Criminal Risks and Regulations in Internet Business Data Link

Huiwen Sun [1, †] Shunyao Ye [2, †] Yuchen Zhang [3, †*]

[1] School of Public Finance and Taxation, Zhongnan University of Economics and Law, Wuhan, 430073, China
[2] School of Foreign Languages, Shanghai Lixin University of Accounting and Finance, Shanghai, 201600, China
[3] Faculty of Law, Qingdao University, Qingdao, 266000, China
[†]These authors contribute equally.

*Corresponding author. Email: 2018202499@qdu.edu.cn

Abstract. Internet Business Data Link refers to the whole process from the collection to the application of the Internet business data by enterprises. It can be divided into four stages, which include data collection stage, data application stage, data storage stage, and data association stage with the third parties. The main research object of this paper is the criminal risks existing in each stage. It may not only constitute the crime of infringing citizens' personal information and other criminal network crimes in criminal law, but also may constitute the accessory crime of related traditional crimes. It is urgent to regulate them through the regulations of criminal law. In addition, it can be regulated from three perspectives, which are the behaviour subject, the behaviour mode and the behaviour consequence. What's more, the specific approaches include interpreting existing legal provisions reasonably, setting new accusations and so on.

Keywords: Internet Business Data Link, data collection stage, the crime of infringing citizens' personal information.

1 INTRODUCTION

The development of the Internet has led to the rise of the Internet industry, subsequently promoted the extensive use of Internet business data, and gradually formed a mature Internet Business Data Link. According to the dimension of the risk scenario, it can be divided into the following four stages including data collection stage, data application stage, data storage stage, and data association stage with third parties. The formation and development of Internet Business Data Link has brought huge benefits to the national economy. It is an indispensable force of economic development in China.

However, what has to admit is that the Internet Business Data Link creates both huge economic benefits and some legal risks. Internet business data is increasingly widely used and plays an increasingly important role in daily life. Therefore, the legal

A. Holl et al. (Eds.): ICHESS 2022, ASSEHR 720, pp. 502–513, 2022.
https://doi.org/10.2991/978-2-494069-89-3_59

risks, especially the criminal risks with serious social harm need to be analysed and avoided. From the perspective of criminal law, what kind of criminal risks exist in different stages of the link need to be clearly understood. Meanwhile, special attention needs to be paid to some relevant dilemmas.

At present, both Chinese and foreign scholars have made some researches on the issue of Internet business data protection. Many different protection approaches have been proposed. For example, construct the criminal compliance system by the network platform itself or an independent third-party professional institution [1]. It can realize the effective prevention and timely monitoring of illegal behaviours, and repair of loopholes and defects in the system timely [2]. Besides, using criminal law norm to adjust some important enterprise obligation can strengthen the management of enterprises [3]. However, at present, no scholar has discussed the criminal risks by taking the Internet Business Data Link as a subject.

Therefore, the purpose of this paper is as follows. Firstly, this paper explores the different criminal risks on each stage of Internet Business Data Link. Secondly, this paper proves the importance and necessaries about the criminal regulations. Thirdly, this paper puts forward how to use the criminal law to regulate them. In addition, the methods of OLS mode and case analysis will be used in this paper.

After the regulations, the Internet Business Data Link can create economic benefits and keep its security at the same time. What's more, its crime rate and social harmfulness will be reduced. Then the smooth operation and further development of the Internet economy can be ensured.

2 CRIMIANAL RISKS IN INTERNET BUSINESS DATA LINk

In recent years, cybercrimes have occurred frequently, and a considerable proportion of them are pure cybercrimes such as crimes that endanger the security of computer information systems. At the same time, traditional crimes are increasingly migrating to the Internet, using information technology to obtain new fields and tools [4]. In order to cope with the increasingly severe cybercrime situation, it is necessary to discuss the criminal risks in the Internet Business Data Link. Therefore, according to the division of Internet Business Data Link stage, the criminal risks of data collection, data application, data storage and the criminal risk associated with the third party are analysed [5].

