Judicial Regulation Predicament and Countermeasure Analysis of Data-Flow Type of Underground Industry in the Era of Bigdata

Zhiyan Xie[1], Guangxuan Chen[1](✉), Di Wu[2], Guangxiao Chen[3], and Qiang Liu[1]

[1] Zhejiang Police College, No. 555 Binwen Road, