Pak. j. life soc. Sci. (2024), 22(2): 11535-11544 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences
www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2024-22.2.00870

RESEARCH ARTICLE

Consumer Privacy Protection and Data Ethics: Social Responsibility and Risk Balance in Business Administration

Feng Gao*

MBA, Nilai University Malaysia, Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia.

ARTICLE INFO

Received: Sep 16, 2024

Accepted: Nov 1, 2024

Keywords

Consumer Privacy

Privacy Paradox

Collaborative Path of Multiple Subjects

Privacy Violation

***Corresponding Author:**

18600476571@163.com

ABSTRACT

As consumer data becomes more accessible and more valuable, it also becomes more vulnerable, resulting in unprecedented attention to consumer privacy protection. This paper constructs an integrated framework to explore the consumer privacy protection path of collaboration among multiple entities including customers, technology, enterprises and government by sorting out the formation and resolution of the consumer privacy paradox. The paper first analyzes the differences in consumer privacy protection behaviors in different situations and constructs evaluation criteria for the rationality of privacy response behaviors, including comparative studies on the consistency, differences and root causes of consumer privacy protection behaviors in different situations, and how consumers should respond; the paper explores the causes and solutions to the consumer privacy paradox from multiple perspectives, and examines the conditions and contexts in which consumer privacy concerns affect privacy protection behavior; the paper strengthens the research on the measurement, formation and cultivation mechanism of consumer privacy literacy, including the development of a new privacy literacy scale, the exploration of theoretical mean standards for the difference between subjective and objective privacy literacy, and specific measures to improve consumer knowledge and skills; the paper deeply examines the antecedents and influencing mechanisms of consumer privacy fatigue, helping to gain insight into consumers' psychological activities and behavioral differences when using consumer privacy information; the paper comprehensively considers the dynamic balance of responsibilities and interests of all parties, highlights the synergy, and deeply explores the consumer privacy protection path of collaboration among multiple entities. Experimental data shows that the number of incidents involving tens of millions of data leaks under the multi-subject collaborative path is between 163 and 381, while under the traditional protection path it is between 324 and 615, which is significantly higher than the multi-subject collaborative path and different from the traditional protection path. Compared with the protection path, the occurrence rate of privacy invasion incidents is significantly reduced. The paper concludes by highlighting the importance of privacy protection and providing guidance to businesses on the ethical challenges and social responsibilities they face when processing personal data.

1. INTRODUCTION

With the rapid advancement of information technology and the full arrival of the big data era, the issue of consumer privacy protection and its relationship with data ethics are gradually becoming a hot topic of discussion in public opinion and academia. In this context, this paper explores the balance between social responsibility and risk in consumer privacy protection in the field of business administration, aiming to find an effective way to reasonably meet corporate data utilization needs and practice their social responsibility while fully respecting and protecting consumer privacy. To this end, this paper constructs a comprehensive analytical framework. Through a detailed analysis of the root causes and solutions to the consumer privacy paradox, this paper further explores the issue of building a consumer privacy protection mechanism with the participation of multiple parties, thereby providing new insights and strategies for understanding and responding to this complex issue.

The paper begins by explaining the macro-background and practical significance of the research, clarifying the core issues that this paper aims to explore and its dual contributions to theory and practice, and outlining the basic structure of the entire paper. Subsequently, the current status of consumer privacy protection, the challenges it faces, and the ethical dilemmas and social responsibility requirements that companies encounter when processing personal information data are reviewed. In the methods section, this paper explains the research design ideas, data collection channels, and data analysis methods, especially the construction of an integrated framework and the setting of evaluation criteria for the rationality of privacy response behaviors. Based on the collected data and analysis results, this paper analyzes the nature of the consumer privacy paradox, the lack of privacy literacy and the influencing mechanism of privacy fatigue in the results and discussion section, and explores the implementation effect and potential advantages of the consumer privacy protection strategy involving multiple parties in collaboration. Finally, in the conclusion, this paper summarizes the research findings and proposes a series of practical guidelines and policy recommendations based on them, aiming to promote the deep integration and sustainable development of consumer privacy protection and data ethics in business management practices, and contribute to building a more secure, fair and transparent data environment.

2. RELATED WORK

How consumers can protect their privacy while enjoying the convenience of technology, and how to achieve effective privacy management in different application scenarios have become urgent issues to be solved. Based on the protection motivation theory, Chen and Wei [1] took privacy protection burnout and self-efficacy as mediating and moderating variables, respectively, and launched a large-scale questionnaire survey in 16 cities across the country, aiming to explore the occurrence mechanism of privacy paradox in the context of smart media and the differences in privacy protection behavior among individuals, and to provide theoretical reference for promoting platform privacy management. Because the damage to data privacy is difficult to quantify, the price-centered approach of traditional antitrust law cannot be directly applied. Lin and Luo [2] established the applicable principle of prudent intervention and set the goal of balancing market competition and privacy protection. They applied regulatory approaches based on the specific behaviors and scenarios of data privacy violations, reasonably weighed the protection needs of the interests involved, and on this basis optimized privacy protection analysis tools and innovated theoretical tools for antitrust protection. In order to solve the problems of privacy leakage and multi-task allocation in crowd sensing, Ao et al. [3] considered that crowd sensing tasks have geographical proximity characteristics, used the improved fuzzy clustering (FCM) algorithm to cluster and combine task locations, and proposed an edge-assisted crowd sensing location privacy protection (EALP) multi-task allocation mechanism. Gao et al. [4] proposed a crowd testing task privacy protection (CTTPP) scheme based on blockchain and ciphertext-based attribute encryption

(CP-ABE) strategy to improve the crowd testing (crowdsourcing testing) data sharing system in the cloud environment and solve the data security and privacy protection problems in the crowd testing field. Guo et al. [5] proposed a decentralized, revocable, privacy-preserving self-managed identity (SSI) scheme based on blockchain to address the problem of digital identity management for vehicle users in the vehicle-to-vehicle network (VANET) environment. They also conducted a detailed analysis of the security properties of the scheme and proved that the scheme can meet the proposed security goals.

Boerman et al. [6] used panel data to analyze individuals' privacy protection behaviors at different time points and the motivations behind these behaviors. Quach et al. [7] analyzed the interactions and conflicts between privacy, data usage, and marketing practices through a literature review. Keshta and Odeh[8-17] explored the current challenges by analyzing the security and privacy protection measures of electronic health record systems. Nguyen et al.[9] analyzed the need for privacy protection by reviewing the potential technologies and challenges of 6G technology. Rigaki and Garcia[10] studied privacy attacks on machine learning and analyzed the working principles and impacts of these attacks. This study analyzes the importance of consumer privacy protection and explores the ethical challenges and social responsibilities faced by companies when processing personal data.

3. METHODS

3.1 Research Design

In this study, we focus on two core components: the construction of an integrated framework and the formulation of evaluation criteria for the rationality of privacy response behaviors, which together form the basis for in-depth analysis and solution strategies for consumer privacy protection and data ethics issues.

First, an integrated framework is constructed to systematically analyze and address the complex issues of consumer privacy protection and data ethics in the field of business administration. This framework not only integrates the theoretical and practical essence of multiple disciplines such as law, ethics, psychology, sociology, and business administration, but also provides a broader cognitive perspective by introducing a multi-dimensional perspective. This framework clearly defines the roles and interactions of different entities such as consumers, technology providers, businesses and governments in the privacy protection process, and deeply analyzes how these entities jointly shape and influence the practical dynamics of privacy protection[11-19]. In the context of business administration, the application of this framework will help to more effectively identify and address challenges in consumer privacy protection and data ethics.

The purpose of formulating the evaluation criteria for the rationality of privacy coping behavior is to provide a scientific and comprehensive evaluation system to measure and guide the rationality of consumers' privacy protection behavior. These standards cover many key dimensions such as legal compliance, ethical rationality, consumer satisfaction and corporate responsibility, ensuring a comprehensive consideration of the effectiveness and rationality of privacy protection measures [12-16]. By using these standards, the actual effects of different privacy protection strategies can be evaluated more accurately, and then useful guidance can be provided for enterprises to help them protect consumers' privacy rights and interests while taking into account business development and social responsibility. It is worth noting that the formulation process of these evaluation standards fully draws on the data collected by in-depth interviews and other research methods, ensuring that they can closely meet the privacy protection needs of consumers and the actual business practice of enterprises.

3.2 Data Collection

In the research on consumer privacy protection and data ethics, the data collection process involves two dimensions: cross-cultural and localization[13-14].

The cross-cultural study selected three countries with different cultural backgrounds in Asia, Europe and North America for comparison. Through online interviews, 500 valid samples were collected from each country, totaling 1,500 data points. The questionnaire included consumers' knowledge of privacy protection, behavioral habits, attitudes towards different privacy policies, etc. The survey was completed within one month to ensure the comparability of the data, as shown in Table 1:

Table 1: Interview data

Participant ID	Age	Gender	Education Level	Privacy Awareness	Privacy Policy Reading Habits	Attitude Towards Privacy Policies
001	25	Male	Bachelor's	High	Often reads privacy policies	Supports
002	34	Female	Master's	Moderate	Occasionally reads privacy policies	Neutral
003	42	Male	Bachelor's	High	Always reads privacy policies	Supports
004	29	Female	Master's	High	Never reads privacy policies	Opposes
005	37	Male	Bachelor's	Low	Occasionally reads privacy policies	Supports
006	45	Female	Doctorate	Moderate	Always reads privacy policies	Supports
007	28	Male	Bachelor's	High	Never reads privacy policies	Neutral

Localization research is conducted in different regions within China. Through in-depth interviews and focus group discussions, 30 in-depth interview samples and 3 focus group data are collected in each region to explore consumers' views on local companies' privacy protection measures, perceptions of personal privacy rights, and concerns about privacy leaks. The in-depth interviews and focus group discussions are completed within two months.

3.3 Data Analysis

In view of the data analysis focus mentioned above, this study conducted the following specific data analysis and discussion, focusing on the analysis of the causes of the consumer privacy paradox, the development of the consumer privacy literacy scale, and the analysis of the impact mechanism of consumer privacy fatigue.

In the analysis of the causes of the paradox of consumer privacy, this study found that consumers showed a contradictory attitude and behavior in the face of personal privacy protection. Although they are generally worried about the risk of personal information disclosure, they are still willing to share personal information on the network platform in actual network behavior. This contradiction is called the paradox of consumer privacy. This study summarizes several factors that contribute to this paradox: after weighing the potential benefits and risks that personal information disclosure may bring, consumers often choose to disclose information because the expected benefits outweigh the potential costs; privacy fatigue describes consumers' sense of helplessness and fatigue in the

face of complex privacy protection behaviors, which urges them to give up the protection of personal privacy: optimistic deviation and lucky deviation make consumers overconfident and think that the risk of privacy disclosure will not happen to them; when consumers have a high degree of trust in a certain platform, they are more likely to voluntarily disclose personal information.

When developing the consumer privacy literacy scale, based on the comprehensive characteristics of computer skills, attitudes and beliefs, this study designed a scale that includes two dimensions: procedural knowledge and declarative knowledge. Procedural knowledge mainly examines consumers' understanding of the implementation of privacy protection strategies, while declarative knowledge focuses on consumers' mastery of Internet privacy protection technology and legal knowledge.

This study finds that privacy fatigue is a negative emotion that consumers have on privacy protection in the process of using information technology and network services. This kind of fatigue leads consumers to spend less energy when making privacy decisions, so they are more likely to give up the protection of personal privacy. The manifestations of privacy fatigue include "consent fatigue" and "information disclosure fatigue". The former is due to the complexity of privacy statement and service agreement, which makes it difficult for consumers to read and understand, and then gives up their attention to these statements; the latter is because of the risks caused by data leakage and information abuse, which makes consumers feel powerless and disappointed. Privacy fatigue has a negative impact on consumers' privacy protection, which can be attributed to consumers' underestimation of privacy protection ability or underestimation of the risk of privacy information disclosure [15-18].

4. RESULTS AND DISCUSSION

4.1 The Formation and Resolution of the Consumer Privacy Paradox

The formation of the consumer privacy paradox involves multiple levels. First, consumers have a stronger awareness of protecting their personal data in the digital economy era, but at the same time, due to their pursuit of convenience and insufficient awareness of privacy risks, they often neglect privacy protection in practice, leading to the emergence of a privacy paradox. Analyzing the differences in consumer privacy protection behaviors in different situations and constructing evaluation criteria for the rationality of privacy response behaviors are a key direction for future research. This means that there is a need for more detailed examination of consumers' attitudes and behaviors towards privacy in different contexts, as well as the psychological and social motivations behind these behaviors.

In order to resolve this paradox, the study proposed exploring multiple perspectives, including the conditions and contextual range under which consumer privacy concerns affect privacy protection behavior, as well as the measurement, formation and cultivation mechanisms of consumer privacy literacy. These research directions not only help to better understand the complexity of consumers' privacy protection behavior, but also provide theoretical support for the formulation of effective privacy protection strategies.

4.2 Measurement and Cultivation of Consumer Privacy Literacy

The privacy literacy scale is designed to assess consumers’ mastery of privacy protection-related knowledge and their ability to protect privacy, including multiple dimensions such as privacy awareness, privacy knowledge, privacy skills, and privacy behavior. Data were collected through face-to-face interviews and reliability tests were used to ensure the validity and reliability of the scale. The application results showed that consumers' privacy literacy levels varied and were

closely related to their privacy protection behaviors. Figure 1 shows the scale test results for different consumers:

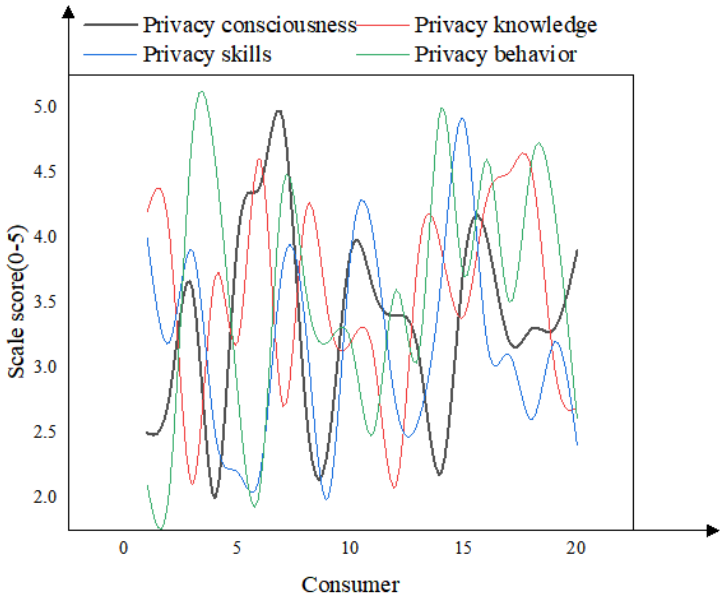

Figure 1: Scale test results

As shown in Figure 1, this study conducted a comprehensive data analysis of the privacy awareness, privacy knowledge, privacy skills, and privacy behavior scale scores of 20 consumers. First, by calculating the mean and standard deviation of each dimension, an overview of the overall score and data distribution was obtained. The average score of privacy awareness is 3.35, showing a certain degree of dispersion; the average score of privacy knowledge is 3.535, slightly higher than privacy awareness, indicating that the score distribution is relatively wide; the average score of privacy skills is 3.17; the average score of privacy behavior is 3.515, indicating that consumers show a certain diversity in privacy behavior. By calculating the correlation coefficient, we preliminarily speculate that there is a positive correlation between privacy awareness, privacy knowledge, privacy skills, and privacy behavior. This means that consumers' improvement in privacy awareness may be accompanied by an increase in privacy knowledge, an improvement in privacy skills, and more active privacy behavior.

The scale results can be used to identify consumers' weaknesses in privacy protection and provide a basis for subsequent education and training. To improve consumers' privacy knowledge and skills, a variety of measures can be taken, including raising consumers' awareness of the importance of privacy protection through educational activities and public publicity, holding seminars, workshops and online courses, developing easy-to-understand and easy-to-operate privacy tools and applications to help consumers better manage their privacy settings, encouraging corporate transparency and requiring companies to clarify their policies on data collection, processing and use, and simplifying the wording of privacy policies to make them more user-friendly. Governments and regulators can also play a role by protecting consumer rights by formulating and enforcing privacy protection regulations, supporting relevant education and training programs, strengthening digital literacy and privacy protection content in school education, and cultivating good privacy protection habits from the younger generation. Through these measures, consumers' privacy literacy can be effectively improved and their self-protection capabilities in the digital economy can be enhanced, while also providing guidance and support for businesses and governments in privacy protection.

4.3 Antecedents and Impacts of Consumer Privacy Fatigue

Privacy fatigue is prevalent among consumers and has a significant impact on their investment and actions in privacy decisions. Specifically, consumers with higher levels of privacy fatigue tend to invest less energy when faced with privacy protection issues and are more likely to take a "do nothing" attitude towards the abuse of personal information, thereby actively or passively giving up privacy protection.

When exploring the specific manifestations of privacy fatigue, this study mainly focuses on "consent fatigue" and "information leakage fatigue". First, "consent fatigue" stems from the complex privacy statements and service agreements issued by companies before providing services. These policies are often lengthy and difficult to understand, causing consumers to feel confused and exhausted when choosing whether to agree, and they tend to give up reading and understanding and make decisions directly. This "one-click consent" behavior model actually weakens consumers' ability to protect their privacy.

"Information leakage fatigue" is caused by the risks brought by data leakage and information abuse. When consumers frequently encounter information leakage incidents or see others suffer losses due to privacy leakage, they may feel powerless and disappointed. When this emotion accumulates to a certain level, it will cause consumers to give up active protection of privacy and instead adopt a passive attitude to deal with it.

The reasons why privacy fatigue has a negative impact on consumer privacy protection can be attributed to two aspects. On the one hand, although consumers are well aware of the possibility of privacy infringement and the negative consequences, they often have to sacrifice some of their privacy rights in order to use certain functions and services of enterprises. This trade-off makes consumers feel powerless and believe that they cannot effectively control their privacy. On the other hand, some consumers lack sufficient understanding of the risks of privacy leakage or underestimate its severity. They believe that the management of personal privacy is ineffective in the Internet environment, and the only way to prevent privacy leakage is to completely withdraw from the Internet. However, this approach is not realistic for most people, so they feel helpless about privacy and eventually give up privacy protection.

4.4 Consumer Privacy Protection Path Based on Collaboration among Multiple Subjects

This paper focuses on how to strengthen privacy protection through cooperation and interaction among different subjects. This governance model includes multiple entities such as governments, businesses, consumers, and technology providers, which jointly participate in the decision-making and implementation process of privacy protection. In order to effectively integrate diverse interests, these entities need to cooperate at every level of responsive personal information governance and design specific forms of cooperation. This article compares the incidence of privacy violations under the consumer privacy protection path of multiple subjects in different regions and the number of incidents with data leakage of tens of millions under the traditional protection path, as shown in Figures 2 and 3, to reflect the effect of the consumer privacy protection path of multiple subjects:

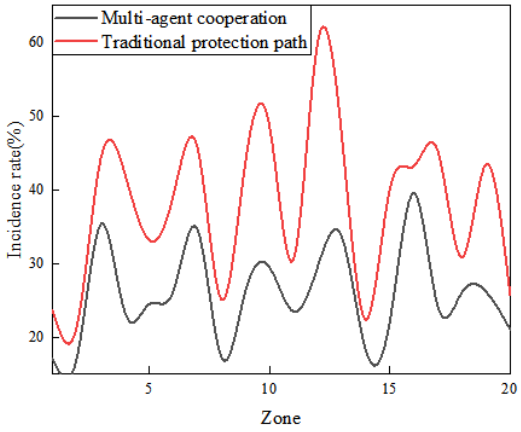

Figure 2: The incidence of privacy violations

As shown in the data in Figure 2, it can be found that from the perspective of data distribution, the data distribution under the multi-subject collaborative path is more compact, that is, the difference between the incidence rates of privacy infringement incidents in different regions is relatively small. This suggests that privacy protection strategies based on collaboration among multiple entities may be more stable and reliable, and can maintain relatively consistent privacy protection effects under different circumstances. By comparing the highest and lowest incidence rates of privacy violations under the two paths, it can be found that the highest incidence rate under the multi-subject collaborative path (39.6%) is lower than the lowest incidence rate under the traditional protection path (59.9%). This means that even when serious privacy violations occur under the multi-subject collaborative path, their incidence is still lower than the general level under the traditional protection path. This further proves the advantage of the multi-subject collaborative path in privacy protection.

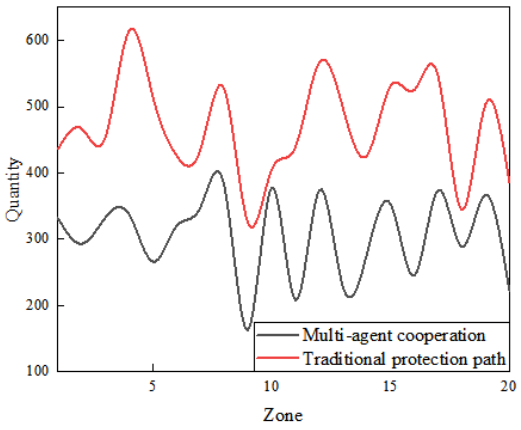

Figure 3: Number of incidents with data leakage of tens of millions

According to the data in Figure 3, the number of incidents involving tens of millions of leaked data under the multi-subject collaborative path is between 163 and 381, while the number of incidents under the traditional protection path is between 324 and 615, which is significantly higher than the multi-subject collaborative path. This shows that the consumer privacy protection path that involves collaboration among multiple entities is more effective in reducing large-scale data breaches. This difference is due to the fact that the multi-agent collaborative path can better

integrate the resources and expertise of different participants, thereby taking more comprehensive and coordinated measures to prevent and respond to data leakage risks.

Privacy concerns have different representations and influences in different cultures and business environments. Future research needs to conduct cross-cultural and cross-regional comparisons on topics related to consumer privacy concerns to further reveal which aspects are consistent, which aspects are different, what are the roots of the differences, and which cultural and other environmental factors are at work.

5. CONCLUSION

This paper provides a multi-dimensional theoretical perspective to analyze and solve consumer privacy protection and data ethics issues by constructing an integrated framework and formulating evaluation criteria for the rationality of privacy response behaviors. Research results show that the privacy protection path coordinated by multiple subjects is more effective in reducing large-scale data leakage incidents. Compared with the traditional protection path, it significantly reduces the incidence of privacy violations. This study not only reveals the formation mechanism of the consumer privacy paradox, but also explores the measurement and cultivation of privacy literacy, as well as the antecedents and impacts of privacy fatigue. This paper provides valuable insights and practical guidance, but the research samples are mainly concentrated in specific cultures and regions, which may limit the general applicability of the research results. At the same time, the dynamic nature of privacy protection and the rapid changes in technological development mean that research frameworks and scales need to be continuously updated and verified, while the research design of this article mainly relies on interviews, which may be subject to subjective bias. Looking ahead, research on consumer privacy protection and data ethics needs to be further expanded to different cultural and legal contexts around the world to enhance the universality of research findings.

REFERENCE

[1]Chen Subai, Wei Juan. The “cost” of self-efficacy: A study on the paradox of privacy protection behavior of smart media users [J]. Modern Intelligence, 2024, 44(5): 58-69.

[2] Lin Yanping, Luo Danrui. Antitrust law analysis of data privacy protection: application dilemma and solution [J]. China Maritime Law Research, 2024, 35(1): 64-74.

[3]Ao Shan, Chang Xian, Wang Hui, Shen Zihao, Liu Kun, Liu Peiqian. Edge-assisted crowd-sensing location privacy-preserving multi-task allocation mechanism[J]. Journal of Computer Applications, 2024, 41(4): 1208-1213.

[4] Gao Gaimei, Zhang Jin, Liu Chunxia, Dang Weichao, Bai Shangwang. Crowdsourcing test task privacy protection scheme based on blockchain and CP-ABE strategy hiding[J]. Journal of Computer Applications, 2024, 44(3): 811-818.

[5]Guo Xian, Yuan Jianpeng, Feng Tao, Jiang Yongbo, Fang Junli, Wang Jing. Privacy-preserving autonomous identity management scheme for Internet of Vehicles[J]. Journal of Electronics & Information Technology, 2024, 46(7): 2783-2792.

[6]Boerman S C, Kruikemeier S, Zuiderveen Borgesius F J. Exploring motivations for online privacy protection behavior: Insights from panel data[J]. Communication Research, 2021, 48(7): 953-977.

[7]Quach S, Thaichon P, Martin K D, et al. Digital technologies: tensions in privacy and data[J]. Journal of the Academy of Marketing Science, 2022, 50(6): 1299-1323.

[8]Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges[J]. Egyptian Informatics Journal, 2021, 22(2): 177-183.

[9]Nguyen V L, Lin P C, Cheng B C, et al. Security and privacy for 6G: A survey on prospective technologies and challenges[J]. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2384-2428.

[10]Rigaki M, Garcia S. A survey of privacy attacks in machine learning[J]. ACM Computing Surveys, 2023, 56(4): 1-34.
[11]Rosenberg J M, Borchers C, Burchfield M A, et al. Posts about students on Facebook: A data ethics perspective[J]. Educational researcher, 2022, 51(8): 547-550.
[12]Bezuidenhout L, Ratti E. What does it mean to embed ethics in data science? An integrative approach based on microethics and virtues[J]. Ai & Society, 2021, 36(3): 939-953.
[13]Batlle J C, Dreyer K, Allen B, et al. Data sharing of imaging in an evolving health care world: report of the ACR Data Sharing Workgroup, part 1: data ethics of privacy, consent, and anonymization[J]. Journal of the American College of Radiology, 2021, 18(12): 1646-1654.
[14]Tursunbayeva A, Pagliari C, Di Lauro S, et al. The ethics of people analytics: risks, opportunities and recommendations[J]. Personnel Review, 2022, 51(3): 900-921.
[15]Nguyen A, Ngo H N, Hong Y, et al. Ethical principles for artificial intelligence in education[J]. Education and Information Technologies, 2023, 28(4): 4221-4241.
[16] AL-Qadri, A. H., Zhao, W., Li, M., Al-khresheh, M., & Boudouaia, A. (2022). Emotional intelligence scale for international students: a Proposal for a developed version. *Frontiers in Education*, 7,853303.https://doi.org/10.3389/feduc.2022.853303
[17]Al-khresheh, M. H., & Orak, S. D. (2021). The Place of Grammar Instruction in the 21st Century: Exploring Global Perspectives of English Teachers towards the Role of Teaching Grammar in EFL/ESL Classrooms. *World Journal of English Language*, *11*(1). https://doi.org/10.5430/wjel.v11n1p9
[18]Helaudho, B., Mukhtar, S., & Pahala, I. (2024). Optimizing Performance: The Role of Job Rotation in Employee Motivation and Satisfaction. *Pakistan Journal of Life & Social Sciences*, *22*(2).
[19]Jam, F. A., Singh, S. K. G., Ng, B., & Aziz, N. (2018). The interactive effect of uncertainty avoidance cultural values and leadership styles on open service innovation: A look at malaysian healthcare sector. *International Journal of Business and Administrative Studies*, *4*(5), 208-223.