2.1 The Criminal Risks of Data Collection Stage

Data collection stage is the beginning stage of Internet Business Data Link. The main methods of the data collection stage include direct information collection from users and data collection from third parties. Data, as the foundation of Internet enterprises, is easily affected by economic interests in the stage of data collection and leads to criminal risks.

Firstly, in terms of user information collection, Internet enterprises, as a business entity, should legitimize the collection of user information according to relevant national laws. However, under the current Internet economy, the collection of user information is often excessive, so the security of citizens' personal information is seriously harmed. Based login data, users' personal information for the rights of Internet businesses tend to have mandatory, do not give authorization cannot obtain related services. If the data obtained at this time exceeds the data permissions required for basic login, it may commit the crime of infringing citizens' personal information. Users' personal information is often used for analysis of user preferences algorithm is recommended. At this time, the invisible user personal information obtained in the background of the software is even more massive. This information includes the user's location information, facial information and even more private personal information. Then if implemented using illegal users background personal information technology, the risk of infringing citizen's personal information crime is greater.

Secondly, in terms of third-party data acquisition， the user's personal information data is obtained directly from third-party data without authorization from the user. Some Internet companies obtain users' personal information through illegal purchases, etc., which may constitute the crime of infringing on citizens' personal information. Internet companies may also directly invade third-party databases to obtain their data through malicious web crawlers and other technical means that infringe on the legal interests of data. These acts may constitute the crime of illegally obtaining data from a computer information system or the crime of illegally intruding into a computer information system. If an enterprise causes the computer information system to fail to operate normally in the process of acquiring data, it may constitute the crime of destroying the computer information system. In short, when Internet enterprises go beyond the limits set by laws and regulations or collect and adopt data by illegal means, it will lead to the risk of criminal crimes.

2.2 The Criminal Risks of Data Application Stage

Data application stage is the core stage of Internet Business Data Link. Internet enterprises can carry out more diverse criminal activities of illegal use of data in the process of data application, so they are faced with greater criminal risks. Internet companies rely on user information to carry out their next business operations. Therefore, there is a larger space for permissions to process users' personal data in the data application stage. This may create the following criminal risks.

Firstly, illegally selling and providing citizens' personal information can constitute the crime of infringing citizens' personal information. Even if the legally collected personal information is provided to others without the consent of the person being collected, and no technical measures of anonymity are taken, it also constitutes the crime.

Secondly, establishing websites or communication groups to illegally sell or provide citizens' personal information constitutes the crime of illegal use of information networks [5]. The criminal act of illegally selling users' personal information has

seriously disrupted the business order of Internet companies. These actions also have irreversible consequences for users' personal privacy and information leakage.

Thirdly, in the data application stage, Internet enterprises not only touch their own crime risk, but also combine with upstream and downstream crime to cause serious criminal consequences. Internet companies are selling or providing users' personal information collected by themselves to others to engage in criminal activities, which violates citizens' personal information rights. In addition, this kind of behaviour may also constitute an accomplice in the crime of helping information network criminal activities or illegal business, fraud, pyramid selling and other related crimes. At present, the upstream crimes of telecommunications network fraud are mostly illegal acts of selling users' personal information. Internet enterprises are easy to become the providers of helping behaviours in other criminal chains.

2.3 The Criminal Risks of Data Storage Stage

Data storage is the basic function of data processing [6], and data storage stage is an important stage in Internet Business Data Link. Its main content is that the enterprises use the Internet security technology to store the data obtained in other stages in the enterprises' special and confidential database. The criminal risks at this stage mainly include the following three aspects.

Firstly, enterprises go beyond their proper authority and store one-time data that they don't have permission to store. The prerequisite is that data holders authorize their data to the enterprises for use for one thing or storage or for a period of time. However, after the authorization period expires, some enterprises still store and make profits from these data. At this time, the storage of these data by enterprises belongs to a state of illegal acquisition, which can constitute the crime of infringing citizens' personal information.

