Scholar Publishing Group
International Journal of Big Data Intelligent Technology
https://doi.org/10.38007/IJBDIT.2025.060101
ISSN 2790-0932 Vol. 6, Issue 1: 1-10

The Dilemma And Solution Of Citizen Privacy Protection In The Governance Of Network Social Security

Xinying Huang[1, a*]

[1]*Goldsmiths, University of London*

[a] *email: wojiaohxy123@gmail.com*

[*]*corresponding author*

Keywords: online society; Security governance; Citizen privacy; hacker

Abstract: In today's era, information technology is developing rapidly at an unprecedented speed, and the online society has deeply integrated into people's daily lives, becoming an indispensable part. However, at the same time, in the field of security governance in the online society, citizen privacy protection is facing a series of severe challenges. These challenges cover multiple aspects, including unavoidable technological vulnerabilities that make citizens' privacy information vulnerable to illegal access and abuse; There are obvious imperfections in laws and regulations regarding the protection of online privacy, resulting in a lack of clear and strong legal basis and protection in practical operations; And the general lack of privacy awareness among citizens often leads to their unintentional exposure of personal privacy in online activities, providing opportunities for criminals to take advantage of. This article will delve into the underlying causes of these dilemmas and strive to propose targeted and actionable solutions. Specifically, we will focus on exploring how to enhance the security of network systems through strengthening technological innovation, such as developing more advanced encryption technologies, access control measures, and data anonymization methods, in order to build a solid protective barrier for the transmission and storage of citizens' privacy data. At the same time, it emphasizes the importance of improving laws and regulations, calls for the development of specialized and detailed regulations on online privacy protection, clearly defining the scope and specific content of citizens' privacy rights, strictly regulating the behavior of network operators, and significantly increasing the punishment for online privacy infringement to form an effective legal deterrent. In addition, we will also focus on how to strengthen citizen education through diverse channels and forms, such as conducting extensive cybersecurity publicity activities, publishing practical online privacy protection guidelines, and setting up relevant courses in schools and communities, effectively improving citizens' awareness of privacy protection and self-protection ability, and promoting them to develop good and safe internet usage habits. In summary, the core objective of this article is to explore feasible paths for effectively protecting citizens' privacy in the online society.

1. Introduction

In today's digital age, network technology is permeating every aspect of people's lives at an unprecedented speed. Its popularity undoubtedly brings immeasurable convenience to people, completely changing their way of life, work patterns, and social forms. People can easily access information from around the world through the internet, enabling remote work and instant communication with distant family and friends. Online shopping allows people to buy their desired products without leaving their homes, online education breaks through the limitations of time and space in learning, and various social media platforms enable people to share their daily lives with people from different corners of the world. However, just as a coin has two sides, while network technology brings many conveniences, it also raises a series of security issues that cannot be ignored. Among these issues, the protection of citizen privacy is particularly prominent and urgent. With the continuous development and application of network technology, the collection, storage, transmission, and use of personal information have become increasingly frequent and complex. From various mobile applications and websites we use in our daily lives to various IoT devices, we are constantly collecting our personal information, including name, age, gender, contact information, home address, consumption habits, interests and hobbies. These information are not only stored in large quantities on cloud servers and databases, but also frequently transmitted and shared between different platforms and institutions. At the same time, network hackers, criminals, and some unscrupulous enterprises are also coveting these valuable personal information. They steal citizens' privacy information through various means such as cyber attacks, malware, phishing websites, etc., and use it for illegal activities such as fraud, extortion, and illegal marketing. This poses an unprecedented threat to citizens' privacy. Once sensitive privacy such as personal photos, financial information, and health data of citizens are leaked, it may cause serious economic losses, mental harm, and even endanger personal safety. Moreover, the impact of privacy breaches is not limited to individuals, but may also affect the stability and security of the entire society.Therefore, it is of great practical significance to explore in depth the difficulties faced by citizens' privacy protection in the governance of network social security and to find effective ways out. This is not only related to the vital interests of every citizen, but also a necessary prerequisite for building a safe, stable, and harmonious online social environment. Only by addressing the issue of citizen privacy protection can we truly enjoy the convenience brought by network technology, rather than being troubled by the risks it brings. Through in-depth research and practical measures, we can provide effective protection for citizens' privacy in cyberspace, making the internet a powerful tool for promoting human development and progress, rather than a hidden danger that threatens individual rights and interests.

