IJDSEA
International Journal of Data Science Engineering, and Analytics

e-ISSN : 2807-1689
p-ISSN : 2798-9208

Navigating The Duality: Privacy And Security Concerns In Knowledge Management Systems (KMS)

Iswanda F. Satibi [1] and Ragil Tri Atmi [2]

[1] Department of Digital Business, UPN Veteran Jatim ; satibi.if@upnjatim.ac.id
[2] Department of Library and Information Science, Airlangga University; ragil.tri.atmi@fisip.unair.ac.id

Vol. 04, No 02, Page 1-14.
Received: 13 Nov 2024
Accepted: 19 Nov 2024
Published: 2 Dec 2024

Abstract: This study examines the relationship between privacy and security within Knowledge Management Systems (KMS). It identifies and analyzes distinct employee perceptions of these intertwined issues within a company's KMS environment. By exploring these perspectives, the authors aim to clarify the situation surrounding privacy and security in KMS settings. The research employed an explanatory sequential mixed method design. First, a questionnaire survey was distributed directly to KM staff across three companies. This was followed by semi-structured interviews with four KM staff members. The findings reveal a high level of employee awareness regarding the importance of KMS and, consequently, the significance of personal information privacy and security. The study further distinguishes between privacy and security concerns within KMS. Privacy concerns—spanning confidentiality, trust, and behavior—are primarily addressed at the organizational layer. Security aspects, on the other hand, are seen as aligned with the ICT layer, governed by legal frameworks and KMS architecture.

Keywords: 1; knowledge management system 2; privacy 3; security

1. Introduction

The rapid evolution of Information and Communication Technologies (ICT) in recent decades has disrupted traditional approaches to Knowledge Management (KM). These advancements have created an unprecedented platform for facilitating the efficient dissemination of data, information, and knowledge within organizational structures [1], [2], [3], [4]. In recognition of knowledge as the most valuable organizational resource, companies have increasingly sought to optimize knowledge extraction processes by aligning them with business strategies. This is often achieved through the implementation of complex information systems and robust ICT infrastructure [5]. This alignment fosters the development of a diverse array of competitive enterprise architectures that facilitate communication and collaboration within knowledge management (KM) practices [6], [7], [8]. Knowledge management systems (KMS) have emerged as a powerful metaphor for this new generation of ICT platforms. Within this context, KMS offers the potential to address the complexities of knowledge management by providing contextualized knowledge repositories within an organization's ICT environment. In essence, KMS platforms are increasingly recognized for their role in facilitating social interaction and knowledge sharing within organizations.

However, these overwhelming development of KMS brought some classic issues that have been proliferated in KM for many years. Surbakti (2015) found that both privacy and security issue are critical in KM practices [9]. Furthermore, it has traditionally been assumed that the privacy and security issues in KMS inline with research area in the information system and information technologies [10], [11], [12]. Thus, an unexpected consequence of these rapid development has been followed by the vary dimensions of privacy issue [13], [14] and complexity of ICT security in the organization [1], [15]. Surprisingly, this does not appear to be the case in the current KMS research although most research in this area has been investigated the personal information as an important domain of privacy issue. This is a serious shortcoming in KMS research because most research in this area have investigated the potential threats to individual and organizational privacy.

With the advance of ICT as a backdrop, the perspective about privacy has shifted from a predominant focus on commercial threats (e.g. [16], [17]) to a widely recognized as an important thing that deserve protection in the sphere of internet surveillance and national security [15], [18]. In this new landscape, it is rather difficult to explore privacy issues within organization. Matzner (2014) mentioned that most companies still have misconception about the term and the notion of privacy while adopting the ICT to support the business processes. In particular, issues of confidentiality and security, how and by whom the personal information is threatened by organizations are common themes in recent KMS research. This encompasses the potential distinction between a set of ICT environment and employees as individual in workplace or companies towards privacy issue in the recent KMS settings. Bertino et al. (2006) highlight the privacy and security are specific concern in digital environment along with confidentiality and trust [19].

Whilst previous studies have attempted to identify the different facet of privacy and security concern in the KM practices, most KMS research have focused on the simplistic notion of privacy through the lens of ICT layer associated with the strategic alignment of information system and IT infrastructure (e.g [5], [9], [20], [21]). Very few studies have ventured the employee's perspective and the dimension of privacy and security in KMS environment. Because of this breadth of scope, the alignment between KM stakeholders and privacy issue in order to assure sensitive personal information of individual in companies become a serious concern. Therefore, this study consider a more cohesive constructs of privacy that have been frequently investigated in the current research (e.g. [13], [22]), and the security constructs of KMS as one of emerging ICT adoption in the companies (e.g. [2], [11], [19]).

This study attempts to identify the distinct of privacy and security issues that are simultaneously operant in the KMS practices. Authors then explore how the individual perspective in the companies conceptualize these issues based on theoretical background in this topic. It is, therefore, this study are expressed in the following research question:

1. What are the distinct dimensions of privacy and security that can be identified by employee in the KMS setting at the companies?
2. How does the these dimension of privacy and security identified associated with the importance of employee's personal data protection in KMS practice.

The current study commences with a brief review of the literature on privacy and security issues in KMS. Then, the research methodology is then outlined and the findings of the analysis are

presented and discussed. This study concludes by noting the conceptual direction of privacy and security in KMS and the limitations of the current study as well as suggestions for future research.