Secondly, in the process of data storage, enterprises fail to fulfill its data confidentiality obligation. For example, the enterprises know it clear that there are some data security program bugs, but they decide not to repair them. Then what will be found is that the existence of the bugs makes it possible for others to steal the personal data stored by these enterprises. Then if these data are used for crime, the enterprise will clearly constitute a careless mistake. Because the risks of the data reveal have foreseen and should be avoided, it is obvious that there should be relevant criminal liability. However, if the enterprise's storage system doesn't have obvious bugs, it will be difficult to determine liability. Now the regulation problem mainly lies in the difficulty of determining the responsible subject, the different severity of consequences, and the uncertainly determination of damage facts [7]. Therefore, it is difficult to directly adopt the corresponding crimes to regulate it. It needs the help of other crimes.

Thirdly, some enterprises disclose intentionally information to an unauthorized third party for the purpose of seeking financial or other benefits. For example, some enterprises intentionally inform the third parties of their protection program bugs. These enterprises can be charged as the crime of infringing citizens' personal information or accomplices to other traditional crimes.

2.4 The Criminal Risks of Data Association Stage with Third Parties

The third parties in the data field include the upstream data provider, the midstream data agent, the downstream data receiver and so on. Enterprises are often implicated and bear the joint liability of the third parties [5]. At present, because of the frequent occurrence of network crimes, the possibility of criminal risks triggered by the cooperation between Internet enterprises and third parties is also increasing. It should be noted that the third parties refer to the subjects that have authorization of legally viewing and applying the relevant data. In the data storage stage, they refer to the unauthorized third parties. For example, the using of many applications doesn't mean a mandatory requirement of registering a new account. It can be replaced by existing WeChat account for authorization. Therefore, these applications have the chance to call your friends, reveal user's account information, and even use these data for illegal and criminal activities. Once a third party commits an illegal act, the enterprise may ultimately be presumed to constitute an "unsystematic unit crime" due to its acceptance and connivance attitude [8]. Enterprises may constitute new crimes such as the crime of infringing citizens' personal information or helping information network criminal activities. In addition, if the third parties use enterprises' data to carry out traditional crimes, then the enterprises may also constitute an accomplice of related crimes. Suppose A's downstream data reception party B, uses the data authorized by A to engage in fraud. If A knows B may or must use its authorized data for criminal activity, but doesn't know the specific kind of crime, A may be charged as the crime of helping information network criminal activities. If A confirms that B is committing fraud and still authorizes data to B without restrictions, then A may be identified as an accomplice to fraud.

In addition, constitute a crime must have the subjective intent. Internet criminal activities have high secretiveness, so it is possible that enterprises have no way to know which third parties have performed the crimes. This situation shall be deemed as an accident, the enterprise also doesn't need to bear criminal responsibility. Connected the assumption above, if A can prove that he has no knowledge of B's criminal behaviour, then A doesn't bear any joint criminal liability for B's criminal behaviour.

3 THE CRIMINAL RISKS ANALYSIS

3.1 Empirical Analysis of Criminal Risks

The Empirical Purposes. In criminal regulation, the size of crime and criminal responsibility should be consistent and matched, and the punishment should be also proportional to the crime, so as to achieve responsibility for criminal suit. If a certain type of crime could not be punished properly, it shows that there is a certain criminal risk, that is to say, there still have space to be improved in the field of criminal law.

For the traditional sense of the network data crime, its legal regulation is concentrated in the civil field. But as information technology advances, the level of harm caused by such behaviour has the tendency to expand, so it is necessary for criminal

law to intervene, in order to protect individual as well as social rights and interests. In analysis of the regulatory effect of criminal law, it may not be accurate to start with the absolute increase in the number of relevant cases, since the growth in cybercrime-related jurisprudence may be based on a number of reasons. The effectiveness of criminal law regulation can only be regarded as one of the important bases. Therefore, it should be based on the precision of the case to show whether the trial result of this kind of crime could achieve responsibility for criminal suit.

The adaptation of crime, responsibility and punishment requires judges to judge cases strictly in accordance with the criminal law and the facts of cases. Furthermore, it should be also applied to the field of Internet data crimes. That is to say, a judge should make a final decision strictly in accordance with the provisions of the criminal law, a comprehensive assessment of the amount involved and circumstances of sentencing.

Following this train of thought, related debates will be described in detail about how to build an analysis model as follows.