2. The dilemma of citizen privacy protection in the governance of network social security

2.1. Technical challenges and lagging laws and regulations

2.1.1. Technical aspect

The cyberspace has become an important target for hacker attacks. Hackers use various advanced technological means to search for vulnerabilities in network systems, thereby invading the network devices of enterprises, government agencies, and even individual users, stealing a large amount of information containing citizens' personal privacy. These hacker attack methods are becoming increasingly complex and diverse, ranging from traditional network scanning and vulnerability exploitation to more targeted advanced persistent threat (APT) attacks, making it difficult for people to defend against. For example, by sending carefully disguised phishing emails

to lure users into clicking on malicious links or downloading malicious attachments, once the user is deceived, hackers can easily break through the network defense line and obtain sensitive data. Malicious software is also a major threat to citizens' privacy. Various types of malicious software such as spyware, ransomware, and adware are constantly emerging. Spyware can be quietly installed on devices without the user's knowledge, monitoring their network activities and collecting privacy information such as browsing history, entered passwords, chat records, etc. Ransomware encrypts users' important files, threatening them to pay ransom to recover data, and in the process, users' personal information may also be leaked. Advertising software will constantly pop up annoying ads, which not only affect user experience, but may also collect information about users' browsing habits and interests for precise advertising placement. Data breaches are not uncommon, as insufficient network security measures by enterprises and institutions, or negligence by internal personnel, result in a large amount of user data being exposed on the internet. These data contain users' personal identity information, financial information, health information, etc. Once obtained by criminals, it will bring great harm to users. For example, a data breach incident on a large e-commerce platform resulted in the disclosure of millions of users' names, addresses, phone numbers, and credit card information, causing panic among users about personal privacy and security.

At the same time, emerging technologies such as big data, cloud computing, and the Internet of Things, while providing convenient services for people, have also increased the difficulty of privacy protection due to their own characteristics. Big data technology can process and analyze massive amounts of data, but in the process of data collection and analysis, it is often difficult to ensure sufficient protection of personal privacy. Due to the wide range of data sources and diverse types, it is difficult to clearly define which data belongs to personal privacy and which can be used for analysis. Moreover, big data analysis may reveal sensitive information that individuals are unwilling to disclose, such as their health status, consumption habits, social relationships, etc. Cloud computing enables data storage and processing to be transferred from local to cloud, and users' control over their own data is relatively weakened. Once there are vulnerabilities in the security measures of cloud service providers or improper encryption of data during transmission between different cloud platforms, it may lead to data leakage. In addition, there are differences in laws and regulations among different countries and regions, and data may also face compliance issues during cross-border transmission. The Internet of Things connects various devices to the network, making everything from household appliances to industrial equipment a potential source of data. However, many IoT devices have weak security protection capabilities and are easily hacked. The large amount of personal life data collected by these devices, such as household activity patterns, personal health data, etc., if stolen, will seriously violate citizens' privacy.

2.1.2. Technical aspect

In the face of these technological challenges, China's existing laws and regulations on network privacy protection appear to be inadequate. Firstly, legal provisions are scattered across different laws and regulations, lacking systematicity and integrity. The regulations related to online privacy protection may be scattered in multiple laws such as the Cybersecurity Law, Civil Code, Criminal Law, etc., which makes it difficult to apply and coordinate the law in practical applications and form an effective legal protection system. The specificity of laws and regulations is not strong. For the privacy protection issues brought by emerging technologies, such as privacy boundaries in big data analysis and security regulations for IoT devices, existing laws have not provided clear and specific provisions, resulting in a lack of clear legal basis when dealing with related issues. And the insufficient punishment is also a prominent issue. In cases of online privacy infringement, even if

the infringer is found to be illegal, the punishment they face is often relatively light and cannot form sufficient deterrence. This has led some companies and individuals, driven by their own interests, to take risks and invade citizens' privacy. For example, in actual cases of online privacy infringement, victims often find it difficult to protect their legitimate rights and interests. Due to unclear legal provisions, they may encounter many obstacles in seeking legal remedies and not know which law or clause to rely on to assert their rights. Moreover, even if rights can be protected through legal means, due to insufficient punishment, infringers may not receive substantial punishment, and victims may find it difficult to obtain sufficient compensation and indemnification. This situation not only damages the personal rights and interests of citizens, but also hinders the healthy development of the entire online society. If citizens' privacy is not effectively protected, they will develop fear and distrust towards network technology, thereby hindering its further promotion and application. Meanwhile, the imperfection of laws and regulations can also affect the innovation and development of enterprises, as they may hesitate to utilize new technologies due to legal uncertainty or give up some potential business models in order to avoid legal risks.

