interest. *The Journal of Individual Psychology*, 71(2), 103–113.

Turkle, S. (2011). Alone together: Why we expect more from technology and less from each other. New York: Basic Books.

Vogus, T. J., & Hilligoss, B. (2016). The underappreciated role of habit in highly reliable healthcare. *BMJ Quality & Safety* 25(3), 141–146.

Walterbusch, M., Fietz, A., & Teuteberg, F. (2017). Missing cloud security awareness: investigating risk exposure in shadow IT. *Journal of Enterprise Information Management*, 30(4), 644–665.

Walters, R. (2013). Bringing IT out of the shadows. *Network Security*, 2013(4), 5–11.

Webster, J. & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26, xiii–xxiii.

Weiss, F., & Leimeister, J. M. (2012). IT innovations from the consumer market as a challenge for corporate IT. *Business & Information Systems Engineering*, 6, 363–366.

Zimmermann, S., Rentrop, C., & Felden, C. (2014). Managing shadow IT instances–a method to control autonomous IT solutions in the business departments. In Proceedings of the Twentieth Americas Conference on Information Systems, Savannah.

Zimmermann, S., & Rentrop, C. (2014). On the emergence of shadow IT-a transaction cost-based approach. In Proceedings of the Twenty Second European Conference on Information Systems, Tel Aviv.

Zimmermann, S., Rentrop, C., & Felden, C. (2017). A multiple case study on the nature and management of shadow information technology. *Journal of Information Systems*, 31(1), 79–101.

5 ARTICLE 2: THE MEDIATING ROLE OF SOCIAL PRESENCE IN THE RELATIONSHIP BETWEEN SHADOW IT USAGE AND INDIVIDUAL PERFORMANCE: A SOCIAL PRESENCE THEORY PERSPECTIVE.

Abstract[2]

The use of unauthorized technologies in the workplace, called shadow IT, is increasing within organizations. Research has identified that employees frequently use unauthorized solutions to collaborate and communicate at work, which can ultimately enhance their performance. This research aims to examine the mediating role of social presence on the relationship between shadow IT usage and individual performance. We performed a survey among 286 employees from three large companies. The results show a positive relationship between shadow IT usage and social presence, suggesting that some aspects of social presence, such as perceived higher levels of sensitivity and comprehension, are significant outcomes related to the use of shadow IT. The results also provide empirical evidence to show social presence has a mediating role in the relationship of shadow IT usage and individual performance. Thereby, this research contributes by providing new insights into the consequences of shadow IT usage, and partially explaining the impact the use of shadow IT has on employee performance. In addition, the findings highlight the importance of social presence in relation to technology-mediated communication within organizations.

Keywords: Shadow IT, Collaboration, Social Presence Theory, IT Management.

5.1 INTRODUCTION

The increasing use of unauthorized technologies within organizations is driving a debate among managers and researchers about the reasons for and outcomes of this behavior in the workplace. A recent report by CIO digital magazine shows that

[2] A previous version of this paper was published in EnADI 2017, Curitiba – Brazil, where it received the Best Paper Award. The updated version was published in the journal Behaviour & Information Technology of Taylor & Francis.

more than 80 per cent of CIOs had seen some kind of unauthorized technology usage within their companies (Suer, 2017). This phenomenon has been called shadow IT usage, which is defined as the voluntary use of any IT (information technology) resource that infringes IT norms, such as security policies, in the workplace, as a reaction to perceived situational constraints, with the objective of improving work performance (Haag and Eckhardt 2014).

Although some companies try to embrace different policies to manage IT use, such as Bring Your Own Device (BYOD), or ratify unauthorized technology to have control over it instead of leaving it in the "shadows," in practice the situation is often more complicated. The academic and commercial literature has discussed many instances of shadow IT and its consequences, and in fact, managing such complexity is a challenge to many organizations (e.g., Furstenau and Rothe 2014; Silic and Back 2014; Silic 2019). The negative side of shadow IT has been widely discussed, primarily the issues related to organizational information security (e.g., Walters 2013; Silic and Back 2014; Haag and Eckhardt 2015; Silic, Barlow and Back 2017). Recent literature (e.g., Haag, Eckhardt and Bozoyan 2015; Mallmann, Maçada and Oliveira 2018; Silic 2019) has shown, however, that focusing only on the drawbacks of shadow IT can be a very limited approach for adequately coping with this kind of occurrence. Consequently, we aim to explore a positive side by investigating the relationship between the use of shadow IT and individual performance, which is a relationship suggested by previous research (e.g., Haag, Eckhardt and Bozoyan 2015).

Despite significant investments by companies in information systems, including solutions for communicating and collaborating at work, Shumarova and Swatman (2008) point out the increasing rate at which informal collaborative information technology is being implemented autonomously by employees to help them perform their work. Similarly, Silic and Back (2014) found that employees are using shadow IT, such as Skype, Facebook and Google Talk without formal permission, thereby improving their productivity and enabling faster and better collaboration and communication. Moreover, the findings from Mallmann, Maçada, and Oliveira (2018) suggest the use of shadow IT allows for more efficient and instant communication, which may consequently facilitate information and knowledge sharing.

Considering the above arguments, the literature provides evidence for the existence of a positive relationship between shadow IT usage and technology-mediated communication and collaboration for performing work tasks (e.g., Shumarova and Swatman 2008; Mallmann, Maçada, and Oliveira 2018), which may ultimately improve employee performance (e.g., Haag, Eckhardt and Bozoyan 2015). Social presence theory (SPT) was chosen as the theoretical lens through which to analyze this relationship. Briefly, this theory seeks to explain how users select communication channels, suggesting that media differ in terms of their capability to transmit the signals that create user-awareness of other social actors (Short, Williams, and Christie 1976).

The extant literature has shown that not only media resources (e.g., tools used to deliver information) but also social factors, such as social presence, have a profound influence on the ways in which individuals perceive and use technology (e.g., Yoo and Alavi 2001; Shin 2013; Shin and Choo 2011). At a time when the use of social networking solutions for communicating, collaborating and sharing information is increasing (e.g., Yoo and Alavi 2001; Turkle, 2011; Turner, 2015), the concept of social presence may well provide relevant insights into user behavior with regard to digital technologies, including a better understanding of deviant workplace behaviors, like the use of shadow IT.

The general purpose of this research, therefore, is to examine the mediating role of social presence on the relationship between shadow IT usage and individual performance. The role of a mediating variable is to explain or clarify the relationship between the original constructs (Hair et al. 2016). In this sense, Haag and Eckhardt (2017) argue that it is crucial to apply new perspectives to reveal and explain the challenges and opportunities presented by shadow IT usage. Similarly, previous studies have suggested the need to determine the pros and cons of using shadow IT, which is crucial to managing it efficiently (e.g., Silic and Back 2014; Haag and Eckhardt 2015; Haag and Eckhardt 2017). The debate regarding the virtues and vices of shadow IT usage continues, not only among practitioners but also among researchers. There are, however, few empirical studies in the literature investigating the consequences of shadow IT. The present study, therefore, aims to contribute by exploring individual performance as a positive consequence of shadow IT usage from the perspective of the social presence theory.

This article is organized as follows: Section 2 provides a review of the literature on shadow IT and social presence theory; Section 3 describes the model and hypotheses development. Section 4 outlines the research method. Section 5 shows the analysis and results. Section 6 discusses the findings, contributions, limitations and possible directions for future research. Finally, Section 7 offers a brief conclusion.

5.2 THEORETICAL REVIEW

5.2.1 Shadow IT: Definitions and Types

According to the literature, shadow IT is any IT solution built, introduced, and used by employees to perform their work tasks without explicit approval or even knowledge of the organizational IT department (Silic and Back 2014; Haag and Eckhardt 2017). The definition of shadow IT states that it may be explicitly unauthorized or unknown technologies and, consequently, these technologies do not have the support of the IT department. Shadow IT, then, is a form of decentralized computing implemented by individuals, workgroups or whole business units (e.g., Zimmermann and Rentrop 2014; Furstenau, Rothe, and Sandner 2017) that does not technically or strategically involve the organizational IT service management (Zimmermann and Rentrop 2012).

The focus of research into shadow IT has changed over time. The first studies discussed the emergence of shadow IT after the adoption of ERPs. For instance, the use of Excel's spreadsheets instead of the officially implemented ERP system when performing work tasks (e.g., Jones et al. 2004; Behrens and Sedara 2004; Raden 2005). Since 2012, several studies have approached shadow IT at the organizational level of analysis, focusing on IT governance mechanisms to cope with shadow IT and minimize security risks (e.g., Györy et al. 2012; Zimmermann and Rentrop 2014; Furstenau, Rothe, and Sandner 2016; Zimmermann, Rentrop, and Felden 2017).

More recently, studies have begun to consider the individual level, analyzing behavioral aspects (e.g., motivations or antecedents) related to shadow IT usage (Haag and Eckhardt 2014). Those studies have sought to examine the motivations from the employee’s perspective, as well as the relationship between shadow IT usage and its outcomes, such as individual performance (e.g., Haag and Eckhardt 2014; Haag, Eckhardt, and Bozoyan 2015). Distinct terms related to the phenomenon have also emerged from these research streams. The term shadow IT refers to the unauthorized technology itself, while the employee's behavior in using this kind of technology has been called shadow IT usage. This research adopts the definition of shadow IT usage proposed by Haag and Eckhardt (2014) who define it as "the voluntary usage of any IT resource violating injunctive IT norms at the workplace as a reaction to perceived situational constraints with the intent to enhance the work performance, but not to harm the organization" (Haag and Eckhardt 2014).

As the definition suggests, shadow IT usage encompasses a variety of possibilities, since it can be the use of any software or hardware, on-premise or on-demand, self-developed or purchased, subject to or free of charge, and whether complementing or substituting the organizational IT infrastructure (Silic and Back, 2014; Haag and Eckhardt, 2014). For instance, an installed application, a spreadsheet, a cloud service, a peripheral device, or a combined solution are some examples of how employees use shadow IT in the workplace (Huber et al. 2016). Given this complexity, we performed a review of the literature on shadow IT in an attempt to clarify the ways in which individuals use shadow IT at work. We identified four broad types of shadow IT usage, namely: unapproved cloud services, self-made solutions, self-installed applications, and self-acquired devices. This categorization is based on technological aspects regarding the implementation and use of unauthorized technologies by employees. Table 5 presents the four types of shadow usage, their descriptions and the corresponding authors.

Table 5 – Types of Shadow IT Usage

Shadow IT Usage Types	Description	Authors
Unapproved cloud services	Use of Internet-based Software and Software as a Service (SaaS) that are not approved by or are unknown to the IT department. These systems are also called Mobile Shadow IT since they can be accessed outside the workplace. Examples of these systems are WhatsApp, Facebook, Google Sheets, Skype for Web, Dropbox, Google Docs, etc.	Rentrop and Zimmermann (2012); Györy *et al*. (2012); Furstenau and Rothe (2014); Silic and Back (2014); Haag and Eckhardt (2014); Zimmermann, Retrop and Felden (2014); Gozman and Willcocks (2015); Huber *et al*. (2016); Walters (2013); Meulensteen (2014); Walterbusch, Fietz and Teuteberg (2017); Silic *et al*. (2017), Mallmann *et al*. 2018.
Self-made solutions	Use of solutions developed by employees on the company's computers to perform their work tasks. For example, any software developed by employees, such as a system	Jones *et al*. (2004); Rentrop and Zimmermann (2012); Furstenau and Rothe (2014); Zimmermann *et al*. (2014); Huber *et al*. (2016).

	to communicate, collaborate, control or monitor information, etc.	
Self-installed applications	Use of software installed by employees to perform their work tasks, on the company's computers. For example, downloading and installing a software available free of charge on the internet (e.g., Pidgin, Skype…).	Jones *et al*. (2004); Rentrop and Zimmermann (2012); Furstenau and Rothe (2014); Zimmermann *et al*. (2014); Silic and Back (2014), Mallmann *et al*. 2018.
Self-acquired devices	Use of mobile devices, notebooks, servers, routers, printers or other peripherals purchased and used by employees without formal permission. These devices are purchased directly from retail rather than being ordered through the official IT department catalogue. It includes the use of applications in the employee's personal devices at the workplace. For example, smartphones, tablets, notebooks, etc. and the personal application access on the company's network.	Rentrop and Zimmermann (2012); Silic and Back, (2014); Zimmermann *et al*. (2014); Gozman and Willcocks (2015), Huber *et al*. (2016).

Source: Prepared by the author

The first type, unapproved cloud services, refers to software accessed via the internet (e.g., Furstenau and Rothe 2014; Haag, 2015; Silic, Barlow, and Back 2017; Walterbusch, Fietz, and Teuteberg 2017) which, therefore does not need to be installed on any device in order to be used. Self-made solutions are those developed and used by employees on the company's computers to perform their work tasks (e.g., Jones et al. 2004; Zimmermann, Retrop, and Felden 2014; Zimmermann, Rentrop, and Felden 2017). Such solutions may vary from a simple excel spreadsheet to more complex applications developed by employees to be used to facilitate work tasks, sometimes, by a whole business unit when communicating, controlling and/or monitoring information. In turn, self-installed applications represent items of software installed and used by employees on the company's devices (e.g., computers or tablets provided by the company) (e.g., Rentrop and Zimmermann 2012; Silic and Back 2014). Such applications are sometimes available free of charge on the web and need to be downloaded and installed to be used, instead of accessed via the internet.

Finally, the category, self-acquired devices, represents shadow IT hardware and encompasses devices owned by the employees and used at work without formal approval instead of the company's devices. This also includes the use of applications in the employee's personal devices at the workplace (e.g., Rentrop and Zimmermann 2012; Gozman and Willcocks 2015). Here it is crucial to emphasize that shadow IT is distinct from closely related concepts such as bring-your-own-device (BYOD) (Haag and Eckhardt 2017). By definition, BYOD is a policy that allows employees to bring and use personal devices at work (e.g., French et al. 2014). Although BYOD can facilitate or drive shadow IT usage because employees can use their devices in an inappropriate way. They differ in that BYOD assumes the use of personal devices at work is permitted, while shadow IT usage represents a deviation from rules, assuming personal devices are used without formal permission.

5.2.2 Social Presence Theory

The concept of social presence is particularly relevant at a time when the use of social networking solutions to communicate, collaborate and share information is increasing, as many studies in psychology suggest (e.g., Turkle 2011; Turner 2015). Social presence theory (SPT) was proposed by Short, Williams, and Christie (1976) to explain how users select communication channels. The theory suggests that media differ in terms of their ability to transmit signals that create for their users the awareness of other social actors (Mennecke et al. 2011). SPT studies how the "feeling of being with another" is shaped and affected by the interfaces, for example, a set of pixels in form of a smiling face, a voice through a speaker, or a text that appears on a chat room screen create the feeling of "being with the other," explain Biocca, Harms, and Burgoon (2003). The same authors also emphasize that the term social presence is specifically used to refer to interactions in technology-mediated environments.

The term social presence, then, is defined as a "feeling of being with the other in a mediated environment," that is, an awareness of the copresence of a body mediated by technology and the sense of accessibility to the psychological, emotional and intentions of another person (Biocca and Harms 2002). In that sense, social presence has often been used to assess the ability of people to connect via telecommunications systems, as well as measuring the degree to which people feel that the interface is able to provide some sense of access to another mind (Nowak and Biocca 2003).

Ogara, Koh, and Prybutok (2014) conceptualize social presence as the extent to which, along a continuum, a particular technology is sociable or unsociable, insensitive or sensitive, personal or impersonal. Thus, individuals may understand that different technologies provide different levels of social presence, which may influence their perception of technology and drive their behavior. Users can feel motivated to use the media available to change the sense of social presence for a wide range of activities, including meeting someone, exchanging information, problem solving and decision making, exchanging opinions, generating ideas, resolving conflicts, and maintaining friendly relations (Biocca, Harms, and Burgoon 2003).

The social presence construct and the means of measuring it are ongoing because many of the interested authors seem to define it and measure it in different ways (e.g., Lowethal 2010; Kim, Song, and Luo 2016). Biocca and Harms (2002), for instance, argue that social presence is best conceptualized and measured on three levels. The first is called the perceptual level, where there is a sense of copresence of another individual mediated by technology. The second is the subjective level that focuses on perceived accessibility. At this level, users have access to the emotional state and are aware of the understanding and behavioral interaction of the other person. Finally, the third level is the intersubjective level, which is known as mutual social presence, that is, the user's sense of social presence is partly a function of how they perceive the sense of social presence of themselves and the others.

We searched the literature on social presence to define the elements to be used in this research. Table 6 presents a summary of the most relevant elements of the social presence theory found in the literature, which we explain below.

Table 6 – Elements of Social Presence

Elements of Social Presence	Description	Authors
Copresence	Access: the feeling of being more accessible and have more access to another person. Shared environment: the feeling of being in the same space (e.g., in the same room). Proximity: the feeling of being close to another person.	Mennecke *et al*. (2011); Biocca and Harms (2002); Biocca, Harms, and Burgoon (2003); Nowak and Biocca (2003); Ogara (2011); Kim, Song, and Luo (2016)
Sensitivity	The feeling of perceiving the emotions of others and conveying one's emotions to others. This could be facilitated by using, for instance, emoji, pictures…	Lowenthal (2010); Biocca and Harms (2002); Ogara, Koh, and Prybutok (2014); Ogara (2011); Shin (2013); Kim, Song, and Luo (2016)
Comprehension	The feeling of being understood and understanding the intentions, motivations, and thoughts of the other.	Biocca and Harms (2002)

Source: Prepared by the author

The concept of copresence, which is widely used in studies on social presence, is related to the sense of connection between two people (Nowak and Biocca 2003) and may include the act of "being together" with someone in a technology-mediated environment with a sense of togetherness, as argued by Mennecke et al. (2011). Thus, copresence refers to the feeling of being close to another person in the same environment (same meeting room, for example) and therefore having the feeling of greater access and attention in relation to each other.

Sensitivity refers to how a particular technology allows the user to perceive the emotions of others as well as convey their emotional state during the interaction. The communication channels with the highest levels of perceived social presence, according to SPT, are described as sociable, warmer and personal (Ogara 2011, 31). The ability to perceive and understand the emotional state of others is essential to establish and maintain a connection with another person, according to Biocca and Harms (2002). Shin (2013) points out that social presence includes not only the perception of being with others but also the general feeling of emotional belonging. Thus, sensitivity is the element of social presence that refers to the extent to which the user is able to recognize the mood and emotions of others in technology -mediated communication. In the literature, terms such as personality or warmth are also used to describe this element of social presence (e.g., Ogara, Koh, and Prybutok 2014).

Biocca and Harms (2002) define comprehension as the degree to which a person feels that she/he has a similar view about the intentions, motivations, and thoughts of another. That is, both people realize there is a mutual understanding between them. This element can be related to the ease with which the communication channel can be used to transmit information, facial expressions, posture and nonverbal cues, thus facilitating both understanding between the parties and aiding the process of transmitting and understanding emotions.

It is important to note that social presence is social, that is, based on mutual interactions (e.g., Biocca, Harms, and Burgoon 2003). The elements involved in social presence listed above should be mutual, which is crucial for the perception of social presence in technology-mediated interaction.

Research on human-computer interaction often considers social presence because it is thought to mediate the effects of other central variables of interest to researchers, such as attitudes towards others, resource interfaces, etc. (Biocca, Harms, and Burgoon 2003). Thus, social presence offers a means to explore various aspects of technology and its effects on user behavior.

5.3. RESEARCH MODEL AND HYPOTHESIS DEVELOPMENT

Trang, Zander, and Kolbe (2014) argue that explanatory power should not be the first and only criterion when deciding to adopt a base model for a study, because each model (e.g., TAM, UTAUT) has different empirical strengths at different stages of adoption, while models also apply different theoretical lenses and have different theoretical emphases. Thus, the authors suggest that when designing a new study regarding the adoption and use of IS (Information Systems), theoretical considerations should be decisive at the outset. Accordingly, we have developed the research model for this study based on the IS literature, specifically previous studies on shadow IT and social presence theory.

5.3.1 Shadow IT Usage and Individual Performance

The research conducted to date has contributed greatly towards our understanding of the relationship between shadow IT usage and individual performance. Although some authors suggest that shadow IT can harm productivity and represents a severe risk to organizational information security (e.g., Raden 2005; Walters 2013), recent research has shown that shadow IT can have positive consequences for organizations (e.g., Silic and Back 2014; Haag, Eckhardt, and Bozoyan 2015). Singh (2015), for instance, argues that shadow IT reflects employee innovativeness in adapting to environmental change or in using emerging technologies to enhance their performance. Findings from Haag, Eckhardt, and Bozoyan (2015) showed that, compared to the users that did not deviate from the mandatory system, shadow IT users performed significantly better in their tasks. Similarly, Haag (2015) found that users think that by using shadow IT they will finish the task quickly and ultimately achieve a better performance compared to using the systems provided by the organization.

Despite these findings, studies continue to call for further research into the outcomes of using shadow IT at work since the issue on the positive and negative consequences of shadow IT remains relatively underexplored (e.g., Haag and Eckhardt 2017). Thus, one of the goals of this study is to examine how shadow IT usage impacts individual performance, while also analyzing what mediates the relationship.

Shadow IT may offer, then, an efficient way for users to cope with deficiencies of the mandatory systems (Haag and Eckhardt 2014). In that sense, the literature on shadow IT provides evidence of the relationship between shadow IT usage and individual performance. Thus, we propose the following hypothesis:

H1: Shadow IT usage is positively related to individual performance.

5.3.2 Social Presence and Shadow IT Usage

Studies on human-computer interaction are looking beyond factors such as utility and usability, addressing issues concerning technology-mediated social interaction. Not only in the personal but also in the work life, interactions are increasingly being mediated by telecommunications systems as the infrastructure for those systems expands. The increased bandwidth, greater mobility, and more immersive projects are providing a better sense of access to real and virtual places, increasing the sense of telepresence (Biocca, Harms, and Burgoon 2003). Developments in the conceptualization of social presence have also highlighted its role in geographically distributed organizations (e.g., Shin 2013). In the context of a global market where employees of an organization need to contact colleagues, clients and external partners often from distant geographical locations, the sense of social presence provided by technology becomes increasingly important.

Shin (2013) argues that social presence may represent a substitute for face-to-face communication in physical interaction. When classifying forms of communication in terms of levels of social presence, face-to-face interaction provides the highest sense of social presence, followed by video, audio, and text (e.g., Biocca, Harms, and Burgoon 2003; Parameswaran and Kishore 2017). Given that different technologies provide different levels of social presence (e.g., Mennecke et al. 2011), employees may prefer a technology that offers them the level of social presence necessary to achieve the interpersonal involvement required to perform a task (Parameswaran and

Kishore 2017), even when this technology deviates from organizational security policies.

Silic and Back (2014) investigated the kinds of software identified as shadow IT within organizations. Most organizations listed productivity software (e.g., Google Apps) first, followed by communications software (e.g., Skype). The authors found Skype, Google Talk, and Facebook were the three primary applications used by employees to communicate and collaborate at work, often, without formal permission from the organizational IT department. These types of software share common characteristics: they allow instantaneous communication, including the use of text, visual aids (e.g., pictures, emoji), audio, and video resources. Thus, this sort of collaborative software, which often appears in the list of shadow IT, may allow a greater sense of social presence. Accordingly, we can infer that shadow IT usage increases the sense of social presence by using interactive tools that provide instantaneous and dynamic interaction. Consistent with the above arguments, we propose the following hypothesis:

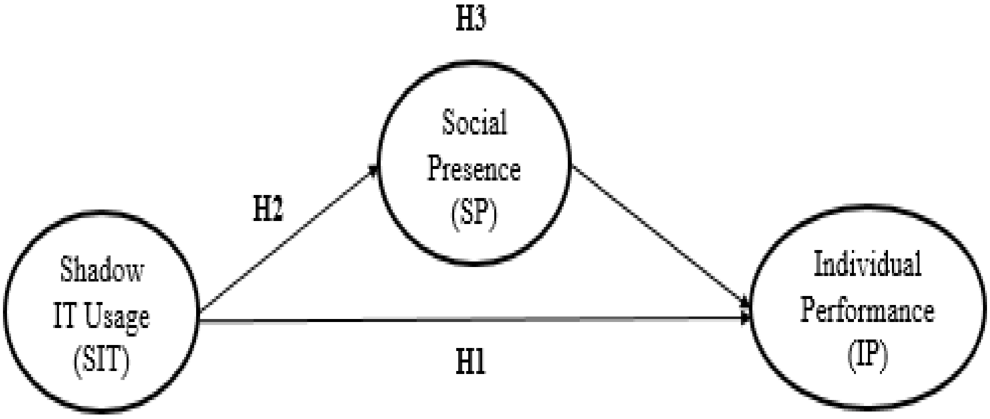
H2: Shadow IT usage is positively related to perceived social presence.

The literature shows that social presence greatly influences usability in technology use (Shin 2013). The evaluation of satisfaction with communication systems and the productive performance in teleconferencing and collaborative virtual environments is largely based on the level of social presence they provide (Yoo and Alavi 2001; Biocca, Harms, and Burgoon 2003). Thereby, social presence is shown to be positively related, directly and\or indirectly, to task performance (Shin 2013; Parameswaran and Kishore 2017; Shin 2018). Hence, we propose:

H3: The relationship between shadow IT usage and individual performance is mediated by social presence.

Figure 2 illustrates the research model for this research. To recapitulate, this study predicts: firstly, that shadow IT usage is positively related to individual performance; secondly, that shadow IT usage is positively related to social presence; and thirdly, that the relationship between shadow IT usage and individual performance is mediated by social presence.

Figure 2 – Research Model



Source: Prepared by the author

5.4. METHOD

5.4.1 Research Setting and Data Collection

We conducted a quantitative study to empirically assess the research model. A web-based survey was used to gather relevant information. Before conducting the survey, we designed a questionnaire based on the existing IS literature following the guidelines suggested by MacKenzie et al. (2011). The questionnaire was created in Google Form, a free online tool to create and analyze surveys, and was distributed by e-mail using a link.

Since shadow IT is a behavioral phenomenon that arises from the employee, this research has focused on the individual level. We aimed to investigate the shadow IT used by employees as collaborative and communication systems on company devices or personal devices. The sample consisted exclusively of IT users in administrative business units from three large companies located in Brazil. By administrative business units, we mean employees working in such business units as: marketing, human resources, financial, commercial and sales. The respondents and companies were ensured confidentiality, and we offered access to the survey results to the IT managers in order to aid them manage shadow IT. First, we sent an e-mail to the IT manager of those companies asking about the presence of shadow IT in the organizational processes. After receiving a positive response, we sent an exclusive link with the questionnaire to each company, which allowed us to control the sample and develop an executive report of the survey results for each company. A total of 286 respondents from the three companies completed the survey.

5.4.2 Measures

Respondents were required to complete the questionnaire that included questions about shadow IT usage, social presence, and individual performance. All the items in the variables were measured on a 7-point Likert scale, where ‘1=strongly disagree’ and ‘7 = strongly agree’.

To ensure the significance of the sample, the first part of the questionnaire contains the definition of shadow IT, according to Haag and Eckhardt (2014). To ensure all the respondents have the same understanding of the term, we provided some common examples of shadow IT as reported by previous studies (e.g., Silic and Back 2014; Mallmann, Maçada and Oliveira 2018), such as the use of WhatsApp, Skype, Dropbox or Google Drive at work without official permission of the organization. Thereby, we required the respondents to think about the technologies they use in the workplace that do not have formal approval from the organizational IT department, based on the definition and examples from the literature. Then, we asked them to answer the following yes/no question “Have you ever used technology without formal approval to perform your work tasks?”. This first step allowed us to identify the actual shadow IT users, and exclude the non-shadow IT users from the sample, which is recommended when investigating shadow IT user behavior (e.g., Haag, Eckhardt and Bozoyan, 2015; Silic 2019).

5.4.2.1 Development of the independent and dependent variables

We followed the guidelines for scale development provided by MacKenzie et al. (2011). After conceptualizing the constructs, we used extant literature to develop items that represent definitions of the focal constructs. Two further steps were incorporated to ensure the validity and reliability of the measures according to MacKenzie et al. (2011). First, we asked four IT experts (2 IT managers and 2 doctoral students in IS) to proofread and analyze the questionnaire to assess the content validity of the items. Second, we conducted a pre-test study among 52 employees from a large company in the communication sector to purify and refine the scale.

The items of the independent variable, shadow IT usage, are based on a review of the relevant literature (see Table 5), such as Silic and Back (2014) and Haag and Eckhardt (2014). As discussed above, shadow IT is defined as any information technology voluntarily adopted and used by employees without the approval of the IT department to perform work tasks (Haag and Eckhardt 2014). Considering that definition of shadow IT, two essential aspects of measuring shadow IT usage arise. First, employees do not only adopt shadow IT but also use it regularly to perform work tasks. Second, the phenomenon arises from the employees, which means from the individual level (Haag and Eckhardt 2014). Therefore, our objective here is to assess the post-adoption level of shadow IT from the employee’s perspective, that is, the use of shadow IT at the individual level. In line with previous studies on shadow IT at the individual level, shadow IT usage was assessed based on self-reported measures (e.g., Haag and Eckhardt 2014; Haag, Eckhardt and Bozoyan 2015; Silic, Barlow and Back 2017). The final version of the construct shadow IT usage behavior consists of four items.

Social presence was operationalized from previous studies such as Ogara, Koh, and Prybutok (2014) and Biocca, Harms, and Burgoon (2003) (see Table 6). In turn, individual performance was measured based on the perceived impacts on performance of using shadow IT to execute work tasks, which implies a mix of improved efficiency, improved effectiveness, and/or higher quality of an individual's work (cf. Goodhue and Thompson 1995). We based our understanding and operationalization of individual performance on previous studies that also measure individual performance, such as Goodhue & Thompson (1995), Stone, Good and Baker-Eveleth (2007), Mohammadyari and Singh (2015). The next step was to adapt the items to the context of shadow IT usage. To do so, we used previous studies on shadow IT that discuss some of the outcomes of using unauthorized technology at work (e.g., Silic and Back 2014; Haag and Eckhardt 2015; Mallmann, Maçada and Oliveira 2018).

The construct individual performance has five items involving the perceived impacts of shadow IT on performance, productivity, exchange of information and problem-solving. It is important to highlight that a subjective measure of performance was preferred in this case because of the challenges of measuring the outcomes of shadow IT using an objective measure, especially given the different task portfolios of individuals and the range of contexts in which shadow IT can be used, which is in line with prior literature (e.g., Goodhue and Thompson 1995; Stone, Good and Baker-Eveleth 2007; Mohammadyari and Singh 2015). Table 7 shows the measurement items used in this research.

Table 7 – Measurement Items

Construct and Items	Source
Shadow IT Usage SIT1: I use Internet-based software or cloud services that are unauthorized or unrecognized by the IT department. Examples of these systems are WhatsApp, Facebook, Google Sheets, Skype for Web, Dropbox, Google Docs, etc. SIT2: I use a solution developed by me or another employee on the company's computers that is unauthorized or unrecognized by the IT department to perform my work tasks. Examples: any software developed by employees, such as a program to control and monitor information, collaborative tools, excel spreadsheet, etc. SIT3: I use software installed by me or another employee on the company's computers that is unauthorized or unrecognized by the IT department to perform my work tasks. Examples can be any free download software (Pidgin, Skype) to communicate, share information, execute tasks, etc. SIT4: I use my own devices at work without permission from the IT department, including applications on my mobile device on the company's network. For instance, Smartphone, tablets, notebook, etc.	Based on the shadow IT literature (e.g., Rentrop and Zimmermann 2012; Györy *et al*. 2012; Silic and Back 2014; Haag and Eckhardt 2014; Gozman and Willcocks 2015; Zimmermann, Rentrop, and Felden 2017, Silic *et al*. 2017, Mallmann *et al*. 2018).
Social Presence SP1: I feel like I am more accessible and I have more access when I use shadow IT at work. SP2: I have the feeling of being in the same space as the other person (e.g., in the same room) when I use shadow IT. SP3: I feel I am closer to the other person when I use shadow IT. SP4: I feel I can better understand people's emotions when I use shadow IT. SP5: I feel I can best convey my emotions to others when I use shadow IT. SP6: I feel I am more easily understood when I use shadow IT at work. SP7: I feel I can better understand the others when I use shadow IT at work.	Based on the authors of Table 6 (e.g., Biocca and Harms 2002; Lowenthal 2010; Ogara 2011; Ogara, Koh, and Prybutok 2014).
Individual Performance IP1: My productivity increases using shadow IT. IP2: I can perform my work tasks faster using shadow IT. IP3: I exchange information with my colleagues more effectively using shadow IT.	Based on Goodhue and Thompson (1995); Stone, Good and Baker-Eveleth (2007); Mohammadyari and Singh (2015) and adapted to

IP4: I can solve problems faster using shadow IT. IP5: Overall, the use of shadow IT improves my performance.	the shadow IT context (e.g., Silic and Back 2014; Haag and Eckhardt 2015; Mallmann, Maçada and Oliveira 2018).