The Empirical Approach. This part selects the recent three years on the Internet commercial data crimes of the relevant effective judgments, adopting comprehensive use of EViews software to make a quantitative analysis. Through the statistics of sample data, group comparison and the establishment of empirical model, this paper demonstrates the necessity of criminal regulation of Internet Business Data Link.

Furthermore, this part is based on the practical demand of strengthening the criminal law regulation of the Internet Business Data Link, ranging by the timeliness of the criminal law precedents. Selecting the relevant precedents of the Internet Business Data Link crimes in the past three years as the research data is in order to maintain the stability of a certain time limit. This is done to analyse the correlation between the criminal responsibility and the harm result of this kind of crime as well as different circumstances of sentencing. It is also done to quantify the criminal risks, in other word, to demonstrate whether the court achieve responsibility for criminal suit.

As for the research method, through the collection of integrated decision data, the establishment of the OLS model uses the measurement software EViews for simulation analysis. When it comes to the explanatory and the interpreted variables, priority is given to the use of the data specified in the judgements. These are namely the length of the sentence and the amount of money involved, based on quantifiable reasons. For this kind of financial crimes, the harm result is directly reflected in the amount of money involved, and it is also one of the main bases for sentencing judges. Criminal punishment, as the direct-viewing expression of the deterrent power of criminal law, is the fundamental task of the criminal law to regulate crime. Therefore, it is necessary to strengthen the criminal law regulation about this kind of crime by using the processed criminal punishment data.

The multiple linear regression model is established as which is shown in the following formula:

$$Y_G=\beta_0+\beta_1X_1+\beta_2X_2+\beta_3X_3+\beta_4X_4+\beta_5X_5+\beta_6X_6+\beta_7X_7+u_i. \quad (1)$$

Among them, the dependent variable Y_G is a quantifiable comprehensive criminal punishment. It is assumed that the suspended death sentence will be 24 years and the life imprisonment will be 22 years [9].

Y_G = 1 * suspended death sentence+ 1 * life imprisonment + 1 * fixed-term imprisonment + 0.000001 * fine.

The explanatory variables X_1-X_7 are respectively the amount of money involved in the crime, whether to return compensation, whether to surrender, whether the principal offender, whether to confess, whether to plead guilty, and whether several crimes were combined punishment. For the interpreted variable X_2-X_7, assign a value of 1 if there is one, or 0 if there is no one. Among them, based on the endogenous problem, the non-dominant factors (such as the referee's personal qualities, and some factors which are taken into account in the judgment but not reflected in the judgment) which can't be quantified will be distributed into the error value u_i.

The Measurement Result. The EViews input results are shown in the table1 below.

As can be seen from the table, R^2 = 86.4087%, conforming that the model fitted well. In addition, Durbin-Watson stat is within the range of 1.5-2.5, which demonstrates that the sequence has no obvious correlation. From this analysis, it can be concluded that the current criminal law for the relevant regulation of network data crime, still contains a certain amount of criminal risks, so there is still a great room for improvement.

3.2 Theoretical Analysis of Criminal Risks

At the same time, it is also necessary to circumvent the criminal risk of Internet Business Data Link.

Firstly, from the status quo of our regulation, at present the risk prevention of Internet Business Data Link in the country is mostly limited to the level of civil law and other general violations. It is also less involved in the level of criminal offences, that is, the application of criminal law to regulate. Therefore, the criminal law can't completely regulate the criminal risks hidden in the process of its operation. Furthermore, the total number of the relevant criminal cases involved in the operation of the Internet Business Data Link in our country is increasing. At the same time, the attitude of current legislation and supporting policies towards such cases is becoming severer and severer [10]. Therefore, from a realistic point of view, it is urgent to control and regulate the criminal risks of Internet Business Data Link.