The challenges at the technical level and the lag in laws and regulations jointly constitute a major dilemma in protecting citizens' privacy in the governance of network social security. To solve these problems, efforts need to be made simultaneously in technological innovation and legal improvement, forming a situation of mutual cooperation and promotion.

2.2. Lack of industry self-discipline and weak privacy awareness

In the tide of the network society, some Internet enterprises, driven by commercial interests, have deviated from due moral and responsibility norms, posing a serious threat to the protection of citizens' privacy. In order to maximize profits, these companies resort to any means necessary to excessively collect users' personal information. When designing applications and services, they often embed various hidden data collection mechanisms, ranging from basic user identity information such as name, age, gender, to more sensitive financial status, health data, geographic location, etc., all of which are within their collection scope. This excessive collection behavior not only exceeds the reasonable scope required to provide services to users, but also largely infringes on users' autonomy and right to know. What is even more worrying is that these companies use the collected personal information for various commercial activities without the explicit consent of users. Advertising push is one of the most common methods, where companies accurately push various advertisements to users based on their personal preferences, consumption habits, and other information, in order to obtain substantial advertising revenue. Data analysis is also one of their commonly used methods. Through deep mining and analysis of a large amount of user data, enterprises attempt to discover market trends and user needs, optimize products and services, and enhance their competitiveness. This unauthorized use not only violates the user's trust, but also seriously infringes on the user's privacy rights. For example, a certain social platform was exposed for providing users' personal data to third parties for precise advertising without their knowledge, which has sparked strong public dissatisfaction and questioning. And some enterprises have serious vulnerabilities in data security management, which further exacerbates the risk of user privacy data leakage. Due to the lack of sufficient security investment and professional technical personnel, the database protection capability of enterprises is weak, making them easy targets for hacker attacks. At the same time, internal management chaos may also lead to employees being able to access and process large amounts of user data at will, increasing the possibility of data being maliciously leaked or manipulated. For example, a well-known hotel group's database was hacked, resulting in millions of customers' personal information, including names, credit card numbers, accommodation records, etc., being stolen and sold on the dark web, causing huge economic losses and credit risks

to users.

Citizens generally show neglect of personal privacy protection when enjoying the convenient services brought by the internet. In this era of information explosion, people are immersed in the rich content and convenient functions of the internet, often failing to fully realize the potential risks to personal privacy. They freely disclose personal information on the internet, such as revealing their life details, family situation, work experience, etc. on social media. Once these information are obtained and utilized by criminals, it may bring many troubles to individuals. Moreover, when downloading and using various software, many users often easily agree to the software's privacy terms without hesitation. These privacy terms are often lengthy and complex, filled with professional terminology and legal provisions, making it difficult for ordinary users to understand their true meaning in a short period of time. However, in order to quickly use the software's features, users often choose to ignore the potential risks and blindly click the "agree" button. This behavior is actually unconsciously surrendering one's personal privacy. The reasons for this phenomenon are multifaceted, and the rapid development of network technology makes it difficult for citizens to adapt to new privacy protection needs in a short period of time. Faced with an endless stream of new technologies and applications, citizens often lack sufficient knowledge and skills to assess privacy risks. Some citizens have insufficient awareness of the value of personal privacy, believing that their information is not important or holding a lucky mentality, believing that privacy breaches will not happen to them. Some misleading information in the online environment has also played a role in fueling the situation. Some unscrupulous merchants use false advertising and exaggeration to make users mistakenly believe that providing personal information can provide more discounts and convenience, thereby inducing users to voluntarily give up privacy protection. For example, some free internet service providers claim that users only need to provide a large amount of personal information to enjoy premium services, but in reality, this information is used for other commercial purposes. The current situation of weak citizen privacy awareness poses a huge challenge to the governance of network social security. Firstly, it makes it easier for criminals to access and exploit citizens' personal privacy, thereby carrying out various illegal and criminal activities such as fraud, extortion, identity theft, etc. Secondly, the neglect of privacy protection by citizens has weakened the supervisory power of society over enterprises and governments, making it difficult for some violations to be corrected and punished in a timely manner.

The lack of industry self-discipline and the weak awareness of citizen privacy jointly constitute the two major challenges in protecting citizen privacy in the governance of network social security. To solve these problems, it is necessary for the government, enterprises, and individual citizens to work together, strengthen supervision, enhance self-discipline, raise awareness, and create a good atmosphere for the whole society to jointly protect citizens' privacy.

3. The way out for citizen privacy protection in the governance of network social security

3.1. Strengthen technological innovation and improve regulations

In the governance of network social security, strengthening technological innovation and improving regulations are key ways to protect citizens' privacy. The government, enterprises, and research institutions should work together to invest more resources in technology research and development, including not only funding but also talent cultivation and infrastructure construction. By establishing special research funds and providing tax incentives and other policy measures, we encourage researchers and enterprises to actively engage in innovative research on network security technology.

Improving the security and stability of network systems is the foundation for protecting citizens' privacy. One of the core components is the adoption of advanced encryption technology.

Encryption technology can convert citizens' private data into ciphertext, making it difficult to crack and read even if the data is intercepted during transmission. For example, using asymmetric encryption algorithms to provide high-strength encryption protection for data transmission, ensuring that only authorized recipients can decrypt and obtain data. Access control technology can restrict access to citizens' private data. By using techniques such as role-based access control or attribute based access control, it is strictly stipulated that only authorized personnel or systems can access specific data, thereby reducing the risk of unauthorized access to data. Data anonymization technology is also an important means of safeguarding citizens' privacy. In the process of data use and sharing, desensitize the data containing sensitive information, such as partially hiding or replacing the name, ID number number, bank card number, etc., which can not only meet the needs of data analysis and application, but also prevent the direct disclosure of sensitive information. Strengthening research and standardization of emerging technologies is imperative. With the rapid development and widespread application of emerging technologies such as artificial intelligence, blockchain, and 5G, new privacy protection issues are constantly emerging. For example, artificial intelligence algorithms may inadvertently leak citizens' privacy during training, the tamper proof nature of blockchain may make it difficult to delete private data once it is on the chain, and the high speed and low latency of 5G networks may increase the risk of data leakage. Therefore, it is necessary to conduct timely research on these emerging technologies, develop relevant technical standards and safety guidelines, and guide the rational application of technologies.

It is of great significance to formulate specialized laws for the protection of online privacy. Currently, China's laws and regulations on online privacy protection are scattered among different laws and regulations, lacking systematicity and specificity. Developing a specialized internet privacy protection law can clarify the scope and content of citizens' privacy rights, providing clear legal basis for citizens' privacy protection. This law should provide detailed regulations on citizens' rights to control, be informed, and delete personal information, clarify which information falls within the scope of citizens' privacy, and under what circumstances it can be collected, used, and shared.

Standardizing the behavior of network operators is one of the important tasks of the Internet Privacy Protection Law. Network operators should follow the principles of legality, legitimacy, and necessity in the process of collecting, storing, and using citizens' privacy data, and take corresponding security protection measures. The law should clarify the disclosure obligation of network operators, that is, before collecting user information, they must inform users of the purpose, method, and scope of the collection in a clear and explicit manner, and obtain users' explicit consent. At the same time, network operators should establish a sound data security management system, conduct regular security assessments and risk monitoring, take timely remedial measures for data leakage incidents, and report to relevant departments. Increasing the punishment for online privacy infringement can form an effective legal deterrent. For acts that violate the Internet Privacy Protection Law, severe administrative penalties and civil compensation responsibilities should be imposed, and even criminal liability should be pursued in serious cases. High fines, compensation amounts, and criminal sanctions can impose heavy costs on infringers, thereby curbing the occurrence of infringement.

In addition, strengthening the connection and coordination between different laws and regulations is also the key to building a complete and effective legal system for protecting online privacy. The protection of online privacy involves multiple legal fields, such as civil law, criminal law, administrative law, etc., and consistency and coordination should be maintained between different laws and regulations. For example, the provisions on civil compensation liability for citizens' privacy rights in civil law should be aligned with relevant provisions in the Internet Privacy Protection Law, and the criteria and sentencing range for the crime of infringing on citizens'

personal information in criminal law should be coordinated with other relevant laws and regulations. By strengthening technological innovation and improving regulations, we can build a strong defense line for protecting citizens' privacy. Technological innovation provides powerful tools and means for privacy protection, while regulatory improvement provides clear norms and constraints for technological applications. Only by combining technology and regulations can we effectively protect citizens' privacy in the online society and promote its healthy and stable development. For example, in a certain financial institution, the security of customers' transaction data and personal information has been successfully ensured by adopting advanced encryption technology and access control technology. Meanwhile, due to the continuous improvement of China's laws and regulations on online privacy protection, this financial institution has become more standardized and cautious in its data processing, effectively avoiding customer privacy breaches caused by illegal and irregular operations. For another example, when developing new applications, an Internet enterprise followed the relevant technical standards and security guidelines, reasonably collected and used user data, and assumed corresponding legal liabilities according to a sound legal system after the occurrence of a data leakage event, timely took measures to compensate for user losses and safeguard the legitimate rights and interests of users. Strengthening technological innovation and improving regulations are important ways to protect citizens' privacy in the governance of network social security. It requires the joint efforts of the government, enterprises, research institutions, and all sectors of society to continuously promote and implement them.

