Research on Privacy Protection Under the Background of Digital Economy

2021, Vol.2 No.1
© Economics & Management Review 2021
DOI: 10.37420/j.emr.2021.002
https://masonpublish.org

Yan Jing*, Wenting Chen
Zhejiang Financial College, Zhejiang, China
***Corresponding author, e-mail: J18966170058@163.com**

Abstract

In the context of the gradual advent of the economic era, the value of data is constantly improving, and the relationship between data security and economic operation security, national security, personal legitimate rights and interests, and social public security is getting closer. In the digital economy era, there are new frame, business, and technology, which leads to new requirement about privacy protection and data security. In this context, data security threats are becoming more and more serious, and major data security incidents occur frequently. Data leakage and privacy issues have become the main factors restricting the development of the digital economy, and the establishment of a data security system is the main link in the healthy development of the digital economy. Hence, this article analyzes personal information leakage and privacy protection issues in the era of digital economy, seeks for problems in the process of privacy protection, and proposes effective approaches to protect privacy in the digital economy context.

Keywords

Digital economy; Privacy protection; Information privacy

Introduction

In the 21st Century, with the continuous development of social economy and scientific technology, e-commerce and social network have expanded the scope of Internet usage. The volume of data is increasing continuously and penetrating various industries and fields widely. Data becomes the main factor of production gradually. As the enduring increase in the volume of data, traditional data processing technologies could not satisfy the modern environment demands, therefore the new generation of data processing technologies are required to solve this problem.

The foreign scholar Bloustein classified the privacy into group privacy and individual privacy. He indicated that group privacy refers to the way of people's privacy in their relationship with others, while individual privacy refers to the state of being undisturbed and alone. R.Gavison stated that privacy mainly includes anonymity, solitude, and confidentiality. Confidentiality means that the party who knows the information of others must keep the information confidential; anonymity means that people are able to express freely, and will

not be noticed by others in a certain situation; solitude means to hide, and does not want others to approach. British scholar Keelung O'Hara explained the privacy threats caused by current data technology and analyzed the advantages of data technology. He believes that people's work and life in the process of being monitored increasingly rely on data technology, if people's data marks are in the electronic activity, they would leak their privacy in this process anytime. American scholar Davis and others published the first related big data ethics research monograph, which stated that people are currently living in an era of changing technology. Gong Yongqin(2016) proposed that n this era, the development of big data technology provides people with the urgency of new thinking and requires better ethical thinking.

China has also launched relevant research in the era of the digital economy. Guodeng Feng and others analyzed security protection technologies, including role mining, data anonymous release protection, and social anonymity protection, etc. In addition, they fully study the lack of big data privacy research at this stage. In his opinion, there are a lack of research on big data privacy and security protection, the issues of big data privacy and security are able to be solved effectively only through combining corresponding technical means and policies and regulations. Moreover, some scholars have conducted research on location-aware technology in the digital economy era, analyzed the threat of location-aware technology to privacy, summarized and created location data supply models, and analyzed location privacy protection technology base on this. Finally, the direction of user privacy protection technology in the future development process is proposed. Researchers from the Chinese Academy of Social Sciences have studied the ethical issues in the R&D, innovation, and use of big data technology. In the process of analyzing privacy issues, they believe that in the era of big data, personal information has many aspects, and it is prone to abuse in business or other areas. Under this situation, the main factors for the sustainable development of big data are put forward: First, consumers benefit more than the cost of sharing data; second, ensure high transparency in the process of using data; third, protect personal privacy.

In conclusion, modern scholars have made abundant research achievements on digital economy, big data and privacy through diversified perspectives. However, there are still some problems with big data privacy research. At present, the study on privacy security in the digital economy era are scattered. Most of the study are short journal articles and lack of comprehensive new systematic research. Therefore, this paper analyzes the privacy security issues in the digital economy era from a comprehensive perspective.