Secondly, from the perspective of social harmfulness, with the rapid development of digital economy in the country, the commercial activities based on the internet information data have gradually flourished. Driven by economic interests, data-focused cyber-crime is becoming increasingly rampant, causing serious harm to citizens' personal rights, democratic rights and social management order. The criminal risk involved in the Internet Business Data Link is not a crime but a series of crimes. It is more likely to combine with traditional crimes to form upstream and downstream

criminal acts [11]. Moreover, all kinds of criminal acts under the Internet Business Data Link often conclude huge sums of money in the case, and the target is often not restricted in a single person. The harm caused by huge amounts of data often spread over a large area, therefore, the social harm caused is also very significant. Facing such huge social harmfulness, it is necessary to take criminal action to regulate and prevent it.

Thirdly, from the perspective of personal information protection, users often submit some of the personal information to the Internet enterprises in order to have access to their services. Therefore, Internet companies have a huge amount of personal information related to the users' data. Once the personal information is not properly used, it will cause serious harm to citizens' personal information security. In recent years, it has been a good trend that the country pays great attention to the protection of personal information, and at the same time citizens themselves are more aware of the protection of personal information.

4 THE CRIMIANAL REGULATIONS OF RELATED CRIMINAL RISKS

Some criminal risks of these stages can be directly regulated by specific accusations with the current criminal law, but not all harmful behaviours with criminal risks can be effectively regulated through it [12]. At the same time, in the second chapter, what can be clearly found is that can appear in various stages of many of the same accusations. For example, almost every stage involves the infringement of citizens' personal information. Therefore, if the regulations are discussed from the stage classification, there will be a large number of repetitive parts, which will cause unnecessary trouble to readers. Therefore, from the perspective of Legal Education, this chapter will reclassify three perspectives including the behaviour subjects, behaviour modes and behaviour consequences.

4.1 The Perspective of The Behaviour Subjects

In view of the criminal risks on the Internet Business Data Link mentioned above, the following two criteria should be clarified to solve the problem of the identification of the subject of the crime. Firstly, it is necessary to make sure that the crime is committed by the unit, natural person or both parties. Secondly, in the case of unit crime, the way to allocate accusations and criminal responsibility need to be reasonable.

In view of the first criterion, the subjective aspects when the subject performs the relevant behaviour should be taken as the standard to measure. If the starting point of the subject to carry out the act is to profit for themselves or a few members, then it should be identified as a natural person crime. If the starting point is to make profits for the unit or all members of the unit, then it shall be identified as a unit crime. What is more special is the case that both parties are deemed to constitute a crime. If two subjects commit a joint crime with the subjective consciousness of making profits for their own members, they should be convicted separately according to their specific

behaviours. For example, employee Mary steals the personal information and gives it to enterprise N. If the income shared by Mary and N's all employees, then the main body of infringement of citizens' personal information crime should be both natural person and unit crime.

In view of the second criterion, the reasonable distribution of accusations and criminal responsibilities should be carried out from the behaviour pattern. The behaviour pattern of unit crime is systematic and organized. For example, sometimes Internet Business Data Link' internal personnel implement related crime without the knowledge of the principal in the enterprise. If there is no organized, standardization of the phenomenon of mutual cooperation among the member, the enterprise will not be charged as the subject of the crime.

In addition, it should be emphasized that whether the unit identifies the crime subject has nothing to do with whether the unit liability exists or not. Unit liability has fault and integrity, which should be judged by combining unit and natural person [13]. Therefore, if some employees are identified as crimes, it should also be examined whether the supervision and management obligation of the unit is indeed in place.

4.2 The Perspective of The Behaviour Modes

The basic point of criminal law evaluation is concrete behaviour, which can't define the connotation of legal interest protected by criminal law without the stereotyped behaviour of infringing legal interest [14]. The criminal risk in each stage of Internet Business Data Link has high coincidence and crypticity, hence it is necessary to discuss the behaviour mode of high-frequency crimes.