3.2. Strengthen industry self-discipline and public education

In the online society, protecting citizens' privacy requires not only technological innovation and improving regulations, but also strengthening industry self-discipline and enhancing public education. Internet enterprises, as network service providers and main data processors, should establish correct values, put users' interests first, consciously abide by laws, regulations and ethics, and assume the important responsibility of protecting users' personal information. In the fierce market competition, enterprises cannot only pursue short-term economic benefits and ignore the privacy and security of users. It should be recognized that only by winning the trust of users can enterprises achieve long-term sustainable development.

Establishing a sound internal data management system is a key measure for enterprises to protect user privacy. Firstly, enterprises need to clarify the purpose and scope of data collection, ensuring that only user information directly related to and necessary for providing services is collected. When collecting data, users should be informed of the reasons and purposes of the collection in a clear, explicit, and easily understandable manner, and obtain their explicit consent. For sensitive information, such as ID card number and bank card information, strict encryption and protection measures should be taken. In terms of data usage, enterprises should follow the principles of legality, legitimacy, and necessity, strictly use it for the purpose declared in advance, and shall not change its purpose or use it for other unauthorized commercial activities without authorization. At the same time, establish a strict data access permission system, and only authorized employees can access and process user data when necessary. The data storage process cannot be ignored either. Enterprises should adopt secure and reliable storage technologies and devices, encrypt user data for storage, and regularly backup data to prevent data loss. In addition, it is necessary to strengthen the security protection of storage systems to prevent hacker attacks and illegal intrusions. In terms of data destruction, enterprises should establish clear processes and standards. When a user requests the deletion of their personal information or data and the retention period has expired, the enterprise should ensure that the relevant data is completely deleted and cannot be recovered. Meanwhile, industry associations should play an active supervisory role in promoting corporate self-discipline.

Industry associations can establish industry norms and self regulatory conventions to provide clear guidance and constraints for the behavior of enterprises. These norms and conventions can cover all aspects of data processing, including the legality of data collection, the reasonableness of use, the security of storage, and the thoroughness of destruction. For enterprises that violate industry norms and self-discipline conventions, industry associations should take serious disciplinary measures, such as warnings, public criticism, fines, and even revocation of membership. Through this approach, companies are encouraged to comply with industry standards and jointly maintain a good market order and user privacy security.

In addition to strengthening industry self-discipline, enhancing education on online privacy protection for citizens is also an urgent task. Through various channels and forms, extensive education on online privacy protection can enhance citizens' awareness of privacy and self-protection capabilities, thereby reducing the risk of privacy breaches at the source. The government and social organizations can regularly organize cybersecurity publicity weeks. During the event, knowledge and skills on online privacy protection will be disseminated to the public through lectures, exhibitions, online and offline interactions, and other forms. Invite experts, scholars, law enforcement personnel, and technical experts to explain cases, causes, and prevention methods of online privacy breaches to the public, and raise public awareness. Publishing online privacy protection guidelines is also an effective way of education. A guide can introduce the basic principles of online privacy protection, common privacy threats, and countermeasures to citizens in easy to understand language. For example, how to set strong passwords, how to identify phishing websites, and how to use public wireless networks with caution. These guidelines can be widely disseminated through government websites, social media, public service venues, and other channels to facilitate citizens' access and learning.

Offering relevant courses in schools and communities, incorporating online privacy protection education into the formal education system, can fundamentally enhance citizens' awareness of privacy protection. In schools, corresponding course content and teaching methods are designed for students of different age groups to cultivate good internet usage habits and privacy protection awareness from an early age. In the community, residents can be organized to participate in online privacy protection training, and professionals can be invited to give lectures and answer questions to solve privacy protection issues encountered by residents in their actual lives.