Source: Prepared by the author

5.4.3 Analysis

This research adopts the partial least squares (PLS) approach to structural equation modelling (SEM) to test the research model. PLS-SEM is widely used in business research fields, such as information systems, marketing, and operations management (e.g., Peng and Lai 2012). Given that our research aims to predict the relationship between shadow IT usage and individual performance mediated by social presence, PLS may be considered suitable because it is an appropriate method when the research objective is prediction and theory development (Hair, Ringle, and Sarstedt 2011).

5.5 RESEARCH FINDINGS

As commonly recommended, this research follows a two-stage approach to evaluation: 1) assessment of the measurement model and 2) estimation of the structural model and hypothesis tests (Hair et al. 2016).

5.5.1 Assessment of the Measurement Model

Several statistical tests were applied to validate the measurement model. First, the analysis assesses the factor loadings, which must be larger than the recommended minimum of 0.7 (Hair et al. 2016). The factor loading values ranged from 0.645 to 0.948. Only two items of the construct shadow IT usage (SIT2: 0.668 and SIT3: 0.645) did not reach the minimum value of 0.7. However, the items were retained because their values were close to the threshold of 0.7 and, consequently, their deletion would not lead to a considerable increase in the AVE or in the composite reliability values (Hair et al. 2016). Second, the analysis of internal consistency and the scale reliability was checked using Composite Reliability (CR). Hair, Ringle, and Sarstedt (2011) suggest 'composite reliability' as a replacement for 'Cronbach's alpha' in assessing internal consistency reliability. CR values should be higher than 0.70. As shown in Table 8, all the constructs are above that threshold, demonstrating consistency and internal reliability. Next, the convergent validity of the constructs was calculated using Average Variance Extracted (AVE), that should be higher than 0.50 (Hair, Ringle, and Sarstedt 2011). With a minimum of 0.50, all AVE values are higher than the acceptable threshold of 0.5. Table 8 presents the CR and AVE values, as well as the correlation matrix of constructs.

Table 8 – Composite Reliability (CR), AVE and Correlation Matrix of Constructs

Constructs	CR	AVE	Shadow IT Usage	Social Presence	Individual Performance
Shadow IT usage	0.799	0.50	**0.707**		
Social Presence	0.943	0.702	0.506	**0.838**	
Individual Performance	0.965	0.845	0.625	0.710	**0.919**

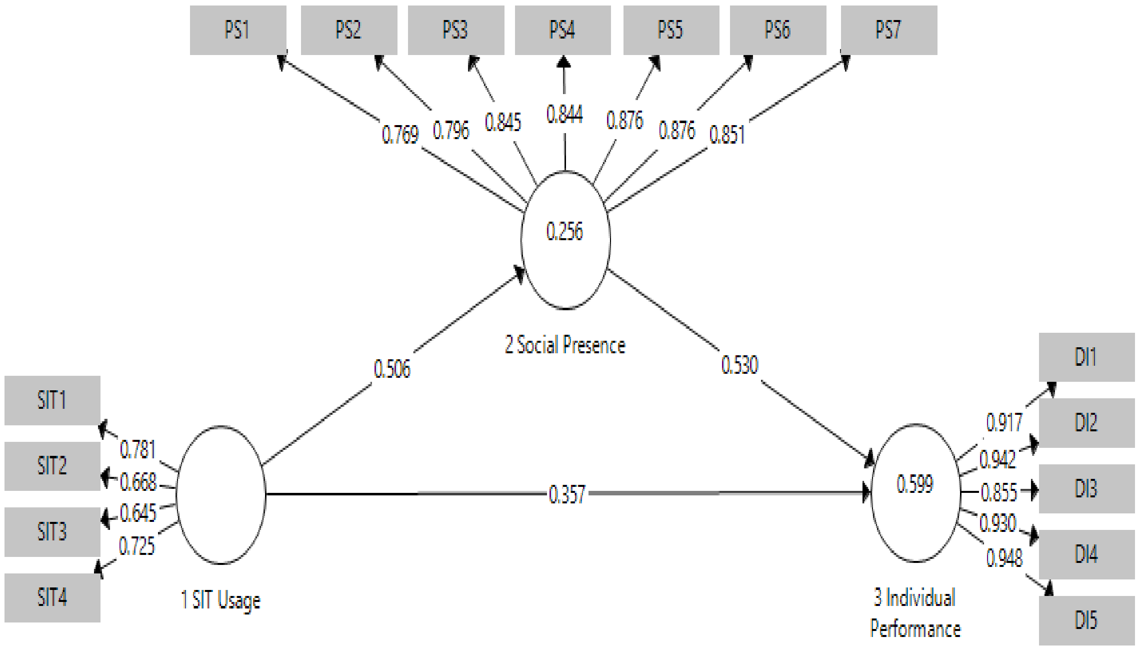
Source: Prepared by the author

The discriminant validity was assessed based on two criteria. First, we followed the Fornell–Larcker criterion. The correlation matrix in Table 8 shows the results for discriminant validity, which determines the extent to which a construct is empirically distinct from other constructs in the path model. The square root of the AVE for each construct should be greater than its highest correlation with any other construct (Hair et al. 2016). Thus, the discriminant validity was established for all constructs. Second, the study applies the Heterotrait-Monotrait Ratio (HTMT), with which the values obtained for the reflective variables were lower than the most conservative criterion of 0.85 (Henseler, Ringle, and Sarstedt 2015), thus reinforcing the internal validity of the measurement model.

5.5.2 Estimating the Structural Model

After confirming the reliability and validity of the construct measures, we assessed the structural model. Figure 3 shows the structural model with the results of PLS analysis.

Figure 3 – Structural Model with Results of the PLS Analysis



Source: Prepared by the author

The following results are based on the application of the bootstrapping procedure provided by SmartPLS. We followed the guidelines provided by Hair, Ringle, and Sarstedt (2011) for a minimum number of 5,000 bootstrap samples.

First, the collinearity was examined using Variance Inflation Factor (VIF) values. The result showed the VIF values for all the independent variables ranged between 1.000 (shadow IT usage) and 1.343 (social presence), indicating the results were not negatively affected by collinearity, as they were larger than 0.20 and smaller than 5 (Hair et al. 2016). Regarding Path coefficients, the three paths are significant at p< 0.01-level, as shown in Table 9.

Table 9 – Hypothesis Testing for Relationships among Constructs

Hypothesis	Path	Path coefficient	Standard error	t-Statistic (a)	P Value	Decision
H1	SIT → IP	0.357	0.045	11.770***	0.000	Supported
H2	SIT → SP	0.506	0.044	11.379***	0.000	Supported
H3	SIT → SP → IP	0.268	0.034	7.910***	0.000	Supported

(a) t-values for two-tailed test. ** 1.96 (sig. level =5%); *** t-value 2.57 (sig. level =1%) (Hair et al. 2016). Source: Prepared by the author.

Shadow IT usage is positively related to individual performance (β = 0.357, $p < 0.01$), providing empirical support for hypothesis H1. H2 was also supported, showing shadow IT usage is positively related to social presence (β = 0.506, $p < 0.01$). Furthermore, the relationship between shadow IT usage and individual performance is mediated by social presence, supporting hypothesis H3 (β = 0.268, $p < 0.01$), which is a relationship explored in more detail in the next section.

The R^2 value is a measure of the variance explained in each endogenous construct and of the model's predictive accuracy. In social and behavioral sciences, Cohen (1988) suggests assessing the R^2 values for endogenous latent variables as follows: 26% as a substantial effect, 13% as moderate, and 2% as weak. The R^2 value of the endogenous constructs, social presence and individual performance, are 0.256 and 0.599, respectively. This result represents a substantial effect of the variance explained in the endogenous constructs, according to Cohen’s (1988) criterion, confirming the predictive accuracy of the model.

Stone–Geisser’s Q^2 measure was calculated to assess the model’s predictive relevance. Running the blindfolding procedure with an omission distance of seven yielded cross-validated redundancy values for the endogenous constructs are above zero (Hair, Ringle, and Sarstedt 2011), thus supporting the model's predictive relevance. Finally, the study assessed the standardized root mean square residual (SRMR) as an appropriate measure of model’s fit. Assuming a cut-off value of 0.08 as recommended for PLS path models (Henseler, Hubona, and Ray 2016), the SRMR value resulted was 0.07. Hence, the model shows a good fit.

5.5.3 Mediating Analysis

H3 states the relationship between shadow IT usage and individual performance is mediated by social presence. The mediation analysis was conducted in accordance with the guidelines from Hair et al. (2016). First, the direct and total effect of the impact of the independent variable on the dependent variable were assessed (see Table 9). Next, we assessed the indirect effect, that is, the impact of the independent variable on the dependent variable through the mediating variable. We ran a full model using a bootstrapping procedure with 5000 bootstrap samples (e.g., Zhao, Lynch and, Chen 2010; Shujahat et al. 2017).

As reported above, H3 was supported. The direct effect of shadow IT on individual performance was found to be positive and significant (β = 0.357, p < 0.01; Table 9). Subsequently, we evaluated the indirect effect of shadow IT usage on individual performance via the mediating construct, social presence, to analyze the mediating relation. The indirect effect was also found to be positive and significant (β = 0.268, p < 0.01; Table 10). Finally, the total effect was also found to be positive and significant (β = 0.628, p < 0.01). Table 10 shows the values.

Table 10 – The Direct, Indirect and Total Effect

Relationship	Direct Effect	Indirect effect	Total effect
SIT → SP → IP	0.357	0.268	0.628

Source: Prepared by the author

Therefore, the results suggest a complementary mediation (partial mediation) in the relationship of shadow IT usage and individual performance mediated by social presence, and H3 is accepted. Complementary mediation means that the indirect effect (mediated effect) and direct effect both exist and point in the same direction (Zhao, Lynch, and Chen 2010; Hair et al. 2016). Therefore, the results provide empirical support for the hypothesized mediating relationship.

5.6. DISCUSSION

This research examined the mediating role of social presence on the relationship between shadow IT usage and individual performance. The three hypotheses tested in this research were supported by empirical data. The results provide empirical evidence to show shadow IT usage is positively related to individual performance. According to our findings, the respondents consider that using shadow IT allows them to solve problems faster and complete tasks in a more efficient way, thus increasing their productivity. Therefore, the results show that, in general, shadow IT usage improves task performance from the employees' perspective. This result is consistent with the literature (e.g., Haag and Eckhardt 2014; Haag 2015). Findings from Haag, Eckhardt, and Bozoyan (2015), for instance, show shadow system usage has a positive impact on job performance of individuals. The relationship between shadow IT and individual performance is more thoroughly explored below in the mediation analysis.

The findings also suggest shadow IT usage is positively related to perceived social presence. Previous studies (e.g., Shumarova and Swatman 2008; Silic and Back 2014; Mallmann, Maçada, and Oliveira 2018) found shadow IT often involves the use of technologies that enable instant communication and, consequently, facilitate information and knowledge sharing. Shumarova and Swatman (2008) posit that synchronous conversational media (e.g., instant messaging or chat) enable interaction that is similar to face-to-face conversation, motivating people to respond quickly and consequently increasing the perceived social presence.

The results also indicate cloud-based services represent the most widely used type of shadow IT in the workplace. Employees frequently use cloud-based services to communicate and share work information with co-workers, clients or external partners. Typical examples are Facebook, WhatsApp and Google Apps. Several factors may explain this preference. First, cloud services are easy to access and their use does not usually demand expert technical knowledge or skills. Second, many employees are already familiar with cloud-based applications because they use them in their personal lives. Third, most of those services are available free of charge on the internet and are accessible online, with no need to download the application onto a computer.

The use of unauthorized self-installed applications and personal devices to access some applications at work is not as prevalent as the use of cloud-based services. Nevertheless, they are also frequently used by employees and can provide communication and collaboration features. In these scenarios, employees use chat applications such as Pidgin or Skype, which have to installed on a device in order to be used, or they use communication features provided by personal mobile devices, for example, smartphone resources to increase social presence (express opinions, thoughts, or emotions) via voice message or video calling.

5.6.1 The Mediating Role of Social Presence

Finally, the results suggest social presence plays a mediating role in the relationship between shadow IT usage and individual performance. As discussed above, the use of unauthorized collaborative tools and their resources (e.g., instant messengers, video calls, voice message, and emoji) that enable instant communication and better collaboration can increase perceived social presence, which drives gains in individual performance.

Shin (2018) argues that improved image quality leads users to experience increased social presence and, consequently, achieve a flow experience (a state of profound enjoyment and concentration) during activities. For example, Emoji is a resource that is quickly being integrated into digital communication which may improve image quality and provide a better conversation flow (e.g., Shin 2018). According to a survey reported by The Wall Street Journal, more than half of the employees have used emoji to communicate at work. The book "Semiotics of Emoji" by Marcel Danesi (2016) analyses this specific form of communication. Danesi argues that emoji have emerged as a compensatory universal language since it is controlled by a centralized body and regulated across the web. In that sense, the increasing use of emoji within organizations represents an example of how these little faces and images aid effective communication in a global and multicultural organizational environment.

Considering the elements of social presence assessed in this study, the findings show that shadow IT usage can allow people to communicate their emotions better by using visual aids, such as emoji, pictures and video, increasing the conversation quality and flow (e.g., Shin 2018). This result suggests the use of shadow IT enhances sensitivity in computer-mediated communication. Similarly, the findings also suggest employees believe they can be more easily understood and better understand others when using shadow IT to communicate at work. Therefore, sensitivity and comprehension represent relevant aspects of the social presence provided by shadow IT usage. This may be related to what is perceived as the enhanced quality of communication arising from the possibility of transmitting information through facial expressions, posture and nonverbal cues, which corroborate towards understanding among people (e.g. Biocca and Harms, 2002).

Considering the mediating role played by social presence in the relationship between shadow IT usage and individual performance, the findings suggest that shadow IT usage improves individual performance by enhancing computer-mediated communication and collaboration. This result helps explain why the use of unauthorized technologies at work, such as unauthorized collaborative tools analyzed in this study, may represent an efficient way of circumventing deficiencies in mandatory systems and, consequently, enhance employee performance (e.g. Haag, Eckhardt, and Bozoyan 2015; Shin 2018).

5.6.2 Theoretical and Practical Contributions

This research provides both academic and practical contributions. It offers new insights into the post-adoption level literature, primarily regarding the use of unauthorized technology in the workplace. The model applied in this study identifies some consequences of shadow IT usage, besides explaining, to some extent, how shadow IT usage impacts individual employee work performance. In addition, the results point to the importance of the social presence perspective in the workplace, such as the capacity to express opinions, thoughts, or emotions in technology-mediated communication. These findings contribute towards the knowledge available on and our understanding of shadow IT, which is an emerging and largely unexplored topic that has attracted the attention of the academic community in recent years. Nevertheless, the topic demands the development of a more robust theoretical basis and further research to elucidate the phenomenon. Below, we detail the academic and practical contributions of this study.

Firstly, we provide contributions to the literature on shadow IT. This research contributes by analyzing shadow IT usage from a new theoretical perspective, as called for in previous studies (e.g., Haag and Eckhardt, 2017). Considering that social factors profoundly influence user behavior toward the adoption and use of technologies (e.g., Venkatesh et al., 2003; Wang, Meister and Gray, 2013), this study contributes by examining the impact of shadow IT on individual performance through the lens of social presence theory, which also helps explain the individual use of shadow IT. From a conceptual perspective, the study offers a discussion on the definition of shadow IT usage and categorizing the commonly used types of shadow IT, based on previous research and validated by empirical data. More importantly, the study contributes towards the discussion on the consequences of shadow IT (e.g., Haag and Eckhardt 2017). The study finds there are some interesting outcomes of using shadow IT to carry out work tasks, such as faster and more dynamic communication, improved collaboration among co-workers and, ultimately, better individual performance.

Secondly, Yoo and Alavi (2001) call for further studies that consider social factors in the dynamics of technology-mediated communication environments within organizations, since they can profoundly influence the individual's perception and use of technology. The study's findings suggest that adding social features like social presence to technology can enhance performance, which consequently motivates individuals to adopt and use technology (e.g., Shin 2013), including unauthorized solutions. Thus, we provide insights into new patterns of IS usage, and the infusion, and diffusion of digital technology in organizations.

Thirdly, this study also contributes towards human-computer interaction (HCI) research. Studies on HCI are looking beyond factors such as the utility and usability of technologies in striving to understand user behavior. The pervasiveness of technology in private and professional lives has considerably altered the way people socially interact, while also changing their preferences regarding the communication channels they use to exchange content with others (e.g. Turkle 2011). Considering this context, the present study also highlights issues related to immersion and presence (Shin 2018) regarding the use of technology within organizations. As our results suggest, those issues are relevant to employees in an organizational setting because they can affect the execution of daily work. In a similar vein, the absence of suitable social presence features can harm the execution of work tasks. In that sense, we demonstrate how social presence contributes to individual performance in technology-mediated communication in the workplace. In line with findings from Shin (2018), our results also suggest the importance of social aspects such as the ability to express and understand thoughts and emotions via instant communication. Moreover, our findings show how visual resources drive individuals to experience increased social presence during activities that rely on communication and collaboration with co-workers, leading to work tasks being executed more efficiently.

These academic contributions also have important implications for managers. The study's findings imply that adding social features to technology intended for use in work tasks positively impacts employee performance, which also leads to the greater adoption and use of unauthorized technology in the workplace. Hence, organizations need to be aware that the main driver behind shadow IT usage is the complete or partial absence of adequate IT solutions that meet their employees’ requirements (Walterbusch et al. 2017). The findings suggest shadow IT can be very valuable for organizations because it helps improve communication and collaboration among employees, clients and external partners. More effective communication and work information sharing with co-workers, clients and partners can enhance job performance. Thus, although the use of shadow IT may represent risks to organizational security, managers should not consider it solely as a threat to be eliminated. Instead, managers must take into account the social capabilities (e.g., communication) needed by business units and employees to efficiently perform their tasks and, consequently, organizations can invest in technologies that provide users a greater sense of social presence, such as instantaneous and dynamic communication among co-workers.

Similarly, the study’s findings can be used by IT managers to develop strategies to cope with shadow IT. Silic and Back (2014) suggest that if shadow IT improves employee productivity and innovation, it could be a valuable decision-making factor regarding a company's future strategic directions. In addition, organizations need to fully understand the reasons for, and consequences of deviant workplace behaviors, such as shadow IT usage in the workplace. Therefore, knowing not only how to mitigate the security risks presented by shadow IT, but also recognizing the opportunities shadow IT offers would seem to be strategic to business success and survival in a modern organizational environment.

5.6.3 Limitations and Future Research Directions

This research has some limitations that may provide opportunities for future research. Firstly, it focuses on a specific sort of shadow IT, that is, unauthorized technology used to collaborate and communicate at work. Thus, caution is required before applying our conclusions more generally since the findings are not based on all possible forms of shadow IT, for example, internet browsers and PDF tools (e.g., Silic and Back 2014).

Secondly, the practical and the academic literature discuss various perspectives of shadow IT usage, such as shadow IT as an organizational threat to information security (e.g., Walters 2013; Silic and Back 2014), but also as an opportunity to drive innovation and enhance individual performance (e.g., Furstenau and Rothe 2014; Haag et al. 2015). Thus, there is a consensus among researchers and managers that shadow IT has potential benefits and drawbacks. However, the present study focuses on the positive consequences of shadow IT, which may limit the value of the findings to some extent considering the complex scenario of managing shadow IT.

Thirdly, a complementary mediation, as is the case of social presence in this research, supports the hypothesized mediating relationship, but it suggests another mediator of this relation may exist (Hair et al. 2016). In that sense, there are other factors to be analyzed in the relationship between shadow IT and individual performance that could be addressed in future research.

Fourthly, the concept of social presence is relevant at a time when the dependence on technology to interact with people is increasing, including in organizations (Yoo and Alavi 2001), especially among digital natives (Turkle 2011). In addition, previous studies have suggested the use of consumer technologies are more prominent among younger people, known as tech-savvy, or the millennial or Y generations (e.g., Harris, Ives, and Junglas 2012; Turner 2015). Therefore, it could be fruitful to test other drivers that might improve the explanatory power of the equation, such as a study involving tech-savvy users or digital natives.

Finally, other issues related to the concept of social presence can be better explored in future studies. For example, social presence theory can be discussed from the immersion perspective (e.g., Shin 2018; Shin, 2019), since this issue might also influence user behavior regarding technology in the workplace. Moreover, our study has assessed sensitivity, which is the perception and conveyance of emotions to others, as part of the social presence construct. Further studies could better explore this aspect of social presence by investigating the extent to which the sense of emotional reality appeals to users and the feeling of emotional belonging relates to the use of technology at work (Shin 2013).

References

Bazzaz, D. 2016. “Emoji at Work: Managing with a Wink and a :).” The Wall Street Journal, July 12. https://www.wsj.com/articles/emoji-at-work-managing-with-a-wink-and-a-1468346237

Biocca, F., and Harms, C. 2002. “Defining and Measuring Social Presence: Contribution to the Networked Minds Theory and Measure.” Paper presented at the Proceedings of Presence of 2002, Porto, October 9-11.

Biocca, F., Harms, C., and Burgoon, J. K. 2003. “Toward a More Robust Theory and Measure of Social Presence: Review and Suggested Criteria.” *Presence* 12 (5) : 456-480.beh

Cohen, J. 1988. Statistical Power Analysis for the Behavioral Sciences. New York: Psychology Press.

Danesi, M. 2016. The Semiotics of Emoji: The Rise of Visual Language in the Age of the Internet. London: Bloomsbury Publishing.

Furstenau, D., and Rothe, H. 2014. “Shadow IT Systems: Discerning the Good and the Evil.” Paper presented at the Proceedings of the Twenty-Second European Conference on Information Systems of 2014, Tel Aviv, June 9-11.

Furstenau, D., Rothe, H., and Sandner, M. 2017. “Shadow Systems, Risk, and Shifting Power Relations in Organizations.” *Communications of the Association for Information Systems* 41 (1): 3.

French, A. M., Guo, C., and Shim, J. P. (2014). “Current Status, Issues, and Future of Bring Your Own Device (BYOD)”. *Communications of the Association for Information Systems*, 35 (10): 191-197.

Goodhue, D. L., and Thompson, R. L. 1995. “Task-technology fit and individual performance”. *MIS Quarterly*, 19 (2), 213-236.

Gozman, D., and Willcocks, L. 2015. “Crocodiles in the Regulatory Swamp: Navigating The Dangers of Outsourcing, SaaS and Shadow IT.” Paper presented at the Proceedings of the Thirty-Sixth International Conference on Information Systems of 2015, Fort Worth, December 13-16.

Györy, A. A. B., Cleven, A., Uebernickel, F., and Brenner, W. 2012. “Exploring the Shadows: IT Governance Approaches to User-Driven Innovation.” Paper presented at the Proceeding of the Twentieth European Conference on Information Systems of 2012, Barcelona, June 10-13.

Haag, S. 2015. “Appearance of Dark Clouds?-An Empirical Analysis of Users' Shadow Sourcing of Cloud Services.” Proceedings of the Wirtschaftsinformatik: 1438-1452.

Haag, S., and Eckhardt, A. 2014. “Normalizing the Shadows–The Role of Symbolic Models for Individuals’ Shadow IT Usage.” Paper presented at the Proceedings of the Thirty-Fifth International Conference on Information Systems of 2014, Auckland, December 14-17.

Haag, S., Eckhardt, A., and Bozoyan, C. 2015. “Are Shadow System Users the Better IS Users?–Insights of a Lab Experiment.” Paper presented at the Proceedings of the Thirty-Sixth International Conference on Information Systems of 2015, Fort Worth, December 13-16.

Haag, S., and Eckhardt, A. 2017. “Shadow IT.” *Business & Information Systems Engineering* 59 (6): 469-473.

Hair, J. F., Ringle, C. M., and Sarstedt, M. 2011. “PLS-SEM: Indeed a Silver Bullet.” *Journal of Marketing Theory and Practice* 19 (2): 139-152.

Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2016. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Los Angeles: Sage.

Harris, J., Ives, B., and Junglas, I. 2012. “IT Consumerization: When Gadgets Turn Into Enter-prise IT Tools.” *MIS Quarterly Executive* 11 (3).

Henseler, J., Hubona, G., and Ray, P. A. 2016. “Using PLS Path Modeling in New Technology Research: Updated Guidelines.” *Industrial Management & Data Systems* 116 (1): 2-20.

Henseler, J., Ringle, C. M., and Sarstedt, M. 2015. “A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling.” *Journal of the Academy of Marketing Science*, 43 (1): 115-135.

Huber, M., Zimmermann, S., Rentrop, C., and Felden, C. 2016. “The Relation of Shadow Systems and ERP Systems—Insights from a Multiple-Case Study.” *Systems* 4 (1): 11.

Jones, D., Behrens, S., Jamieson, K., and Tansley, E. 2004. “The Rise and Fall of a Shadow System: Lessons for Enterprise System Implementation.” Paper presented at Proceedings of the Fifteenth Australasian Conference on Information Systems of 2004, Hobart, December 1-3.

Kim, J., Song, H., and Luo, W. 2016. “Broadening the Understanding of Social Presence: Implications and Contributions to the Mediated Communication and Online Education.” *Computers in Human Behavior* 65: 672-679.

Lowenthal, P. R. 2010. The Evolution and Influence of Social Presence Theory on Online Learning. Online Education and Adult Learning: New Frontiers for Teaching Practices. Pennsylvania: IGI Global.

Mallmann, G. L., Maçada, A. C. G., and Oliveira, M. 2018. “The influence of shadow IT usage on knowledge sharing: An exploratory study with IT users.” *Business Information Review* 35(1):17–28. https://doi.org/10.1177/0266382118760143

MacKenzie, S. B., Podsakoff, P. M., and Podsakoff, N. P. 2011b. “Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques,” *MIS Quarterly* (35:2), pp. 293–334.

Mennecke, B. E., Triplett, J. L., Hassall, L. M., Conde, Z. J., and Heer, R. 2011. “An Examination of a Theory of Embodied Social Presence in Virtual Worlds.” *Decision Sciences* 42 (2): 413-450.

Mohammadyari, S., and Singh, H. 2015. “Understanding the Effect of E-learning on Individual Performance: The Role of Digital Literacy.” *Computers & Education* 82: 11-25.

Nowak, K. L., and Biocca, F. 2003. “The Effect of the Agency and Anthropomorphism on Users' Sense of Telepresence, Copresence, and Social Presence in Virtual Environments.” *Presence: Teleoperators and Virtual Environments* 12 (5): 481-494.

Ogara, S. O. 2011. “Design for Social Presence and Exploring Its Mediating Effect in Mobile Data Communication Services.” PhD diss., University of North Texas.

Ogara, S. O., Koh, C. E., and Prybutok, V. R. 2014. “Investigating Factors Affecting Social Presence and User Satisfaction with Mobile Instant Messaging.” *Computers in Human Behavior* 36: 453-459.

Parameswaran, S., and Kishore, R. 2017. “A Social Presence Model of Task Performance: A Meta-Analytic Structural Equation Model.” Paper presented at Twenty-third Americas Conference on Information Systems of 2017, Boston, August 10-12.

Peng, D. X., and Lai, F. 2012. “Using Partial Least Squares in Operations Management Research: A Practical Guideline and Summary of Past Research.” *Journal of Operations Management* 30 (6): 467–480.

Raden, N. 2005. “Shedding light on shadow IT: Is Excel running your business.” DSSResources.com

Rentrop, C., and Zimmermann, S. 2012. “Shadow IT. Management and Control of Unofficial IT.” Proceedings of the Sixth International Conference on Digital Society (ICDS): 98-102.

Shin, D.H. and Choo, H., 2011. “Modeling the acceptance of socially interactive robotics: Social presence in human–robot interaction.” *Interaction Studies*, 12(3), pp.430-460.

Shin, D.H., 2013. “Defining sociability and social presence in Social TV.” *Computers in human behavior*, 29(3), pp.939-947.

Shin, D., 2018. “Empathy and embodied experience in virtual environment: To what extent can virtual reality stimulate empathy and embodied experience?” *Computers in Human Behavior*, 78, pp.64-73.

Shin, D. 2019. How do users experience the interaction with an immersive screen? *Computers in Human Behavior*, 98. 302-310. doi.org/10.1016/j.chb.2018.11.010.

Short, J., Williams, E., and Christie, B. 1976. The Social Psychology of Telecommunications. London: John Wiley & Sons.

Shujahat, M., Sousa, M. J., Hussain, S., Nawaz, F., Wang, M., and Umer, M. 2017. “Translating the Impact of Knowledge Management Processes into Knowledge-based Innovation: The Neglected and Mediating Role of Knowledge-worker Productivity.” Journal of Business Research, 94, pp.442-450.

Shumarova, E., and Swatman, P. A. 2008. “Informal Ecollaboration Channels: Shedding Light on “Shadow Cit”.” Paper presented at BLED Proceedings of 2008, Bled, June 29 – July 9.

Silic, M., and Back, A. 2014. “Shadow IT–A View from Behind the Curtain.” *Computers & Security* 45: 274-283.

Silic, M., Barlow, J. B., and Back, A. 2017. “A New Perspective on Neutralization and Deterrence: Predicting Shadow IT Usage.” *Information & Management*, 54 (8): 1023-1037.

Silic, M., 2019. Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the Shadow IT context. *Computers & Security*, 80, pp.108-119.

Singh, H. 2015. “Emergence and Consequences of Drift in Organizational Information Systems.” Paper presented at Proceedings of the Pacific Asia Conference on Information Systems of 2015, Singapore, July 6-9.

Stone, R.W., Good, D.J. and Baker-Eveleth, L., 2007. “The impact of information technology on individual and firm marketing performance”. *Behaviour & Information Technology*, 26(6), pp.465-482.

Suer, M. F. 2017. “Is Shadow IT Something CIOs Should Worry About?” CIO.com, June 6. https://www.cio.com/article/3199236/application-development/is-shadow-it-something-cios-should-worry-about.html

Trang, S., Zander, S., and Kolbe, L. 2014. “E-Business Adoption at the Firm Level: Comparing the Predictive Power of Competing IS Adoption Models.” Paper presented at Proceedings of Thirty-Fifth International Conference on Information Systems, 2014, Auckland, December 14-17.

Turkle, S. 2011. Alone Together: Why we Expect More from Technology and Less from Each Other. New York: Basic Books.

Turner, A. 2015. “Generation Z: Technology and Social Interest.” *The Journal of Individual Psychology* 71 (2): 103-113.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D., 2003. “User acceptance of information technology: Toward a unified view”. *MIS quarterly*, 27 (3), pp.425-478.

Walterbusch, M., Fietz, A. and Teuteberg, F. 2017. “Missing Cloud Security Awareness: Investigating Risk Exposure in Shadow IT.” *Journal of Enterprise Information Management* 30 (4): 644-665.

Walters, R. 2013. “Bringing IT out of the Shadows.” *Network Security* 2013 (4): 5-11.

Wang, Y., Meister, D.B. and Gray, P.H., 2013. “Social influence and knowledge management systems use: Evidence from panel data.” *MIS Quarterly*, 37 (1), pp.299-313.

Zhao, X., Lynch Jr, J. G., and Chen, Q. 2010. “Reconsidering Baron and Kenny: Myths and Truths about Mediation Analysis.” *Journal of Consumer Research* 37 (2): 197-206.

Yoo, Y. and Alavi, M., 2001. “Media and group cohesion: Relative influences on social presence, task participation, and group consensus.” *MIS quarterly*, 25 (3), pp. 371-390.

Zimmermann, S., Rentrop, C., and Felden, C. 2014. “Managing Shadow IT Instances– A Method to Control Autonomous IT Solutions in the Business Departments.” Paper presented at the Proceedings of the Twentieth Americas Conference on Information Systems of 2014, Savannah, August 7-10.

Zimmermann, S., Rentrop, C., and Felden, C. 2017. “A Multiple Case Study on the Nature and Management of Shadow Information Technology.” Journal of Information Systems 31 (1): 79-101.

6 ARTICLE 3: WE ARE SOCIAL: A SOCIAL INFLUENCE PERSPECTIVE TO INVESTIGATE SHADOW IT USAGE.

Abstract[3]

Shadow IT can be used by one individual or a group of employees, which suggest two levels of use: an individual and collective use of shadow IT. The study here takes a social influence perspective to investigate the mechanisms that underlie the dissemination process of shadow IT among individuals. We performed a survey among employees of four companies. The results show that the social influence varies depending on the group of reference in question (peer, superior, mass influence). We found that employees are strongly influenced by their peers and by a mass of people to use a shadow IT, such as co-workers, professional workmates, and employees from other departments, suggesting a broader range of social influence that can affect the use of shadow IT. We aid to clarify some reasons why employee uses shadow IT and how the dissemination process occurs among users. Also, as social influence is based on communication and social interactions, organizations may pay attention in creating initiatives and taking actions to engaged users in the information security policies, which is one of the primary concern related to shadow IT.