In the Internet Business Data Link, the enterprises are easiest to violate the criminal risk of infringing the personal information of citizens. Their behaviour mode often displays various forms, which include both act and omission. It is a typical form of act crime for enterprises to exceed the authority in the data collection and application of users' personal information. It may trigger the crime of infringing citizens' personal information. Besides, it should be noted that there are many similar behaviour patterns in related crimes of infringing the personal information of citizens. Therefore, it is absolutely impossible to equate a pattern of behaviour with a certain accusation. It needs to be a case-by-case analysis. What's more, the behaviour of omission in criminal law regulation issues need to be stressed. It should be noted that the precondition of punishing harmful omission is that the actors have the clear obligation to act. Therefore, the premise of regulating harmful omission in Internet Business Data Link is to list corporate obligations clearly. The key to whether the act constitutes the crime of omission is to examine the possibility and validity of the obligation out of the range of established regulation [15].

In addition to the criminal risk of infringing the personal information of citizens, the acts on the Internet Business Data Link also easily constitute the accomplices of traditional crimes. From the analysis of the second chapter, it is known that the act of offering assistance to a downstream crime may arise in two stages. They include data application stage and data association stage with third parties. However, their specific acts point to different objects. In the data association stage with third parties, only the

third parties who have the access to apply the data can act as the principal criminals of traditional crime. While in the data application stage, any subject involved has potential to be the principal criminals of commit traditional crimes. Furthermore, the behaviour must also have the purpose of traditional crime. It is only when the subject knows or ought to know the person he helped is committing a crime that the subject can be regarded as an accomplice.

4.3 The Perspective of The Behaviour Consequences

In view of the mentioned possible risks in the storage phase, "data leakage", which has no existing direct crime to be regulated, should be the focus of this section. The data leakage refers to an "unauthorized disclosure of information" [16]. It belongs to the behaviour of infringing the personal information of citizens which infringes citizens' personality interests, property interests and social interests [17]. Therefore, this paper believes that it can be regulated from the perspective of behaviour consequences.

Firstly, accusations should be established based on the different consequences of their actions. Some behaviours that lead to serious consequences in data leakage can be targeted, and define them as relevant crimes corresponding to serious consequences. In this way, the abuse of criminal law to regulate those behaviours that do not have serious social harm can be avoided. For example, if an enterprise's data leakage directly leads to a large-scale fraud, this enterprise should be identified as a crime related to the event according to the consequences of the behaviour. On the contrary, if the data leakage is an accident, then the enterprise doesn't bear the relevant criminal responsibility.

The second point is the establishment of new accusations, serious circumstances as the establishment of the condition. In view of the problem of data leakage, the most effective means of criminal law regulation is undoubtedly to establish a new accusation. What's more, the constitutive elements of this crime should be accurately set. Especially in the way of behaviour, the consequence of serious circumstances must be added. For example, in terms of objective aspects, the crime of data disclosure can be stipulated as including but not limited to intentional disclosure or trading of data. Helping to disclose data, refusal to perform or incomplete performance of protection obligations should also be considered. Besides, the circumstances are required to be serious. In case of serious circumstances, provisions shall be made from various aspects. It need includes causing other major crimes, the huge amount of leaked data and the data belongs to important information (such as state secrets and scientific research achievements). In addition, if it constitutes another crime, it shall be punished by the felony.

Table 1. EViews analysis results

Dependent Variable: Y		
Method: Least Squares		
Sample: 1 15		

Included observations: 15				
Variable	Coefficient	Std. Error	t-Statistic	Prob.
X1	2.84E-08	1.07E-08	2.646035	0.0331
X2	1.760885	1.198632	1.469079	0.1853
X3	-0.441075	1.480177	-0.297988	0.7744
X4	0.176310	1.024684	0.172063	0.8683
X5	0.442049	0.883813	0.500161	0.6323
X6	-0.479230	0.920065	-0.520866	0.6185
X7	5.462825	1.258746	4.339895	0.0034
C	1.364642	1.037443	1.315389	0.2298
R-squared	0.864087	Mean dependent var		3.122200
Adjusted R-squared	0.728174	S.D. dependent var		2.541424
S.E. of regression	1.325019	Akaike info criterion		3.705258
Sum squared resid	12.28974	Schwarz criterion		4.082885
Log likelihood	-19.78943	Hannan-Quinn criter.		3.701235
F-statistic	6.357660	Durbin-Watson stat		1.929028
Prob(F-statistic)	0.013056			

5 CONCLUSION

The development of Internet Business Data Link has made a lot of contribution to the economic development of our country. However, there also exists some criminal risks. Carrying on the reasonable criminal law regulation to its existing criminal risks has the clear necessity and the legitimacy. Besides, it is the important issue that the criminal law academic circle should pay attention to and discuss for a long time.