Through these educational measures, citizens can fully understand the importance of personal privacy. Recognizing that personal privacy is not only related to individual dignity and rights, but also to social fairness, justice, and the rule of law. At the same time, master the methods and techniques for protecting personal privacy, learn how to identify potential privacy threats in the online environment, such as links from unknown sources, applications that excessively request permissions, etc., and take corresponding preventive measures, such as refusing to provide unnecessary personal information and regularly checking the permission settings of applications. Developing good internet usage habits is an important aspect of protecting privacy. For example, avoid entering sensitive personal information on untrusted websites, refrain from disclosing too many personal life details on social media, regularly update passwords and use different strong passwords, etc. For example, an Internet enterprise actively responded to the call for self-discipline in the industry, established a sound data management system, strictly regulated the collection, use, storage and destruction of user data, and strengthened data security protection through technical means. At the same time, the company also participates in training and exchange activities organized by industry associations, continuously improving its level of privacy protection, establishing a good corporate image, and winning the trust of users and market recognition. For example, in a certain community, by carrying out online privacy protection education activities, residents' privacy awareness has been significantly improved. They are more cautious when using

online services, actively paying attention to the privacy policies of applications, and learning how to protect their own and their family's privacy information. The number of online fraud and privacy breaches within the community has significantly decreased, making residents' online lives safer and more reassuring. Strengthening industry self-discipline and enhancing public education are important ways to protect citizens' privacy in the governance of network social security. Only when Internet enterprises consciously fulfill their responsibilities, industry associations play an effective role in supervision, and citizens have sufficient awareness and ability of privacy protection, can we jointly build a safe and reliable network environment and protect citizens' privacy rights and interests.

4. Conclusion

The rapid development of the online society undoubtedly brings unprecedented challenges to the protection of citizens' privacy. On the one hand, the rapid and widespread dissemination of information makes personal privacy information more easily accessible and abused; On the other hand, the continuous emergence of new technologies has also brought many privacy and security risks that are difficult to predict and prevent. But we should not only see the challenges, but also realize that this development provides us with valuable opportunities for innovation and improvement in citizen privacy protection. Strengthening technological innovation can create a stronger defense line for citizens' privacy protection. Continuously developing new encryption technologies, security algorithms, and monitoring methods can effectively prevent privacy information from being stolen and leaked. Improving laws and regulations can clarify the boundaries and protection standards of citizens' privacy rights, provide powerful legal remedies for victims, and form a strong deterrent against infringers. Strengthening industry self-discipline can encourage enterprises to consciously follow ethical and legal norms while pursuing economic benefits, and actively protect user privacy. Strengthening civic education can enhance citizens' awareness and ability to protect their privacy, and reduce the risk of privacy breaches from the source. Through the joint efforts in various aspects mentioned above, we are confident in gradually getting rid of the dilemma of citizen privacy protection, and building a safe, reliable, and harmonious online social environment is no longer an unattainable dream. In such an environment, citizens can enjoy the convenience brought by the internet without any worries, freely communicate, obtain information, and carry out various activities. Their privacy rights will be fully protected and respected, and they will no longer constantly worry about personal information being exposed or abused. This is not only an inevitable requirement for the development of the online society, but also an important manifestation of realizing citizens' rights and social fairness and justice. Only when citizens' privacy is effectively protected can they truly feel freedom and equality in cyberspace, and the online society can achieve healthy, orderly, and sustainable development, creating more value and well-being for humanity.

References

[1] Nissenbaum, Helen. "Protecting privacy in an information age: The problem of privacy in public." The ethics of information technologies. Routledge, 2020. 141-178.

[2] Bojović, Živko, et al. "Interconnected Government Services: An approach toward smart government." Applied Sciences 13.2 (2023): 1062.

[3] Chentouf, F. Z., & Bouchkaren, S. (2023). Security and privacy in smart city: a secure e-voting system based on blockchain. International Journal of Electrical and Computer Engineering, 13(2), 1848.

[4] Khaskheli M B, Wang S, Yan X, et al. Innovation of the social security, legal risks, sustainable management practices and employee environmental awareness in the China–Pakistan economic corridor[J]. Sustainability, 2023, 15(2): 1021.

[5] Vasudevan, S., Piazza, A., & Carr, M. (2023, March). A decade of studies on cyber security training in organizations using social network analysis: a systematic literature review through keyword co-occurrence network. In 2023 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1-6). IEEE.

[6] Zhang, H., Mi, Y., Liu, X., Zhang, Y., Wang, J., & Tan, J. (2023). A differential game approach for real-time security defense decision in scale-free networks. Computer Networks, 224, 109635.