Main Ways of Information Leakage

Mobile Devices

Table 1 is a statistical table of Internet device usage in 2019, which shows that mobile phones have the highest usage rate. As of the end of December 2019, the proportion of mobile Internet users in my country accounted for 98.6%, an increase of 2.5 percentage points from the previous year. The probability of privacy leakage increases by using smartphones widely. People get used to storing their personal information, words into their phones, and criminals could get personal information in simple ways, which could lead to privacy leakage.

Table 1. Statistics on Internet Device Usage in 2019

Number	Device	Percentage /%
1	Desktop	53.1%
2	Television	28.1%
3	Mobile phone	98.6%
4	Laptop	35.9%
5	Flat computer	26.9%

Wireless Network

In the process of continuous development of network, the development of wireless network is promoted to make people's life and work more convenient. Most people can use free wireless network anytime and anywhere to surf the Internet and realize data transmission. However, there are vulnerabilities in the use of wireless networks. Criminals use mobile devices connected to wireless networks to obtain user information and then steal payment accounts, thus causing property losses to customers.

Public Facilities

With the development of digital economy, the progress of scientific technology has been promoted. Meanwhile, China reinforces security governance, and constantly regulates public behaviors. The government is enabled to monitor and manage people’s routine behavior in urban security and traffic management by HD cameras. When the crime happens, this device can record the evidence and clue of it. However, people’s lives are monitored, and people have lost a certain right to privacy. Although the public security department can provide data support through the electronic monitoring system to improve public security during the investigation of the case, it also reveals people's daily activities. Zhou Hui et(2013) considered if information leakage occurs, residents will face huge privacy security risks.

Mobile Payment

With the constant development of information technology, the progress of mobile payment has been promoted. The scale of mobile payment users is also continuously increasing, and so is online payment. In addition to takeaways, taxis, shopping, etc., mobile payment has been widely used in public service departments, and it has gradually shifted from the early payment of utility bills to medical care and public transportation. In the process of using mobile payment, Hung, H. and Wong, Y.H. (2009) found that users are required to provide their own information. But if the third-party information database is leaked, it will cause the losses of personal property and privacy.

Fingerprint Identification

Biometric identification technology has been gradually developed in the process of continuous technological progress, and people started to use fingerprint identification and facial recognition on a large scale. Various

phone manufacturers have also developed advanced and convenient ways to unlock phones, such as facial recognition. Most manufacturers use iris recognition and 3D facial scanning in the design of facial recognition. Lacking high security recognition technology, manufacturers mostly use software algorithms and 2D photos, so there are a lot of technical vulnerabilities. Users can unlock the face with simple methods, such as printing photos. Tan Xiaxia(2019) found that with the continuous development of science and technology, modern security identification system also appears the possibility of cracking. Secondly, the secure storage of personal privacy information for fingerprint recognition and face recognition is uncertain.

Abuse of Personal Information

In the process of the rapid development of the global digital economy, personal information protection laws have received much more attention. In the production process of the digital economy, data is the main material, and data is related to the development of the digital economy. The analysis and mining of large amounts of data can realize the generation of big data, thereby providing a new engine for the development of the digital economy. Base on this, data in an enterprise refers to wealth, and those who have more and more important data are equivalent to having a mass of productive materials and is enabled to turn data to profit. Applying big data to digital economy enterprises can optimize their own services, realize precision marketing, risk control and so on, which can meet their own development needs. However, it can also violate personal information, leading to the conflict between the protection of personal information and the development of the digital economy.

Firstly, personal information is abused in the process of using big data. The enterprise must meet the original purpose of personal information collection and cannot change the purpose of data. However, in the course of practice, through personal information collection, digital economy companies use big data to carry out precision marketing, or big data "kill cooked"—Services and goods are the same, while the price of old customers is higher than that of new customers. For mobile phone personal information, a few digital economy companies also use data to conduct illegal transactions for profit.

Secondly, there is a situation that some digital economy enterprises have an excessive collection of personal information. Obtaining personal information beyond the scope has become an unspoken rule in the development of the industry, and users' own information is excessively collected by enterprises without users' knowledge. Some apps still have compulsory rights, requiring users to uniformly read information content and communication rate, realize the sharing of location information, obtain user rights, etc. Otherwise, users cannot use the software.

Thirdly Enterprises cannot guarantee the security of personal information. Some enterprises collect user information and lack high-security assurance. Not only can companies cause personal information to leak, but they can also be stolen by insiders or hackers. According to research by management consulting firms and other research institutions, 69% of 208 companies surveyed had experienced data theft by insiders in the past year.

To sum up, the big data era promotes the development of the digital economy and affects personal information protection. Vincent Mosco (2018) proposed that the future development of digital economy enterprises is

closely related to the level of personal information protection.

Research on Privacy Protection

Harm of Data Leakage

At present, digital development is more and more rapid, big data is widely used in every corner. In the process of enjoying the convenience advantages of big data, corresponding network security incidents will also occur. It mainly includes data privacy leakage event, which brings certain harm to people.

One is the personal level. The sensitive information in the user's identity information will be exposed in the network, which poses a serious threat to the property and personal security. In recent years, there have been a large number of data privacy leakage incidents, and criminals are using more and more ways to leak data, common means including network fraud, telecommunications fraud and so on. In addition, the leakage of data privacy will affect users' thinking, and some criminals will get the wrong guidance of data analysis users' thinking.

Second, the social level. The leakage of user privacy is only a small part compared with that at the social level, and the resulting impact is smaller than that at the social level. Some criminals will hack into government departments to collect data and carry out illegal activities, and the loss of government data will threaten the departments. For some companies, data leaks can cause irreparable damage.

At present, frequent network security incidents, whether property loss or thought kidnapping, will lead to irreparable impact on the society, the country and users. In the process of continuous development of big data, the big data system is also expanded. Therefore, the need for rigorous computer data protection and storage. However, in the data storage procedure, most of the data will be stored in the set database, if the database protection problems will lead to a large number of data leakage and loss. Therefore, more and more network security incidents, resulting in the loss of a large number of assets, affecting the user's thinking. In the context of the modern era, the development of digital technology has promoted the disclosure of personal information in the network, in the instant messaging, the use of disguised information, so as not to disclose their own information in the network is a mistake. With the continuous development of the Internet, personal information is involved in both online browsing and online shopping. Yi Xianrong (2019) proposed that in the digital age, everyone is invisible.

Legal Limitations of Privacy Protection

In addition to the issue of information disclosure in privacy protection, there are also existing legal limitations. One is that legislation is not systematic. The relevant privacy protection clauses in Chinese laws are relatively few and scattered, so a large number of laws, regulations and regulations should be inquired in the specific use process. Because the main body that promulgate, make is different, this law makes a standard to also differ, effectiveness grade is poorer, cannot echo each other. Generally speaking, the privacy protection directly mentioned is regulated and regulated at a low level, while the highly effective laws and regulations

are only the spirit of privacy protection, without clear stripes of privacy protection, leading to the lack of sufficient support for the lower level law in the legislative process.

Second, there is a lack of direct protection. At present, although privacy is displayed in the department law in China, it is realized by means of protecting the right of honor and reputation. In the past, the connotation of privacy right was limited and personality right such as reputation right was protected. In the process of continuous development of technology, privacy right gradually exists independently from other personal rights, and also shows the characteristics of property right, which cannot be protected by the old law. Privacy has a rich connotation and promotes the enactment of relevant legislation for the protection of personal data and information, but the three are different and cannot be fully applied to meet the needs. There is no direct reference to the privacy law, whether in the Constitution or any other branch of law. Generally speaking, China's modern personal privacy protection laws are only general principles without specific implementation rules. The scope of privacy protection and the concept of privacy need to be further clarified and modified.

Third, the relief method is limited. Most of the individual privacy protection laws in China are vested rights and political power. After the legal consequences of the illegal protection obligation, they have the tendency of lightening the civil right confirmation and civil liability, and emphasizing the administrative management and criminal punishment. Most privacy protection is carried out according to the right of reputation, and the corresponding responsibility is assumed in the form of compensation for loss, elimination of influence, restoration of reputation and cessation of infringement, etc. However, the privacy violation is irreversible, so whether it is to eliminate the impact or restore, it cannot be achieved in practice. When it comes to damages, there are no rules for measuring losses. In the era of digital development of big data, privacy infringement will lead to property loss, and even the damage of personality right will finally be shown through economic interests. To deter offenders, the cost of breaking the law will rise. Therefore, it is particularly important to set the economic compensation liability for infringement of privacy and determine the way of compensation.

Data Collection Link Leakage

In the process of data collection, there are many kinds of big data, large volume and complex sources, and it is difficult to verify the integrity and authenticity of the data. At present, there is no strict means to identify and monitor the credibility and authenticity of the data, and it is impossible to identify and eliminate malicious and false data. If hackers use network attacks to inject dirty data into the data collection end, the authenticity of the data will be damaged. Jiang Yingwei (2017) found that the data analysis results will be intentionally changed to lead to a preset direction, so as to attack the analysis results of the operation.

Risks of Data Storage

In the era of digital economy, large amounts of data are stored and secure for data analysis. In the era of digital economy, people generate a large amount of data every day, with a scale of PB, and have diversified data sources, including structured and unstructured data types, which require the management of large-scale data through the storage system. Secondly, the data storage system should not only store massive data, but also provide basic support of data processing technology to ensure the effective use of the system. At present, data

protection technology cannot meet the purpose of data protection, such as access control technology and log-in access control technology, so that data will be tampered, stolen, destroyed and other problems in the stored procedure, and personal privacy will be disclosed.

Today, the way data is stored is changing as modern information technology continues to evolve. The computer, mobile phone and other smart devices used by people can realize data storage. This device can save credit card, consumption record, chat record, search record and other information in People's Daily life, and exchange data through network terminal and automatic transmission. A large amount of tedious data makes people delete in a simple way. Because people delete the data in smart devices, they have to delete the data uploaded by smart devices to the data storage system. In this process, there are many problems, and the data cannot be completely deleted. The data will be stored forever in the data storage system of the service provider. Therefore, the service provider can use it in unknown circumstances and cannot delete the data. As a result, people cannot control their own information, and personal privacy will also be compromised and violated.

Confidentiality Protection in Data Processing

In the era of digital economy, a large number of enterprises and organizations have to participate in industrial chain collaboration and realize production activities based on data flow and cooperation. In the data cooperation and sharing application scenario, data is a joint operation that breaks through the boundary flow between the organization and the system to achieve cross-system access or Multifaceted data aggregation. To guarantee the confidentiality of trade secrets, personal information and unique data resources in the cooperation process is the basis for organizations and enterprises to participate in data sharing cooperation, and it is also the main problem to be solved for the orderly flow of data.

Complex Data Flow Paths Provide Security Tracking and the Complexity of Tracing the Source

The usage system of big data is relatively powerful. Frequent data sharing and exchange improves the interleaving of flow paths. Data generation and destruction is not a simple flow mode of single path and one-way, nor is it just the internal flow of an organization, but through one data control personnel flow channel and another controller. In the whole process, it is difficult to trace the data across the data controller or the security domain in the heterogeneous network environment, especially the binding security of data markup, data content and credibility of data sources.

Traditional Privacy Protection Technology

In the big data environment, enterprises realize deep mining and association analysis for multiple sources and multiple types of data sets, which can restore the anonymized data, identify the designated personnel, and obtain valuable personal information. In the traditional privacy protection process, data controllers independently choose privacy protection technologies and parameters for a single data set to protect individual tender data, especially through masks, codes and other technologies, which cannot solve the privacy leakage

problems caused by multivariate data analysis and mining in the big data scene.

In addition, in the era of digital economy, data is semi-structured, dynamic and unstructured. For the unstructured data, which accounts for more than 80% of the total amount, non-relational database storage technology is generally used to achieve big data management, capture and processing. However, non-relational databases do not have strict access control mechanism and perfect privacy protection tools. Most of the current privacy protection technologies, such as anonymous technology and desensitization technology, are applied to relational databases, which cannot meet the non-relational database requirements of big data.

Governance Mechanism of Privacy Protection

Create a System Privacy Protection System

In the research of modern privacy protection law, the hope of improving privacy protection in China lies in the civil law. As for the issue of privacy and property in the digital era, it fully demonstrates the definition of the scope of privacy. In addition to the definition of personal right, it can also reflect the economic value of privacy in the era of big data. It enriches the connotation of privacy right, changes the violation of the law and the way of subsequent liability in privacy infringement, and increases the scope and way of the subject of infringement. Therefore, the specialized law should list the obligations and powers of different subjects in the process of privacy protection, such as the right of privacy subjects to participate in the collection of information and the right to correct the subsequent circulation of wrong information. After mastering the right and obligation of privacy protection, it is necessary to stipulate the responsibility for violating the obligation and damaging the right. Because of the duality of the right of privacy and property, the way of responsibility should be able to fully show the economic compensation and spiritual comfort. The way of relief and case jurisdiction after privacy infringement should also be shown in the special law.

In the aspect of specific responsibility, it is distinguished by the difference of infringement object. Due to the invasion of privacy, the disclosure of personal secrets, invasion of private space, and interference in the decision-making of the dead, the consequences also include property damage, reputation damage and mental damage. In case of invasion into private space, the original state shall be restored and the damage shall be stopped, and the collection shall be realized in accordance with the legal provisions on the protection of the right of reputation when necessary. In the era of digital economy, it deepens the degree of commercialization of privacy. Privacy leakage will not only cause spiritual damage, but also cause property loss. Therefore, after the actor carries out the privacy infringement, he should not only compensate for the property damage caused by the privacy infringement according to the provisions of Chinese law, but also bear the direct property loss caused by the infringement.

Although digitization and big data are not directly mentioned in other relevant policies and regulations, they can be incorporated into big data by means of interpretation to protect personal privacy in the digital era by restricting information collection, use and transmission. Since relevant statutes and policies are relatively scattered, legal indexes should be established to classify relevant provisions according to the links of information collection, dissemination, analysis and use, so as to facilitate the inquiry of administrative and judicial

organs in the process of handling cases. At present, there may be semantic ambiguity, contradiction and unclear definition in interpretation, and specific cases are combined to clarify the corresponding laws.

Strict Security of Information Collection and Storage

China should resolutely protect the private information of individuals and avoid the information acquisition and snooping of big data through any potential collection equipment. For the information that has been disclosed, the first one is personal information recorded by non-governmental organizations for various reasons, such as training records, medical records, housing rental, etc., and other subjects can be inquired based on legal requirements and justified reasons. For such personal information, the relevant responsible departments shall strengthen supervision, establish a good information management system for collecting citizen information, and design the software and hardware for maintaining and storing personal information for regular inspection, so as to guarantee the security of such information. Information cannot be sold or provided free of charge by big data institutions without the consent of the parties concerned; The second is that the information subject voluntarily publishes personal information in a public environment, such as real-time geographical location and photos in social networking sites, or personal resumes in recruitment websites. In the process of protecting information, the confidentiality obligation of service information providers should be enhanced. First of all, users are required to upload their personal information to the website to remind, warning that it will reveal personal privacy. Wu Tao (2018) found that the security management of public platform service providers is required to be strengthened to guarantee user information and avoid large-scale and large-scale leakage of resources, and profits cannot be made from the information mastered.