2. Related Works

Today, the prevailing concepts of privacy and security are becoming increasingly important topics of research with many definitions and a complex dimensions. Prior studies have investigated the changing landscape of these issues in the digital age. From a classic point of view, the concept of privacy focused on protection of individual and mainly highlighted a right to be let alone [23]. From this, Charles Fried (1968) developed the notion of privacy, is not simply an absence of information about us in the minds of others; rather it is the control we have over the information about ourselves [24]. A clear distinct of privacy and new coming technologies specifically developed by Westin (1968) who conceptualize the prominence of privacy as the "right of informational self-determination" of individual for disclosure and interaction with environment conditions and social norms.

Matzner (2014) explored privacy in the context of "ubiquitous computing" and big data. The ubiquitous computing enable privacy threats for individual whose personal data are only indirectly involved and even for individual about whom no personal data have been collected and processed [12]. Recently, much of this concern is focused on privacy of personal information which proliferated by ICT infrastructure and the ease of data transmission in a virtual collaborative environment. In a virtual environment, there may be any number of formal and informal group which employed particular set of privacy concern that must be addressed, especially about the data protection and preservation of an individual entity's privacy [20].

Personal data may be perceived as not information privacy in the company, rather it is part of employment identity. Almost personal data captured in company's public space, interestingly, are based on contractual relations which is slightly different with the notion that privacy in public space mentioned in the prior literature [10], [25]. Thus, the term personal data and information privacy used interchangeably in this study. Wilton (2017) argued that the general perceptions of threats in digital privacy landscape "has shifted from a predominant focus on commercial threats to a recognition that government activities, in the sphere of intelligence and national security, also give rise to significant privacy risk" (p. 334). To date, the complexity of privacy has pushed the companies to enhance the expression capability for some complex notion, such as provisions and obligations.

2.1. Privacy and Security Issues in KMS

It seems difficult to transpose conceptual notion of privacy and security in the context of KMS in companies. There has been a common understanding that KMS is a public space which provide virtual collaborative environment in organization through a complex ICT infrastructure [1], [5]. Furthermore, KMS in many organizations has played an important role in order to increase organizational effectiveness [26]. It helps organizations to systematically capture, distribute, and transfer both explicit and tacit knowledge of individual in organizations through the rapid pace of ICT environment [27]. It is, therefore, the investigation of the very concept of privacy and security are derived with the vulnerability of personal information in both layers; organizational and ICT. According to Skinner et al. (2006), privacy in organizational emphasized the protection and preservation of an organization and its committed individual as employee. Therefore, the employee personal information must be treated appropriately according to different sphere of individual,

which raises particular scrutiny of personal information [28]. In addition, privacy issue related to employee is likely to arise in a KMS because its primary role is to organize both single-owner privacy information and multi-owner privacy information in the companies [17].

Within a given context of KMS, privacy issue might bring up substantial companies benefits, which at least challenges the notion of individual privacy concerns in the workplace. He, Qiao, & Wei, (2009) explored the dimensions of social relationship and its importance of a KMS usage for employee knowledge sharing by investigating the social relationship construct and its three dimensions; tie strength, shared norms, and trust [29]. Kristie Ball (2012) identified the dimension of employee privacy fro three distinct notion; the concern for personal information privacy, the concern for working environment privacy, and the concern for solitude privacy [13]. From this, privacy issue in KMS can be clearly understood by exploring the workplace and ICT environment in organization.

From the ICT layer, KMS refer to an information technology (IT) infrastructure with a complex architecture of information system developed by organizations to support knowledge management processes in a digital platform. It performs as a public sphere of collaborative environment for creating, managing, and sharing organization's knowledge. KMS, therefore, has its own set of privacy concern in regards to protect and preserve the personal information of members. Furthermore, privacy in companies are different from the general understanding of privacy [13]. In a public space, such as workplace in a company, personal data is not simply integrated with the public domain, vice versa. Bajpai and Weber (2017) have extrapolated the concept of privacy in the current digital landscape into new technological shape and to shape policy agendas [10]. In such digital landscape, A shared perception of privacy rights and limitations exists within the workplace, which common stock of privacy existed in the companies as a common place.

Another issue that has been emerged in the KMS is security. Prior studies showed the various approach of secure knowledge management. Bertino et al. (2006) wrote that maintaining security in KM processes is one of challenges because it utilize various aspects of security, such as confidentiality, trust, and privacy [19]. Within the growing interest towards ICT as major impetus for KMS settings, the layer of its technologies for secure data management and information management increasingly leverage the needs of sophisticated database, information system, semantic web, and data mining. Satapathy and Moharana (2017) reported that organization extensively adopted KM to to strengthen their information system [30]. It also reported that most organizations had poor KM policy and the employee are lacking proper security issue. However, employee may not seen KMS as company critical sector although it is important part of overall operation and management of the business processes [31], which highlighted the unique security risks posed by KMS practices [25]. Therefore, utilizing authentication and encryption should be considered in order to provide secure access towards confidential information, which might need very specific conduct or general conduct through general operating system of database features. In order to explore security issues in KMS practices, therefore, privacy issues must be considered from the beginning.