As far as the current criminal law is concerned, although it has a certain regulatory role, it still has some deficiencies and limitations. Therefore, relevant criminal laws and judicial interpretations should follow the pace of the development of Internet Business Data Link. It's their responsibility to improve and adjust themselves reasonably and timely to ensure their advanced nature and practicability. The key is to constantly develop thinking and broaden horizons, which can be helpful to anticipate the possible criminal risks in Internet Business Data Link. This paper argues that the reasonable explanation of the relevant regulations in criminal law should be applied. Meanwhile, new limitations should be added to help the development of the link.

REFERENCES

1. P. Wang, M. Li, The Doctrinal Analysis of Criminal Law Compliance of Network Platform, in: Jiangxi Social Sciences, vol. 5, 2022, pp. 139-150.
2. R.H. Chen, On the Nature of Corporate Compliance, in: Journal of Zhejiang Gongshang University, vol. 1, 2021, pp. 46-60.

3. G.X. Sun, The Transformation of Criminal Policy of Unit Crime and the Reform of Corporate Compliance, in: Journal of Shanghai Institute of Political Science and Law, vol. 6, 2021, pp. 21-38.
4. H.B. Yu, Fragmentation of Cybercrime Forms and Systematization of Criminal Governance, in: Science of Law (Journal of Northwest University of Political), vol. 3, 2022, pp. 58-70. DOI: 10.16290/j.cnki.1674-5205.2022.03.011
5. Y.X. Mao, Research on Data Protection Compliance System, in: Journal of National Prosecutors College, vol. 30, 2022, pp. 84–100.
6. B.S. He, The Legal Significance of Numbers, in: Law Science, vol. 7, 2022, pp. 3–22.
7. T. Zhang, Explore the Dimension of Risk Control Approaches of Personal Information Protection, in: Law Science, vol. 6, 2022, pp. 57–71.
8. R.H. Chen, Three Modes of Decriminalization by Corporate Compliance, in: Journal of Comparative Law, vol. 3, 2021, pp. 69–88.
9. L. Chen, An Empirical Study on The Balance of Sentencing in The Crime of Embezzlement and Bribery, in: Forum on Politics and Law, vol. 38, 2020, pp. 89–105.
10. X.Q. Liu, X. Shi. The Construction of The Criminal Law System of Network Data Crime, in: The Study of The Rule of Law, vol. 6, 2021, pp. 44–55. DOI: 10.16224/J. CNKI. CN33-1343/D. 20211022.012.
11. W. Ma. Idea Turning and Regulation: The Path of Criminal Law Regulation of Data Crime of Network Organized Crime, in: Academic Exploration, vol. 11, 2016, pp. 81–90.
12. X.Q. Liu, Z. Wang, Criminal Risk and Criminal Law Response in the Metaverse, in: Law Science Research, vol. 2, 2022, pp. 3–14. DOI: 10.16224/j.cnki.cn33-1343/d.20220217.003.
13. B.C. Li, Reflection and Reconstruction of The Theory of Unit Criminal Responsibility, in: Global Law Review, vol. 42, 2020, pp. 39–60.
14. L.J. Jing, On Criminal Law Protection of Enterprise Information Right, in: Northern Legal Science, vol. 13, 2019, pp. 73–86. DOI: 10.13893/j.cnki.bffx.2019.05.007.
15. C. Yu, The Demarcation of The Criminal Liability of The Internet Service Provider's Omission from The Perspective of "Dichotomy", in: Contemporary Law, vol. 33, 2019, pp. 13–26.
16. Y. Peng, A Trade-Law Dimension for Cross-border Data Privacy Protection, in: Journal of Law Application, vol. 6, 2022, pp. 16–28.
17. Y. Shen, S. Jiao, Research on Data Protection Compliance System, in: People's Judicature • Application, vol. 10, 2022, pp. 14–19.