Keywords: Shadow IT, Social Influence, Workplace Deviant Behaviour, IT Management.

6.1 INTRODUCTION

"No man is an island entire of itself; every man is a piece of the continent, a part of the main," said the 17th-century British poet John Donne. Over the years, science has been proving that he was right, indeed. Individuals exist within society; they are influenced by society and influence the society (Stets and Burke, 2000). The fact is

[3] This paper was published in the Proceedings of the Twenty-Sixth European Conference on Information Systems (ECIS2018), Portsmouth, UK.

that human's brain is designed to be influenced by others because they are built to ensure that we will hold the beliefs and values of people around us (Lieberman, 2013). In a few words, we are social, and that can be influencing our behaviour regarding the technological choices as well.

The pervasiveness of technology is causing relevant changes to individuals, organizations, and society. In addition to the greater availability of technology, it is also notable the increasing knowledge and ability of users regarding the use of technology (e.g., Eckhardt, Laumer and Nguyen, 2010; Carter and Gruver, 2015). These two factors together are bringing several challenges to manage technology within organizations. People are finding ways to use consumer technologies from their personal lives in the workplace (e.g., Harris, Ives and Junglas, 2012). As a consequence, the traditional IT adoption logics have been completely reversed in the last years because, instead of IT departments deciding which solution their employees should use, employees autonomously adopt and use solution that meets their needs at work (Stryker and Burke, 2000; Haag and Eckhardt, 2017).

Within the context exposed above, emerges the use of unauthorized technology in the workplace called shadow IT usage. The literature posits that this phenomenon emerges at the individual level (e.g., Györy et al., 2012; Haag, Eckhardt, and Bozoyan, 2015). Shadow IT is a form of decentralized computing implemented by individuals, workgroups or whole business units (e.g., Zimmermann and Rentrop, 2014; Fürstenau, Rothe, and Sandner, 2017), which suggest the adoption and use of shadow IT may disseminate among employees within a company.

Although people frequently think of themselves as "independent-minded and immune of some kinds of social influence", others are daily influencing us in many ways (Lieberman, 2013). Considering the individual as a member of a group that is influenced and influences others, we ask:

RQ: What factors drive the use of shadow IT among individuals?

We take a social influence perspective to investigate the mechanisms that underlie the dissemination process of shadow IT among employees, uncovering some reasons why shadow IT usage disseminates from one individual to another, spreading to a whole group of people. In that sense, we use the social influence perspective to capture the cumulative individual effect of these influences on individual behaviour (e.g., Karahanna, Straub and Chervany, 1999). The findings suggest that employees are strongly influenced by their peers and by a mass of people, in general, to use a shadow IT, such as co-workers, professional work-mates, and employees from other departments, suggesting a broader range of social influence that can affect the individual.

Understanding the effect of social influence on IS usage it is not a recent concern. Since more than a quarter century, social influence is considered as a focal determinant for individual's behavioural intention and, consequently, profoundly affects user behaviour (e.g., Li, 2013; Wang, Meister and Gray, 2013; Hsu and Lu, 2004). Previous studies have identified that the social structure and user's environment are also determinants for the proliferation of IT use and its benefits from individual to organizational level (e.g., DeLone and McLean, 2003; Eckhardt, Laumer and Nguyen, 2010). In addition, social influence has greater importance for the use of work systems since the use of these systems has more tangible and extrinsic value (Eckhardt, Laumer and Nguyen, 2010). Thus, we use the social influence perspective to investigate the use and dissemination of shadow IT among employees in the workplace.

Although shadow IT is not a new phenomenon, it demands further studies from new perspectives in order to reveal, explain, and control its challenges, as well as to exploit its opportunities (Haag and Eckhardt, 2017; Silic, Barlow and Back, 2017). Furthermore, investigating individual behaviour related to the use of technology is central to manage shadow IT since it emerges from the employee's level (Győry et al., 2012; Haag, Eckhardt, and Bozoyan, 2015; Fürstenau, Rothe, and Sandner, 2017). Regarding the theoretical lens, managers and research need to understand how social influence occurs and affects the potential IS user to prevent malicious IS use (Eckhardt, Laumer and Nguyen, 2010).

The paper advances as follow. The following section provides the theoretical background of shadow IT and social influence. Next, we developed the hypotheses of our research mode. The following methodology section describes the applied research method. The result section presents the statistical analysis. Next section discusses the results and implications for theory and practice, as well as the limitations and further research.

6.2 THEORETICAL BACKGROUND

6.2.1 Shadow IT

Shadow IT can be any hardware, software, or services built, introduced, and/or used to work without explicit approval or even knowledge of the organization (e.g., Silic and Back, 2014; Haag and Eckhardt, 2017). The term shadow IT refers, then, to the unauthorized information technology and its usage has been referred as shadow IT usage. This paper follows the definition of shadow IT usage provided by Haag and Eckhardt (2014), which states that shadow IT usage is “the voluntary usage of any IT resource violating injunctive IT norms at the workplace as reaction to perceived situational constraints with the intent to enhance the work performance, but not to harm the organization”.

Shadow IT is a form of decentralized computing implemented by individuals, workgroups or whole business units (e.g., Zimmermann and Rentrop, 2014; Fürstenau, Rothe, and Sandner, 2017). Depending on their business needs, different units and individuals implement a wide range of solutions, using a variety of unauthorized technologies (e.g., Huber et al., 2017). Thus, employees can use shadow IT in a variety of ways: shadow IT can be a hardware, software, or any other solution, such as a ready-made spreadsheet, cloud services, or a self-developed appli-cation (e.g., Silic and Back, 2014; Zimmermann, Rentrop and Felden, 2017).

We reviewed the shadow IT literature in an effort to clarify how individuals use shadow IT at work. Four types of shadow IT emerged. The first type, called unauthorized cloud services, rep-resents the software accessed through the internet (e.g., Fürstenau and Rothe, 2014; Haag, 2015; Walterbusch, Fietz and Teuteberg, 2017) and, thereby, to be used, it does not need to be installed in any device. The second type is called self-developed solutions and are solutions developed and used by employees on the company’s computers to perform their work tasks (e.g. Zimmermann, Rentrop and Felden, 2014; Zimmermann, Rentrop and Felden, 2017), which may vary from a simple excel spreadsheet to a more complex application developed by employees to be used by a whole business unit. The third type is called self-installed software applications and represents those applications installed and used by employees on the company’s devices (e.g., computers, smartphones or tablets provided by the company) (e.g., Jones et al. 2004; Silic and Back, 2014). This type of shadow IT usage involves solutions that are often freely available on the web and need to be downloaded and installed prior to use, instead of accessed via internet. Finally and fourth, self-acquired devices represent the hardware layer of shadow IT since it represents the devices purchased and owned by the employees instead of the company's devices, including the use of applications in the employee's personal devices at the workplace (e.g. Rentrop and Zimmermann, 2012; Zimmermann, Rentrop and Felden, 2017). Table 11 summarizes the findings from the literature.

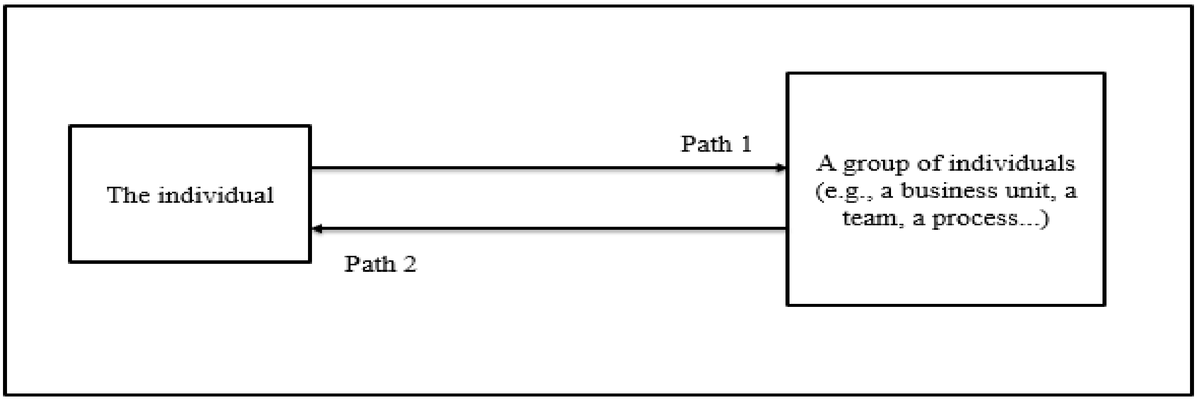
Table 11 – Types of Shadow IT usage

Shadow IT Usage Types	Description	Authors
Unapproved cloud services	Use of Internet-based Software and Software as a Service (SaaS) that are not approved or unknown by IT department. These systems are also called Mobile Shadow IT once it can be accessed outside the workplace (e.g., WhatsApp, Facebook, Skype for Web, Dropbox, Google Apps, etc.).	Rentrop and Zimmermann (2012); Gyory et al. (2012); Fürstenau and Rothe (2014); Silic and Back (2014); Haag and Eckhardt (2014); Zimmermann et al. (2014); Huber et al. (2016); Walterbusch et al. (2017).
Self-made solutions	Use of solutions developed by employees on the company's computers to perform their work tasks. For example, an excel spreadsheet or an application developed by employees.	Jones et al. (2004); Rentrop and Zimmermann (2012); Fürstenau and Rothe (2014); Zimmermann et al. (2014); Huber et al. (2016).
Self-installed applications	Use of software installed by employees to perform their work tasks, on the company's computers. For example, downloading and installing software available free of charge on the internet.	Jones et al. (2004); Rentrop and Zimmermann (2012); Fürstenau and Rothe (2014); Zimmermann et al. (2014); Silic and Back (2014).
Self-acquired devices	Use of devices owned by employees. These devices are purchased directly from retail rather than being ordered through the official catalogue of the IT department. It includes the use of applications in the employee's personal devices at the workplace (smartphones, tablets, notebooks, etc.).	Rentrop and Zimmermann (2012); Silic and Back, (2014); Zimmermann et al. (2014); Huber et al. (2016).

Source: Prepared by the author

Previous studies suggest that shadow IT emerges at the employee's level (e.g., Győry et al., 2012; Fürstenau, Rothe, and Sandner, 2017) and can be used by one individual or a group of individuals, that is, an individual and/or collective use of shadow IT. Figure 4 shows the dissemination paths of shadow IT usage among employees.

Figure 4 – Dissemination Paths of Shadow IT Usage


The individual
Path 1
Path 2
A group of individuals (e.g., a business unit, a team, a process...)

Source: Prepared by the author

Path 1 represents the situations when an individual uses a shadow IT to perform his/her work tasks and, after some time, others employees adopt and use the same shadow IT. In turn, Path 2 represents the situation when a group of individual (e.g., team or department) adopts and use the shadow IT as their work solution and, as new individuals join this group, they consequently adopt and use the same shadow IT as others in the group. Therefore, there are social mechanisms that underlie the adoption and dissemination process of use shadow IT among employees.

6.2.1.1 What is not Shadow IT? Related concepts

To a better definition of shadow IT, it is crucial to define what is and what is not shadow IT. Haag and Eckhardt (2017) highlight that shadow IT distinguishes from closely related concepts such as workaround, bring-your-own-device (BYOD), and IT consumerization. Although those concepts carry some similarities, there are crucial differences that "characterize and justify shadow IT as a unique and relevant concept worthy of future investigation" (Haag and Eckhardt, 2017).

Workarounds are, in a broader way, conscious adaptations of work activities that are not expected or specified to be changed in this manner (Laumer et al. 2017). They are implemented to address constraints related to target IT, personal IT, and/or the IT policies perceived by employees as challenging for their work (e.g., task performance) (Alter, 2014). Therefore, employees create other means to solve those restrictions and help them to perform their work task.

Haag and Eckhardt, 2017 point out three instances of workarounds: 1) non-IT-based workarounds without using any IT, for example, using paper to collect and process information; adapt the mandatory IT and/or approved personal IT and use it in different and unexpected ways, for example, by using MS Word to convert and re-edit contents of PDF documents; and 3) shadow IT, which is bringing unapproved IT and/or change approved IT in unapproved ways, for example, by creating MS Excel macros without approval to automate repetitive work tasks. Considering the definition of shadow IT presented previously, shadow IT can be a workaround, although it is not necessarily a workaround because it is related to the technology, while workaround can also be related to non-IT-devices. In that sense, workaround is a broader concept that encompasses other instances, including shadow IT and both terms can be classified as deviant work behaviour.

Others concepts frequently linked to shadow IT and workarounds are IT consumerization and BYOD. Although these concepts as related to workarounds and shadow IT, they are not a deviant behaviour itself. BYOD can facilitate or drive shadow IT usage because employees can use their device in an inappropriate way. However, BYOD cannot be considered a deviant behaviour once it is a policy that allows employees to bring and use personal devices at work (e.g., French et al. 2014). Finally, IT consumerization is the adoption of consumer devices and applications by employees (Harris, Ives, and Junglas, 2012). That is a broader concept related to all the prior ones (e.g., Haag and Eckhardt, 2017) because consumer IT can be related to the IT-supported solution, to the personal IT (e.g., BYOD) or to the unapproved consumer IT (e.g., shadow IT or workaround).

6.2.2 Social Influence and IS Usage

Social influence is defined as a change in thoughts, feelings, attitudes or behaviour of an individual that results from the communication and interaction with another person or with a group (Eckhardt, Laumer and Nguyen, 2010; Ogara, Koh and Prybutok, 2014). In a general way, the background of social influence has its roots in the nature of changes that are caused by a particular communication or type of communication among individuals (Kelman, 1958).

Social influence has been considered as a major determinant for individual’s behavioural intention and, consequently, profoundly affects user behaviour (e.g., Venkatesh and Davis, 2000; Hsu and Lu, 2004; Li, 2013; Wang, Meister and Gray, 2013). That is because people are more likely to perform a behaviour when they believe that referents think they should perform the behaviour (e.g., use new technology) and they are encouraged to satisfy the expectations of these referents (Venkatesh et al. 2003; Jiang et al., 2016).

Subjective Norm (SN) is the dominant conceptualization of social influence (Lee, Lee and Lee, 2006; Wang, Meister and Gray, 2013). In IS research, the investigation of social influence is linked mostly to the perception of subjective norm and its effect on the adoption and use of technology by individuals (Eckhardt, Laumer and Nguyen, 2010). In line with previous research (e.g., Venkatesh and Morris, 2000; Venkatesh and Davis, 2000; Venkatesh et al. 2003), we used subjective norms to analyse and measure social influence in our study.

Performing a literature review on social influence, Eckhardt and his colleagues found that the point of adoption (pre-adoption vs. post adoption) and the degree of free decision-making (mandatory vs. voluntary) do not affect the impact of social influence (Eckhardt, Laumer, and Weitzel, 2009; Eckhardt, Laumer and Nguyen, 2010). Therefore, these aspects are not a concern in our study.

Top managers, supervisors, subordinates, colleges, organization's IT department, local computer technology experts, and friends can be possible salient referents for the social influence component regarding individuals' adoption and usage of IT in organizations (e.g., Karahanna, Straub and Chervany, 1999; Wang, Meister and Gray, 2013). Regarding this aspect, Eckhardt, Laumer, and Weitzel (2009) suggest that social influence is more significant with an individualized meas-urement than with the basic collective measurement (e.g., “important others”), because individual measures specify the groups of people that exert the influence (e.g., friends, co-workers, superiors). Taking all these aspects in mind, we contextualize the choices regarding the research model in the next section.

6.3 RESEARCH MODEL AND HYPOTHESES DEVELOPMENT

As discussed in the literature review, changes in behaviour due to interaction with others, especially people considered important or close, can influence individual’s behaviour and choices (e.g., Ogara, Koh and Prybutok, 2014). Social influence is critical to understand user behaviour because they could play an essential role in determining how users make their decisions about adopting and using new technologies (Venkatesh and Morris, 2000).

The usage context here is the use of unauthorized information technology to perform work tasks inside organizations, therefore, shadow IT is the target technology for this study (Hong et al. 2013). Previous studies suggest that shadow IT can be used by one individual or a group of individuals, which means that the use of shadow IT disseminates among employees (e.g., Györy et al., 2012; Fürstenau, Rothe, and Sandner, 2017). Moreover, the current IS literature suggests that IT department is losing the influence on the choice of technology used by employees to perform their work (e.g., Stryker and Burke, 2000; Eckhardt, Laumer and Nguyen, 2010). This influence, then, may be coming from people like co-workers, friends, professionals, or even from the head of the business unit. Within this context, the social influence perspective was used as a theoretical lens to investigate the use of shadow IT among employees. We decided to use the social influence perspective, which is an established construct of IS field, to investigate the use of technology among individuals in the context of shadow IT as a manner to capture the cumu-lative individual effect of these influences on individual behaviour (e.g., Karahanna, Straub and Chervany, 1999). That is, we suggest that social influence may be an antecedent of shadow IT usage among employees.

An individualized measurement was used to specify the groups of people (Eckhardt, Laumer and Nguyen, 2010). We identified three groups that may exert social influence in the shadow IT context within organizations, based on prior research in social influence: peer, superior and mass influence (e.g., Hsu and Lu, 2004; Lee, Lee and Lee, 2006; Wang, Meister and Gray, 2013). Although there are several possible referents (e.g., Karahanna, Straub and Chervany, 1999), we selected the salient ones considering the research context. The influence from subordinates and IT department were not considered because 1) most of IT users that use shadow IT do not have subordinates in the hierarchy and 2) shadow IT is regarding the use of unauthorised technology, then it is a deviant work behaviour and not related to the IT department influence. Thereby, we theorized that, in the shadow IT context, employees may be influenced by immediate referents (peers and superiors) toward the use of shadow IT, and, in a broader sense, they can be influenced by a larger and more distant group of people (mass influence), which can be employees form others departments or company's units and colleagues of the same profession.

We focus first on hypothesizing the social influence effects of an individual's immediate referents in the workplace, that is, peer and superior influence. Peers are defined as people (e.g., colleagues, workmates) who work in the same business unit, team or department and, consequently, they have some work task in common, while superiors are defined as all people (e.g., managers, supervisors) in an individual's business unit, team or department who hold higher-level positions (e.g., Wang, Meister and Gray, 2013).

Peer pressure and superiors' influence are well recognized as determinants in technology usage contexts (e.g., Malhotra and Galleta, 2005; Wang, Meister and Gray, 2013). Influence from peers and superiors can play an essential role in determining user behaviour since individuals focus their perceptions to general and abstract criteria that includes complying with the ideas of peers and superiors (Venkatesh and Morris, 2000). This influence can be stronger if the individual perceives the peer or superior as a computer technology expert (e.g., Karahanna, Straub and Chervany, 1999; Weiß and Leimeister, 2012). For instance, if a workmate suggests that a partic-ular technology may be useful to perform work tasks, the person considers this suggestion and are influenced by it and, consequently, starts to use that technology at work (Venkatesh and Davis, 2000).

Extant research points out that the business units are in a better position now to create new digital streams for themselves and engaging with digital tools more intensely than ever (e.g., Fürstenau and Rothe, 2014). Consequently, it is becoming increasingly difficult for IT managers to govern the growing variety of IT systems within companies. Moreover, business units are gaining their budget to implement IT solution without the traditional process of consulting the IT department, which is causing individual impacts to employee's work consequently. In this con-text, digital companies are being driven by a new generation of business managers and employees who do not need technology to be contextualized by an IT department. For example, the head of a team or department can influence his employees to use a certain technology because he considers this technology as more efficient than the mandatory technology. Thus, the employee's choice regarding the technology to perform the work tasks may be influenced by workmates or by the business unit leader that may indicate a solution outside the official scope of the IT department. Consistent with the above arguments, we hypothesised:

H1: Peers influence is positively related to shadow IT usage.

H2: Superiors influence is positively related to shadow IT usage.

Mass influence refers to the fact that a broader range of people can influence the individual. The network externalities is the underlying theoretical concept, which states that the value of a network increases with the square of its number of users (Hsu and Lu, 2004). The more people adopt a particular technology, the stronger the influence of others, and the higher perceived value of the technology (Sun, 2013). Wang, Meister and Gray (2013) examined the influence of individual's extended professional population within the organization, which they define as employees that perform the same kind of work, but do not work in the same location. In the digital and globalized companies nowadays, technology is the primary way of interactions. For instance, employees, frequently, have to communicate and interact with workmates partners and clients geographically distributed, which represent a broader range of social influences. To give a more concrete example, an employee can find out a solution to perform tasks faster than using the mandatory solution and share the new finding with colleagues from other units and departments. Thus, it is necessary to extend the influence beyond immediate colleagues, providing an additional source of social influence (Wang, Meister and Gray, 2013).

Several factors may explain why individuals tend to converge on the same technology. For instance, mass influence can be related to a concept called IT fashion. An IT fashion is a collective transient belief that information technology is cuttingedge regarding innovation, efficiency and practicality (Wang, 2010). In that sense, the belief that the technology is making it known and "fashion" among users, may influence other employees behaviour toward this technology. Similarly, it can lead to a phenomenon called herd behaviour, when people converge on the same form of technology by imitating each other's choices (e.g., Sun, 2013). Thus, we hypothesized:

H3: Mass influence is positively related to shadow IT usage.

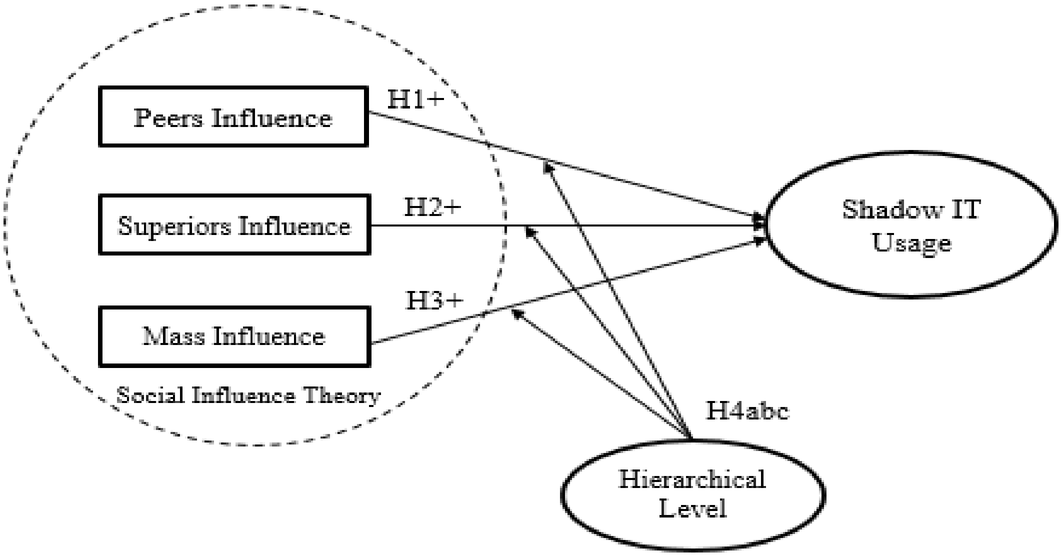
Finally, we theorized that an individual's hierarchical level has a moderating effect on the relationship between social influence constructs and shadow IT usage. Previous studies suggest that the need to use shadow IT is more prominent among the new generation of technology users and top managers of the organizations (Weiß and Leimeister, 2012; Harris, Ives, and Junglas, 2012; Silic and Back, 2014; Zimmermann, Rentrop and Felden, 2014). It is suitable to infer that, on average, there is a relation between age and hierarchical level since young people tend to occupy lower-level positions (e.g., interns and assistants), while higher-level positions tend to be occupied by more seniors people (e.g., managers, supervisors, and presidents).

Compared to junior positions, employees in senior positions are more visible and are more likely to influence others due to their status and expertise. Therefore, high-level senior leaders are less likely to be influenced in general, while low-level junior employees more likely to be influenced by others (Wang, Meister and Gray, 2013). Our last hypothesis says:

H4: Hierarchical level moderates the relationship between a) peers influence; b) superiors influence; c) mass influence, and shadow IT usage in a way that, people who have a higher hierarchical level in the organization are less likely to be influenced by other employees.

The study, thus, set up the research model as appearing in Figure 5.

Figure 5 – Research Model



Source: Prepared by the author

6.4 METHOD

We conducted a field survey to test our model and hypotheses. First, a questionnaire was de-signed based on the existing IS literature to collect data. Two further steps were incorporated to ensure the validity and reliability of the measures. First, two postgraduate students from IS field were consulted to proofread and validate the questionnaire. Second, a pilot study with 34 respondents from a large media company was conducted to test the research model and the questionnaire items.

The sample consisted exclusively of IT users from administrative departments. By administrative departments, we mean employees who work in departments such as marketing, human re-sources, financial, commercial and sales. We do not include IT employees in the sample because their context is significantly different from employees from others business areas. The questionnaire was distributed by e-mail using a link. An initial email was sent in September 2017 to IT managers of five organizations. Four organizations from different sectors engaged in the study (retail, education, financial and communication). We ensured confidentiality to the respondents and companies. A total sample of 148 respondents from four organizations completed the sur-vey. The software GPower 3.1 was used to calculate the minimum sample size, considering the number of predictors (3), statistical power

(80%), probability of error (0,05), and the effect size f2 (0,15), according to Hair et al. (2014). The result showed that the sample size provides actual power to detect significant effects.

Regarding the measurement item, all items of the variables were measured on a 7-point Likert scale, on which ‘1=strongly disagree’ and ‘7 = strongly agree’. The study measured each dimension of social influence by using existing research and scales. More specifically, the constructs of peer influence (four items) and superiors influence (three items) was operationalized from previous studies such as Venkatesh et al. (2003), Wang, Meister and Gray (2013), and Ogara, Kuch and Prybutok (2014) (i.e., “My workmates use shadow IT to perform their work tasks.” and “The boss of my team/department told us about the usefulness of shadow IT.”). Mass influence (three items) was based on the studies of Hsu and Lu (2004) and Wang, Meister and Gray (2013) (i.e., “Colleagues from other business units use shadow IT to perform their work.” and “Many people in my company use shadow IT to accomplish their work tasks.”).

The dependent variable Shadow IT Usage was based on previous studies about shadow IT such as Haag and Eckhardt (2014), Silic and Back (2014) and Silic et al. (2017). The items of shadow IT usage were designed based on the four types of shadow IT from the literature (see Table 1) and it was assessed based on subjective measures, which is in line with previous studies on shadow IT at individual level (e.g., Haag and Eckhardt 2014; Haag, Eckhardt, and Bozoyan 2015; Silic et al. 2017). Finally, the moderator variable hierarchical level was measured on a 2-point scale (yes, if the respondent occupies a management position, or no if he/she does not).

6.5 ANALYSIS AND RESULTS

The dataset was analysed using Partial Least Squares SEM (PLS-SEM) structural equation modelling (Hair et al., 2014). PLS- SEM is an appropriate method if the research objective is prediction and theory development and has become a good alternative to Covariance-based SEM (CB-SEM) for estimating theoretically justified cause-effect relationship models especially when the sample size is small (Hair, Ringle, and Sarstedt, 2011). The software SmartPLS 3.0 was used for model calculation and testing. Following the PLS-SEM guidelines (e.g., Hair et al., 2014), the study performed a two-stage approach to evaluation: (1) assessment of measurement model and (2) estimation of structural model and hypothesis tests.

6.5.1 Assessment of the measurement model

All constructs drew on a reflective measurement model in this study (Hair et al., 2014). First, the reliability and validity of constructs were assessed with several statistical tests. The analysis of internal consistency and the scale reliability were checked with Composite Reliability (CR), which is a more appropriate criterion to measure internal consistency reliability according to Hair et al. (2014). Values of CR between 0.60 to 0.70 are “acceptable” in exploratory research, whereas values higher than 0.70 are “satisfactory to good” (Hair et al., 2014). All CR values are above the minimum threshold of 0.6, demonstrating that all the constructs have high levels of internal consistency reliability.

The outer loadings of the indicators and the average variance extracted (AVE) are considered to establish convergent validity. The outer loadings values ranged from 0.604 to 0.964, being two values below the threshold of 0.70 (Hair et al., 2014). Following Hair et al. (2014) guidelines, we decided to retain these reflective indicators because their deletion does not lead to a considerable increase in the AVE and the composite reliability values. Next, convergent validity of the variables was calculated using Average Variance Extracted (AVE), that should be higher than 0.50 (Hair et al., 2011). With a minimum of 0.50, all AVE values are higher than the acceptable threshold of 0.5, demonstrating convergent validity for all constructs. Table 12 report the results of the Composite Reliability, AVE and Correlation matrix of constructs.

Table 12 – Composite Reliability (CR), AVE and Correlation Matrix of Constructs.

Constructs	CR	AVE	Mass Influence	Peer Influence	Shadow IT Usage	Superior Influence
Mass Influence	0.969	0.911	**0.955**			
Peer Influence	0.941	0.801	0.889	**0.895**		
Shadow IT usage	0.814	0.526	0.733	0.729	**0.725**	
Superior Influence	0.957	0.881	0.655	0.719	0.586	**0.939**

Source: Prepared by the author

Discriminant validity determines the extent to which a construct is empirically distinct from other constructs in the path model. Following Fornell and Larcker criterion, the square root of AVE in each latent variable must be higher than the correlation values with all other latent variables (Hair et al., 2014). The correlation matrix in Table 12 shows that discriminant validity was, thus, established for all constructs in this study.

6.5.2 Estimation of the structural model

After establishing reliability and validity of the construct measures, the study assessed the structural model, which involves examining the model's predictive capabilities and the relationships between the constructs (Hair et al., 2014). The results are based on the application of the bootstrapping procedure provided by SmartPLS. We follow Hair, Ringle and Sarstedt (2011) guidelines for a minimum number of 5,000 bootstrap samples.

Table 13 shows the hypothesis testing for relationships among constructs. The path coefficients represent the hypothesized relationships among the constructs (Hair et al., 2014). As can be seen, two out of three paths are significant on the $p < 0.05$-level (sig. level =5%) and $p < 0.01$-level (sig. level =1%). Mass influence had the strongest effect on shadow IT usage ($\beta = 0.394$, $p < 0.01$), followed by peer influence ($\beta = 0.296$, $p < 0.05$). Therefore, H1 and H3 were supported. The relationship between superior influence and shadow IT usage was not statistically significant ($\beta = 0.115$, $p > 0.1$), then, H2 was not supported.

Table 13 – Hypothesis Testing for Relationships among Constructs

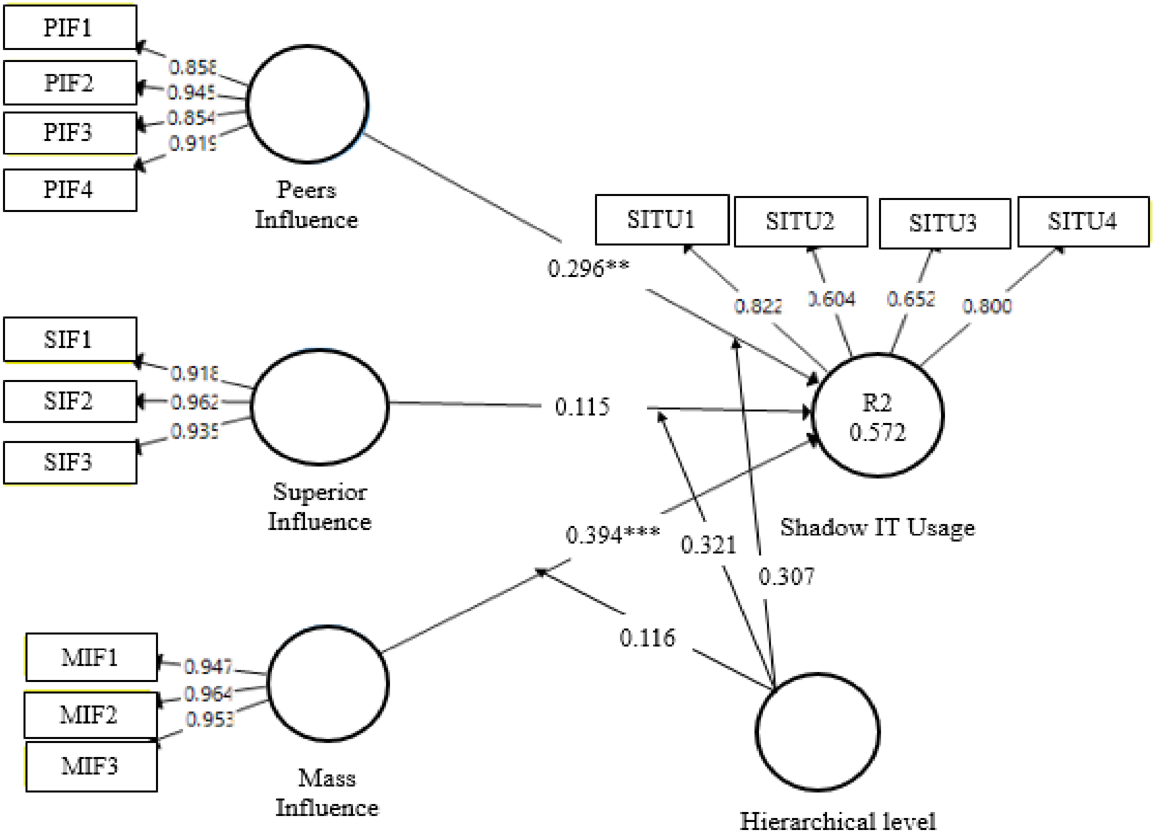
Hypothesis	**Path**	**Path coefficient**	**Standard error**	**t-Statistic (a)**	**P Value**	**Decision**
H1	Peer → SITU	0.296	0.140	2.110**	0.035	Supported
H2	Superior → SITU	0.115	0.094	1.23	0.221	Not Supported
H3	Mass → SITU	0.394	0.126	3.124***	0.002	Supported

(a) t-values for two-tailed test: ** 1.96 (sig. level =5%); *** t-value 2.57 (sig. level =1%) (Hair et al., 2011). Source: Prepared by the author

The R^2 value of each endogenous construct is a measure of the variance explained in each endogenous construct and the model's predictive accuracy (Hair et al., 2014). To social and behavioural sciences, Cohen (1988) suggests assessing the R^2 values for endogenous latent variables as follows: 26% as a substantial effect, 13% as moderate, and 2% as weak. The R^2 value of the endogenous variable shadow IT usage is 0.572, suggesting that the antecedents (social influence groups) explained 57.2% of the variance in the dependent variable shadow IT usage. Thus, R^2 value is considerably high.

Stone–Geisser's Q^2 measure was calculated to assess the model predictive relevance. Q^2 values must be larger than zero, indicating that the exogenous constructs have predictive relevance for the endogenous construct under consideration (Hair, Ringle and Sarstedt, 2011). Running the blindfolding procedure with an omission distance of seven yielded, the cross-validated redundancy values for the endogenous variable shadow IT usage: 0.283 were above zero, supporting the model's predictive relevance. Finally, the study assessed the standardized root mean square residual (SRMR) as an appropriate measure of model fit. Assuming a cut-off value of 0.08 as the more adequate for PLS path models (Henseler, Hubona and Ray, 2016), the SRMR value resulted was 0.06. Thus, the model shows an acceptable fit. Figure 6 shows the research model with the results from the bootstrapping procedure (path coefficients, the significance of the paths, and the amount of variance explained).

Figure 6 – Structural Model with Results of PLS Analysis



*** p<0.01 and ** p<0.05. Source: Prepared by the author

Related to the moderator analysis, we investigate if the categorical variable hierarchical level has a moderator effect, that is if hierarchical level changes the strength or the direction of the relationship between social influence groups and shadow IT usage. When a moderator effect is categorical, the variable serves as a grouping variable that divides the data into subsamples, being suitable to perform a multi-group analysis in this case (Sarstedt, Henseler and Ringle, 2011; Hair et al., 2014). The results here suggest no significant difference between employees who occupy a high-level senior position and those that occupy a low-level junior position.

6.6 DISCUSSION

The study takes a social influence perspective to investigate the mechanisms that underlie the dissemination process of shadow IT usage among employees in the workplace. In summary, the findings show differences in social influence on shadow IT usage behaviour depending on the group of reference in question (peer, superior, mass influence). The results suggest that employees are strongly influenced by their peers and by a mass of people, in general, to use shadow IT. The influences toward the use of shadow IT are exerted from co-workers, professional work-mates and employees from other departments, suggesting a broader range of social influence that can affect the individual. These results also reinforce the blurred barriers between personal, professional, and social lives in contemporary society. Below, we discuss the findings from this research, implications for theory and practice, as well as the study's limitations and suggestions for further research.

6.6.1 Findings and Implications

6.6.1.1 Social influence drives to the use of shadow IT among individuals

Previous studies about shadow IT posit that it can be used by one individual or a group of individuals, suggesting an individual and/or collective use of shadow IT. We took that as a motivation to investigate the use of shadow IT through a social influence perspective to find out what drives the use of shadow IT among individuals. As Kelman (1958) suggests, we have interests in the nature of changes related to use patterns within organizations that are being caused by a particular communication or type of communication among users. The results indicate that the effects of social influence on shadow IT usage differ significantly across groups in an organizational context. Our findings show that peer influence and mass influence effect employees toward the use of shadow IT.

The results indicate that shadow IT users are influenced by observing and interacting with others, adjusting their behaviour according to those social cues. Mass influence shows to have the strongest relationship with shadow IT usage, following by peer influence. Although previous studies suggest that some degree of proximity may be necessary for social influence to occur (e.g., Wang, Meister and Gray, 2013), the findings here suggest that users are not only influenced by those that are closer to them. The study shows that users are influenced by the fact that many people use shadow IT in their companies, including from other teams and departments.

It is essential to take into account the current context of several large organizations. A geographically distributed environment is a reality of digital and cross-country companies, which demands high-level communication and interaction mediated by technology. Employees frequently interact with co-works from other units, external partner and clients. Then, it is suitable to infer that users are exposed nowadays to a broader range of social influences that they were some years ago.

An increasing number of interactions in individual’s professional life, which is not limited to geographical space, is not the only cause for a broader range of social influence. People are experiencing consumer technology in their personal lives and finding ways to use them in the workplace (Harris, Ives and Junglas, 2012; Carter and Gruver, 2015). Therefore, the social cues and personal experience from individuals personal lives are also increasing the number of sources of social influence that may influence user behaviour in the workplace. These results also reinforce the blurred barriers among professional, personal and social lives of individuals (e.g., Carter and Gruver, 2015).

Consistent with Wang, Meister and Gray (2013) findings, our results suggest that superior influence did not appear to be a source of social influence on individual’s shadow IT usage. The superior’s expectancy is that the employee efficiently performs his/her work tasks and maintain a satisfactory individual performance. In the communications and social interactions between the superior and users, the sublunary message understood by the user may be: “keep high performance whatever the technology you use”. From this perspective, employees may not be worried about punishments of not using the mandatory system (e.g., Kelman 1958; Venkatesh and Da-vis, 2000), but their concern can be related to the reward and punishments of achieving or not the performance expectancy. In that sense, superiors can influence users toward shadow IT us-age, however, in an indirect way.

Regarding the moderator variable, the results here suggest no significant difference between employees who occupy a high-level senior position and those that occupy a low-level junior position. As discussed in the literature review, age may have a relationship with hierarchical level since young people tend to occupy lower-level positions and vice-versa. Thus, testing a moderator effect of age on the relationship between social influence and shadow IT usage could be a way to investigate possible differences.

6.6.1.2 Theoretical Implications

The study here provides theoretical implications to the emerging body of knowledge regarding shadow IT usage. Shadow IT is not a recent phenomenon. However, it is still under-studied in the IS literature. This study contributes in that sense expanding theoretical knowledge on shadow IT usage at the individual level by performing an empirical investigation on the antecedents of shadow IT usage from a social influence perspective, which is a widely used construct of IS field. The paper also provides conceptual contribution by defining what is and what is not shadow IT, discussing the similarities and differences from related concepts.

As discussed in the paper, shadow IT may be used by one individual or a group of individuals, emerging an individual and collective level of use of shadow IT. However, this multi-level perspective needs further investigation, including a group-level approach in addition to the individual level to understand how workgroups collectively support shadow IT usage and what are the negative and positive consequences for the group (Haag and Eckhardt, 2017). Taking this gap as motivation, this research contributes to understanding how individual shadow IT usage spreads across the employees within organization. Based on an individual-based social influence analysis, we enlighten some reasons why shadow IT usage disseminates among employees in the workplace, driving to the use of shadow IT in work groups, teams, and in others departments inside organizations.

The study here also provides implications for adoption and post-adoption research. Paying attention to the definition, shadow IT is defined as any resource adopted and used without the approval of the IT department (e.g., Haag and Eckhardt, 2015). Thereby, employees do not only adopt shadow IT but also use it frequently to perform work tasks. In addition, the diffusion level of shadow IT usage is also relevant to understand the phenomenon since it spreads from one individual to a whole group of employees. The post-adoption level, thus, becomes essential to study the phenomenon. In that sense, this study contributes to adoption and post-adoption research investigating the employee’s reason to adopt and use shadow IT, as well as how occurs the diffusion process of shadow IT usage among employees.

To the best of our knowledge, this study was the first to investigate shadow IT from social influence perspective. Social influence is well recognized as a predictor to user behaviour and, for that reason, it has been widely used in the IS field to investigate user behaviour toward adoption and use of technology (e.g., Hsu and Lu, 2004; Li, 2013; Wang, Meister and Gray, 2013). The findings from the study here are consistent with the evidence provided by the social influence literature, validating the results of previous research that social influence has positive effects regarding IT user behaviour, including in the shadow IT context.

6.6.1.3 Practical Implications

The study here also provides practical implications. First, organizations must be aware that shadow IT is a behavioural phenomenon that emerges from the employee's level. Keeping that in mind, managers should better understand employee's behaviour related the use of technology in order to cope with shadow IT. Thus, insights into what drives individuals toward shadow IT usage can aid managers to develop IT strategies and security policies to manage shadow IT.

Second, managers must pay attention to the fact that the main reason for the emergence of shad-ow IT is the complete or partial absence of adequate IT solutions that meet the employees' requirements (Walterbusch, Fietz and Teuteberg, 2017). Therefore, knowing the antecedents of shadow IT usage is also a good opportunity to IT managers understand users expectations and their needs related to technology in order to prevent shadow IT, providing the suitable technology to perform their tasks.

Third, the literature on shadow IT discuss a wide range of consequences, from performance improvements and innovative solution to security risks and compliance. In that sense, balancing the positive and negatives outcomes of shadow IT is another challenge of IT managers. Investigate users behaviour and their motives to use shadow IT is a manner to find out a solution to that complex issue. Taking into account the results here, managers can realize that shadow IT usage is being valuable among employees, and they are sharing the benefits of shadow IT with each other, which help to understand why a whole team or unit uses shadow IT. Thus, better than avoid the use of shadow IT, organizations could find ways to mitigate the risks while recognizing the opportunities for improvements provided by it.

Forth and last, it is also crucial for organizations to understand how social influence occurs and affects the behaviour of IT user related to shadow IT (Eckhardt, Laumer and Weitzel, 2009). Frequently, the problems regarding deviant work behaviour like shadow IT are caused by a deficient communication of IT policies among employees, who are not aware of the recommended information security practices. As social influence relies on communication and social interactions, organizations must pay attention in creating initiatives and taking actions to engaged and active users in the information security policies, which is one of the primary concern related to shadow IT usage.

6.6.2 Limitations and Future Research

This paper is part of a broader project that aims to investigate shadow IT usage at the employee’s level. As Haag and Eckhardt (2017) suggest, it would be valuable to include group-level investigations of shadow IT usage and its consequences for the group through a multi-level perspective, e.g., individual and collective usage. Thereby, future studies can include group-level investigations to understand shadow IT usage at the collective level of analysis.

Taking a social constructivist perspective, we aim to investigate why employees use shadow IT, as well as what drives the dissemination of shadow IT usage among individuals inside organizations. As several studies suggest, the focus only on social norms can be somewhat limited, be-cause users’ values and personal norms play a crucial role in affecting individual usage behaviours (e.g., Malhotra and Galleta, 2005; Lee, Lee and Lee, 2006). Thus, it can be considered as a limitation of this study and an opportunity for future research. We suggest addressing social influence with other theoretical lens (e.g., social identity theory) that permits greater understanding of personal aspects (e.g., individual values, beliefs and goals) and, consequently, capture the nuances of the social environment (Stets and Burke, 2000; Stryker and Burke, 2000; Boudreau, Serrano, and Larson, 2014; Carter and Grover, 2015). Moreover, it would also be interesting to discuss the social influence on each of the four types of shadow IT to see the differences among them.

The literature also provides pieces of evidence to a relationship between the use of shadow IT and age. The dependence on technology to interact with people is increasing, especially among digital natives (Turkle, 2011), which is changing the way we socially interact and bringing sever-al consequences related to those changes.

Previous studies suggest the use of consumer technologies are more prominent among younger generations, called tech-savvy, millennial or Y generations (Weiß and Leimeister, 2012; Harris, Ives, and Junglas, 2012; Turner, 2015). Thereby, age can be a potential factor to understand the role of social influence regarding the use of new technologies. In a broader sense, a study regarding generations and the use of shadow IT may add valuable insights into individual behaviour in a post-modernity society.

References

Akers, R. L., and Sellers, C. S. 2004. Criminological Theories: Introduction, Evaluation, and Application (4th ed.), Los Angeles: Roxbury Press.

Alter, S. (2014) 'Theory of workarounds'. Communications of the Association for Information Systems. 34 (55), 1041-1066.

Boudreau, M. C., Serrano, C., and Larson, K. (2014) 'IT-driven identity work: Creating a group identity in a digital environment'. Information and Organization, 24(1), 1-24.

Carter, M., and Grover, V. (2015) 'Me, my self, and I (T): conceptualizing information technol-ogy identity and its implications'. MIS Quarterly, 39(4).

Cohen, J. (1988) Statistical Power Analysis for the Behavioral Sciences. 2nd ed. New York: Psychology Press.

Delone, W. H., and McLean, E. R. (2003) 'The DeLone and McLean model of information sys-tems success: a ten-year update'. Journal of management information systems, 19(4), 9-30.

Eckhardt, A., Laumer, S., & Weitzel, T. (2009) 'Who influences whom? Analyzing workplace referents' social influence on IT adoption and non-adoption'. Journal of Information Tech-nology, 24(1), 11-24.

Eckhardt, A., Laumer, S., and Nguyen, N. T. (2010) Social Influence in Technology Adoption Research–A Scientometric Study over two Decades Behavior. In Proceedings of the Diffusion Interest Group in Information Technology (DIGIT) Workshop, St. Louis, USA.

Fürstenau, D., and Rothe, H. (2014) Shadow IT systems: Discerning the good and the evil. In Proceedings of the Twenty-Second European Conference on Information Systems, Tel Aviv, Israel.

Fürstenau, D., Rothe, H., and Sandner, M. (2017) 'Shadow Systems, Risk, and Shifting Power Relations in Organizations'. Communications of the Association for Information Systems, 41(1), 3.

French, A. M., Guo, C., and Shim, J. P. (2014) ‘Current Status, Issues, and Future of Bring Your Own Device (BYOD)’. Communications of the Association for Information Systems, 35 (10), 191-197.

Györy, A. A. B., Cleven, A., Uebernickel, F., and Brenner, W. (2012) ‘Exploring the shadows: IT governance approaches to user-driven innovation’. In Proceedings of the European Con-ference on Information Systems, Paper 222, Barcelona, Spain.

Haag, S., and Eckhardt, A. (2014) ‘Normalizing the Shadows–The Role of Symbolic Models for Individuals’ Shadow IT Usage’. Proceedings of the Thirty-Fifth International Conference on Information Systems (ICIS), Auckland.

Haag, S. (2015) ‘Appearance of Dark Clouds?-An Empirical Analysis of Users' Shadow Sourc-ing of Cloud Services’. In Wirtschaftsinformatik (pp. 1438-1452).

Haag, S., Eckhardt, A., and Bozoyan, C. (2015) ‘Are Shadow System Users the Better IS Us-ers?–Insights of a Lab Experiment’. In Proceedings of the Thirty-Sixth International Confer-ence on Information Systems (ICIS), Fort Worth.

Haag, S., and Eckhardt, A. (2017) ‘Shadow IT’. Business & Information Systems Engineering, 1-5.

Hair, J. F., Ringle, C. M., and Sarstedt, M. (2011) ‘PLS-SEM: Indeed a silver bullet’. Journal of Marketing Theory and Practice, 19(2), 139-152.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., and Sarstedt, M. (2014) A primer on partial least squares structural equation modeling (PLS-SEM). Sage Publications.

Harris, J., Ives, B., and Junglas, I. (2012) ‘IT Consumerization: When Gadgets Turn Into Enter-prise IT Tools’. MIS Quarterly Executive, 11(3).

Henseler, J., Hubona, G., and Ray, P. A. (2016) ‘Using PLS path modeling in new technology research: updated guidelines’. Industrial management & data systems, 116(1), 2-20.

Hong, W., Chan, F. K., Thong, J. Y., Chasalow, L. C., and Dhillon, G. (2013) ‘A framework and guidelines for context-specific theorizing in information systems research’. Information Sys-tems Research, 25(1), 111-136.

Hsu, C. L., and Lu, H. P. (2004) ‘Why do people play on-line games? An extended TAM with social influences and flow experience’. Information & Management, 41(7), 853-868.

Huber, M.; Zimmermann, S.; Rentrop, C.; and Felden, C. (2017) ‘Integration of Shadow IT Sys-tems with Enterprise Systems - A Literature Review’. In Proceedings of the Twenty-First Pa-cific Asia Conference on Information Systems, Langkawi.

Jiang, C., Zhao, W., Sun, X., Zhang, K., Zheng, R., and Qu, W. (2016) ‘The effects of the self and social identity on the intention to microblog: An extension of the theory of planned behavior’. Computers in Human Behavior, 64, 754-759.

Jones, D., Behrens, S., Jamieson, K., and Tansley, E. (2004) ‘The rise and fall of a shadow sys-tem: Lessons for enterprise system implementation’. In Proceedings of the ACIS (Australa-sian).

Karahanna, E., Straub, D. W., and Chervany, N. L. (1999). ‘Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs’. MIS Quarterly, 23 (2), 183-213.

Kelman, H. C. (1958) ‘Compliance, identification, and internalization three processes of attitude change’. Journal of conflict resolution, 2(1), 51-60.

Laumer, S., Maier, C., and Weitzel, T. (2017) ‘Information quality, user satisfaction, and the manifestation of workarounds: a qualitative and quantitative study of enterprise content man-agement system users’. European Journal of Information Systems, 26 (4), 333-360.

Lee, Y., Lee, J., and Lee, Z. (2006) ‘Social influence on technology acceptance behavior: self-identity theory perspective’. ACM SIGMIS Database, 37(2-3), 60-75.

Li, C. Y. (2013) ‘Persuasive messages on information system acceptance: A theoretical exten-sion of elaboration likelihood model and social influence theory’. Computers in Human Be-havior, 29(1), 264-275.

Lieberman, M. D. (2013) Social: Why our brains are wired to connect. OUP Oxford.

Malhotra, Y., and Galletta, D. (2005) ‘A multidimensional commitment model of volitional sys-tems adoption and usage behavior’. Journal of Management Information Systems, 22(1), 117-151.

Ogara, S. O., Koh, C. E., and Prybutok, V. R. (2014) ‘Investigating factors affecting social pres-ence and user satisfaction with mobile instant messaging’. Computers in Human Behavior, 36, 453-459.

Rentrop, C., and Zimmermann, S. (2012) ‘Shadow IT. Management and Control of Unofficial IT’. In Proceedings of the Sixth International Conference on Digital Society, 98-102.

Sarstedt, M., Henseler, J., and Ringle, C. M. (2011) ‘Multigroup analysis in partial least squares (PLS) path modeling: Alternative methods and empirical results’. Measurement and research methods in international marketing (pp. 195-218).

Silic, M., and Back, A. (2014) ‘Shadow IT–A view from behind the curtain’. Computers & Se-curity, 45, 274-283.

Silic, M., Barlow, J. B., and Back, A. (2017) ‘A new perspective on neutralization and deter-rence: Predicting shadow IT usage’. Information & management. (in press), 1-15.

Stets, J. E., and Burke, P. J. (2000) ‘Identity theory and social identity theory’. Social psycholo-gy quarterly, 224-237.

Stryker, S., and Burke, P. J. (2000) ‘The past, present, and future of an identity theory’. Social psychology quarterly, 284-297.

Sun, H. (2013) ‘A longitudinal study of herd behavior in the adoption and continued use of technology’. MIS Quarterly, 37(4).

Turner, A. (2015) ‘Generation Z: Technology and social interest’. The Journal of Individual Psychology, 71(2), 103-113.

Turkle, S. (2011) Alone together: Why we expect more from technology and less from each oth-er. Basic Books, New York.

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

Venkatesh, V., and Morris, M. G. (2000) ‘Why don't men ever stop to ask for directions? Gen-der, social influence, and their role in technology acceptance and usage behavior’. MIS Quar-terly, 115-139

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003) ‘User Acceptance of Infor-mation Technology: Toward a Unified View’. MIS Quarterly, vol 27, n° 3, pp. 425–478.

Walterbusch, M., Fietz, A., and Teuteberg, F. (2017) ‘Missing cloud security awareness: investi-gating risk exposure in shadow IT’. Journal of Enterprise Information Management, 30(4), 644-665.

Wang, P. (2010) ‘Chasing the hottest IT: effects of information technology fashion on organiza-tions’. MIS Quarterly, 34(1), 63-85.

Wang, Y., Meister, D. B., and Gray, P. H. (2013) ‘Social influence and knowledge management systems use: Evidence from panel data’. Mis Quarterly, 37(1).

Weiß, D. W. I. F., and Leimeister, J. M. (2012) ‘Consumerization: IT Innovations from the Con-sumer Market as a Challenge for Corporate IT’. Business & Information Systems Engineering, 4(6), 363-366.

Zimmermann, S., and Rentrop, C. (2014) ‘On the Emergence of Shadow IT-A Transaction Cost-Based Approach’. Proceedings of the European Conference on Information Systems (ECIS), Tel Aviv, Israel.

Zimmermann, S., Rentrop, C., and Felden, C. (2014) ‘Managing Shadow IT Instances– A Method to Control Autonomous IT Solutions in the Business Departments’. In Proceedings of the Twentieth Americas Conference on Information Systems, Savannah.

Zimmermann, S., Rentrop, C., and Felden, C. (2017) ‘A Multiple Case Study on the Nature and Management of Shadow Information Technology’. Journal of Information Systems, 31 (1), 79-101.

7 ARTICLE 4: TOWARD A THEORY OF COLLECTIVE IS DEVIANCE: A GROUNDED THEORY APPROACH.

Abstract[4]

Deviance-related behaviors like violations of Information Systems (IS) policies are increasingly common in organizations. These situations of non-compliance with IS policies are subject to various mechanisms inside workgroups, suggesting the collective-level as an important supplement to individual-level explanations to understand deviant acts in the workplace. In line with social psychology and criminology literature, this study considers deviance as collective behavior, addressing deviance as a group-based phenomenon and explaining its importance for IS research. Our purpose is to investigate the mechanisms behind the deviant behavior among workgroup members, uncovering reasons for the occurrence of collective deviance in the workplace. We perform a qualitative study with an exploratory perspective among workgroup members that deviate from IS policies from different companies. As a result, we provide a theoretical model based on empirical data that explains the dissemination and the process of normalization of collective IS deviance. We provide further insights into employees' non-compliance behavior with IS policies, specifically explaining reasons why members of a workgroup collectively deviate from IS policies within organizations. Thus, we provide contributions to research in IS policy compliance and violation, attending the need for further group-level security research.

Keywords: Workplace deviance, Collective IS Deviance**,** Shadow IT, IT Management.

[4] A short paper version of this study was published in the Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy (2018), San Francisco, the USA. A previous version of this paper was accepted in the 80th Annual Meeting of the Academy of Management (AOM2020), Vancouver, Canada. A complete version of this study is planned to be submitted to an AIS basket-of-eight journal.

7.1 INTRODUCTION

Consider the following situation that is based on events in real life. The sales department of a medium-sized company implements a Customer Relationship Management (CRM) system to be used by all employees of the department in their daily activities. There was any formal permission and support from the organizational IT department to implement the system, which also deviates from IS security policies. On the one hand, the use of this CRM allows the department to have predictability on revenue, which is important to manage sales efficiently. The CRM system also aids the department in providing good services for clients and external partners. On the other hand, the use of an unauthorized system like the CRM can represent a potential risk to organizational information security, leaving the information vulnerable to loss or leakage of sales and financial data.

Cases of deviance like the described IS security policy violation are increasingly common in contemporary digital companies (Zhang et al. 2015). Technological tools are widely available to individuals who more and more know how to exploit their functionalities (e.g., Carter and Gruver 2015) and, more importantly, are willing to keep high performance at any cost. Deviance has become, thus, a universal phenomenon in organizations, with nearly 95% of all companies reporting various forms of deviance-related behaviors (Zhang et al. 2015). Thereby, deviant behavior and the related information security risks are a significant challenge for organizations considering its costliness in economic and social terms, such as loss of corporate credibility and monetary damage, primarily to industries that have to deal with confidential information such as banks and health care setting (e.g., Brown and Treviño 2006; Bulgurcu et al. 2010).

Many studies in the IS field have described why people comply with IS policies at the individual level (e.g., Bulgurcu et al. 2010; Ifinedo 2014; Moody et al. 2018, Karjalainen et al. 2019), which are designed for protecting organizational IT assets. Moreover, extant literature has emphasized the crucial role of employees' behavior to achieve and maintain information security, suggesting that the success in information security is achieved when organizations invest not only in technology but also in socio-organizational resources (Warkentin and Willison 2009; Bulgurcu et al. 2010; Siponen and Vance 2010). The study of deviance on workgroups can add knowledge to information systems security by understanding non-compliance behavior within workgroups, aiding the development of policies and strategies to cope with IS policy violations, also balancing the costs and benefits of deviant behavior for the business in a digital setting (Warkentin and Willison 2009; Karjalainen et al. 2019).

Investigations on group level, known as collective deviance or co-offending (e.g., McGloin and Stickle 2011; McGloin and Thomas 2016) have gathered more interest and exploration by researchers from social psychology and criminology, which frequently consider deviance (e.g. crime) as a group-based phenomenon. It is suggested that larger collectives can motivate deviant behavior and push someone who may be naturally disinclined toward crime, delinquency, or different sorts of deviance (McGloin and Stickle 2011). Still, researchers claim for further studies to extend clarity about the factors that predict or explain the instigation of group deviance since it is a productive way for intervention and sanctioning (McGloin and Nguyen 2012).

Prior IS research on deviant behavior primarily focused on individual-level studies, which rarely relying on the context of socio-organizational resources such as collaboration in groups (e.g., Crossler et al. 2013; Ifinedo 2014; Yazdanmehr and Wang 2016; Moody et al. 2018). Johnston et al. (2019) argue that the absence of group-level studies blind researchers in understanding how workgroups influence individual and organizational efforts related to information security. Once the environment and social interactions shape organization and its related processes, the basis for developing organizational theory is the link between organizational phenomena and individual behavior and attitudes (Cappelli and Sherer 1991; House et al. 1995). To fill this void, we adopt a meso- or multilevel research, instead of purely micro-individual-level perspective, as a way to capture the complexity of organizational behavior, generating knowledge about the relations among units at different levels of analysis in an organizational context (House et al. 1995; Klein and Kozlowski 2000).

We choose a group process perspective to understand and explain deviance in IS as a complement to the individual-level explanations (e.g., Robinson and O'Leary-Kelly 1998; Warkentin and Willison 2009), mainly considering the different dynamics and functions of individuals in groups. This study aims to fill the voids and break new ground in workplace deviance at the collective level. Our purpose is to investigate the mechanisms behind deviant behavior among workgroup members, uncovering reasons for the occurrence of collective deviance within organizations, and offering a theoretical model that explains the phenomenon.

It is also important to acknowledge that deviance is a multifaceted phenomenon. Some scholars argue that studies on deviant behavior has extensively focused on negative behaviors and overlooked the functional nature of deviance (e.g., Spreitzer and Sonenshein 2004; Galperin 2012). In contrast, research on positive or constructive deviance has gained importance in workplace studies (e.g., Warren 2003, Mainemelis 2010; Jetten and Hornsey 2014; Mertens et al. 2016). Research in this area has suggested that deviance can change group norms for the better, enhance creativity and allow the establishment of innovative practices that can aid to achieve corporate sustainability (Fielding et al. 2006; Lawrence and Robinson 2007; Mainemelis 2010; Galperin 2012; Walls and Hoffman 2012; Jetten and Hornsey 2014; Mertens et al. 2016). In addition, studies have shown that individuals in groups are exposed to more ideas, larger pooling of information, and cognitive stimulation, which drives to the development of creative ideas, aid to complex problem solving and can actually enhance performance (Hill 1982; Paulus and Yang 2000; Van Der Vegt and Bunderson 2005). Thus, studies on collective deviance can also represent a key element to enhance performance and innovation within organizations. In that sense, IS scholars must also consider that different types of deviance should be treated in terms of their differential impacts on workgroups and organizations (cf., Coser 1962) once the examination of both sides of deviance may provide a more coherent understanding of workplace deviance and its multifaceted nature (Galperin 2012).

The general research question we aim to answer is: *Why does collective deviance occur and disseminate in the workplace?*

We answer our research question by explaining the occurrences of those mechanisms that lead to collective IS deviance. We performed a qualitative study with an exploratory perspective following the guidelines by Corbin and Strauss (2015). We investigated cases of collective deviance in 5 workgroups, performing interviews with 21 members, among superiors and peers. The results show that not only the dissemination of the deviance among the group members occurs, but also that the proliferation of the deviant act continues indefinitely overtime in an uninterrupted way despite changes in group size and membership, turning into a group subculture. Ultimately, the deviant act becomes normalized. We develop a process model describing the mechanisms and components that allow the normalization of the deviant behavior within the group.

The paper is organized as follows. The next section presents a brief review of the relevant literature highlighting the theoretical contributions of our work, followed by a description of the research method. We then present the results by developing a theoretical model for collective deviance in IS. At last, we discuss the findings, their implications, as well as the limitations and future research directions.

7.2 LITERATURE REVIEW

Overall, there are four primary fields of knowledge that offer different perspectives to investigate collective deviance: sociology, social psychology, criminology, and management. According to Jetten and Hornsey (2014), sociology focuses on keeping deviance within bounds, perceiving deviants as healthy and natural behavior to a group, while social psychologists mostly examine how groups aim to eradicate deviance, suggesting that a healthy group life can exist only after the deviant has been removed (see Jetten and Hornsey (2014) for a review). In contrast, criminology engages in research on the negative side of deviance, such as crime (e.g., violence, destruction of property or theft) or chronic offenders, which include individuals with pathological issues (e.g., McGloin and Stickle 2011; McGloin and Thomas 2016). Because of the destructive nature of those instances, deviant behaviors in criminology studies implicate severe formal sanctions (e.g., being arrested or detained by police). At last, studies on management try to explain the complexity of investigating the phenomenon and put some effort in distinguishing the term of collective deviance or deviant behavior (Robinson and Bennett 1995) from other concepts such as organizational misbehavior (Vardi and Wiener 1996), or antisocial behavior (Robinson and O'Leary-Kelly 1998). Those studies overlap to the extent that they all address counter normative behavior (Treviño et al. 2006). The instances of deviant acts in organizational studies include offend, curse and make fun of coworkers, sexual harassment, stealing, etc. (e.g., Robinson and Bennett 1995; Treviño et al. 2006)

Whereas research in criminology has understandably more focused on a negative view of deviance (e.g., crimes and antisocial behaviors), literature on sociology and social psychology have open space to address the phenomenon not only from a negative perspective but also as something that can provide positive outcomes. For example, deviance as a way to enhance creativity (e.g., Warren 2003; Mainemelis 2010) or as a natural element to the functionality of groups (e.g., Lawrence and Robinson 2007; Jetten and Hornsey 2014). As this somehow counteracts with those negative counter normative instances of deviant acts described above, research in the IS field needs more thorough investigation to examine deviance also considering deviant behaviors as reactions to perceived situational constraints that may violate IS policies at the workplace motivated by benevolent intentions to benefit an organization, for example, the objective of enhancing work performance (e.g., Silic and Back 2014; Dahling et al. 2012; Karjalainena et al. 2019).

IS literature especially studies on IS policy violation and compliance discusses a wide range of deviant behaviors. Siponen and Vance (2010), for example, rely their analysis on the concept of Akers and Sellers (2004), from criminology literature, to explain deviance as any deviant behavior that violates social norms, whether or not such behavior also violates the law. Some instances of deviance are using another person's password without authorization, sending confidential information unencrypted, using laptops carelessly outside of the company, among others. Crossler et al. (2013), in turn, labeled deviant behavior as those acts that are intentional, such as sabotage, stealing, and industrial or political espionage, and those that are unintentional called misbehavior, which includes selecting a simple password or clicking on phishing links on emails. Complementing research on deviance, there are also many studies in IS investigating why people comply with IS policies that are designed for protecting organizational IT assets from security breaches such as unauthorized disclosure of information, fraud, and other abuses (e.g., Bulgurcu et al. 2010; Ifinedo 2014; Moody et al. 2018; Johnston et al. 2019; Karjalainena et al. 2019). The prevailing perspective of those studies has been the individual level based on theories to investigate individual perceptions, motivations, and behaviors within organizations (Johnston et al. 2019). However, micro-level research has neglected the influence of the organizational contexts in its explanation of individual behavior, which leads to the development of incomplete and misspecified models (Cappelli and Sherer 1991; Klein and Kozlowski 2000).