3. Research Method

This study examined the distinct of privacy and security issues in KMS at companies, and conceptualize these issues based on theoretical background. Thus, an explanatory sequential mixed

method research design was adopted. A purposive sampling was carried out to collect data for this study. The use of this sampling method was motivated by a wish to mitigate the possible obstacles that may occur regarding the company's confidentiality information and privacy issue, which is often viewed as a sensitive topic. As mentioned in previous studies, e.g. [22], [32], [33], conducting research in the field of privacy and security at companies was very difficult due to the highly potential lack of understanding in regards to confidentiality of information gained during the research. Out off 28 invitation letter and research proposal were sent to companies that operate KMS in East Java, only three of them accepted to join this research; PT. Semen Indonesia (PTSI) located in Gresik, PT. Perusahaan Listrik Negara (PLN) branch Surabaya, and Perusahaan Daerah Air Minum (PDAM) Surabaya. Invitation and data collection took place from May until September 2018. A questionnaire survey was administered by researcher personally handing to KM staff in three companies, followed by semi-structure interviews with four KM staff.

A set of questionnaire was developed based literature review. It was constructed by some questions about the basic demographic and employment information, one close-ended, a matrix question and two scaled questions. This study brought Daniel Solove's (2008) notion about privacy definitions to explore employee's understanding about privacy. To better understand the privacy-related term, respondents were given additional open text answer in the survey instrument. A matrix question consisting eight items related to the importance of management of privacy and security issues in company's KMS settings ranked on a 5-point Likert scale, coded from 1 (strongly agree) to 5 (strongly disagree). Two further items asked respondents to indicate their perspective about the security of personal information and to rate how important the privacy policy in KMS based on five-point Likert scale raging from 1 (very important) to 5 (very unimportant). The semi-structured interviews covered the following topics: the current position of employee, the role and responsibility in company, and company's strategies to encounter privacy and issues in KMS.

4. Results and Analysis

Out of 30 administered questionnaires, 20 valid responses received (response rate = 67%). Although it is recognized that the responses is small sample, it was not a significant issue since the surveys were distributed across representative KM staff which reasonably indicate the actual situation in the companies. An online Qualitrics software was used for statistical analysis, which cover the calculation of an unweighted mean score and standard deviation for each of items to represent the emergent privacy and security issues in KMS. Interviews were conducted in three companies with total of four KM staff. The qualitative data from the interview transcribed and translated into English. Then, the translated interview transcript coded using NVivo version 12 using axial coding analysis technique. Authors developed 17 codes which broadly grouped into personal information, confidentiality, trust, behavior, and security aspects. All these codes were developed during data analysis to examine covered constrains from literature review and the findings from the survey.

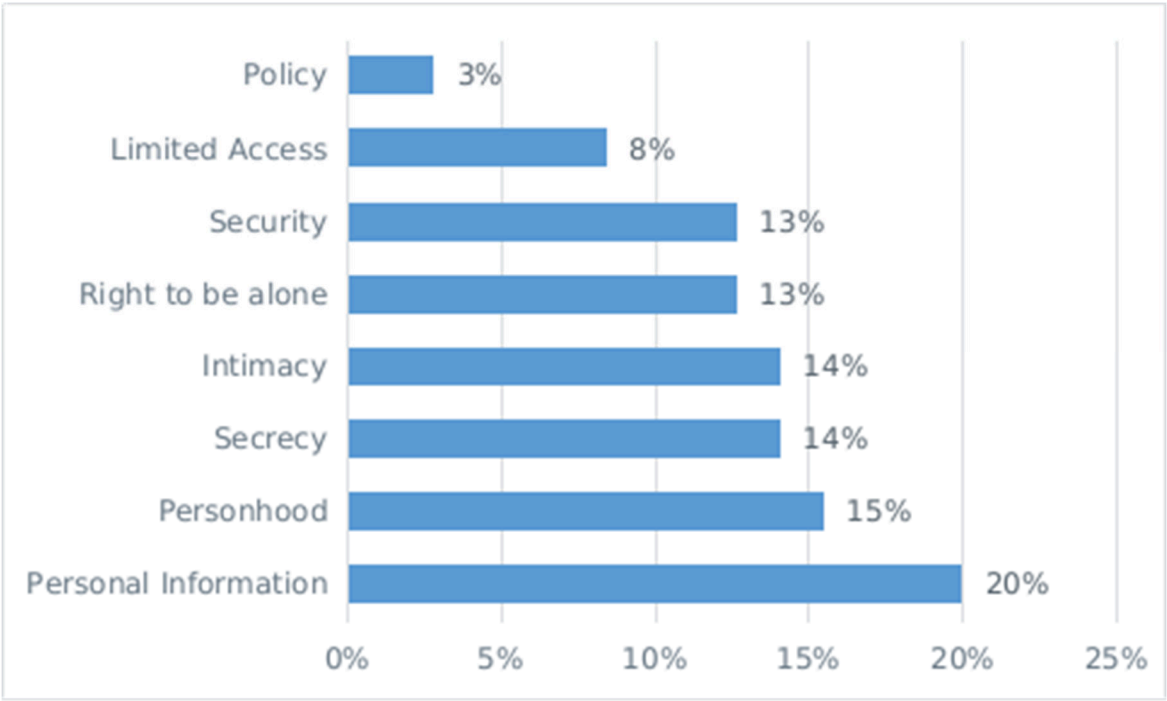

Figure 1. Privacy-related definitions in Company's KMS Settings

As can be seen from Figure 1, employee's perceptions about privacy term are vary (n=71). Most of employee identified privacy as personal information (20%), while the second most related definition of privacy was personhood (15%). Besides, the six privacy-related term provided by Daniel Solove [34], respondents raised two additional terms, which are policy (3%) and security (13%). A number of KM staff identified that the personal information can be publicly available if the information has consented as a public domain of the companies. KM manager at PTSI commented: "*Privacy to me, is personal, private things, like my identity, personhood, about family… but at company, privacy might be our databases because it is a vital.. I mean, it is a company privacy where the information is all bout business processes*." Another KM manager at PLN described privacy as: "*Something that should not be shared.. it is like a make limitations between employee's personal information and company's related information*."