Limit the Use of Big Data Analysis

In the process of using large data, the sources of private information mainly include direct collection and data mining analysis. Regardless of the source of privacy information, its transmission, circulation, analysis and use are obtained through data mining. For the first kind of personal privacy information, it is recognized by the privacy subject in the collection process. During the analysis and use of such privacy information, the scope of authorization of the privacy subject shall not be exceeded. If in the process of subsequent use beyond the scope of authorization or to other agencies for use, it is necessary to get the subject of information permission and unity. For obtaining private information through analysis and mining, in addition to re-authorization, original data analysis should also be included in the scope of personal privacy protection.

In addition, in the process of information use and transmission, the information integrity and authenticity of the information subject should be checked to improve the accuracy of big data analysis results and reduce the infringement problems caused by wrong information. Data processing institutions that do not meet the privacy protection requirements shall refuse to transfer personal information data. Personal privacy information, in the process of use, transmission, processing, in order to realize the processing of anonymous, big data analysis structure of personal privacy without authorization, the privacy subject before the new authorization can't sell and use, and properly kept, again after the authorized the implementation of the anonymous, can continue to use.

Strengthen the Supervision of Enterprise Information and Data

At present, there is a lack of supervision on enterprise information data in China, and the outflow of some information is closely related to the supervision of enterprises. Enterprises should strictly keep the user information legally collected in the process of work, standardize the supervision of the database, avoid illegal personnel to view and copy, and avoid the outflow of personal information. Measures to strengthen the supervision of enterprise information and data include the following contents to improve the privacy protection of users and enhance the attractiveness of the network:

First, issue a privacy policy statement. Set the column of enterprise privacy policy statement in a prominent position on the home page to show that users' privacy is valued. The content of this declaration is: not be able to illegally collect, disseminate, use and leaked personal information; The user checks and queries the data and corrects the wrong data; Collection of transfer data under specified circumstances; Website operators shall be notified before receiving personal information; Remedies for infringements of users' rights. Users provide personal information to the website under the following circumstances: First, they have great trust in the website and the website will not abuse personal information; Second, provide personal information after feedback. In this way, if the website information is guaranteed, no personal information can be sold to third parties without the user's permission.

Second, network privacy authentication. From the perspective of promoting enterprise development, industry self-discipline is the focus of privacy protection mode. So the industry needs to creates nonprofit, independent organizations and reviews privacy policies and practices within the organization. As long as the privacy industry guide website, can take advantage of and set up in the website authentication mark. In this way, the business reputation of the website can be improved, and the information about Internet use can be improved by the users, so as to remove the consumer's concerns about protecting personal privacy.

Third, update technology. The content of data security protection is as follows: the website realizes the software development of personal privacy protection, and users can browse through whether the software can protect privacy. In addition, users can use the site to determine whether to input information, and avoid output information will not violate privacy. Besides, to keep the website technology updated, to avoid hacker attacks. For a large number of hacker attacks, the protection of personal data security, corporate responsibility is great.

Enterprises should further strengthen the training of internal data management personnel in the process of strengthening website authentication, so as to improve the work quality of staff, avoid data leakage, and effectively ensure the security of personal privacy. In the process of supervising personal data, enterprises should formulate the supervision standards, so that data managers have rules to follow, and improve the personal data protection technology.

Improve Personal Protection Awareness

Through the protection of personal information by all sectors of the society and the government, the public is

required to strengthen the awareness of personal information protection, to avoid personal information leakage from the source.

First, you can't disclose your private information to a third party. When filling in personal registration information in the website, pay attention to whether the website has set up a system to protect user privacy. If not, be careful when filling it out. Even if there is a privacy policy, if there is no special requirement, Just fill in data that doesn't expose privacy.

Second, strengthen computer security protection. Install the firewall and virus protection software into the computer system; Regular scanning system, to ensure that no virus infection, in the computer boot to achieve the design of virus protection software. Some special programs also connect to the Internet to perform background scanning system;

Thirdly, regularly clean up digital information that reveals privacy. In the process of using the computer, regularly clean the computer records to avoid losses due to computer intrusion. Regular clear document history, each version can open the document history, in the start menu can display all history programs, documents and commonly used software, the application opened, will be the latest access to the document record; Periodically clean the search engine, such as search records in the search engine toolbar; Clean up the recycle bin regularly.

Strengthen Technical Supervision

In the process of personal data protection, due to the diversity of personal data sources, it is necessary to use different means for the data in different source channels, so as to strengthen the storage system security management and personnel training in the process of data storage.

One is strict data search. In the process of data collection, data from three different sources are generally included, so the regulatory measures used for data from different sources are also different. First of all, private personal information does not need to be provided to any individual, organization or institution if it does not affect the public interest. In addition, for observation data, information collected by institutions for various reasons, such as shopping records, medical records, etc., is based on meeting the legal requirements, and the individual requires the data collector to provide information explanation. Finally, for the information voluntarily provided by individuals, such as personal videos, location information, photos, etc., according to the enhanced implementation of the service provider's confidentiality Signing agreement, the service provider uses supplementary terms in the process of user registration and use to sign the personal confidentiality agreement with users. Elhai, J.D.,et (2017) found that Digital privacy protection behavior was related to hacking anxiety and privacy self-efficacy.

Second, data storage management. The data management party shall strengthen the management of hardware and software facilities of personal data, and carry out security inspection and security training to guarantee the information security. Zeng Yunjing(2018) proposed that the data management system should be improved to strengthen the security transactions of enterprise personnel and avoid data leakage.

In the digital economy, data use and privacy are at opposite ends of a natural conflict. To solve the privacy protection problem in the application of big data through corresponding measures can promote the development of digital economy era. In addition, the main problem of privacy protection technology is efficiency. The research on confidentiality in the process of data storage and use should be strengthened, so as to improve the level of privacy protection technology in the digital economy.

References

Gong, Y. Q. (2016). Study on International Standards of Data Privacy Management in Enterprises. *Technical economy and management research*, (8), 76-80.

Zhou, H., Meng, Z. P., Ao, Z. M., & et al. (2013). Privacy protection of Consumer Data in the Online environment—A policy framework for privacy protection and innovation promotion in the global digital economy. *Internet Law Review*, (1), 193-218.

Hung, H., & Wong, Y. H. (2009), "Information transparency and digital privacy protection: are they mutually exclusive in the provision of e, services?". *Journal of Services Marketing*, 23(03), 154-164.

Tan, X. X. (2019). Research on the Transformation of Hospital Financial Management under the background of digital economy. *Guide to Economic Research*, (16), 35-37.

Mosco, T., Xu, L., & Liu, C. (2018). Can the Internet of Things lead to Democracy: Perspectives on privacy, Labor, and the environmen. *The press*, (1), 72-73.

Yi, X. R., Chen, Y. Y., & Wei, Y. S. (2019). Research on Several Major Theoretical Issues iabout the Digital Economy—Based on General Analysis of Modern Economics. *Economists*, (7), 135-137.

Jiang, Y. W. (2017). Research on Network Security and Privacy Protection under the background of Big data. *Science and Technology Outlook*, 27(7), 62-67.

Wu, T. (2018). Research on the Development of Digital Economy in Yunnan under the Concept of Green Development. *In the age of wisdom and wealth*, (3), 53-58

Elhai, J. D., Levine, J. C., & Hall, B. J. (2017). "Anxiety about electronic data hacking: Predictors and relations with digital privacy protection behavior". *Internet Research*, 27(3), 631-649.

Zeng, Y. J. (2018). Research on development Opportunities and Challenges of conformity assessment and standardization in digital Economy. *Fortune Today (Intellectual Property In China)*, (10), 83-89.