To date, Johnston et al. (2019) is one of the very few security-related studies at the collective level by suggesting that an employee group serves as the foundation upon which its members’ security incident responses are formed, which they called collective security efficacy. The authors found that employee groups within organizations act uniquely in their collective responses to information security incidents, showing that a group-level analysis can aid to examine security issues within companies. Hereby, some authors claim for further security-related studies at the collective level (e.g., Warkentin and Willison 2009; Karjalainen et al. 2019) since the absence of group-level studies blind researchers in understanding how workgroups influence individual and organizational efforts related to information security (Johnston et al. 2019).

Despite many studies on individual deviant behavior (e.g., D'Arcy, Hovav & Galletta, 2009; Siponen & Vance, 2010), the literature in IS has failed to consider possible contributions and functional aspects that deviance can provide to the context in which it occurs. Some scholars argue that research on deviant behavior, in general, has extensively focused on negative behaviors and overlooked the functional nature of deviance (e.g., Spreitzer and Sonenshein 2004; Galperin 2012). Studies on positive or constructive deviance have shown that deviant behavior may bring positive consequences to individuals, workgroups and organizations, such as improve performance, enhance creativity and innovation, maintain the employees’ needs for autonomy and sense of self-respect, and the achievement of corporate sustainability (e.g., Fielding et al. 2006; Lawrence and Robinson 2007; Mainemelis 2010; Galperin 2012; Walls and Hoffman 2012; Jetten and Hornsey 2014; Mertens et al. 2016).

Considering the different facets of deviance, there is a necessity to develop a comprehensive definition of deviance encompassing condemnable acts that violate IS policies or norms, but also those acts that have a beneficial purpose despite the deviance from organizational norms (e.g., Galperin 2012; Karjalainena et al. 2019). In line with Robinson and Bennett (1995), Dahling et al. (2012), and Schabram et al. (2018), we define collective IS deviance *as coordinated actions of the majority of a group that violate top-down IS policies in the workplace in the interest of effectively responding to perceived demands from tasks, supervisors, or coworkers*.

This research accounts deviant acts that violate norms established by an organization to whom all members of a workgroup belong. The studies of deviance in the workplace focus on behavior that deviates or violates organizational norms, which is not necessarily an unethical behavior once the deviance is not being judged in terms of law or justice that determines the morality of the behavior (cf. Robinson and Bennett 1995). Thereby, our definition excludes minor and major infractions of larger collective rules, such as societal guidelines, justice, or government. In addition, the definition of collective deviance is more accurate by considering it as a workgroup characteristic, such as shared and configural group properties that are originated by the complex interplay of members' actions within a group (e.g., Kozlowski & Klein, 2000; Schabram et al. 2018).

7.3 METHOD

In line with the objective of developing a theoretical model, we performed qualitative research with an exploratory perspective and followed the guidelines proposed by Corbin and Strauss (2015) for data collection and analysis. Applying these guidelines has proven to be extremely useful for developing context-based, process-oriented descriptions and explanations of IS-related phenomena, being accepted as a suitable method to help generate theories in IS research (Urquhart et al. 2010).

7.3.1 Data Collection

The data was collected through interviews and observations among employees from deviant workgroups. We considered semi-structured interviews as the most suitable technique for data collection as they provide a way to capture many nuances of the respective phenomenon. We performed pilot interviews with deviant employees from different workgroups in other organizations to check for the appropriation of the unit of analysis and refined the data collection instrument, accordingly. The data from the pilot interviews was not used in the analysis. We noticed during the pilot interviews that most of the respondents were not aware of the deviant behavior of their workgroups and the issues related because it represented, in their perspective, an ordinary part of their work routines. Therefore, a qualitative data collection technique is necessary to extract the relevant data.

To ensure covering the primary elements of the phenomenon, we build a semi-structured interview guide based on prior literature, selecting some topics of interest to guide the collection. We were careful to maintain flexibility to make adjustments during the data collection process by adding and adjusting questions, which is necessary to theory construction according to Corbin and Strauss (2015). Thereby, the initial round of data collection, starting with the pilot interviews, was exploratory to capture the big picture and the workgroups' perspective concerning the phenomenon. The second round of interviews was performed toward developing a process-oriented model of collective IS deviance based on a normalization perspective, which is presented in the next section. We performed four pilot interviews, followed by ten interviews in the first wave of research, and eleven in the second wave. The interviews lasted, on average, 1 hour and were performed between January and May of 2019. We recorded all interviews digitally with the permission of the interviewees and transcribed them, afterwards.

Our units of analysis are workgroups that deviate from organizational norms. To ensure a more representative view of the phenomenon, we selected interviewees from different positions within the workgroup, as well as from different companies. We interviewed superiors (e.g., department managers and team leaders) and employees with different roles in teams or departments that deviate from organizations' IS policies by using unauthorized technology in the workplace. We regard this as an instance of deviance to analyze deviant behaviors in an organizational environment. Participants and organizations were assured of confidentiality. Table 14 provides an overview of the workgroups investigated, including information about their context and deviance.

Table 14 – Data Sample – Workgroups Investigated

Workgroups	Context	Deviance	Interviewees
Workgroup 1 (WG1)	The Sales Department (SD) in a publishing group. The department is divided into two subgroups, led by a sales executive manager and a market planning manager. In total, there are 22 employees in the department, including two managers and a department director.	The department has implemented an unapproved CRM tool in 2014. The tool was supposed to be used by the whole department. The initiative was led by the managers and the director of the SD. The implementation has been done without permission and support from the IT department. To date, the ITD is unknowing and not involved in the use and management of the tool.	Seven (5 employees (E1-E5), 1 team leader (TL), 1 department manager (DM))

Workgroup 2 (WG2)	A business unit for one of the products in the same publishing group. There are 18 people in the unit. People in the business unit are grouped into three teams: Customer service solution deployment (8 employees), graphic design for production of content (6 employees), and institutional designers in charge of quality control (4 employees).	Although the organization provides Skype for Business, the whole business unit (BU) uses an unapproved instant messaging tool to communicate and collaborate at work. The members of the workgroup adopted the tool when the BU was created. It's been in use for 5 years.	Six (1 senior deployment analyst (SDA), 1 deployment analyst (DA), and 2 graphic designers (GD1 and GD2), 2 institutional designers (ID1 and ID2))
Workgroup 3 (WG3)	Audit team of a multinational professional services firm. The team has 5 employees, including a director, a senior manager and three auditors.	The audit team uses several unapproved productivity tools (e.g., PDF Editing Software) to handle client documents to audit. The professional services firm does not provide technologies to meet all their individual demands. To meet their own demands, the employees search online for helpful tools and share them via USB flash drive among team members.	Three auditors (AU1 – AU3)
Workgroup 4 (WG4)	Team of communication and brand in the Public Relations department of a large communication group. The team has 6 employees, including a manager.	The team uses unapproved cloud services such as Dropbox and Google Drive to share content with internal colleagues in the Public Relations department and external partners from advertisement agencies.	Two (1 assistant (AS), and 1 senior analyst (SAT))
Workgroup 5 (WG5)	Team of store profitability in the operations and sales department of a large retail firm. The team has 2 employees and a manager.	The team uses a variety of unapproved cloud services to communicate and share information with salespeople and regional managers located in the stores owned by the organization.	Two (1 employee (EP), and 1 manager (MG))
			Total: 21 interviewees

Source: Prepared by the author

7.3.2 Data Analysis

We adopted an interpretive approach and inspired our analysis in some elements from the grounded theory methodology (GTM), which is a common practice in several interpretive studies (Walsham 1995; Karjalainen et al. 2019). In addition, an interpretive approach allows accommodating a stronger role for the literature in data analysis, which is appropriate for qualitative studies.

The gathered data was analyzed using content analysis following the framework provided by Corbin and Strauss (2015). This choice is in line with our primary objective of developing a theoretical model (Urquhart et al. 2010). Corbin and Strauss (2015) suggest that researchers should be careful about the use of existing literature before doing exploratory empirical research and while performing analysis. The objective is to ensure that they do not impose ideas from the literature on that coding (Urquhart et al. 2010). In that sense, some degree of knowledge allows familiarity with the relevant literature to enhance theoretical sensitivity, but not too much that can bias interpretations and block the discovery of new concepts (Corbin and Strauss 2015). That also means that literature should not be handled as data per se. Moreover, the method requires the carrying out of data collection, coding and analysis together because separating these steps might hinder the development of theory and harm the specific rigor and the higher level of detail that is demanded (Urquhart et al. 2010).

Accordingly, we sought in the first interviews to uncover why and how collective IS deviance disseminates among employees within workgroups, trying not to be guided by any theoretical perspective at this moment. The concomitant data collection and analysis allowed an iterative examination of the data collected, emerging interesting and unexpected characteristics of the phenomenon, such as the transmission of the deviance among workgroup generation and its perpetuation as a subculture over time. In a second round, we sought then to rely on a theoretical sensitivity (Glaser 1978) to understand deeply the characteristics and dynamics that were emerging from the interviews, to later develop the theoretical model. The strategy for theorizing about the process of collective IS deviance involved interpreting the narratives of the group members to find a temporal sequence among the dynamics that leads to the occurrence of the phenomenon over time. We based the theorizing in studies on collective action in social psychology and criminology research.

The ultimate purpose of our analysis is the emergence of a theoretical model. According to Corbin and Strauss (2015), a theory is a set of well-developed categories (themes, concepts) in terms of properties and dimensions and interrelated through statements of relationship to form a theoretical framework that explains, to some extent, a phenomenon. In the beginning, the analysis was detailed to delineate the lower-level concepts. In a later stage, it became more general to develop concepts and the relationship between them. The step of integrating concepts (here the components) around a core concept (the mechanisms of dissemination), called category, elevates description or conceptual ordering to the level of theory (the proposed theoretical model of collective deviant dissemination), as suggested by Corbin and Strauss (2015). Accordingly, we first identified the open codes, which were later combined in higher-level categories and organized into a preliminary theoretical framework.

The process of iterative data collection and analysis took place until we achieved an adequate level of theoretical saturation, which means that we stopped the data collection once we felt that adding further data would not result in a new or different understanding of the phenomenon. In addition, our interpretive approach is based on a deep understanding of the interviews, which is not necessarily obtained by performing more interviews with similar viewpoints (Karjalainen et al. 2019). Therefore, we finished the data collection process when we realized that the data added was not changing or enhancing the results.

7.4 THEORETICAL SENSITIVITY AND RESULTS

This section presents our findings regarding collective IS deviance within workgroups. First, we discuss the theoretical underpinnings that guide the analysis of the phenomenon. Second, we introduce and explain the process-oriented model of collective IS deviance, providing quotes from the narratives to illustrate the findings based on empirical data.

7.4.1 Theoretical Underpinnings of Collective IS Deviance

The development of our analysis of the process-oriented model of collective IS deviance was influenced by the empirical data by performing data collection, coding, and analysis simultaneously (Urquhart et al. 2010). We started this research with the assumption that deviant behavior disseminates among members of a group, emerging to a group activity called collective deviance. However, since the first round of interviews, the data revealed a much richer and complex picture of the phenomenon. First, the deviance disseminates among the group members since the moment it was initiated by one or some members. Second, deviance not only disseminated within the workgroup but also among different workgroup generations. In our sample, the workgroups suffered many changes in their configuration over the years, including changes in some or many of their members (peers and superiors). Thereby, the data captured by the interviews suggest that the dissemination of the deviance continues to occur regardless of the original configuration of the group and, consequently, is not dependent on how long the individuals are part of the group. Third, the dissemination of the deviance continues indefinitely overtime in an uninterrupted way.

The empirical data suggests, thus, a process-oriented explanation for collective IS deviance. Although the initiation of deviance may be triggered by individual action, its subsequent proliferation and persistence are best explained through incremental and collective processes that lead deviance to become part of a group's norms and culture (Earle et al 2010). In addition, the deviance occurs as a process of steps over an extended period as a result of the summation of multiple decisions made or avoided (Pinto 2014). Therefore, the core aspects of the phenomenon suggested by the interviews reinforced the relevance of a process approach where not only the dissemination of the deviance takes place, but also a normalization process occurs leading to a subsequent perpetuation of the deviant act as a subculture (Zucker 1977; Ashforth and Anand 2003; Earle et al 2010). By normalization process, we refer to the investigation of how deviant behavior becomes normalized, which means embedded in the workgroup, enacted mindlessly and perpetuated over time (Ashforth and Anand 2003). A normalization perspective adds a social dimension to understanding why deviance disseminates and endure in a group setting, including the importance of local meaning and context in explaining the persistence of deviant practices (e.g., Earle et al. 2010; Hung 2008; Pinto 2014).

Theoretical sensitivity is a key concept when following grounded theory guidelines (Glaser 1978; Corbin and Strauss 2015). It refers to the researcher's ability to conceptualize data, form core categories, extract insights, and analyze relationships between emerging categories and their properties (Glaser and Strauss 1967). Accordingly, we adopt a normalization perspective as a sensitizing device (Glaser 1978) to guide further data collection and analysis.

Ashforth and Anand (2003) proposed three pillars of nominalization, which contribute to the collective execution and indefinite perpetuation of a deviant act. Those three pillars are institutionalization, rationalization, and socialization. Institutionalization is the process by which deviance is enacted as a matter of routine, becoming part of the structures and processes. Rationalization refers to the process by which individuals who engage in the deviance use socially constructed narratives/interpretations to justify and valorize deviance, developing ideologies to legitimate the act in their own eyes. In turn, socialization is the process by which newcomers are taught to perform the deviance, which is perceived as permissible and, in many cases, desirable.

The pillars are processes mutually reinforcing and overlapping and all three must occur for deviance to become an ongoing, collective, and normalized behavior (Ashforth and Anand 2003; Hung 2008; Earle et al. 2010). Accordingly, those processes served as a solid ground to develop the process model of this study. Because of the interdependence of the three pillars of normalization, they appear, at some extend, in every stage of the process model of collective IS deviance, mutually interacting and reinforcing as the time passes. This allowed us to develop a rich understanding of the phenomenon by including social dynamics, group meanings, shared properties and how they interact and evolve over time within a group setting (e.g., Klein and Kozlowski 2000; Earle et al. 2010; Hung 2008; Pinto 2014).

Considering the evolvement of the deviance to a group subculture, it becomes important to gather elements in the literature to understand cultural persistence. The process of institutionalization, which is part of the normalization perspective, deserves extra attention. Zucker (1977) argues that institutionalization is not simply present or absent, rather institutionalization is a variable that can vary in terms of degrees of institutionalization, differing from several previous approaches. Thereby, acts may vary in the degree of institutionalization, which influences the process of cultural persistence.

Three important elements must occur for cultural persistence: transmission, maintenance, and resistance to changes, which have the degree directly related to the degree of institutionalization (Zucker 1977). First, transmission from one generation to the next must occur, followed by maintenance of the culture, and finally, cultural persistence depends on the resistance to attempts to change. Once the three pillars of normalization are mutually reinforcing and reciprocally interdependent (Ashforth and Anand 2003), the degrees of institutionalization also influence the socialization and rationalization process. Institutionalization defines social reality that will be transmitted and maintained as fact, which initially depends on direct sanctions to establish and maintain the behavior in those individuals who are not fully "socialized" (Zucker 1977). However, the greater the degree of institutionalization, the lower the necessity of direct social control, or other intervening mechanisms as internalization, for maintenance because of the uniformity of cultural understanding (Zucker 1977).

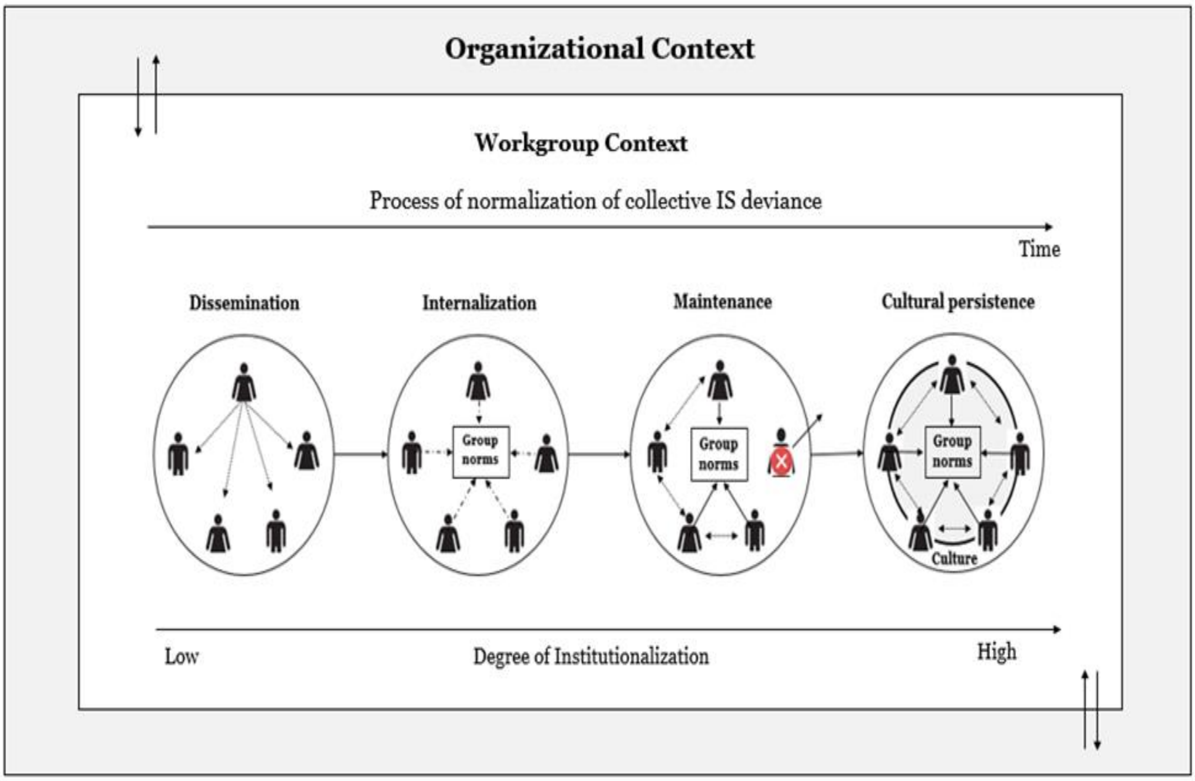
Therefore, we use a normalization perspective to guide the data collection and analysis to explain collective IS deviance. We could not find previous studies that adopt a normalization perspective to understand deviant behavior within workgroups in the IS domain. Consequently, we can provide potential insights by theorizing on collective deviance from a normalization perspective in the IS context.

7.4.2 A High-level Process View for Collective IS Deviance

Based on the introduced cases and taken a normalization perspective, we now present a process model for collective IS deviance that emerged from the interviews with workgroup members. As we explained above, we do not analyze the reasons that deviance is initially adopted in a group but instead focus on the explanation of the diffusion and persistence of deviant behavior in a workgroup context. Moreover, we provide quotes from the narratives to illustrate the findings based on empirical data.

Figure 7 shows an introduction to the mechanisms that compose the model. The four circles in the figure refer to deviating workgroups and the corresponding intragroup dynamics and mechanisms that take place on each stage. The components behind every mechanism are reinforced over time and become more subtle, consequently turning the deviance into a group norm, and later into a group subculture that perpetuates over time. We detail and explain the mechanisms of the process and the related components in the next sections. In addition, the main theoretical elements of the model are presented in bold to better show the link between the explanation of the model and the figure.

Figure 7 – Process Model of Collective IS Deviance



Source: Prepared by the author

7.4.2.1 Dissemination: the Deviance Inception and Diffusion

Since the first moment the deviance is introduced within the group, the process of dissemination starts among its members. We found three components that trigger the process of dissemination. The first component that triggers the process are **perceived benefits** that refer to the advantages of the deviance to meet or even overfulfill work demands. Members of the same workgroup usually have highly interdependent tasks, where the outcomes of one are influenced by the actions of another (Saavedra et al. 1993; Hyatt and Ruddy 1997; Chen and Klimoski 2003). The concept of task interdependency refers to the extent to which a member needs information, materials, and support from other team members to be able to perform work tasks (Somech et al 2009).

In that sense, the perception of the benefits drives the inception and fast dissemination of the deviance because of the interdependency among members, who share the benefits of the deviance to perform and coordinate work.

> “*The more people see that the tool that I use is being useful to them to perform their daily tasks, the more they will use it. This is the key. We seek to engage people on tool usage showing them how useful it is*” (MD WG1).

Additionally, the commitment to common goals among the members, which is the extent to which members have defined, accepted and are committed to the group’s goals, drives their behavior toward the achievement of those goals (Hyatt and Ruddy 1997; Saavedra et al. 1993). Thereby, a common goal such as maintaining productivity and enhancing performance functions as an initiation driver to engage in the deviant act of using the unauthorized tool by perceiving it as a benefit of the deviance.

> “*People are practical-minded, they want to solve problems, find solutions… it’s about delivering the solution in an effective way. The tool doesn’t matter, people think about the results*”, reported the assistant of WG4. Hereby, the use of the unauthorized tool “*starts to make sense to people in daily activities*” (E3 WG1) and “*refuse to use would not make much sense*” (TL WG1) once it can imply in “*taking longer to finish the task*” (AU3 WG3).

The high task interdependence within the workgroups increases the need for collaboration and intensive interactions among team members because mutual adjustments are important to immediate performance (Saavedra et al. 1993; De Dreu 2007; Somech et al 2009). Within this context, all workgroup members are located close by, thus typically communicating more, and sharing higher amounts of information. Thereby, due to the collaborative climate of the workgroup, which means each member’s behavior and willingness to cooperate, communicate, help and assist each other regularly (Hyatt and Ruddy 1997), the second component is the **Group-World-of-Mouth** among members (peers and superior) to instigate the deviance and disseminate it.

The benefits mentioned above and the group goals (e.g., maintaining performance), as well as manners to achieve it, are frequently shared among members through informal communication. This pattern of informal communication among members takes place since the inception of the deviance. Direct messages among members introduce and advocate the deviant act to one another based on the primary purpose of being collaborative and helpful to the group.

> "*We shared the tool via USB drive saying, 'ah, I found a tool that can help you, you can download it, too'; and if we think something can be useful, we include that on the USB to share with others*." (AU1 WG3).

This influence to engage in deviance also may be performed by the superior of the group, who supports and/or advocates the deviance in order to maintain group performance.

> "*I received (the suggestion) from people in higher positions*" (AS WG4).

Thus, the superior also can engage in informal communication because he/she is seen as part of the group who shares the same goals and concerns.

The third component of this mechanism refers to **low technical barriers** to adopt and use technological resources. The unauthorized tools are mostly user-friendly and intuitively to use (e.g., cloud services), which allows users to get familiar with different tools, rather quickly.

> "*It was very simple to spread the use of the tool because the tool is very simple… it's a very intuitive learning process, you do not need to teach anyone, on how to use it…*", mentioned the assistant from the WG4.

Therefore, the low technical barriers faced by the members drive the inception and dissemination of unauthorized tools among members because of the vast amount of technological resources available on the internet free of charge and that demand no specific knowledge to use (Harris et al. 2012; Carter and Grover 2015). Also, many of those tools can be accessed without any formal authorization to install and use because access is provided via the internet.

7.4.2.2 Internalization: Deviance Becomes a Group Norm

At this stage, the deviance is already disseminated among group members. From here, a mechanism takes place that turns the deviance into a legitimate practice within the group structures and processes, thus considerably increasing the degree of institutionalization of the deviant act (Zucker 1977; Ashforth and Anand 2003). To explain how and why it occurs, we divided the explanation into two subsections. First, we take an intragroup perspective to analyze how the deviant act turns into a group norm. Second, we explain the components behind the change of group perception, uncovering the reasons why deviance becomes a group norm.

8.4.2.2.1 Shifting the perspective: how the deviant act becomes a group norm

To define and identify deviance, we need to consider organizational norms, for example, IS security policies that are violated when employees use unauthorized technologies. This perspective is commonplace in criminology, sociology, and management studies, which conceptualize deviance as intentional acts that violate organizational or societal norms (e.g., Robinson and Bennett 1995; Brown and Treviño 2006). When we think about organizational or societal norms such as the given example of IS security policies, we take into consideration something external to the group that exerts to some extent influence on group decisions.

Besides that theoretical consideration of the group as part of something larger and subject to external norms, a complementary perspective becomes necessary to understand the dynamics within the group. Here, an intragroup perspective turns the focus to an in-group analysis, considering the individuals as members of a group with its own norms. Within the intragroup perspective, deviance is defined as the violation of the norms of a group, no longer refereeing to deviance as crime, delinquency, or forms of negative and harmful behavior, according to Jetten and Hornsey (2014). Thereby, this perspective examines deviance focusing on norms created by individuals as part of a group, which can differ from organizational norms and change the status of the deviant act to its members.

Within the case of this research, the members of the workgroups also considered something external to the groups when asked about unauthorized technologies they use. They took into consideration external elements to the group to evaluate the tools, such as organizational policies, IS use norms, or tools that other groups use. Within this perspective, the respondents referred to the deviance as something “informal”, “unofficial” and “not provided by the organizational IT department”. They also constantly made a parallel between “us” meaning for the group, versus “they” meaning for the rest of the organization. This not only shows the separatism and differentiation between the group and external instances, but also outlines that members of the group try to catch external information, such as about organizational norms, and the organization as a whole. However, when evaluating the meaning and value of the unauthorized tool, the interviewees took into consideration elements legit only to the members of the group, such as the demands of work, relationship among members, shared views about the deviance, etc. The focus on the elements that come from inside the group gives to the deviance a normalized facet, being referred by the interviews as “official” to the group.

The intragroup perspective is necessary to understand the group dynamics and mechanisms that allow dissemination and perpetuation of the deviance over time. This is because the perspective of the members, from this stage, turns more and more over time to the development of their internal group norms. Although external norms from the organization still posit the act as deviant, the internal dynamics and the mechanisms created by the group lead to the formalization of the deviance into an accepted group norm, which we explain below. We continue to detail this perspective later on to explain the next stages.

8.4.2.2.2 Internalization: why the deviant act becomes a group norm

Individuals and groups repeatedly drift apart from what are acceptable standards of practice until the drift has become the norm to them (Pinto 2014). Internalization is an intervening process that aids to turn the deviance into social knowledge that perpetuates itself, also by increasing the degree of institutionalization of the deviance (Zucker 1977). It is solely after a norm is internalized that it can be identified as institutionalized, becoming part of objective reality, which may be transmitted on that basis (Zucker 1977; Ashforth and Anand 2003). We identified five components from the empirical data that trigger the mechanism of internalizing the deviance as a group norm.

The first component is **sense of ownership** regarding deviance as a group choice. The deviance is seen as an initiative of the group that is based on the members' needs, emerging the feeling of possessiveness and being psychologically tied to it (Pierce et al. 2001; Barki et al. 2008). The internalization of the deviance within the group occurs because of the perception of collective ownership that the deviance, in this case, the unauthorized tool, is owned by the group, e.g., “our tool” versus the “company’s (their) tool”, and shared by the group members (Pierce et al. 2003).

Once the deviance is a group initiative based on the members’ needs, they feel confident to consider themselves able to make the best choice based on their knowledge about the demands of the group.

> “*The company uses (name of the authorized tool), which is a service from Microsoft. However, it is a very limited tool; it makes work harder. So the (name of the unauthorized tool) is the best alternative*” (GD2 WG2).

It also allows them to differentiate the group from others.

> “*They (referring to members of another department) have been here longer and use Skype, which is the tool the company provides (*GD2 WG2)*… now, the company asks us to use Skype, too. But we still use (name of the unauthorized tool)*” (DA WG2).

Moreover, it is interesting to notice that even though the manager of the group sometimes forces the deviance, such as in the case of WG1, the members of the group perceive it in a different way.

> “*It wasn’t something top-down, it was something that helps the sales department and the respective teams and we realize the benefits*”, reported one of the employees (E3) of WG1.

It emphasizes the perception of the deviance as “from one of us to us”, in a sense that they do not see it as forced because they regard the manager as a member of the group helping them to meet the workgroup’s needs and goals.

The second component of this mechanism is **deviance routinization**. Because the deviance meets the workgroup’s needs and goals, which are a shared perspective by the members (e.g., Hyatt and Ruddy 1997; Chen and Klimoski 2003), the deviant act becomes embedded in the processes and routinized as a shared procedure (Ashforth and Anand 2003; Earle et al. 2010). Consequently, the whole group starts to perceive it as a central and essential tool in the work process.

> "*Today it's already a standard component of our work process, in our work in the sales department*" (E3 WG1), "*so, nowadays, everybody agrees that the tool is essential*…" (TL WG1), "*for us, it's an official tool*" (E1 WG1).

By becoming an integral part of daily activities, the members may be unable to see the inappropriateness of the behavior regarding organizational regulations and policies (Ashforth and Anand 2003).

Within the normalization perspective, deviance becomes a routine activity that is frequently used, which can also keep the individuals involved from openly questioning or challenging this behavior (Earle et al 2010). Thus, the perception of deviance as a common tool is also continuously communicated to the new members:

> "*To the new ones, we introduce the tool as a basic work tool"* (GD1 WG2).

The introduction of the unauthorized tool to the new member "is automatic when the person starts" (GD2 WG2). The deviance in that sense becomes a routine capability, which means a capability associated with the device-enabled routine allowing the accomplishment of some tasks, which are, in many cases, executed in coordination and socially in common among the members (Swanson 2019).

The third component of this mechanism is the **legitimate authority**. The group superior has legitimate authority in two ways. First, the superior has a formal hierarchical power from the organizational structure by being in a higher position in the organizational hierarchy (e.g., Ashforth and Anand 2003; Brown and Treviño 2006), sometimes even higher than the head of the IT department, as is the case of WG1 and WG2. One of the employees (E1) of WG1, for instance, pointed out the hierarchical power of their superior:

> "*if the sales manager wants to change something, there may be some dispute in the beginning, but later everybody has to call that tool official, even if it is unapproved by our IT department*." (E1 WG1)

Second, the authority of the group superior is also legitimated by the members of the group, who consider him/her as part of their group and a representative of the organization’s interests inside the group and of the group interest to the organization (e.g., Chang et al. 2015).

> “*The senior gave us the tool. So, I feel like I am just obeying rules…*” (AU1 WG3).

Thus, the superior is perceived as a legitimate agent of the organization and the group, receiving both formal and informal power (Ashforth and Anand 2003).

The superiors can serve as a role model by supporting, forcing, ignoring or condoning the deviance, either directly or indirectly (Ashforth and Anand 2003). The presentation of deviance by someone with authority may also increase enactment and transmission to newcomers by increasing perceptions of superior’ competence and the propriety of deviance, changing members’ perception about how official the deviant act is to the organization (Younts 2008; Banja 2010). The narrative below from the senior analyst of WG4 depicts the legitimate authority of the superior.

> *“If the instruction to use the (name of the unauthorized tool) comes from the manager of the team, who is a nominated person and a leader in the company, we expect that her instruction would be correct and according to the company interest, so we would follow her instructions. The closest leader to us is the spokesperson who advocates the company's interest. So, if she gives us instruction, it is the instruction of the company communicated through her.*” (SAT WG4).

Therefore, superiors not only can increase the level of institutionalization but also are powerful role models for group members (Ashforth and Anand 2003). In sum, the higher status position drives the internalization of the deviance within the group by directly or indirectly taking part in forcing or supporting the deviance. The direct or indirect involvement of the superior can help to hide the deviant characteristic of the act, which may be seen as an organizationally normative act because of the superior involvement.

The fourth component of this mechanism is **socially constructed justifications** used by the deviants as explanations to justify and valorize the deviance (Earle et al. 2010). The notion behind this component is that individuals and groups tend to resolve the inherent ambiguity of their actions and outcomes in a way that serves their self-interests (Ashforth and Anand 2003). For example, by reframing the meaning of the acts, negating negative interpretations, and developing narratives of why the deviance is justifiable or excusable exceptions to the general normative rules and treating them as if they were facts (Sykes and Matza 1957; Ashforth and Anand 2003).

Members develop narratives, based on the workgroup's context and demands, that provide them with a sense of being fair and correct as a way to legitimate the deviance. These socially constructed narratives also include the view that the group has no choice due to circumstances beyond their control (Ashforth and Anand 2003; Sykes and Matza 1957). For instance, a common justification is that the deviance is legit because the mandatory tool does not meet the needs. For example:

> "*we did not see ourselves as doing anything wrong. It was necessary to perform our work*" (AU1 WG3); "*they (IT department) cannot punish us for doing something they know they could not provide us*" (DM WG1); or "*it was a good initiative, something that brings benefits to our work*" (E3 WG1).

These are justifications used to change the members' perception of norm violations to something that is necessary, fair, and good.

In a similar vein, the decision to engage in collective deviant action can rely on the number of people, who are involved in the deviance (Granovetter 1978; McGloin and Thomas 2016). Thus, another common way of justifying the deviance used by members is the idea that the majority of the group engages in deviance, including the superiors of the group. Whether "it's hidden or not… everybody uses it, from the managers to the employees" (DA WG2), thus the deviant act gains a sense of normality inside the group.

7.4.2.3 Maintenance: Prevalence of the Deviance as a Group Norm

As a result of the previous mechanisms, the deviance is disseminated and internalized by the members at this stage, being part of the group norms. However, from the organizational perspective, the deviant act continues to be something that violates norms postulated by the organization, such as IS security policies. The normalization perspective suggests that, although some behaviors may appear deviant to people outside the group, for members of the group the deviance often stays unrecognized because it is simply taken as a normal occurrence (Pinto 2014). Thereby, within this perspective, the unexpected becomes the expected, and, untimely, the accepted, turning the deviance into a permissible and desirable behavior among the members (Ashforth and Anand 2003; Earle et al. 2010).

Within this section, we explain the mechanism that ensures the prevalence of the group norms, causing the maintenance of the deviance inside the group. First, it is relevant to notice some additional information to set the scene. All workgroups investigated reported a long existence of the deviance inside the group, for example, 4 and 5 years in WG1 and WG2, respectively, or some groups that are not aware of how long the group has already taken part in the deviant act, for example, in WG3 and WG4. In addition, all the workgroups have experienced significant changes in the group configuration over the years. For instance, the sizes of the group increased, the members of the group changed (some new members arrived, while others left the group) and the organization of the group changed by rearranging the group, for example, the department into different subgroups and managers. Considering that, we intend to explain the internal dynamics and components that take place ensuring the predominance of the group norms and, consequently, the continuity of the deviance over time, despite those group changes.

To explain why the group norms predominate, we again take the intragroup perspective introduced in the last section. This perspective considers deviance as the violation of the norms of a group (Jetten and Hornsey 2014), considering the group as an institution filled with meaning and having norms, habits, tools, etc., postulated and validated by its members. Thus, the focus here is on the norms developed by the group, which at this point already have the deviant act as an inherent and accepted part, as explained above. Considering these arguments, we realize a turning point to start understanding the predominance of the group norms. Once the deviance becomes a norm, from the intragroup perspective, the deviant actor is the very same who deviates from the new norm and former deviance. For instance, in our setting, the deviant is the one that refuses to use the IT internalized by the workgroup. However, from the organizational perspective, the unapproved IT of the workgroup still represents a deviant act.

Taking the explanation above into account, we discourse here the components of this mechanism responsible for ensuring the prevalence of the group norms. The first component is the **group tight relationship**. The dynamics of socialization of individuals within the group occurs “in a social cocoon, a localized, self-referential world where skewed behaviors and ideologies are presented as normal and acceptable - if not desirable" (Ashforth and Anand 2003).

All of the respondents defined the relationship among the members as close, not only professional but also as amicable.

> “*We have a very close relationship. That classic: you spend more time at work than with your family. So, you start to create a closer relationship with people here. We also meet outside of work*” (TL WG1).

They also defined the group at work as a good or pleasant environment and added the fact that many of them “have worked together for many years (DA WG2), consequently, “many of us already have a history together” (E3 WG1). These pieces of information lead to the idea of a sense of belonging to the group as a place they wish to stay and be part of, mainly because they spend many hours of the day at work sharing the same limited space (e.g., office). In addition, the deviant act can add a sense of connection to the group among those members engaging in coordinated deviance, emerging motives, and opportunities to connect to the team and create a basis of affective trust (Schabram et al. 2018). Thus, following the group norms by engaging in deviance is a path for the maintenance of group connection and acceptance.

The second component here is the **group pressure** toward the group norms. The members face a strong social situation that allows them to perceive sufficient volition to encourage the newcomers to internalize the deviance as their own (Ashforth and Anand 2003). In this situation, direct and indirect signals from the group members (peers and superiors) compel the deviance as the only existing or acceptable way. We could capture from the data a sense of obligation toward the group norm and the inexistence of other options besides the ones already defined by the group.

> “*Over time, the tool was getting important, so the pressure to use it increased, mainly from the director and managers*” (E3 WG1).

It is important to note that the respondents specified and emphasized the superior pressure, but they do not separate the superior from the group. The employee E1 from WG1 described the superior role as "the bigger force" because he/she has the legitimate power to support and, in some cases, force decisions on group members.

> "*From the group perspective, the use of the tool is mandatory, totally, mainly from the directors that use the tool to control performance. It is not about wanting or not; you have to use it*" (TL WG1).

Specifically, about the pressure from the peers, the respondents mentioned a "psychological pressure" related to the execution of work tasks, for instance:

> "*it is like a psychological pressure saying you are taking longer to finish your task*" (AU1 WG3). "*Everybody has to do his/her task for the senior revise in the end, according to the plan. So, there is pressure from the group. In the end, the group pressure, the day by day work, the managers, all those things become more relevant than the IT rules"* (AU3 WG3).

Thereby, the group pressure can cause a sort of situational and psychological stress, which drives members' behavior in maintaining the deviance in order to cope with that (Zhang et al. 2015).

The group pressure also forces the individuals to adapt to the group in the sense of acting according to the group requirements (Ashforth and Anand 2003).

> "*You have to work according to the way the place works*," (TL WG1).

Thereby, from the group perspective, engaging in deviance, which in our case is using the unauthorized technology, "it is an adaptation issue" (GD2 WG2). Otherwise, the group members may assume:

> that this person "*is not adapting to the group; the managers have always used this tool, then, there is pressure from the group to use the tool too*" (GD1 WG2).

Consequently, there is a pressure toward adaptation to group norms to avoid negative reactions from the group members and ensure social acceptance to maintain the “good environment”.

Related to the two components above, the last component of this mechanism is the **perception of social punishments**. The general idea behind this component is the fear induced by coercion, which is the threat of negative consequences such as disapproval, embarrassment, rejection, exclusion (Ashforth and Anand 2003; Heerdink et al. 2013). When the group pressure toward the norms failed or is not enough to drive some members to join the deviant act, the perception of potential punishments from peers takes place to ensure the continuity of the group norm. Thereby, the perception of social punishments differs from the last component in the sense that it is a consequence of refusing to follow the group norm or only resisting to group pressure.

In that sense, this component refers to perceived social punishments from the group members to those that do not engage in the group initiatives that have the potential to cause social pain, which is the distressing experience emerging from the perception of actual or potential psychological distance from close others or a social group (Eisenberger and Lieberman 2004).

We identified a wide range of punishments from the group in the narratives, such as disapproval, seclusion, embarrassment, discharge/termination, mistrust, exclusion, invalidation, mocking, bad evaluation, negative impacts of personal image. For example:

> “*if we refuse to use the technology, we certainly would be rejected. Why do you not use it? That's ridiculous, you have to do that’. Maybe I fear to receive a bad evaluation for declining to do something, because, ultimately, it is to facilitate the work*” (AU2 WG3).

The employee (GD2) of WG2 mentioned that the negative group reactions like exclusion are not necessarily intentional; it is a natural consequence for not following the group norms.

> “*The one that refuses would feel dislocated and excluded… not that others would exclude her/him, but this one would feel excluded because he/she is not using the tool everybody is usin*g. *it would cause mistrust and discomfort among*

> *colleagues. I think it would impact the relationship between the people in a negative way*".

Another punishment from the group is the disregard or invalidation of someone's work, which can also be expressed as a joke.

> "*We make jokes that if something is not on (name of the unauthorized tool), it has never happened*" (TL WG1).

This suggests that the group does not recognize the work as being done if it wasn't done using the unauthorized tool, which can cause frustration to the person, whose work was invalidated. Similarly, group punishment can be exerted by negatively affecting someone's image, as a professional, colleague or even as a friend once all groups consider having a friendship among the workgroup members.

> "*There are people I worked with that would say 'you are not good enough because you are not doing what I am saying.' It's like, if you are not the same as me, you are doing wrong*" (AU1 WG3).

Thus, the person would be poorly judged by the members as incompetent, unproductive, unhelpful, unprofessional, etc.

> "*I imagine that if I or anyone refuses, he/she would be called incompetent*" (MG WG5). "*they could say that as a professional I wasn't doing enough I could to help the team*" (AU2 WG3).

An employee (E3) from WG1 summed up the group perception in an analogy:

> "*it is like a soccer player refusing to train, it is part of the scope of your position*." (E3 WG1).

Finally, it also important to notice that all interviewees reported to not fear any punishments from the organization or the IT department, which one of them referred to as "unthinkable" (E1 WG1).

7.4.2.4 Cultural Persistence: the Perpetuation of the Deviance as a Subculture

Cultural persistence is the last mechanism of the process-oriented explanation of collective IS deviance. As the deviance becomes embedded in the ongoing routines of the group and the mechanisms to disseminate, internalize and maintain the deviance are already settled, a subculture emerges within the group to normalize the deviant act over time (Ashforth and Anand 2003). The mechanisms that normalize the deviance increased in complexity and power over time, becoming pervasive inside the workgroup. At this point, all the important aspects for achieving cultural persistence (transmission, maintenance, resistance to change) took place because of the high degree of institutionalization of the deviance (Zucker 1977). Cultural persistence embraces the idea of the perpetuation of the deviance as a group subculture throughout forces allowing to continue it indefinitely without interruption, despite changes in the group configuration, and without direct social control for its maintenance.

To begin the explanation of this mechanism, we provide some narratives that illustrate some key elements for further understanding of the components. For example, the department manager (DM) of WG1 referred to the deviance as a cultural issue to the group: "*today, it is already part of the culture*," and "*nowadays, everybody agrees that the tool is essential*," complemented the team leader (TL) of WG1.

Two significant elements emerged from the perception of deviance as a **manifestation of the workgroup subculture**. First, the members perceive the mechanisms for perpetuation of the deviance as a natural process, including the social control from the group to engage in the deviance is also considered normal and expected because it occurs mindlessly.

> "*This is a natural process (the group pressure). It is something that happens because you are part of the group. Not that you realize it, or really feel pressure. Once your own boss uses the tool, you feel safe; you do not see any problem. So, there is more influence from the group than from the ITD because you want to meet the work demands*" (AS WG4).

This element is also visible in the contradictory narrative of the employee GD2 of WG2:

> "*when someone joins, we say at once how we work and the person usually gets adapted, but it is not imposed or by pressure. It's a normal tool like the others. We do not present an alternative; we only introduce the tool because it is what everybody uses."(GD2 WG2).*

The persistence of deviance can be an indicator of functional necessity (Zucker 1977). Because of the commitment of the members to common goals (e.g., Hyatt and Ruddy 1997), the perception of the deviance as something necessary that can help the group to meet their work demands is part of the objective reality.

This leads us to the second element, the unlikely ending of the deviance at this stage. Once the deviance is already rooted inside the group, change or ending the deviance at this stage is something unlikely because it represents a substantial change to the group, causing discomfort and conflicts. Thus, resistance to change the deviant act evolves within the group. This is explained by the team leader of WG1:

> "*abandon the tool now would be a big change, something really extreme because we have all the history there, and neither the director nor the IT department would like to backup that someplace else*" (TL WG1).

The high degree of institutionalization of the deviant act plays an important role to understand the scenario. Highly institutionalized acts only need transmission for maintenance because they are perpetuated as a fact, while low institutionalized acts need direct social control or other intervening mechanisms for transmission and maintenance (Zucker 1977). The whole processes reduce the salience of the deviant act, which becomes a normative act to the group members, who now engage and perpetuate the act mindlessly (Ashforth and Anand 2003). For this reason, it is sufficient, at this level of institutionalization, for one member simply to tell another that this is how things are done, motivating the individuals to comply because otherwise their actions in the system cannot be understood by the rest of the group (Zucker 1977).

The first component leading to a cultural persistence is **habit**. As deviance becomes institutionalized and repeatedly enacted, it becomes habitual, causing the resistance of the members to attempts of changing because it demands a more conscious effort to discontinue than continue the deviance (Zucker 1977; Ashforth and Anand 2003). The narratives of the WG2 shows this idea of persistence, what they also refer to as habit:

> "*it is about habit. I think someone is unlikely to arrive here and say he/she doesn't want to use it because everybody uses it so much, so there is no room to say 'I don't want to use it'.*" (GD2 WG2).

Therefore, the deviance, as a routinized practice among the members, becomes a habit, representing high cost and effort to change and no longer with the necessity of direct social control for maintenance.

> "*I think when you have a context where a tool like (name) or any other is already being used, and the use of the tool was already disseminated, also people are already adapted to it, then it is almost impossible to have an alternative solution. It was not an environment where I was invited to suggest another tool or where I was given another alternative. The department already used the tool, the manager supported it, so that was the tool.*" (SDA WG2).

Another important component for cultural persistence is the transmission across generations, which will ensure the perpetuation regardless of the turnover of the group members (Zucker 1977). Hence, the second component of this mechanism is cultural transmission. The narratives show that the members develop a perception of a tradition seeing deviance as a practice that always has been part of the group and it has been passed through group generations over the years. For example:

> "*when I started to work there, someone gave me a USB flash drive; I saved everything on my computer. When another person started, I saved everything on a USB and gave it to the person and so on, so forth..., it was something that our superiors gave us, when we started, in the first week, and we gave to others over time, passing from one to another, from seniors to trainees*" (AU2 WG3).

Thereby, the perception of the deviance as a subculture increases the likelihood and uniformity of transmission to new group members, which also implies that the perpetuation of deviance can occur even when the individuals engaged do not personally support the behavior and have no material interest in doing so (Younts 2008). Moreover, groups can develop traditions related to choices that aim to maximize earnings and the stronger the dependence between choice and earnings (e.g., gains in productivity), the stronger may become the tradition (Baum et al. 2004). This becomes important when we take into account that the deviance is a group choice strongly related to the members' functional necessity (Zucker 1977).

The transmission of a subculture relies also on the permanence of the deviance inside the group. The fact that "*when I started to work there it was already being used*" (AU3 WG3) or "*when I joined the team it was already disseminated*" (AS WG4) provides to group members, in particular the new ones, the idea of permanence over time. This drives an individual perception of the idea of a practice already stipulated and consolidated inside the group that is not open to discussion but to be followed.

> "*When someone new joins the group we say 'we use these tools and we work this way*.'" (GD2 WG2).

The long existence of the deviance reinforces this perception, which can be seen in the narrative of one of the auditors (AU2) of the WG3:

> "*it was shared one by one in a USB flash drive since always, it is historic!*" (AU2 WG3).

Ultimately, the perception is that the deviant act…

> "*was not something that spread; it's something that always existed in our unit"* (GD1 WG2).

Due to the development of a subculture, the personal characteristics of the members can develop into a group identity that influences their behaviors in perpetuating the deviance, which is the third and last component of this mechanism.

Group identity refers to the collective level of group identification occurring across all members that determines, whether they will be inclined to act according to the group norms and goals (Lembke and Wilson 1998; Somech et al 2009).

Identities are social products because they are formed and maintained through the social processes of 1) locating the self in socially recognizable categories, 2) identification and exchange in interaction to others, and 3) the confirmation and validation of self-concepts (Burke and Reitzes 1981). Within a social identity perspective, the meaning of one’s identity is a result of membership in a social group (Hogg et al. 1995). Consequently, individuals in groups, mainly the newcomers, are encouraged to affiliate and bond with the other members, raising desires to identify with, emulate and please the workmates (Ashforth and Anand 2003). Social identity becomes then relevant in the group situation, as well as subjectively important to the individual.

To preserve a good social identity, the members tend to reframe the meaning of their acts to justify their behavior, as already explained before. This becomes important at this point again because individuals are predisposed to find positive qualities in roles and acts to provide meaning to their identities (Ashforth and Anand 2003). For example, the SAT2 of WG4 mentioned “the profile of not being passive and accept the things how they are, instead find a solution to solve it” as a profile well-valued by the group, driving the members to identify with those values e beliefs and act accordingly.

> *“It is related to the profile of the people here, question things…Our unit is known for being the most laid-back unit in the company. The unit here is the biggest and has people with different backgrounds, ages... so I think this creates the idea of a more open, easygoing, informal group”* (ID2 WG2).

This narrative shows that characteristics such as laid-back, big and dynamic, informal, tach savvy, innovative are shared by the members as a group identity, which can determine their behavior act according to the group norms and goals. The deviance existence inside the group, ultimately, has the meaning of being, for example, innovative or proactive, which are characteristic values at the collective level that should be preserved.

In sum, all those components ensure the perpetuation of deviance as a subculture in a subtle and pervasive way due to the high degree of institutionalization of the deviance. The deployment analyst from the WG2, who arrived in the group later compared to the other members, illustrates how subtle the transmission can be at this point:

> "*I think that some people do not even realize it's not an official company tool. When I started to work, it took me some time to realize that it wasn't a tool from the ITD. When you arrived in the group, you started to use the solutions they use, since the beginning, so you do not notice that*" (DA WG2).

This illustrates the idea that deviance as a highly institutionalized part of a subculture has no longer the need for direct social control such as direct sanctions from the group to perpetuate. Table 15 presents the mechanisms and components of the process model of collective IS deviance.

Table 15 – Mechanisms and Components

Mechanism	Description	Components	Description
Dissemination	Mechanism triggering inception and diffusion of the deviance	Perceived Benefits	The advantages of the deviance from meeting the work demands perceived by the members drive the inception and fast dissemination of the deviance within the workgroup because of task interdependency and the commitment to common goals of the members.
		Group-World-of-Mouth	Due to the collaborative climate of the group, which means the behaviors and willingness to cooperate, communicate, help and assistance each other regularly, members (peers and superior) informally communicate (direct and clear messages send orally) to instigate the deviance and disseminate it within the group.
		Low technical barriers	Low barriers to adoption and use drives the inception and dissemination of the tool among members because of the vast amount of technological resources available on the internet that demand no financial resources and no specific knowledge to use (e.g., cloud services).
Internalization	Mechanism turning the deviance into a group norm	Sense of Ownership	The internalization of the deviance within the group occurs because of the perception that the deviance is owned by the group, an initiative that is based on the members' necessity (our tool vs. the company's (their) tool), giving to the deviance a face of legitimate to the members.
		Deviance routinization	Because the deviance meets the workgroup's needs and goals, it becomes embedded in the processes, which turns the deviance into a routine as the main and usual tool for working.

		Legitimate authority	Because the superior has a formal hierarchical power from the organization and informal from the group perspective for being considered part of the group, the higher status position drive the normalization of the deviance within the group by directly or indirectly taking part, forcing or supporting the deviance.
		Socially constructed justifications	Members create excuses to justify and support their deviant behavior based on the workgroup context and demands as a way to legitimate the deviance. The members believe the deviance is legit because the mandatory tool does not meet the needs, as well as because of the engagement of the majority of the group once the decision to engage in collective deviant action can rely on the number of people, who are involved in deviance.
Maintenance	Mechanism ensuring the prevalence of the group norm	Group tight relationship	The closeness and friendship among the members make the group a pleasant place to be and feel part, mainly due to the shared time and space at work, driving the predominance of the group norms to avoid disturbing the pleasant environment.
		Group Pressure	Direct and indirect signals from the group members (peers and superiors) compelling the deviance as the only existing or acceptable way, driving to the predominance of the group norm.
		Perceived Social Punishments	Punishments from the group members to those that do not engage in the group initiatives that have the potential to cause social pain, which is the distressing experience emerging from the perception of actual or potential psychological distance from close others or a social group.
Cultural persistence	Mechanism leading to the perpetuation of the deviance as a subculture	Habit	After some time, deviance becomes a habit and, because it is a routinized practice among the members, it represents high cost and effort to change, which aids in the perpetuation of the deviance within the group, no longer with the necessity of direct social control.
		Cultural transmission	Because of the long existence of deviance inside the group, the members develop a perception of tradition, seeing deviance as a practice that always has been part of the group and it has been passed through group generations over the years.
		Group Identity	Due to the development of a subculture, the personal characteristics of the members can develop to a group identity, which refers to the collective level of group identification occurring across all the members that determines whether they will be inclined to act according to the group norms and goals.

Source: Prepared by the author

7.5 DISCUSSION AND CONCLUSION

This research aimed to investigate the dissemination of collective deviance within organizations, uncovering reasons and mechanisms behind it in order to offer a theoretical model that explains the phenomenon. Below we present and discuss the main findings of this research, theoretical and practical implications, as well as limitations and future research.

7.5.1 Findings on Collective IS Deviance

In summary, the results show that not only the dissemination of the deviance among the group members occurs but also that the proliferation of the deviant act continues indefinitely overtime in an uninterrupted way despite changes in group size and membership, turning into a group subculture. Ultimately, the deviant act becomes normalized. The process model proposed describes the mechanisms and components that allow the normalization of the deviant behavior within the group. Below we discuss these findings based on previous studies.

The first result is that the deviance diffuses among group members, as expected. The process of dissemination of deviance starts, since the moment it was created by one or some members of the workgroup and continues over time. This is in line with extant literature that found out that deviant behaviors exhibited by a workgroup are a significant predictor of an individual's deviant behavior at work (e.g., Robinson and O'Leary-Kelly 1998; Zhang et al. 2015), driving the dissemination of the deviant act among group members.

Second, the results here suggest that the dissemination of the deviance continues to occur regardless of the original configuration of the group and, consequently, is not dependent on how long the individuals are part of the group. In our sample, the workgroups suffered many changes in their configuration over the years, including changes in some or many of their members (peers and superiors). This can be part of what Schabram et al. (2018) called configural property arguing that their results on collective deviance depend on whether the team engaged in coordinated deviance or independent deviance of some or many of its members. All the workgroups investigated by this research engaged in coordinated deviance of many of its members, newer and older ones. Furthermore, Robinson and O'Leary-Kelly (1998) found that the influence of a group's deviant behavior on an individual's deviant behavior became stronger as the individual's time in the group increased. Our results do not deny it but suggest that staying longer within the group is not a necessary condition for maintaining the deviance.

It is true that the longer the individual is part of the group, the stronger will be the relation and influence of the group on the individual, increasing the feeling of being “one of us”, as Robinson and O’Leary-Kelly (1998) observed. However, the maintenance of the deviance relies on the relationship between the group and their norms, which in this case includes the deviance. The explanation for that are the components behind the second and third mechanism of the deviance dissemination process. Our findings suggest that a change in the group perception about norms occurs, allowing the transformation of the deviance into a group norm, and later mechanisms take place to ensure the obedience and maintenance of the group members.

This leads us to the third finding that suggests the dissemination of the deviance continues indefinitely over time in an uninterrupted way, what we called perpetuation of deviance. The reasoning behind that are the mechanisms responsible for disseminating the deviance among the group members increase in complexity, power, and subtleness over time, which is more or less a cumulative effect of the previous stages. Moreover, the effect of those mechanisms will be as powerful and subtle in a newer member as it is in an older member. For example, if a new member joins the group in the fourth stage of the dissemination deviance process (perpetuation of the collective deviance), the mechanisms will drive him/her to engage in the deviant act without questioning or noticing it as pressure because of the group’s understanding that the deviance is a habit and it is part of the group culture, which is already settled to an older member. This can be related to what Robinson and O’Leary-Kelly (1998) called groups with stronger deviant climates that, according to their findings, appeared to have greater ability to influence individual members toward deviance. Ultimately, our results suggest that the deviance disseminations among the group members over time and perpetuates inside the group regardless of the original configuration of the group, not depending on how long the individuals are part of the group.

Some miscellaneous findings of the dissemination process are also worth mentioning. The fact that many of the group members, including the superiors, engage in the deviant act triggers several mechanisms in the deviance dissemination process (e.g., peer and superior influence, infusion in the work processes, group pressure, justification mechanism, manifestation of the group culture). This is in line with McGloin and Thomas (2016), who found that, as the number of people involved in the deviant act increases, the perception of anticipated rewards increases (i.e., fun/excitement and social inclusion). In addition, the perception of sanction risk decreases, as well as the anticipated sense of responsibility for the device decreases, as more people get involved in the deviant act. Our results show that to feel being part of the group is important to members, mainly because there is a friendship among the members and one way to ensure the inclusion is following the group norms. Moreover, the findings also show that because everyone inside the group engages in the deviance, they are not concerned about any kind of formal punishment from the organization. However, our results differ from McGloin and Thomas (2016) on the social cost associated with inaction. In their study, respondents did not report higher levels of anticipated social ridicule or exclusion for not engaging in the deviance as more people were involved. Differently, we found a high social cost associated with refusing to engage in the group deviance, which is related mainly to the group pressure (peers and superiors) and the group punishments for not following and adapting to the group, such as being rejected and excluded by the group, bad evaluation from your immediate superior, and a negative impact on your image (unprofessional or inefficient).

Specifically about the superior role in the dissemination of the deviance, our results suggest that the direct or indirect support of the group superior (e.g., manager or leader) can intensify those perceptions on rewards, risks, and social costs. Brown and Treviño (2006) argue for a direct influence on the person in charge and the amount of deviance in workgroups, reaffirming the strong influence supervisors have on their direct employees. This is what Younts (2008) called the endorsement of deviance. According to the author, the endorsement of deviance by one's peers is sufficient to legitimate deviance within a situation, increasing its enactment and transmission, as well as the presentation of deviance by a higher status member (superior) also increased enactment and transmission of deviance. Moreover, Younts (2008) findings suggest that endorsement of deviance within a particular situation increases the probability and uniformity of transmission to new group members, possibly leading the institutionalization of deviance within the group's culture, implying that the dissemination and persistence of legitimated deviance can occur even when the individuals involved do not personally support the behavior. Thereby, the findings here support and complement Younts (2008) by explaining the mechanism behind the normalization of the deviance inside the group until it becomes a manifestation of the group's culture, which ensures the dissemination and perpetuation of the deviance inside the group, including to the new members.

7.5.2 Theoretical Contributions

Based on empirical data from workgroups, we developed a process-oriented theoretical model to explain IS-related collective deviance in the workplace. By doing so, we provide some empirical, conceptual and theoretical contributions to management research in general, and IS research in particular. First, our results have interesting contributions to the deviance literature, especially to the growing research on workplace deviance by addressing it as a group-level phenomenon. Although deviance frequently occurs within and by groups (e.g., Gardner and Steinberg 2005; McGloin and Thomas 2016), most research on deviant behavior has focused exclusively on the individual-level (Robinson and O'Leary-Kelly 1998; Schabram et al. 2018). In that sense, we provide conceptual contribution by conceptualizing the phenomenon at the collective level and describing and explaining it inside of the workplace context, specifically IS oriented.

Second, this research has self-reported information from members of deviant workgroups about the reasons why deviants act with companions over time in the workplace, providing narrative data that reflect several of the mechanisms of collective deviance, patterns on behavior and the meaning of group to the deviant members (McGloin and Stickle 2011). Our research also accounted for the configuration that underlies group deviance, as suggested by Schabram et al. (2018). We contribute in that sense by providing insights into how group deviance configurations change over time, which was useful for a better understanding of workgroup behavior regarding the deviance. Moreover, the results reinforce the importance of situational characteristics in the decision process of engaging in deviance (McGloin and Thomas 2016). Therefore, we contribute by identifying how the perceptions of workgroups regarding the deviance are developed, communicated, and enforced, reaffirming the evidence that a group effect does occur and enhancing the understanding of why, when, and how people in groups deviate at work (Robinson and O'Leary-Kelly 1998).

Third, we provide advances into the processes by which group norms become legitimate and, consequently, diffuse and perpetuate through cultural transmission, which Younts (2008) suggested as a critical goal of future research. In that sense, the results here provide further insights into the extent to which endorsement by peers and superiors leads to the enactment and transmission of deviance in natural settings (Younts 2008). Our research shows that the validation of deviance by the group members within a situation may legitimate the deviant act and turns it into a group norm, even when it violates external norms such as the organizational security policies.

Fourth, our study also provides some contributions to research in IS policy compliance and violation, attending the need for further group-level security research. To the best of our knowledge, this research is the first to investigate IS-related deviance as a group phenomenon. To incorporate new theoretical foundations and expand our horizons, we rely on the collective deviance literature from social psychology and criminology to explain workplace deviance in the IS context, as suggested by Warkentin and Willison (2009). We provide further insights into employees' behavior regarding IS policy compliance, specifically explaining reasons why members of a workgroup deviate from IS policies. By using a qualitative approach, we could provide a broader view of the phenomenon, including the emergence of different concepts and group dynamics that impact employee's behavior regarding IS policies, such as the development, dissemination, and permanence of the deviant act as a group norm, and later also as a group culture (Ifinedo 2014).

In a similar vein, Moody et al. (2018) claim for further studies that examine to what extent the social nature of the information security acts, such as compliance or violation, are linked to subjective norms or other social factors. In this regard, we provide insights about IS policy violation considering social factors of workgroups, such as social influence, communication, social punishments, and the group relationship, showing how these social factors influence the members of workgroups toward the deviance and violation of IS policies. The accounting of social factors also allowed us to contribute by exploring workgroup culture to enhance the understanding of IS policy violation from that perspective, as suggested by Yazdanmehr and Wang (2016). Finally, little research in the IS security field has explored the effects of habits on security-related behaviors (Moody et al. 2018). Our results provide contributions by examining the process that leads to members of a group becoming habitual non-compliers. In that sense, we provide insights into how the deviant behavior turns into a habit to group members, which collaborate to maintain the deviant act inside the group.

7.5.3 Practical Implications

We believe the findings from this study could help managers to better understand deviant behavior at work and, consequently, help organizations to enhance employees' compliance with organizational security policies. It is important to mention that one of the main reasons for the emergence of unauthorized technology inside workgroups is the complete or partial absence of adequate IT solutions that meet the employees’ requirements. Thereby, creating effective communication between the IT department and business units is vital to provide suitable tools to perform work tasks. In the same vein, effective communication between IT department and workgroups may include the communication and clarifications of organizational security policies, and the risks associated with its violation, which would help to enhance the employees’ information security awareness.

This research also provides implications for the management of workgroups regarding the use of technologies and policy violations by understanding how some social factors occur and affect individuals and the group toward the deviant act. In this regard, our results point out the role of superiors that was extremely emphasized in the respondents’ narratives because they have a legitimate power that comes from the organizational hierarchy and charismatic power by being seen as “one of us” from other members of the group (e.g., Brown and Treviño 2006; Younts 2008; Aguilera and Vadera 2008). Thereby, the superior is an authority that has legitimate power from the organizational and group perspective to not only disseminate and perpetuate the deviance but also the power of doing the opposite, that is, change the course of the deviance. Organizations can profit from this information by engaging their leaders in better security practices to communicate with workgroups. For example, the superior may be a key figure in managing the gradual change from an unauthorized tool to a homologated tool, introducing new practices into the group, and mediating the relationship and conflicts between the group needs and the IT department.

7.5.4 Limitations and Future Research

We believe our study brings contributions to the sparse work on collective deviance in the IS field. However, it still has limitations that can inform directions for future research. First, the research is based on a very specific sort of workplace deviance (use of unauthorized technology at work), not all types of deviant workplace behaviors. Thus, further research must use caution before applying our conclusions more generally to other deviant acts. In any case, we hope that highlighting the effects of workgroups on deviant behaviors will encourage future research on collective deviance in the workplace, especially in the IS field to understand deviances such as IS policy violation, workaround behavior, and shadow IT usage within organizations (e.g., Warkentin and Willison 2009; Haag and Eckhardt 2017).

Second, the results reinforce the importance of situational and configurational group characteristics, which can shape group dynamics regarding deviant acts. However, the findings here rely only on five workgroups from four different companies. In addition, the method applied does not provide much information on the context of each group and company. Therefore, it is important to consider that the results can vary in different group contexts and business segments. In that sense, future research may explore better the situational characteristics and the configurational properties of the group by considering the context. Other concepts and mechanisms from different contexts can emerge that influence the group decision process of engaging in deviance. Third and last, quantitative research would be valuable to test the model applicability regarding the mechanisms that compose each stage. Hereby, future research would contribute by extending the sample within a quantitative perspective to test the applicability of the model and its mechanisms and allow its generalization.

References

Aguilera, R.V. and Vadera, A.K., 2008. The dark side of authority: Antecedents, mechanisms, and outcomes of organizational corruption. Journal of Business Ethics, (77:4), pp. 431-449.

Ashforth, B.E. and Anand, V., 2003. The normalization of corruption in organizations. Research in organizational behavior, 25, pp.1-52.

Banja, J., 2010. The normalization of deviance in healthcare delivery. Business horizons, 53(2), pp.139-148.

Barki, H., Paré, G. and Sicotte, C., 2008. Linking IT implementation and acceptance via the construct of psychological ownership of information technology. Journal of Information Technology, 23(4), pp.269-280.

Baum, W.M., Richerson, P.J., Efferson, C.M. and Paciotti, B.M., 2004. Cultural evolution in laboratory microsocieties including traditions of rule giving and rule following. Evolution and Human Behavior, 25(5), pp.305-326.

Brown, M.E. and Trevino, L.K., 2006. Socialized charismatic leadership, values congruence, and deviance in work groups. Journal of Applied Psychology, (91:4), pp. 954.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), pp.523-548.

Burke, P.J. and Reitzes, D.C., 1981. The link between identity and role performance. Social psychology quarterly, pp.83-92.

Cappelli, P., and Sherer, P., 1991. The missing role of context in OB: The need for a meso-level approach. Research in Organizational Behavior, 13, 55-110.

Chen, G. and Klimoski, R.J., 2003. The impact of expectations on newcomer performance in teams as mediated by work characteristics, social exchanges, and empowerment. Academy of management Journal, 46(5), pp.591-607.

Corbin, J. and Strauss, A., 2015. Basics of qualitative research: Techniques and procedures for developing grounded theory. Sage publications.

Coser, L.A., 1962. Some functions of deviant behavior and normative flexibility. American Journal of Sociology, 68(2), pp.172-181.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R., 2013. Future directions for behavioral information security research. Computers & Security, 32, pp.90-101.

Dahling, J.J., Chau, S.L., Mayer, D.M. and Gregory, J.B., 2012. Breaking rules for the right reasons? An investigation of pro-social rule breaking. Journal of Organizational Behavior, 33(1), pp.21-42.

De Dreu, C.K., 2007. Cooperative outcome interdependence, task reflexivity, and team effectiveness: a motivated information processing perspective. Journal of applied psychology, 92(3), p.628.

Earle, J.S., Spicer, A. and Peter, K.S., 2010. The normalization of deviant organizational practices: Wage arrears in Russia, 1991–98. Academy of Management Journal, 53(2), pp.218-237.

Eisenberger, N.I. and Lieberman, M.D., 2004. Why rejection hurts: a common neural alarm system for physical and social pain. Trends in cognitive sciences, 8(7), pp.294-300.

Fielding, K.S., Hogg, M.A. and Annandale, N., 2006. Reactions to positive deviance: Social identity and attribution dimensions. Group Processes & Intergroup Relations, 9(2), pp.199-218.

Galperin, B.L., 2012. Exploring the nomological network of workplace deviance: Developing and validating a measure of constructive deviance. Journal of Applied Social Psychology, 42(12), pp.2988-3025.

Gardner, M. and Steinberg, L., 2005. “Peer influence on risk taking, risk preference, and risky decision making in adolescence and adulthood: an experimental study.” Developmental psychology, (41:4), p. 625.

Glaser, B.G., 1978. Theoretical Sensitivity: Advances in the Methodology of Grounded Theory. Sociology Press, Mill Valley, CA.

Glaser, B. G., and Strauss, A. L., 1967. The discovery of grounded theory: Strategies for qualitative research. Mill Valley, CA: Sociology Press.

Heerdink, M.W., Van Kleef, G.A., Homan, A.C. and Fischer, A.H., 2013. “On the social influence of emotions in groups: interpersonal effects of anger and happiness on conformity versus deviance.” Journal of Personality and Social Psychology, (105:2), p. 262.

Hill, G.W., 1982. Group versus individual performance: Are N+ 1 heads better than one?. Psychological Bulletin, 91(3), pp.517.

Hogg, M.A., Terry, D.J. and White, K.M., 1995. A tale of two theories: A critical comparison of identity theory with social identity theory. Social psychology quarterly, pp.255-269.

House, R., Rousseau, D.M. and Thomas-Hunt, M., 1995. The Meso paradigm-a framework for the integration of micro and macro organizational-behavior. Research in Organizational Behavior: an Annual Series of Analytical Essays and Critical Reviews, Vol 17, pp. 71-114.

Hung, H., 2008. Normalized collective corruption in a transitional economy: Small treasuries in large Chinese enterprises. Journal of Business Ethics, 79(1-2), pp.69-83.

Hyatt, D.E. and Ruddy, T.M., 1997. An examination of the relationship between work group characteristics and performance: Once more into the breech. Personnel Psychology, 50(3), pp.553-585.

Ifinedo, P., 2014. “Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition.” Information & Management, (51:1), pp. 69-79.

Jetten, J. and Hornsey, M.J., 2014. “Deviance and dissent in groups.” Annual review of psychology, 65, pp. 461-485.

Johnston, A.C., Di Gangi, P.M., Howard, J. and Worrell, J., 2019. “It Takes a Village: Understanding the Collective Security Efficacy of Employee Groups”. Journal of the Association for Information Systems, 20(3), pp.186-212.

Karjalainen, M., Sarker, S. and Siponen, M., 2019. Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective. Information Systems Research, 30(2), pp.687-704.

Klein, K.J. and Kozlowski, S.W., 2000. From micro to meso: Critical steps in conceptualizing and conducting multilevel research. Organizational research methods, 3(3), pp.211-236.

Lawrence, T.B. and Robinson, S.L., 2007. Ain't misbehavin: Workplace deviance as organizational resistance. Journal of Management, 33(3), pp.378-394.

Lembke, S. and Wilson, M.G., 1998. Putting the" team" into teamwork: Alternative theoretical contributions for contemporary management practice. Human Relations, 51(7), pp.927-944.

Mainemelis, C. 2010. “Stealing fire: Creative deviance in the evolution of new ideas.” Academy of Management Review, 35: 558-578.

McGloin, J.M. and Povitsky Stickle, W., 2011. “Influence or convenience? Disentangling peer influence and co-offending for chronic offenders.” Journal of Research in Crime and Delinquency, (48:3), pp. 419-447.

McGloin, J.M. and Nguyen, H., 2012. “It was my idea: Considering the instigation of co-offending.” Criminology, (50:2), pp. 463-494.

McGloin, J.M. and Thomas, K.J., 2016. “Incentives for collective deviance: Group size and changes in perceived risk, cost, and reward.” Criminology, (54:3), pp. 459-486.

Mertens, W., Recker, J., Kummer, T.F., Kohlborn, T. and Viaene, S., 2016. Constructive deviance as a driver for performance in retail. Journal of Retailing and Consumer Services, 30, pp.193-203.

Moody, G.D., Siponen, M. and Pahnila, S., 2018. “Toward a unified model of information security policy compliance.” MIS Quarterly, (42:1), pp. 285-311.

Paulus, P.B. and Yang, H.C., 2000. Idea generation in groups: A basis for creativity in organizations. Organizational behavior and human decision processes, 82(1), pp.76-87.

Pierce, J.L., Kostova, T. and Dirks, K.T., 2001. Toward a theory of psychological ownership in organizations. Academy of management review, 26(2), pp.298-310.

Pierce, J.L., Kostova, T. and Dirks, K.T., 2003. The state of psychological ownership: Integrating and extending a century of research. Review of general psychology, 7(1), pp.84-107.

Pinto, J.K., 2014. Project management, governance, and the normalization of deviance. International Journal of Project Management, 32(3), pp.376-387.

Robinson, S.L. and Bennett, R.J., 1995. “A typology of deviant workplace behaviors: A multidimensional scaling study.” Academy of management journal, 38(2), pp.555-572.

Robinson, S.L. and O'Leary-Kelly, A.M., 1998. “Monkey see, monkey do: The influence of work groups on the antisocial behavior of employees.” Academy of Management Journal, (41:6), pp. 658-672.

Saavedra, R., Earley, P.C. and Van Dyne, L., 1993. Complex interdependence in task-performing groups. Journal of applied psychology, 78(1), p.61.

Schabram, K., Robinson, S.L. and Cruz, K.S., 2018. “Honor among thieves: The interaction of team and member deviance on trust in the team.” Journal of Applied Psychology, (103:9), pp. 1057.

Silic, M. and Back, A., 2014. Shadow IT–A view from behind the curtain. Computers & Security, 45, pp.274-283.

Siponen, M. and Vance, A., 2010. Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly, pp.487-502.

Somech, A., Desivilya, H.S. and Lidogoster, H., 2009. Team conflict management and team effectiveness: The effects of task interdependence and team identification. Journal of Organizational Behavior, 30(3), pp.359-378.

Spreitzer, G.M. and Sonenshein, S., 2004. Toward the construct definition of positive deviance. American behavioral scientist, 47(6), pp.828-847.

Swanson, E.B., 2019. Technology as routine capability. MIS Quarterly, Vol. 43 No. 3, pp. 1007-1024.

Treviño, L.K., Weaver, G.R. and Reynolds, S.J., 2006. “Behavioral ethics in organizations: A review.” Journal of management, (32:6, pp. 951-990.

Urquhart, C., Lehmann, H. and Myers, M.D., 2010. “Putting the ‘theory’ back into grounded theory: guidelines for grounded theory studies in information systems.” Information Systems Journal, (20:4), pp. 357-381.

Van Der Vegt, G.S. and Bunderson, J.S., 2005. Learning and performance in multidisciplinary teams: The importance of collective team identification. Academy of management Journal, 48(3), pp.532-547.

Vardi, Y. and Wiener, Y., 1996. “Misbehavior in organizations: A motivational framework.” Organization science, (7:2), pp. 151-165.

Walls, J.L. and Hoffman, A.J., 2012. Exceptional boards: Environmental experience and positive deviance from institutional norms. Journal of Organizational Behavior, 34(2), pp.253-271.

Walsham, G., 1995. Interpretive case studies in IS research: nature and method. European Journal of information systems, 4(2), pp.74-81.

Warkentin, M., and Willison, R. 2009. “Behavioral and policy issues in information systems security: the insider threat,” European Journal of Information Systems, (18:2), pp. 101-105.

Warren, D.E., 2003. Constructive and destructive deviance tn organizations. Academy of management Review, 28(4), pp.622-632.

Yazdanmehr, A. and Wang, J., 2016. “Employees' information security policy compliance: A norm activation perspective.” Decision Support Systems, 92, pp.36-46.

Zhang, H., Luo, X.R., Liao, Q. and Peng, L., 2015. “Does IT team climate matter? An empirical study of the impact of co-workers and the Confucian work ethic on deviance behavior.” Information & Management, 52(6), pp.658-667.

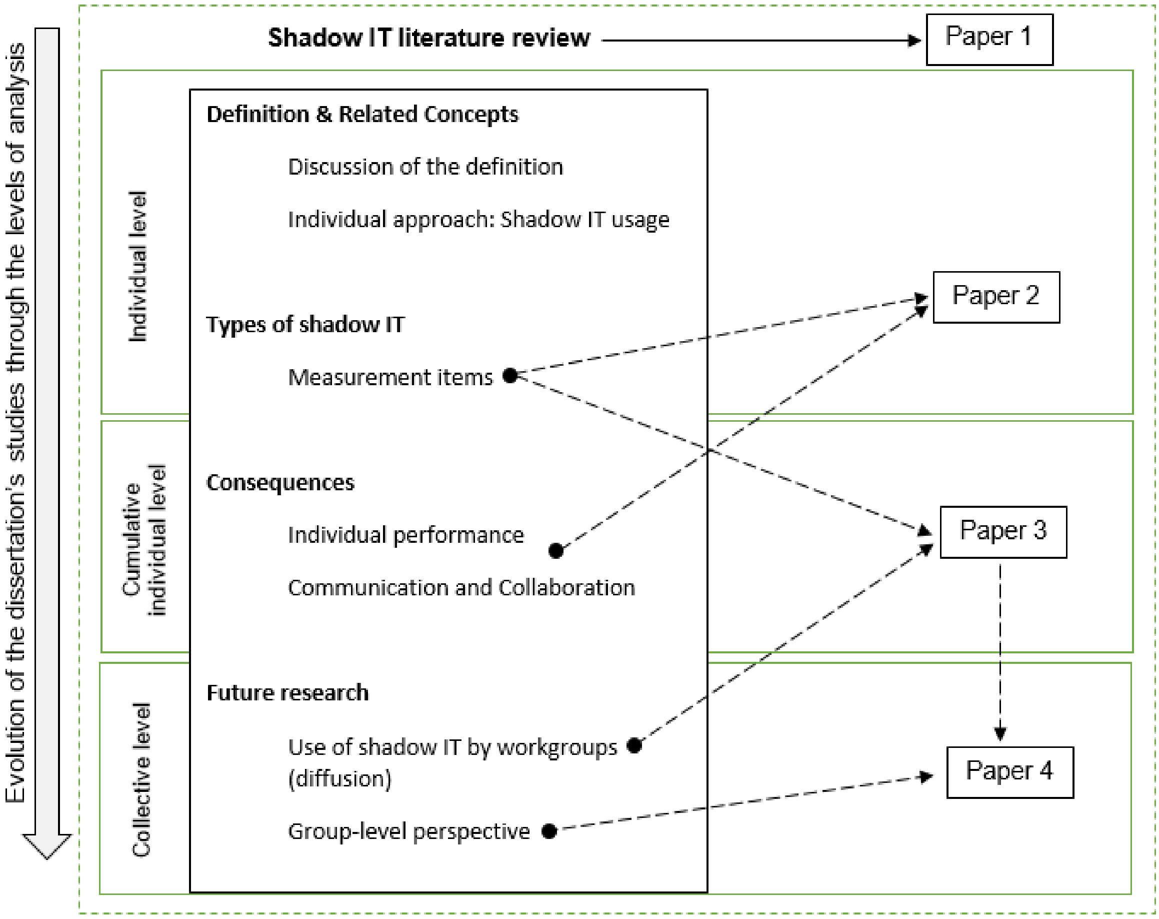
Zucker, L.G., 1977. The role of institutionalization in cultural persistence. American sociological review, pp.726-743.

8 GENERAL DISCUSSION AND CONCLUSIONS

This chapter provides a general discussion of the doctoral dissertation, including the implications for theory and practice, as well as limitations and suggestions for future research. The overall purpose of this dissertation was to investigate the antecedents and consequences of the deviant behavior of using shadow IT considering a multi-level perspective and its different facets. To achieve this purpose, four studies were developed addressing different aspects related to the general objective.

Figure 8 presents an overview of the papers resulted from the dissertation's studies, and how they evolved by level of analysis. The figure also illustrates how the studies interrelate and complement each other. Below, the findings and contributions of each study and the evolution of the dissertation are detailed.

Figure 8 – Multi-level Investigation of Deviant Behavior in IS


Evolution of the dissertation's studies through the levels of analysis
Shadow IT literature review
Paper 1
Individual level
Cumulative individual level
Collective level
Definition & Related Concepts
Discussion of the definition
Individual approach: Shadow IT usage
Types of shadow IT
Measurement items
Consequences
Individual performance
Communication and Collaboration
Future research
Use of shadow IT by workgroups (diffusion)
Group-level perspective
Paper 2
Paper 3
Paper 4

Source: Prepared by the author

8.1 Findings of the Studies

8.1.1 Literature Review on Shadow IT

The first step was to perform a literature review on the definition, related concepts and consequences of the deviant behavior that is the focus of this dissertation, the so-called shadow IT. A literature review on the subject is an important step to advance the knowledge (Webster & Watson, 2002), mainly considering that shadow IT can be considered an underexplored topic in the IS literature (e.g., Silic et al., 2017; Haag et al., 2019).

This study gave rise to the first paper and provided some insights into the next papers that compose the dissertation. First, it is discussed the definitions of shadow IT found in the literature. In the last years, the research on shadow IT has changed the perspective to address the subject, emerging also different levels of analysis to understand the phenomenon. It was found that studies on shadow IT firstly focus on the organizational level, investigating ways of controlling and cope with its occurrences from the managers' perspective. Besides the organizational level, recent studies have approached the subject from an individual-level perspective. Those studies advanced the knowledge on shadow IT by considering it as employees’ behavior that deviates from norms but without the intention of harming the organization, which has been called shadow IT usage (Haag & Eckhardt, 2014). Based on a behavioral approach, studies have been interested in uncovering reasons and motivations that drive individuals to use unauthorized technology in the workplace.

It becomes important, then, to differentiate shadow IT from shadow IT usage, once the first term refers to the unauthorized technology itself, and the last the behavior or using the unauthorized technology to perform work tasks. In addition, it is important to differentiate and specify these two terms because the streams of literature that use only shadow IT focus on the organizational level, while studies on shadow IT usage focus on the individual level to understand employees’ behavior. From this analysis of the definitions and the level of analysis, it was taken the definition of shadow IT usage proposed by Haag and Eckhardt (2014) to be used in the next studies at the individual and cumulative individual level to understand employees’ behavior (papers 2 and 3).

Similarly, there is still confusion among scholars about the definition of shadow IT and similar concepts. The first study extended the discussion of Haag and Eckhardt (2017) by discussing the differences and relations between shadow IT usage and workaround, BYOD, IT consumerization, and cloud-based services. This discussion was helpful to define shadow IT usage and its types used in the next studies.

Paper 1 also brings a discussion on the consequences of shadow IT, which is a complex and unanswered question due to the multiple facets of the subject that can provide positive and negative consequences to individuals and organizations. In this regard, the study highlights some benefits of using shadow found in the literature, such as performance improvements and better collaboration and communication at work. Although security issues are a large concern related to the use of shadow IT, the positive benefits should not be neglected (e.g., Galperin, 2012; Haag & Eckhardt, 2017). This result motivates the next study of the dissertation, paper 2, which aimed to investigate the relationship of shadow IT and individual performance through the lens of social presence theory.

Finally, paper 1 presents some suggestions for future research. In line with Haag and Eckhardt (2017), it was not found any research that addresses the use of shadow IT at the collective level of analysis. Considering the spreading of shadow IT usage among members of teams and departments, paper 1 reinforces the need for further research at group-level to understand the use of shadow IT within workgroups. This last finding served as the main motivation for paper 3 and paper 4 to investigate deviant behavior beyond the individual level of analysis.

8.1.2 Examining some Positive Consequences of Shadow IT Usage

Paper 2 provides an examination, at the individual level, of two positive consequences of shadow IT usage (individual performance and workplace collaboration) based on social presence theory. Some findings from the literature review on shadow IT (paper 1) served as the basis for the second study of this dissertation. First, workplace deviant behavior as shadow IT usage is a multifaceted phenomenon, which means that it can present functional characteristics that can bring benefits to users, besides the negative outcomes (Galperin, 2012; Furstenau & Rothe, 2014; Jetten & Hornsey, 2014). In that sense, an examination of potential positive consequences of using shadow IT is also necessary to manage it efficiently (Haag & Eckhardt, 2017), mainly because the consequences of such deviance remain unclear (Haag et al., 2019). Second, previous studies have identified that shadow IT can facilitate technology-mediated communication and collaboration to perform work tasks (e.g., Shumarova & Swatman, 2008; Silic & Back, 2014), which ultimately may improve employees performance (e.g., Haag et al., 2015).

Then, the general purpose of paper 2 is to examine the mediating role of social presence on the relationship between shadow IT usage and individual performance. The study has based the analysis on social presence theory (SPT) because it is a theory that seeks to explain how users select communication channels, suggesting that solutions differ in terms of their capability to transmit the signals that create user-awareness of other social actors (Short, Williams, & Christie 1976).

In line with individual-level studies (e.g., Haag et al., 2015), paper 2 adopts the definition of shadow IT usage proposed by Haag and Eckhardt (2014) mentioned before. Shadow IT usage is defined as voluntary use of any IT resource that infringes IT norms in the workplace, such as IS security policies, as a reaction to perceived situational constraints, aiming to enhance work performance (Haag & Eckhardt, 2014).

Paper 2 provides empirical evidence to show that shadow IT usage is positively related to employees' performance, and social presence plays a mediating role in the relationship between shadow IT usage and individual performance. The results are consistent with previous studies (e.g., Haag & Eckhardt, 2014; Haag et al., 2015; Haag et al., 2019), showing that, from the employees perspective, using shadow IT allows faster problem solving and more efficient tasks execution, increasing individual productivity consequently.

The findings of the second study also suggest that shadow IT usage is positively related to perceived social presence, which aids to understand why employees frequently use unauthorized technology to communicate and collaborate in the workplace (e.g., Shumarova & Swatman, 2008; Silic & Back, 2014; Mallmann et al., 2016). The dependence on technology to interact socially is increasing, especially among digital natives (Turkle, 2011; Turner, 2015), including in the workplace (Yoo & Alavi, 2001). This context gives rise to the need for understanding employees' behavior toward the use of technology for collaboration and communication. Thereby, the empirical support for the use of shadow IT as a way of positively affect perceived social presence brings some important insights. First, employees’ use of unauthorized technology to communicate and collaborate at work, which is in line with previous studies (e.g., Shumarova & Swatman, 2008; Silic & Back, 2014; Mallmann et al., 2016), suggests that the mandatory solutions provided by the organization for these purposes are not meeting employees' needs. Previous studies (e.g., Mallmann et al., 2016) have found that many companies still use email as the main form of communication among employees, not providing any official solution for instant communication and sharing of content. This represents a challenge for many employees that have to communicate constantly with coworkers, external patterns, and clients to execute their tasks (Mallmann et al., 2016). Thereby, the second insight of the above-referred relationship is that employees' work demands are oftentimes unknown or ignored by organizations and, consequently, they are not being fulfilled by the organizational official solutions. Employees, then, deviate from norms using unauthorized technology that aids them to communicate and collaborate with the aim of efficiently perform their work, such as WhatsApp, Dropbox, Google Drive tools, etc.

Therefore, the use of unauthorized collaborative tools and the resources they provide (e.g., instant messengers, video calls, voice messages, emoji, easy sharing of files) can enable instant communication and better collaboration by increasing perceived social presence, which ultimately drives gains in individual performance. Specifically about the elements of social presence, shadow IT usage enhances sensitivity in computer-mediated communication, which means that shadow IT can allow people to communicate their emotions better by using visual aids, such as emoji, pictures, and video, increasing the conversation quality and flow (e.g., Shin, 2018). Similarly, the findings also show that employees believe they can be more easily understood and better understand others when using shadow IT to communicate at work. Thereby, sensitivity and comprehension represent relevant aspects of social presence provided by shadow IT usage, which also provides the users an enhanced quality of communication due to the possibility of transmitting information through nonverbal cues in addition to verbal means (e.g. Biocca & Harms, 2002).

8.1.3 Antecedents of the Diffusion of Shadow IT Usage

The third study of the dissertation developed a quantitative study to investigate what drives the use of shadow IT among individuals. This is based on pieces of evidence provided by the literature (paper 1) that suggest shadow IT may be adopted and used by individuals, workgroups or whole business units to perform work tasks (e.g., Zimmermann & Rentrop, 2014; Mallmann et al., 2016; Fürstenau et al., 2017). Thereby, the use of shadow IT may disseminate among employees within a company, emerging the need for research that goes beyond the individual level of analysis.

Paper 3 takes a social influence perspective to investigate the diffusion process of shadow IT usage among employees. Social influence perspective allows capturing the cumulative individual effect of the interpersonal influences on individual behavior (e.g., Karahanna et al., 1999). Therefore, the study uncovers some reasons why shadow IT usage diffuses from one individual to another, spreading to a whole group of people.

The results show that employees are strongly influenced by their peers and by a mass of people, in general, to use shadow IT. The influence may come from co-workers, professional work-mates, and employees from other departments, suggesting a broader range of social influence that can affect the individual. This result in line with the theoretical concept of network externalities, which states that the value of a network increases with the square of its number of users (Hsu & Lu, 2004). Therefore, results are consistent with previous studies (e.g., Sun, 2013) that suggest the more individuals adopt a particular technology, the higher the perceived value of the technology and stronger the influence of others.

This result is also in line with criminology literature. Although paper 3 examines the cumulative individual level of using shadow IT, it takes into account the collective use of shadow IT by seeking the reasons for its diffusion among individuals, causing the spreading within teams and departments. There is a strong foundation in the literature that suggests peers are considerably important for deviant behavior (e.g., McGloin & Thomas, 2016; Boman & Mowen, 2018). Previous studies on collective action and deviance (e.g., Granovetter, 1978; McGloin & Thomas, 2016) suggest that an individual's decision to engage in a collective action depends, in part, on how many others participate in that action. Therefore, individuals are influenced by their peers to use shadow IT, as well as by the perception that many people (mass influence) are performing work tasks using unauthorized solutions. One explanation for the peer and mass influence is that the subjective perceptions regarding rewards, informal social costs, and sanction risks of using shadow IT vary under group conditions, such as how many others are engaging in the same action (McGloin & Thomas 2016). By seeing others using shadow IT, individuals may have a perception that the risk of formal sanction from the IT department decreases, while the rewards of following others (e.g., social approval) or the informal social costs of not following the group behavior (e.g., exclusion) increase. This group context will be better explored in the next study (paper 4).

Results from paper 3 also suggest that superior influence did not appear to be a source of social influence on individual shadow IT usage, which is in line with previous studies in IS (e.g., Wang et al., 2013). However, literature on social psychology and criminology has found that higher-status positions have a greater influence on deviant behavior because positions such as leaders can impact employee's attitudes and performance (Younts, 2008; Brown & Treviño, 2006). An important difference in this regard is how superior influence is exerted in a scenario of unauthorized technology use, instead of mandatory technology use. Jetten and Hornsey (2014) argue that norms are more nuanced for leaders, which can give to them the power of questioning established norms and introduce some innovations. Also, it is important to take into account that many employees that engage in the deviance of using shadow IT are not fully aware of the deviation from norms or the risks it can incur to them or the organization, mainly when the superior endorsed somehow the deviant behavior.

Within the context of using shadow IT, one possible explanation for the superior influence is that he/she is more concerned about performance than following the organizational IT norms. The superior’s expectancy is that employees efficiently perform work tasks and maintain satisfactory individual performance. In the communication and social interactions between the superior and employees, the sublunary message understood by the user may be: “keep high performance whatever the technology you use”. From this perspective, it is reasonable to infer that employees may not be worried about punishments for not using the mandatory system. Rather, their concern can be related to the rewards and punishments of achieving or not the performance expectancy. In that sense, superiors can influence employees toward shadow IT usage in an indirect way. Considering the complexity resulting from social dynamics, the role of the superior in the deviant behavior of using unauthorized technology, mainly in a workgroup context, should be better analyzed in future studies, which is discussed later.

8.1.4 Shadow IT Usage as an Instance of Collective IS Deviance

The fourth paper of this dissertation developed a qualitative and exploratory study to investigate the group-level of deviant behavior in IS. This study is based on some premises raised by papers 1 and 3. The literature review on shadow IT (paper 1) pointed out the use of shadow IT by teams and whole departments. In addition, it was not found any study in IS that investigate the subject as a group-phenomenon, emerging the need for further studies on shadow IT at the collective level. In turn, the study at the cumulative individual level (paper 3) was the first attempt to understand how the use of shadow IT diffuses among individuals. Results from paper 3 mentioned before suggest several social dynamics that drive the spreading of shadow IT usage among individuals within and between workgroups. Thereby, paper 4 has the objective of investigating the mechanisms behind deviant behavior at the collective level, uncovering why and how shadow IT usage diffuses among individuals within workgroups.

To perform this study, it was adopted the literature in social psychology and criminology, which consider deviance as a group-phenomenon naming it collective deviance (e.g., Gardner & Steinberg, 2005; McGloin & Thomas, 2016). In management and especially in the IS field, studies on deviance at the collective level are scarce (Zhang et al., 2015). There are recent calls for research that claim additional insights about IS policy violation and compliance by examining deviant behaviors in IS within the social context of workgroups, suggesting the collective-level as a supplement to individual-level explanations (e.g., Robinson & O’Leary-Kelly, 1998; Warkentin & Willison, 2009; Johnston et al., 2019). Paper 4, then, aimed to fill this void and break new ground in workplace deviance at the collective level, investigating the use of shadow IT by workgroups as an instance of collective IS deviance.

Following the guidelines of grounded theory (Corbin & Strauss, 2015), empirical data show that not only the diffusion of deviance occurs but also the proliferation of the deviant act among members continues indefinitely overtime in an uninterrupted way despite changes in group size and membership, turning it into part of the group culture. Ultimately, the deviant act becomes normalized. It was proposed then a process model to describe the mechanisms and components that allow the normalization of the deviant behavior within groups.

The empirical data from the interviews, thus, suggest a normalization process. The normalization perspective refers to the explanation of how deviant behavior becomes embedded in the workgroup, enacted mindlessly and perpetuated over time (Ashforth & Anand, 2003; Earle et al., 2010). The three pillars of normalization suggested by Ashforth and Anand (2003), which are institutionalization, rationalization, and socialization, are present along the process-oriented model of collective IS deviance. The model of collective IS deviance, which is the main result of study four, is a process model to explain the mechanisms and dynamics that drive the diffusion of deviance (the use of unauthorized technology) among workgroup members over time and, ultimately, the normalization of the deviant act.

In line with the normalization framework (Ashforth & Anand, 2003), institutionalization makes the deviant behavior of using an authorized technology to become embedded in the structure and processes of the workgroup and, consequently, a routinized practice that later will become a habit. Rationalization refers to the process of developing self-serving justifications by group members to justify and valorize the use of deviant technology. At last, socialization is the process responsible for inducing newcomers to engage in the deviant practice by providing to the members a perception that the deviant technology is not only permissible but also desirable. Because the three pillars are processes that mutually reinforce each other and are reciprocal interdependent (Ashforth & Anand, 2003; Earle et al., 2010), the collective IS deviance model is a process based on processes that serve as a theoretical ground to explain the phenomenon. That means that the institutionalization, rationalization, and socialization occur, to some extent, along the whole process of normalization of collective IS deviance.

For example, the components of the first mechanism of the collective IS deviance process (Dissemination) are perceived benefits, group-world-of-mouth, and low technical barriers. Perceived benefits, which are the advantages of the deviant technology perceived by meeting the work demands, add the embeddedness of the deviant technology in the work process of the whole group because of task interdependency and the commitment to common goals of the members. Thereby, the benefits of the deviant technology are perceived by all members, who start to use the tool regularly to perform work tasks, embedding the tool in the process. This, consequently, aids to trigger the process of institutionalization. Also, perceived benefits aid to trigger the process of rationalization because members use this perception as a self-serving justification to argue that the use of the unauthorized technology is fair and good because it brings benefits to work, such as it aids to execute tasks quickly. Similarly, low barriers to adopt and use deviant technology also can be used as a justification because members argue that there is no risk in using the unauthorized tool because no formal permission is needed to install and use it. Finally, the socialization process is triggered by the component group-world-of-mouth, which is the informal communication among members to instigate the deviance and diffuse it within the group, giving the perception that it is the desirable behavior to the members.

The aforementioned example shows how the first components that trigger the first mechanism of the process of collective IS deviance relate with the three pillars of normalization. The components of the subsequent mechanisms (internalization, maintenance, cultural persistence) follow the same logic of mutual and interdependent reinforcement (Ashforth & Anand, 2003; Earle et al., 2010), increasing in power over time. For example, the components of the mechanism called cultural persistence are habit, cultural transmission, and group identity. The institutionalization is high at this stage because of the long existence of the deviant practice, which is now a habit that is routinized in the processes and structure of the group (e.g., Zucker, 1977). Rationalization occurs by members saying that the deviant act has been part of the group for a long time and it has been passed through group generations over the years, therefore it is valid and legit. Also, it was passed from superiors to members in some cases, aiding to reinforce the idea and narrative of legitimacy. In turn, the members develop a group identity that is based on group norms and goals, in which the deviant practice takes part. This creates a strong environment to easily socialize new members to follow group norms and expectations. In sum, the examples show how the mechanisms and components trigger and develop the three pillars, which create a situation where the deviant act is practiced collectively by group members and may perpetuate indefinitely by turning the deviance into a normalized practice (Ashforth & Anand, 2003).

It is important to mention that the model of collective IS deviance gives special emphasis to the role of institutionalization because the literature suggests a positive relationship between degrees of institutionalization and cultural persistence (Zucker, 1977). The empirical data show that, ultimately, the deviant act of using the unauthorized technology persists within the group as part of the group subculture. The finding is consistent with Zucker (1977) that suggests that higher the degree of institutionalization of the deviant act, higher the uniformity of cultural understandings between group generations, leading to the maintenance of these understandings, and, consequently, larger the resistance of changing these understandings. The high degree of institutionalization, thus, plays an important role in perpetuating the deviant act within the group for generations. In addition, to high institutionalized acts, transmission is enough to perpetuate the deviance, that is, it is sufficient for one member simply to tell another that the work is done using the deviant tool as a matter of fact (Zucker, 1977). This means that the transmission of the deviance between members and group generations occurs organically because the mechanism and components at this stage (e.g., habits or cultural transmission) are as subtle that the group pressure is not noted anymore. This is because a high degree of institutionalization makes less likely the necessity of sanctions and direct social control for maintenance of deviant practices (Zucker, 1977).

Together with the normalization perspective, the intragroup perspective allowed some interesting findings. To understand group dynamics regarding the deviant act, it is necessary to understand the members' relationship with the norms developed by the group. The intragroup perspective allows this understanding by defining deviance as "any behavior or expression of an opinion or idea that is intentionally or unintentionally different from other group members' behaviors or opinions" (Heerdink et al., 2013). Therefore, it is related to the violation of norms of a group (Jetten & Hornsey, 2014), which in many cases differ from the organizational norms, like in the case of using an unauthorized technology.

As shown by the collective IS deviance model, the adoption and use of unauthorized technology become normalized because it is included in the range of norms of the group, becoming legit to the group members. Within this context, the behavior of the members is evaluated in terms of the group norms. Consequently, those that resist or deny following the group norms may suffer some consequences, such as exclusion, disapproval, and lack of trust. Those results are in line with subjective group dynamics model (Marques et al., 1998; Marques et al., 2001; Ditrich & Sassenberg, 2016), which focuses on the function of norms as a basis for the perceived validity and legitimacy of the group members and serve the regulation of the in-group. According to the model, members are motivated to maintain a psychological representation of a cohesive, well-defined, and normatively legitimated group (Marques et al., 2001). This motivation drives members to follow prescriptive norms without questioning and apply some forms of social control like punishments (e.g., disapproval or exclusion) to those that deviant from group norms, mainly at the early stages of the normalization process when the institutionalization is low.

The negative evaluations of deviant group members to maintain a sense of legitimacy within the group also aids to preserve a positive sense of social identity (Marques et al., 2001; Bown & Abrams, 2003), which was a component identified at the last stage of the collective IS deviance model. Social identity approach proposes that, in a group context, the meaning of one's identity is a result of membership in a social group (Hogg et al. 1995), resulting also in the predominance of social identity over personal identity (Turner et al, 1987). Thus, members that deviant from group norms threaten the collective identities of nondeviant members (Marques et al., 2001). Consequently, members apply forms of social controlling, such as punishments and rewards, as ways of reestablishing the positive social identity of the members (Camiera & Ribeiro, 2014).

8.2 Theoretical and Practical Implications

8.2.1 Theoretical Implications

This dissertation provides some empirical, conceptual, and theoretical contributions to management research in general and IS research in particular. First, it provides theoretical contributions to the emerging body of knowledge regarding shadow IT usage. Shadow IT is not a recent phenomenon. However, it is still under-studied in IS literature (Silic, 2019; Haag et al., 2019). This dissertation contributes to expanding theoretical knowledge on shadow IT usage at the individual level of analysis by performing empirical investigations on the antecedents of shadow IT usage.

Moreover, it contributes to the discussion on the consequences of shadow IT by empirically investigating with employees some positive consequences of using unauthorized technology to perform work tasks.

As aforementioned, shadow IT usage can be addressed as an individual or a group level phenomenon. This multi-level perspective demands further investigation, including a group-level approach in addition to the individual level to understand how workgroups collectively support shadow IT usage and what are the negative and positive consequences for the group (Haag & Eckhardt, 2017). Thereby, this dissertation brings contributions to understand how individual shadow IT usage spreads among employees within organizations. Moreover, this study uncovered, based on a group level perspective, some reasons why employees use shadow IT in the workplace, as well as the mechanisms that underlie the diffusion process among employees, driving the use of shadow IT within workgroups, teams, and in others departments inside organizations.

In a similar vein, this dissertation also provides implications for adoption and post-adoption research by analyzing usage and diffusion of unauthorized technology. The examination of post-adoption stages is important to comprehend the phenomenon under analysis because employees do not only adopt shadow IT but also use it frequently to perform work tasks. Besides, the use of shadow IT diffuses among employees, raising the need for understanding how and why it spreads from one individual to a whole group of employees. Therefore, this dissertation provides contributions to adoption and post-adoption research uncovering employee’s motivations to adopt, use, and diffuse shadow IT in the workplace.

It also provides implications for IS police violations and security research. This dissertation addressed shadow IT as collective deviance, that is, several individuals in a group, team, or department violating organizational IS policies by using shadow IT in the workplace. To the best of our knowledge, this research is the first to investigate IS-related deviance as a group phenomenon. To incorporate new theoretical foundations and expand our horizons, this dissertation relies on collective deviance literature from social psychology and criminology to explain workplace deviance in the IS context, as suggested by Warkentin and Willison (2009). By doing so, it provides further insights into employees’ behavior regarding IS policy non-compliance, specifically explaining reasons why members of workgroups deviate from IS policies.

A better understanding of deviant behavior of employees within organizations can aid to cope with IS policy violations, providing new insights into policy development and strategies to mitigate such behaviors and increase information security.

This dissertation also may have interesting contributions for deviance literature, especially to the growing body of research on workplace deviance by addressing it as a group-level phenomenon. Although deviance frequently occurs within and by groups (e.g., Gardner & Steinberg, 2005; McGloin & Thomas, 2016), most research on deviant behavior has focused exclusively on the individual-level (Robinson & O'Leary-Kelly, 1998; Schabram et al., 2018). In that sense, this dissertation provides conceptual contribution by conceptualizing the phenomenon at the collective level, as well as by describing and explaining it inside of workplace context, specifically IS oriented.

It was not found any previous studies that adopt a normalization perspective to understand deviant behavior within workgroups in the IS domain. Consequently, this dissertation provides interesting insights by theorizing on collective deviance from a normalization perspective in the IS context. A normalization perspective allowed including meanings and contexts of workgroups in the analysis (e.g., Earle et al., 2010), taking into account a richer social dimension for understanding how and why deviant acts diffuse and perpetuate within workgroups. Furthermore, a normalization perspective aids to comprehend why a certain act, such as using an unauthorized technology, may be deviant from one perspective (e.g., organizational IS security polices) and from another (intragroup perspective) the act is not recognized as deviant, but as a normal practice (Pinto, 2014). This change in perspectives can influence the effectiveness of IS security policies and strategies, therefore it is important to be considered.

8.2.2 Practical Implications

This dissertation also provides practical implications for managers and organizations. First, organizations must be aware that shadow IT is a behavioral phenomenon that emerges from the employee's level. Keeping that in mind, managers should better understand employees' behavior related to the use of technology in order to cope with shadow IT. Thus, insights into what drives individuals toward shadow IT usage can aid managers to develop IT strategies and security policies to manage its occurrences. Similarly, managers must pay attention to the fact that the main reason for the emergence of shadow IT is the lack of proper IT solutions that meet employees' work demands (e.g., Haag & Eckhardt, 2014; Walterbusch et al., 2017). Therefore, knowing the motivations of employees to use shadow IT usage is also a good opportunity for IT managers to understand users' expectations and their needs related to technology. In doing so, organizations can provide suitable technologies to perform work tasks, preventing employees of autonomously adopt solutions.

Second, the literature on shadow IT discuss a wide range of consequences, from performance improvements and innovative solutions to security risks and compliance. The results of this dissertation reinforced the fact that the outcomes of shadow IT usage can be several and different ones. Therefore, balancing the positive and negatives outcomes of shadow IT is another challenge for IT managers. In that sense, managers can consider that, better than only avoid the use of shadow IT, organizations could find ways to mitigate the risks while recognizing the opportunities for improvements provided by it.

Specifically, this dissertation shows that shadow IT usage can facilitate collaboration and communication, which represent potential positive consequences of using shadow IT. In digitalized and globalized companies nowadays, technology is the primary way of interactions. Considering that many work tasks rely on communication among internal and external parts to be done, managers should be aware of communication needs of employees in order to offer suitable tools. Synchronous conversational media, such as instant messaging or chat, allows a better flow of conversation and motivates people to reply quickly, providing agility to execute tasks that relies on collaboration (e.g., Shumarova & Swatman, 2008; Shin, 2018). The study on social presence and shadow IT usage shows that employees value resources that improve image quality and provide a better conversation flow, such as video, audio, pictures, and emoji. Therefore, organizations that still use email as the formal way of communication should pay attention to employees' demands as a way to provide better tools. This insight can be helpful to balance the outcomes of shadow IT because by providing a proper tool, organizations may reduce the use of unauthorized technology while ensuring employees' productivity and diminishing security risks.

Third, it is also crucial for organizations to understand social mechanisms and collective action within companies, as well as how it occurs and affects individuals and group behavior regarding the violation of IS policies. Frequently, problems regarding workplace deviant behavior like shadow IT are caused by a deficient communication of IT policies among employees, who are not aware of the recommended security practices and the risks of violating them. Moreover, social dynamics, such as social influence among employees, can drive individuals and workgroups to violate IS policies, as shown by the studies three and four. In that sense, organizations must pay attention to create strategies and take actions to engage users in IS security initiatives, which is one of the primary concerns related to shadow IT usage.

Fourth, the diffusion of workplace deviant behavior can provide some challenges to managers because, as shown by study three, employees are exchanging ideas with people beyond their immediate group. For instance, employees have to communicate and interact frequently with workmates, partners, and clients geographically distributed, who also may exert an influence on their behavior regarding the technology they use to perform work. It represents a broader range of social influence employees may experience, increasing the complexity of managing all possible tools employees get in touch with and adopt on their own. To give a more concrete example, an employee can find out a solution to perform tasks faster than using the mandatory solution and share the new finding with colleagues from his/her workgroup and from other units and departments who have to execute similar tasks. This context reinforces the importance of the IT department actively participating in the business, for example, by providing an effective communication channel to the units to motivate the employees of seeking the support of the IT department when having a demand related to technology.

Fifth and last, the results of this dissertation show that superiors, such as managers and team leaders, play an important role in mediating the relationship between the organization and the employees. A higher-level position holds power because its authority is legit from the organizational and from the group perspective. Therefore, superiors can influence not only the diffusion and persistence of deviance but they have also the power of doing the opposite, that is, change the course of the deviance. Organizations can profit from this information by engaging their leaders in better security practices to communicate with workgroups. For example, the superior may be an important figure in the gradual process of changing from an unauthorized solution to a homologated solution, introducing new practices into the group, managing conflicts, and mediating the communication between the group needs and the IT department.

8.3 Limitations and Suggestions for Future Research

This dissertation has limitations that can inform directions for future research. First, the studies are geographically limited to Brazil. The studies were conducted in Brazil with Brazilian subjects, which can represent a tendency in the results because of cultural reasons and, therefore, researchers should be careful in generalizing the results. This limitation calls for further investigations to test the findings and model applicability in different cultural settings. That is an important consideration because cultural settings play a significant role in understanding human behavior, mainly when considering individuals within groups. In addition, future research would contribute by extending the sample within a quantitative perspective in order to test the applicability of the collective IS deviance model and its mechanisms, allowing its generalization.

Second, the studies have focus on a very specific kind of IS workplace deviance (use of unauthorized technology at work). Thus, further research must use caution before applying the conclusions of this dissertation more generally to other deviant acts. In any case, it is expected that by highlighting the influence of workgroups context and dynamics on deviant behavior will encourage future research on collective deviance in the workplace, especially in the IS field to understand deviances related to IS policy violation, such as workaround behavior, and shadow IT usage within organizations (e.g., Warkentin & Willison, 2009; Haag & Eckhardt, 2017).

Third, this dissertation only examined some positive consequences of using shadow IT (communication, collaboration, and individual performance). The literature on shadow suggests other potential consequences. For example, the use of shadow IT can also be seen as innovative behavior that is constructive and valuable for the organization. Shadow IT usage can be beneficial by meeting individual needs and providing an opportunity for low-cost innovation and rapid response to changing business requirements (e.g., Silic & Back, 2014; Furstenau et al., 2017; Haag et al. 2015). Therefore, the analysis of other consequences of using unauthorized technology can bring contributions to understand the phenomenon.

Similarly, some authors have argued that there is a larger focus on the negative side of deviant behavior, leaving its functional nature underexplored (e.g., Spreitzer & Sonenshein 2004; Galperin 2012). The term deviance itself carries a bad connotation because the key element of deviance is norm-violation. Nonetheless, some studies on sociology and social psychology (e.g., Jetten & Hornsey 2014; Kim & Choi 2017) have open space to address the phenomenon from a more positive view by considering deviance as something that can provide beneficial outcomes. Studies that approach deviance from a positive side have called the phenomenon positive deviance, creative deviance, constructive deviance or pro-social rule-breaking (e.g., Warren 2003; Mainemelis 2010; Dahling et al. 2012; Mertens et al. 2016), suggesting different benefits to organizations such as creativity, organizational citizenship behavior, or prosocial behavior. Thus, researchers should consider the emergence of positive deviance as a way of boosting creativity and innovation, which can be even more relevant in a group setting. Research in this area has shown that, in groups, individuals are exposed to more ideas, larger pooling of information, and cognitive stimulation, which drive the development of creative ideas and aid to complex problem solving (Hill 1982; Paulus & Yang 2000; Kohn et al. 2011). However, group pressure to comply with norms, which can be either organizational norms or norms created and enforced by the group, can inhibit positive deviance (e.g., Kim & Choi, 2017). These pieces of information provide an overview of the complexity of understanding consequences of deviant behavior from a multi-level perspective. Therefore, further research in IS could take into account that different types of deviance can provide different impacts, also depending on the level of analysis, performing investigations on the role of positive or constructive deviance to individuals and workgroups within organizations.

Finally, the role of the superior in the employees' deviant behavior can be better explored to understand motivations, as well as come up with potential solutions to deviant occurrences within organizations. Findings from paper 3 suggest that superior influence does not have a direct positive relationship with individual shadow IT usage. However, paper 4 shows that superiors exert an important role in diffusing and normalization deviant behavior because a higher status position has a formal hierarchical power from the organization and informal from the group perspective for being considered part of the group. This result suggests that superiors have a mediating role between demands and norms from the organization and the ones from the workgroup. Previous studies in criminology and social psychology (e.g., Brown & Treviño, 2006; Younts, 2008) have suggested that superior may influence employee's behavior toward deviance. This can represent a fruitful path for future research and a strategic aspect to organizations by understanding how managers of business units are aligned with the organizational IT department, and vice versa, in terms of goals and norms. Moreover, researchers and organizations can consider superior's influence on workplace deviant behavior to develop strategic measures, such as leadership training programs (Brown & Treviño, 2006), to cope with IS policy violation and compliance.

REFERENCES

Ashforth, B. E., & Anand, V. (2003). The normalization of corruption in organizations. *Research in organizational behavior*, *25*, 1-52.

Aguilera, R. V., & Vadera, A. K. (2008). The dark side of authority: Antecedents, mechanisms, and outcomes of organizational corruption. *Journal of Business Ethics*, 77(4), 431-449.

Akers, R. L., Krohn, M. D., Lanza-Kaduce, L., & Radosevich, M. (1979). Social learning and deviant behavior: A specific test of a general theory. *American Sociological Review*, 44(4), 636-655.

Behrens, S., & Sedera, W. (2004). Why do shadow systems exist after an ERP implementation? Lessons from a case study. PACIS 2004 Proceedings, 136.

Biocca, F., & Harms, C. (2002). Defining and measuring social presence: Contribution to the networked minds theory and measure. *Proceedings of PRESENCE*, *2002*, 1-36.

Boman, J. H., & Mowen, T. J. (2019). Unpacking the role of conflict in peer relationships: Implications for peer deviance and crime. *Deviant behavior*, *40*(7), 882-895.

Brown, M. E., & Trevino, L. K. (2006). Socialized charismatic leadership, values congruence, and deviance in work groups. *Journal of Applied Psychology*, 91(4), 954.

Carter, M., & Grover, V. (2015). Me, my self, and I (T) conceptualizing information technology identity and its implications. *MIS Quarterly*, 39(4), 931-958.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90-101.

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.

Earle, J. S., Spicer, A., & Peter, K. S. (2010). The normalization of deviant organizational practices: Wage arrears in Russia, 1991–98. *Academy of Management Journal*, *53*(2), 218-237.

French, A. M., Guo, C., & Shim, J. P. (2014). Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems*, 35(1), 10.

Furstenau, D., & Rothe, H. (2014). Shadow IT systems: Discerning the good and the evil. In Proceedings of the Twenty-Second European Conference on Information Systems, Tel Aviv, Israel.

Furstenau, D., Rothe, H., & Sandner, M. (2017). Shadow systems, risk, and shifting power relations in organizations. *Communications of the Association for Information Systems*, 41(1), 3.

Gardner, M., & Steinberg, L. (2005). Peer influence on risk taking, risk preference, and risky decision making in adolescence and adulthood: an experimental study. *Developmental psychology*, 41(4), 625.

Galperin, B. L. (2012). Exploring the nomological network of workplace deviance: Developing and validating a measure of constructive deviance. *Journal of Applied Social Psychology*, 42(12), 2988-3025.

Granovetter, M. (1978). Threshold models of collective behavior. *American Journal of Sociology*, 83(6), 1420-1443.

Györy, A., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the shadows: IT governance approaches to user-driven innovation. European Conference on Information Systems (ECIS2012) Proceedings. Paper 222.

Haag, S., & Eckhardt, A. (2014). Normalizing the shadows–The role of symbolic models for individuals' shadow IT usage. In Thirty Fifth International Conference on Information Systems (ICIS) Proceedings, Auckland.

Haag, S., Eckhardt, A., & Bozoyan, C. (2015). Are shadow system users the better IS users?–insights of a lab experiment. In Thirty Sixth International Conference on Information Systems (ICIS) Proceedings, Fort Worth.

Haag, S., & Eckhardt, A. (2017). Shadow it. *Business & Information Systems Engineering*, 59(6), 469-473.

Haag, S., Eckhardt, A., & Schwarz, A. (2019). The Acceptance of Justifications among Shadow IT Users and Nonusers–An Empirical Analysis. *Information & Management*, 56(5), 731-741.

Harris, J., Ives, B., & Junglas, I. (2012). IT consumerization: When gadgets turn into enterprise IT tools. *MIS Quarterly Executive*, 11(3).

Heerdink, M. W., Van Kleef, G. A., Homan, A. C., & Fischer, A. H. (2013). On the social influence of emotions in groups: interpersonal effects of anger and happiness on conformity versus deviance. *Journal of Personality and Social Psychology*, *105*(2), 262.

Hill, G. W. (1982). Group versus individual performance: Are N+ 1 heads better than one?. *Psychological Bulletin*, *91*(3), 517.

House, R. J., Rousseau, D. M., & Thomas-Hunt, M. (1995). The third paradigm: Meso organizational research comes to age. *Research in organizational behavior*, 17, 71-114.

Hsu, C. L., & Lu, H. P. (2004). Why do people play on-line games? An extended TAM with social influences and flow experience. *Information & management*, *41*(7), 853-868.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51(1), 69-79.

Jetten, J., & Hornsey, M. J. (2014). Deviance and dissent in groups. *Annual review of psychology*, 65, 461-485.

Johnston, A. C., Di Gangi, P. M., Howard, J., & Worrell, J. (2019). It Takes a Village: Understanding the Collective Security Efficacy of Employee Groups. *Journal of the Association for Information Systems*, 20(3), 186-212.

Jones, D., Behrens, S., Jamieson, K., & Tansley, E. (2004). The rise and fall of a shadow system: Lessons for enterprise system implementation. ACIS 2004 Proceedings, 96.

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly*, 183-213.

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective. *Information Systems Research*, 30(2), 687-704.

Kim, M. J., & Choi, J. N. (2018). Group identity and positive deviance in work groups. *The Journal of Social Psychology*, *158*(6), 730-743.

Klein, K. J., & Kozlowski, S. W. (2000). From micro to meso: Critical steps in conceptualizing and conducting multilevel research. *Organizational Research Methods*, 3(3), 211-236.

Kohn, N. W., Paulus, P. B., & Choi, Y. (2011). Building on the ideas of others: An examination of the idea combination process. *Journal of Experimental Social Psychology*, *47*(3), 554-561.

Laumer, S., Maier, C., & Weitzel, T. (2017). Information quality, user satisfaction, and the manifestation of workarounds: a qualitative and quantitative study of enterprise content management system users. *European Journal of Information Systems*, 26(4), 333-360.

Levit, A. (2018). 5 Shadow IT Statistics to Make You Reconsider Your Life. Available on https://www.quickbase.com/blog/5-shadow-it-statistics-to-make-you-reconsider-your-life

Mainemelis, C. (2010). Stealing fire: Creative deviance in the evolution of new ideas. *Academy of Management Review*, 35(4), 558-578.

Mallmann, G. L., Maçada, A. C. G., & Oliveira, M. (2016). Can Shadow IT Facilitate Knowledge Sharing in Organizations? An Exploratory Study. In European Conference on Knowledge Management (p. 550). Academic Conferences International Limited.

Marques, J., Abrams, D., Paez, D., & Martinez-Taboada, C. (1998). The role of categorization and in-group norms in judgments of groups and their members. *Journal of Personality and Social Psychology*, 75(4), 976.

Marques, J., Abrams, D., & Serôdio, R. G. (2001). Being better by being right: Subjective group dynamics and derogation of in-group deviants when generic norms are undermined. *Journal of Personality and Social Psychology*, 81(3), 436.

McGloin, J. M., & Povitsky Stickle, W. (2011). Influence or convenience? Disentangling peer influence and co-offending for chronic offenders. J*ournal of Research in Crime and Delinquency*, 48(3), 419-447.

McGloin, J. M., & Thomas, K. J. (2016). Incentives for collective deviance: Group size and changes in perceived risk, cost, and reward. *Criminology*, 54(3), 459-486.

Mertens, W., Recker, J., Kohlborn, T., & Kummer, T. F. (2016). A framework for the study of positive deviance in organizations. *Deviant Behavior*, 37(11), 1288-1307.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1).

Paulus, P. B., & Yang, H. C. (2000). Idea generation in groups: A basis for creativity in organizations. *Organizational behavior and human decision processes*, *82*(1), 76-87.

Pinto, J. K. (2014). Project management, governance, and the normalization of deviance. *International Journal of Project Management*, *32*(3), 376-387.

Raden, N. (2005). Shedding light on shadow IT: Is Excel running your business. DSSResources. com. Retrieved February, 26, 2005.

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

Robinson, S. L., & O'Leary-Kelly, A. M. (1998). Monkey see, monkey do: The influence of work groups on the antisocial behavior of employees. *Academy of Management Journal*, 41(6), 658-672.

Rogers, M., Smoak, N. D., & Liu, J. (2006). Self-reported deviant computer behavior: A big-5, moral choice, and manipulative exploitive behavior analysis. *Deviant Behavior*, 27(3), 245-268.

Shin, D. (2018). Empathy and embodied experience in virtual environment: To what extent can virtual reality stimulate empathy and embodied experience?. *Computers in Human Behavior*, *78*, 64-73.

Shumarova, E., & Swatman, P. A. (2008). Informal eCollaboration Channels: Shedding Light on" Shadow CIT". *BLED 2008 Proceedings*, 18.

Silic, M., & Back, A. (2014). Shadow IT–A view from behind the curtain. *Computers & Security*, 45, 274-283.

Sillic, M. (2019). Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the Shadow IT context. *Computers & Security*, 80, 108-119.

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & management*, 54(8), 1023-1037.

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

Short, J., Williams, E., & Christie, B. (1976). *The social psychology of telecommunications*. John Wiley & Sons.

Spreitzer, G. M., & Sonenshein, S. (2004). Toward the construct definition of positive deviance. *American Behavioral Scientist*, 47(6), 828-847.

Starke, J. (2016). The Shadow IT Dilemma. Available on https://blogs.cisco.com/cloud/the-shadow-it-dilemma

Sun, H. (2013). A longitudinal study of herd behavior in the adoption and continued use of technology. *MIS Quarterly*, 1013-1041.

Turner, J. C., Hogg, M. A., Oakes, P. J., Reicher, S. D., & Wetherell, M. S. (1987). Rediscovering the social group: A self-categorization theory. Basil Blackwell.

Turner, A. (2015). Generation Z: Technology and social interest. *The Journal of Individual Psychology*, *71*(2), 103-113.

Turkle, S. (2017). *Alone together: Why we expect more from technology and less from each other*. Hachette UK.

Van Akkeren, J., & Buckby, S. (2017). Perceptions on the causes of individual and fraudulent co-offending: Views of forensic accountants. *Journal of Business Ethics*, 146(2), 383-404.

Walters, R. (2013). Bringing IT out of the shadows. *Network Security*, 2013(4), 5-11.

Walterbusch, M., Fietz, A., & Teuteberg, F. (2017). Missing cloud security awareness: investigating risk exposure in shadow IT. *Journal of Enterprise Information Management*, 30(4), 644-665.

Wang, Y., Meister, D. B., & Gray, P. H. (2013). Social influence and knowledge management systems use: Evidence from panel data. *MIS Quarterly*, 299-313.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2), 101-105.

Warren, D. E. (2003). Constructive and destructive deviance in organizations. *Academy of management Review*, 28(4), 622-632.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, xiii-xxiii.

Wells, L. E. (1978). Theories of deviance and the self-concept. *Social psychology*, 189-204.

Yoo, Y., & Alavi, M. (2001). Media and group cohesion: Relative influences on social presence, task participation, and group consensus. *MIS Quarterly*, 371-390.

Yoo, Y., Goo, J., & Rao, H.R. (2020). Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness. MISQ Archivist. Forthcoming.

Younts, C. W. (2008). Status, endorsement and the legitimacy of deviance. *Social Forces*, 87(1), 561-590.

Zhang, H., Luo, X. R., Liao, Q., & Peng, L. (2015). Does IT team climate matter? An empirical study of the impact of co-workers and the Confucian work ethic on deviance behavior. *Information & management*, 52(6), 658-667.

Zimmermann, S., Rentrop, C., & Felden, C. (2016). Governing identified shadow IT by allocating IT task responsibilities. In Twenty-second Americas Conference on Information Systems Proceedings, San Diego.

Zimmermann, S., Rentrop, C., & Felden, C. (2017). A Multiple Case Study on the Nature and Management of Shadow Information Technology. *Journal of Information Systems*, 31 (1), 79-101.

Zucker, L. G. (1977). The role of institutionalization in cultural persistence. *American Sociological Review*, 726-743.

APPENDIX A – ITEMS SURVEY STUDY 3 (ENGLISH VERSION)

Questionnaire on the use of Shadow IT and Social Influence

This questionnaire will be used only for academic purposes and we ensure the confidentiality of the respondents. Please, to understand what we mean by "shadow IT", read this definition below. Thank you!

Shadow IT is any IT solution (software, applications, devices, etc.) used by employees to perform work tasks without the formal approval and support from the organizational IT department. Common examples of shadow IT are the use of WeTransfer, WhatsApp, Facebook, Dropbox, Google Drive without the formal permission of the organization.

Please, consider the shadow technologies you use to perform your work tasks and grade the statements below in a scale from 1 to 7, where 1 means "strongly disagree" and 7 "strongly agree".

Shadow IT usage items

SIT1: I use Internet-based software or cloud services that are unauthorized or unrecognized by the IT department. Examples of these systems are WhatsApp, Facebook, Google Sheets, Skype for Web, Dropbox, Google Docs, etc.

SIT2: I use a solution developed by me or another employee on the company's computers that is unauthorized or unrecognized by the IT department to perform my work tasks. Examples: any software developed by employees, such as a program to control and monitor information, collaborative tools, excel spreadsheets, etc.

SIT3: I use software installed by me or another employee on the company's computers that is unauthorized or unrecognized by the IT department to perform my work tasks. Examples can be any free download software (Pidgin, Skype) to communicate, share information, execute tasks, etc.

SIT4: I use my own devices at work without permission from the IT department, including applications on my mobile device on the company's network. For instance, Smartphone, tablets, notebook, etc.

Social Influence Perspective Items – (peer influence, superior influence, mass influence)

Peer Influence

SIF1: My coworkers have been telling me about the usefulness of using shadow IT at work.

SIF2: My co-workers often use shadow IT to perform work tasks.

SIF3: My co-workers often use shadow IT to communicate.

SIF4: In general, the colleagues in my team/department have supported the use of shadow IT at work.

Superior Influence

SIF5: The head of my team/department has supported the use of shadow IT to perform work tasks.

SIF6: My boss has been telling me about the usefulness of using shadow IT.

SIF7: In general, the head of my team/department has supported the use of Shadow IT at work.

Critical Mass

SIF8: Many people in my workgroup use shadow IT to perform work tasks.

SIF9: Colleagues from other teams/departments use shadow IT at work.

SIF10: Many people in my company use shadow IT to perform work tasks.

Do you hold a management position in the company, such as supervisor, manager, leader, director, or president?

Yes ( )

No ( )

APPENDIX B – SURVEY STUDY 3 (PORTUGUESE VERSION)

Questionário sobre uso de shadow IT e influência social

Este questionário será utilizado apenas para fins acadêmicos e a identidade dos respondentes será mentida em confidencialidade. Importante! Por favor, caso não conheça o termo "Shadow IT", leia esta definição abaixo. Muito obrigado!

Definição de Shadow IT: qualquer solução de TI (softwares, dispositivos, etc.) utilizada pelos funcionários para realizar as tarefas de trabalho sem a aprovação e sem o suporte formal do departamento de TI da empresa. São exemplos frequentes de Shadow IT: uso de WeTransfer, WhatsApp, Facebook, Dropbox, Google Apps sem autorização e suporte do departamento de TI.

Instruções básicas: considerando a definição acima, pense nas tecnologias shadow que você utiliza para realizar suas tarefas de trabalho e marque na escala de 1 a 7, onde 1 significa "discordo totalmente" e 7 "concordo totalmente", o quanto você concorda com as afirmações abaixo.

Uso de shadow IT

SIT1: Utilizo serviços de nuvem (SaaS) no trabalho, como softwares de comunicação e de compartilhamento de informação ou outros serviços de nuvem, para me comunicar e compartilhar informações de trabalho com meus colegas, ainda que sem a aprovação e o suporte formal do departamento de TI. Ex: Whatsapp, Facebook, Skype via web, Dropbox, Box, Google Apps, etc.

SIT2: Desenvolvo soluções (que não as disponibilizadas pela TI) nos dispositivos da empresa para realizar as minhas tarefas de trabalho, ainda que sem a aprovação e o suporte formal do departamento de TI. Ex: algum software desenvolvido pelos próprios funcionários para realizar suas tarefas de trabalho, ou uma planilha excel a parte do sistema oficial da empresa, etc.

SIT3: Instalo outros softwares, além dos disponibilizadas pela TI, nos dispositivos da empresa para realizar as minhas tarefas de trabalho, ainda que sem a aprovação e o suporte formal do departamento de TI. Ex: Um software disponível para download na internet de forma gratuita que, de alguma forma, auxilia nas atividades do trabalho.

SIT4: Utilizo dispositivos próprios para realizar as minhas tarefas de trabalho, ainda que sem a aprovação e o suporte formal do departamento de TI. Ex: smartphones, notebooks, tablets, HD externo, pen drives, etc.

Influência Social

Peer Influence

SIF1: Colegas de trabalho tem me falado sobre a utilidade de usar shadow IT no trabalho.

SIF2: Meus colegas de trabalho usam frequentemente shadow IT no trabalho.

SIF3: Meus colegas de trabalho frequentemente utilizam shadow IT para se comunicar.

SIF4: Em geral, os colegas da minha área/setor têm apoiado a utilização de shadow IT no trabalho.

Superior Influence

SIF5: O chefe da minha área/setor tem colaborado com o uso de shadow IT para realizar as tarefas de trabalho.

SIF6: Meu chefe tem me falado sobre a utilidade de usar shadow IT.

SIF7: Em geral, o chefe da minha área/setor tem apoiado a utilização de Shadow IT no trabalho.

Critical Mass

SIF8: Muitas pessoas no meu grupo de trabalho utilizam shadow IT para realizar as tarefas.

SIF9: Colegas de outros setores/departamentos utilizam shadow IT no trabalho.

SIF10: Muitas pessoas da minha empresa utilizam shadow IT para realizar as tarefas.

Você exerce um cargo de gestão na empresa, como Coordenador, Gerente, Diretor ou Presidente?

Sim ( )

Não ( )

APPENDIX C – INTERVIEW PROTOCOL STUDY 4

Interview guide – Use of technology within companies (Collective IS Deviance)

This is a study on the use of technology in the workplace. So, please think about your work and your daily tasks to answer the questions.

First Block – The deviance and its context

*** Company and department structure

1) When thinking about your work tasks, do the technologies you use help you to perform the tasks? How satisfied you are with the technology?

2) Do you have all technologies you need to perform your work? Is something missing or that could be better? If yes, what is missing…

What do you do?

… Deviance

3) Why do you use this technology?

4) Is this technology not provided by the organizational IT department? Is that not allowed?

Second Block – How the deviance is instigated and diffused

1) Who does start the idea of implement/use that technology?

2) How does it start?

3) How does the idea spread across the team/department?

4) Is there someone in the team/department that always comes up with some new or innovative ideas? Inventor/Instigator the idea vrs. Communicator vrs. Evaluator (one, some, all)

Third Block – The Role of IT department (end-user vrs. IT personnel) – profile of the IT department

1) Does the IT department know about this technology?

2) Did you talk to the IT department before implementing this technology?

3) Why the IT department does not provide this or another technology that is better for the team/department?

4) What does the IT department do regarding unauthorized technology? Do you think the IT department is rigorous with the rules? ...Information security…

Forth Blocks - Social vrs. Organizational Punishment

1) How do you see your relationship with your colleagues? Professional or also a friendship?

2) Did you have options when this technology was implemented? Did you have some alternatives?

4) Do you think you can be penalized because you are using this technology? By who?

5) Are you worried about punishments from the IT department or from the organization? If yes, what kind of punishments?

3) Do you think that if you refuse to use this technology your colleagues will disapprove you? If you refuse to use it can impact your image as professional/ colleague/ employee/ friend … (team vrs. department)

6) Do you feel more pressure from your team/department or from the organization/IT department/ rules?

7) If the IT department asks to change or abandon the technology, how would the group react?