Table 1 describes the mean scores and standard deviation of items relating to bodily privacy and security issues in KMS. Respondents were asked the importance of privacy and security management in company's KMS settings. In addition, this survey data were used to identify the employee's perspective towards their personal information in KMS. Overall, employees had a high awareness of their personal information. Two items (1 and 2) were used to identify the confidentiality constrain. Based on data analysis, interview responses suggested an implicit boundary around the type of personal information which employee perceived as personal private data and which personal information that viewed as company private data, and hence should remain private in the workplace.

Table 1 This is a table. Tables should be placed in the main text near to the first time they are cited.

No.	Items	Scale	Mean	SD
1	To ensure the company appropriately used the personal information and knowledge in KMS	1-5	1.50	0.81
2	To protect and maintain employee's knowledge as important asset for company	1-5	1.40	0.49
3	To provide assessment tools for knowledge process among employees	1-5	1.45	0.59
4	To minimize risks from personal information piracy and misuse of knowledge in company	1-5	1.40	0.58
5	To build trust and intimacy between employee and top-level management in company	1-5	1.60	0.73
6	To provide a clear boundaries of privacy at personal settings and workplace in the company	1-5	1.60	0.92
7	To show the company's role in protecting the employee's rights to privacy and security issue	1-5	1.55	0.80
8	To provide secure knowledge management practices in the company	1-5	1.55	0.67

All KM managers also sought to explore this boundary during interviews. KM manager from PDAM, for instance, described: "*Privacy in company may be.. like information related to business process.. yes it used only for business purposes with customers and partners. However, in KMS settings, don't think it would possible to simplify or say this information or knowledge are belong to company or there are employee's private data. I was thinking, it should be different area, but we are part of this company.. we have to admit it, or.. I don't know… but as employee we have rights to protect our private life.*"

KMS benefits employees in knowledge processes, but challenged by company interest as a workplace. As can be seen from data at item 3 to 5, the most severe problem experienced in business settings was that the employee sometimes lacked the intimacy and trust to other employee, especially with the top level management in the company. Although the all employees positively sought the company's credibility and reputations, their solitude as individual are influenced by trust to someone with a higher position. It is because employee's performance in the KMS is an integral part of company's performance review. The following quote from an employee at PTSI commented: "*Once we create and publish the particular knowledge into KMS, I don't think it will be hijacked or misused… I do trust that our IT division has a good security scheme.*"

Similarly, KM manager at PLN also commented: "*We developed our own KMS software, our IT division is very good on it. Talking about personal data in company KMS, because we are working here, I don't think it is necessary to worry about it. We trust that they will manage our personal data appropriately*." They were, however, extended the notion of trust as essential concern to the company and its policy maker. This constrain was assessed asking employee with a statement, "I believe that my personal information are managed professionally by company". The value of mean and standard deviation for this item are 1.80 and 0.98, respectively.

Analysis of interviews data shows two clear constrains underlying the employee's privacy perspective in the companies are associated with their behavioral roles (item 6 and 7). This behavior, however, has been identified in prior studies about knowledge sharing which focused on participation and contribution of employees in KMS, e.g. [2], [7], [35]. This indicate that the company must carefully maintain the employee role and responsibility in KM activities. He, Qiao, and Wei (2009) suggest an additional management position in order to support KM activities in the company [29]. Employee, therefore, may expect equitable roles in the company as well as expect their own privacy in the workplace environment [36].

Two KM managers from PTSI and PLN described: "*There is a rewards point, we are encouraged to participate in KMS because there is an assessment. On top of that, they also verify the content and bunch of requirements…. We do have a control system for evaluation and monitoring. And it is reported to management and they rewarded to the employee.*" The constrain of security dimension in KMS settings ha been explored using two items. One item was taken from eighth item of privacy construct, while another item bodily related to security construct. Respondents were given a statement about the reliability of the security and sustainability of KMS settings in the company. The value of mean and standard deviation for this item are 1.55 and 0.59, respectively. To exemplify more aspect of security in the KMS settings, interviewee were asked the ICT architecture of KMS in their company. However, most of them spoke without prompting a more detailed answers.

5. Discussion

In this study, rather than promoted additional enhancement from the previous privacy and security in the KM settings, authors elect to develop an preliminary conceptual direction to provide a systematic conceptualization towards the notion of privacy and security. To better understand the distinct between these issues, two important consequences identified from the empirical analysis of this study. First, organizational layer which emphasis the notion of employee's perspective of privacy into three dimensions; confidentiality, trust, and behavior (Figure 2). Second, the important of ICT layer which encompasses two distinct of security issue; legal framework and architecture-infrastructure (Figure 3). A clear distinction between organizational and ICT layer is relevant for KMS settings in companies because it entails subjectivity and context specific towards perspective of employee about privacy and the aspect of security.

5.1. Perspective of Privacy in KMS

In order to be able to discuss the perspective of privacy in KMS, the understanding of what constitutes the term privacy among the employee in the company is important. It may lead to a personal conflict and infringement of privacy when the expectations of the KMS settings contradict with employee's personal matters. It is rarely defined how the degree of confidentiality should be managed by companies KMS settings, rather privacy issue was mentioned in the KM practices. It is, therefore, the confidentiality in the company's KMS settings was driven by two different types of privacy data: single-owner and multi-owner. Single-owner privacy data can also be employee's personal information. It is now widely accepted that public disclosure of private facts can also mean that unreasonably publicity given to another employee personal life. In general, this tort usually includes an employee's use of personal information information gathered by companies during the recruitment processes including application, orientation, screening, or medical examination process.

The second type of privacy data in the KMS settings is multi-owner. This particular multi-owner pricay information are not genuinely private matters. The analysis data shows that employee have difficulties to explain the distinct of privacy as an employee and as an individual. Furthermore, it was unclear whether this particular data exist in company's KMS settings since the nature of KM practices is a collaboration of multiple individual in the company's public sphere. However, the results of this study confirms the existence of multi-owner privacy data in organizations [17].

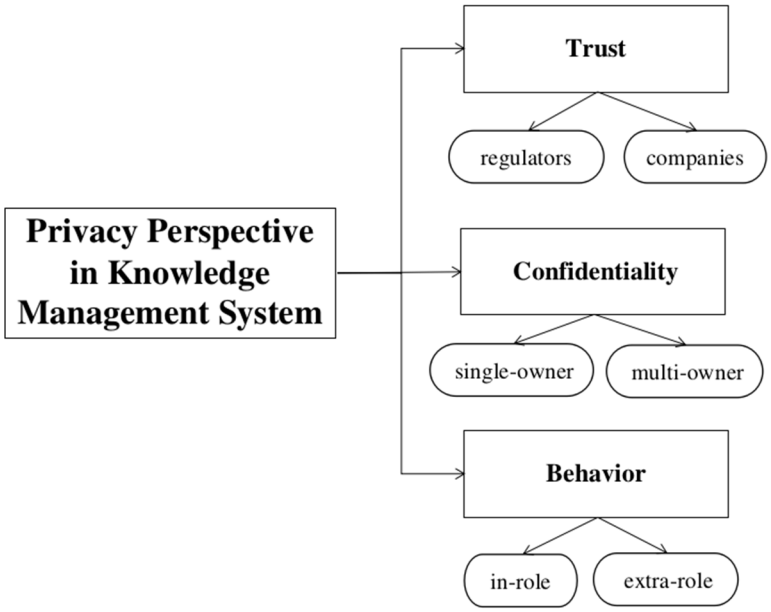

Figure 2. Perspective of Privacy in KMS

The second dimension of privacy in KMS setting is trust. This dimension, based on the analysis data, was influenced by two constrains; trust in companies and trust in regulations. In essence of the findings, employee highly motivated to provide their personal information due to the reliance of companies' reputations. In other words, privacy had been seen as a valuable service that company can offer to build trusting relations rather than as a burden with our stakeholders. To build this kind of relationship, a high degree of openness and relevant regulations are needed. Although personal information in the companies may be given voluntarily by employee in some situations, significant disquiet did exist regarding the collection processes or procedures, which sometimes employed without permission of employee. From this, it was clear that employees had a strong sense of privacy as they described the personal information to which they were comfortable with other having access to and which they were not. Thus, it is important for companies to have a strong and favorable bonding among their loyal and dedicated employees to ensure and maintain an excellent cooperative relationship for enhancing participation in KMS.

Another constrain of trust dimension revealed from the analysis data is related to the regulators. Trust in regulators was more important than the construct of privacy policy in KMS settings. This findings confirm prior studies by [29], which highlight the importance of social relationship among the employee towards the use of KMS in the companies. It is important to highlight that these

relationships are equally valid whether or not the companies provided full consent to access and the usage of employee privacy. While privacy issue engendered employment contention, the translation to a new domain through analogy that is required such debates was fairly rudimentary.

The third dimension uncovered from analysis was behavior. This dimension raised by the assumption s from employee that seems plausible and coherent with their in-role or extra-role in a companies. Wang, Noe, and Wang (2014) concluded that employee might have consideration towards their primary role and additional role before making assumptions in regards to KM practices [2]. All interviewees reported their commitment to the KMS although they felt varying degrees of group identification and privacy related regulation. Indeed, employees had tough business target that sometimes proved difficult to achieve. However, all respondents were aware of this importance and hence had a high awareness of information privacy issues.

Although the participation in the KMS is mostly extra-role of behavior, this study provide evidence that some companies had rewards system that encourage employee to participate in KM practices. It seems to be vague to distinguish between the employee roles in KMS settings. Thus, the companies must know that it would not be unreasonably intrusive to observe what an employee does in KMS settings and to observe the employee's conduct behind closed doors.

In spite of all of this, what further exacerbates the problem was the most companies do not really pay attention to the finer details of the privacy policy employees are agreeing to. This results, therefore, leveraging the potential lack of privacy agreement in its nature and understanding. True, privacy got heavily affected by the latest ICT developments and the rapid transfer of information. Bringing together ICT layer and organizational layer seems particularly fitting for an exploration of this topic; while the legal framework draw on actual real-world examples to lay bare the problems of privacy in the public space.

5.2. Security Aspects in KMS

Security issue is one of challenges in the current KMS practices. In KMS settings, it might be best distinguished by the clarity and transparency in regards to the purpose of data collection and the compliance of personal information with the existing legal framework and the architecture of KMS infrastructure [5]. There is a complex relationship between all of the aspects in terms of information system and security of KMS architecture. Furthermore, the distinct of privacy regulation is debatable because most respondents in this study had different perspective between privacy policy and the rights to the privacy. As previously explained, the first notion of privacy focused primarily on generalized comparisons between the single-owner and multi-owner information in companies, while the security issues comply with privacy-related policies and regulations. Bertino et al. (2006) argue that secure KM depends on the strategies, process, and metrics [19]. However, analysis data shows that the prominent issues in regards to security in KMS were best reflected with two simple dimensions; legal framework and architecture of KMS.

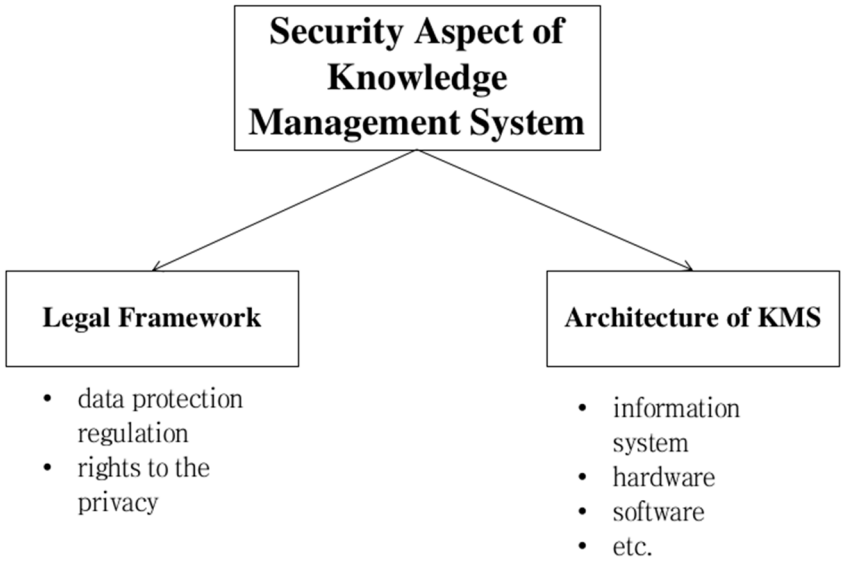

Figure 3. Security Aspect of KMS

Security aspects from legal framework constraints on employee's ability to preserve their personal information relevant to the company's ICT architecture. From this perspective, KMS settings as evolving ICT have different rules and regulations governing the knowledge processes in a companies. The interview responses raised the important data protection regulation in companies although they were not concerned about specific regulatory constructs in KMS settings. An immediate results indicate that the legal framework was the employee's right to privacy and its legal context in the company.

From this vantage point, the distinct perspective of privacy and security in the KMS was conceptualized from both organizational layer and ICT layer of KMS settings. Authors posit that these emergence of conceptual direction in the following section.

5.3. Conceptual Direction of Privacy and Security in KMS Settings

As mentioned previously, this study concentrates on investigating the notion of privacy and security issues in company's KMS settings. From the data analysis, authors identified that organizational layer make up underlying privacy issue, while the ICT layer addressed the aspect of security issue. These layers modeled to five dimensions which three of them corresponding to privacy issue and the other two belong to security aspect of KMS (Figure 4). Within this study, therefore, authors aim to provide a conceptual directions to the fog of misunderstandings around privacy and security that are simultaneously operant in dealing with the KMS practices in companies. This conceptual direction, however, provides the initial practical and theoretical foundation of privacy and security construct in a small competitive enterprise KMS environment and its employee's privacy preferences. It is unrealistic to expect that this conceptual direction will correspond with others types of organizations.

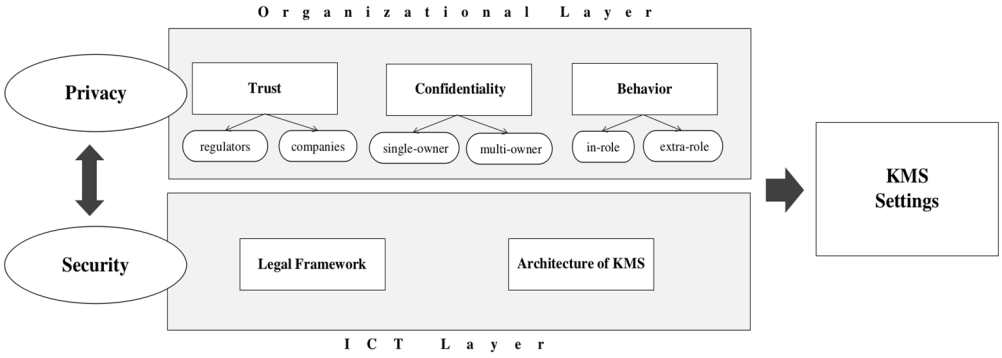

Figure 4. Conceptual Direction of Privacy and Security in KMS

6. Conclusion

This study contributes in several ways to the KMS literature specifically as it relates to privacy and security issues between employee and companies. Employee's perspective on privacy issue in companies can be distinguished from organizational layer of KMS through three dimensions; confidentiality, trust, and behavior. These dimensions have simultaneously operant in the company's KMS settings, which not only organize the information about its business activity but also personal information about their employee. The dimension of privacy towards multi-owner privacy data and single-owner privacy data is still in a stage. While the security aspects in KMS are comply with ICT layer which constructed by legal framework and KMS architecture. Thereby, the aforementioned issues which bodily related to privacy and security in KMS are not seen as an unfortunate constraint.

This perspective of privacy and security issues was explored to re-conceptualize the paradox of privacy in KMS. However, company's understanding towards the potential risk and protection of personal information has lagged behind. In this study, authors have worked through practical examples and demonstrated that a high-level privacy and security in KMS is an important element in reasoning about the sensitivity of personal information.

While the immediate future of KMS is bringing the revolutionary impact on KM practices, its long-term future is highly related to other area of research, such as information systems, databases, software, and metadata. Given the very real importance of privacy and security of personal information in company, authors suggest that this preliminary study benefits the development of an initial ICT infrastructure and software specification of KMS architecture in the companies.

This study, however, has inherent limitations that affect the generalization of the results. First, the sample size were considered low although the companies settings is very broad area. Second, this study used basic statistical analysis technique and did not cover the factor analysis. It is recognized that the current study was explanatory in nature. However, investigating privacy and security issues is rather difficult in companies due to the highly potential lack of understanding in regards to confidentiality of information gained during the research. Further research with larger sample and advanced statistical analysis technique are required to better measurements and tests the underlying privacy and security issues in company's KMS settings.

References

[1] R. Maier, *Knowledge Management Systems: Information and Communication Technologies for Knowledge Management*. Springer Science & Business Media, 2007.

[2] S. Wang, R. A. Noe, and Z.-M. Wang, "Motivating Knowledge Sharing in Knowledge Management Systems: A Quasi–Field Experiment," *J. Manag.*, vol. 40, no. 4, pp. 978–1009, May 2014, doi: 10.1177/0149206311412192.

[3] J. P. Zeiringer and S. Thalmann, "Knowledge sharing and protection in data-centric collaborations: An exploratory study," *Knowl. Manag. Res. Pract.*, vol. 20, no. 3, pp. 436–448, May 2022, doi: 10.1080/14778238.2021.1978886.

[4] A. de Bem Machado, S. Secinaro, D. Calandra, and F. Lanzalonga, "Knowledge management and digital transformation for Industry 4.0: a structured literature review," *Knowl. Manag. Res. Pract.*, vol. 20, no. 2, pp. 320–338, Mar. 2022, doi: 10.1080/14778238.2021.2015261.

[5] J. Choe, "The Construction Of An It Infrastructure For Knowledge Management".

[6] R. Grandinetti, "Absorptive capacity and knowledge management in small and medium enterprises," *Knowl. Manag. Res. Pract.*, vol. 14, no. 2, pp. 159–168, May 2016, doi: 10.1057/kmrp.2016.2.

[7] W. Yu Chung Wang, D. Pauleen, and N. Taskin, "Enterprise systems, emerging technologies, and the data-driven knowledge organisation," *Knowl. Manag. Res. Pract.*, vol. 20, no. 1, pp. 1–13, Jan. 2022, doi: 10.1080/14778238.2022.2039571.

[8] M. Kolyasnikov and N. Kelchevskaya, "Knowledge management strategies in companies: Trends and the impact of Industry 4.0," *Upravlenets*, vol. 11, no. 4, pp. 82–96, Sep. 2020, doi: 10.29141/2218-5003-2020-11-4-7.

[9] Herison Surbakti, "Web Technology Knowledge Management And Its Privacy And Security Challenge," 2015, doi: 10.13140/2.1.3178.2727.

[10] K. Bajpai and K. Weber, "Privacy in Public: Translating the Category of Privacy to the Digital Age," in *Research in the Sociology of Organizations*, vol. 51, R. Durand, N. Granqvist, and A. Tyllström, Eds., Emerald Publishing Limited, 2017, pp. 223–258. doi: 10.1108/S0733-558X20170000051006.

[11] H. Drachsler and W. Greller, "Privacy and analytics: it's a DELICATE issue a checklist for trusted learning analytics," in *Proceedings of the Sixth International Conference on Learning Analytics & Knowledge - LAK '16*, Edinburgh, United Kingdom: ACM Press, 2016, pp. 89–98. doi: 10.1145/2883851.2883893.

[12] T. Matzner, "Why privacy is not enough privacy in the context of 'ubiquitous computing' and 'big data,'" *J. Inf. Commun. Ethics Soc.*, vol. 12, no. 2, pp. 93–106, May 2014, doi: 10.1108/JICES-08-2013-0030.

[13] K. Ball, E. M. Daniel, and C. Stride, "Dimensions of employee privacy: an empirical study," *Inf. Technol. People*, vol. 25, no. 4, pp. 376–394, Nov. 2012, doi: 10.1108/09593841211278785.

[14] C. Liu, J. T. Marchewka, J. Lu, and C.-S. Yu, "Beyond concern—a privacy-trust-behavioral intention model of electronic commerce," *Inf. Manage.*, vol. 42, no. 2, pp. 289–304, Jan. 2005, doi: 10.1016/j.im.2004.01.003.

[15] R. Wilton, "After Snowden – the evolving landscape of privacy and technology," *J. Inf. Commun. Ethics Soc.*, vol. 15, no. 3, pp. 328–335, Aug. 2017, doi: 10.1108/JICES-02-2017-0010.

[16] N. Evans, "Virtue Ethics in Knowledge Management," in *Handbook of Virtue Ethics in Business and Management*, A. J. G. Sison, G. R. Beabout, and I. Ferrero, Eds., in International Handbooks in Business Ethics. , Dordrecht: Springer Netherlands, 2017, pp. 1231–1243. doi: 10.1007/978-94-007-6510-8_94.

[17] Y. Ren, F. Cheng, Z. Peng, X. Huang, and W. Song, "A privacy policy conflict detection method for multi-owner privacy data protection," *Electron. Commer. Res.*, vol. 11, no. 1, pp. 103–121, Jan. 2011, doi: 10.1007/s10660-010-9067-8.

[18] C. Fuchs, "Towards an alternative concept of privacy," *J. Inf. Commun. Ethics Soc.*, vol. 9, no. 4, pp. 220–237, Nov. 2011, doi: 10.1108/14779961111191039.

[19] E. Bertino, L. R. Khan, R. Sandhu, and B. Thuraisingham, "Secure knowledge management: confidentiality, trust, and privacy," *IEEE Trans. Syst. Man Cybern. - Part Syst. Hum.*, vol. 36, no. 3, pp. 429–438, May 2006, doi: 10.1109/TSMCA.2006.871796.

[20] G. Skinner, S. Han, and E. Chang, "An information privacy taxonomy for collaborative environments,"

Inf. Manag. Comput. Secur., vol. 14, no. 4, pp. 382–394, Aug. 2006, doi: 10.1108/09685220610690835.
[21] S. Stalla-Bourdillon, J. Phillips, and M. D. Ryan, *Privacy vs. Security*. Springer, 2014.
[22] C. Mei-Sha Chieh and B. H. Kleiner, "How organisations manage the issue of employee privacy today," *Manag. Res. News*, vol. 26, no. 2/3/4, pp. 82–88, Mar. 2003, doi: 10.1108/01409170310783790.
[23] S. D. Warren and L. D. Brandeis, "The Right to Privacy," *Harv. Law Rev.*, vol. 4, no. 5, p. 193, Dec. 1890, doi: 10.2307/1321160.
[24] C. Fried, "Privacy," *Yale Law J.*, vol. 77, no. 3, p. 475, Jan. 1968, doi: 10.2307/794941.
[25] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A Survey on Blockchain for Information Systems Management and Security," *Inf. Process. Manag.*, vol. 58, no. 1, p. 102397, Jan. 2021, doi: 10.1016/j.ipm.2020.102397.
[26] Y. Kurniawan, A. Hardianto, and F. Meylani, "The Influence of Knowledge Management Capabilities on Organizational Effectiveness," . *Vol.*, no. 18, 2005.
[27] M. Alavi and D. E. Leidner, "Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues," *MIS Q.*, vol. 25, no. 1, p. 107, Mar. 2001, doi: 10.2307/3250961.
[28] I. Rechberg and J. Syed, "Knowledge Management Practices and the Focus on the Individual:," *Int. J. Knowl. Manag.*, vol. 10, no. 1, pp. 26–42, Jan. 2014, doi: 10.4018/ijkm.2014010102.
[29] W. He, Q. Qiao, and K.-K. Wei, "Social relationship and its role in knowledge management systems usage," *Inf. Manage.*, vol. 46, no. 3, pp. 175–180, Apr. 2009, doi: 10.1016/j.im.2007.11.005.
[30] S. K. Satapathy and C. R. Moharana, "Knowledge Management Effectiveness in Securing Information and Network Systems: A Study on Odisha," vol. 6, no. 2349, 2017.
[31] M. Saratchandra and A. Shrestha, "The role of cloud computing in knowledge management for small and medium enterprises: a systematic literature review," *J. Knowl. Manag.*, vol. 26, no. 10, pp. 2668–2698, Jan. 2022, doi: 10.1108/JKM-06-2021-0421.
[32] C. L. Miltgen and H. J. Smith, "Exploring information privacy regulation, risks, trust, and behavior," *Inf. Manage.*, vol. 52, no. 6, pp. 741–759, Sep. 2015, doi: 10.1016/j.im.2015.06.006.
[33] R. Moll, S. Pieschl, and R. Bromme, "Competent or clueless? Users' knowledge and misconceptions about their online privacy management," *Comput. Hum. Behav.*, vol. 41, pp. 212–219, Dec. 2014, doi: 10.1016/j.chb.2014.09.033.
[34] D. J. Solove, *Understanding Privacy*. Harvard University Press, 2010.
[35] T. Dey and S. Mukhopadhyay, "Influence of Behavioral Intentions, Affective Trust and Affective Commitment on Knowledge Sharing Behavior:," *Int. J. Knowl. Manag.*, vol. 14, no. 2, pp. 37–51, Apr. 2018, doi: 10.4018/IJKM.2018040103.
[36] V. Scovetta, "The Impact of Personal and Positional Powers on Knowledge Management Systems:," *Int. J. Knowl. Manag.*, vol. 13, no. 2, pp. 18–34, Apr. 2017, doi: 10.4018/IJKM.2017040102.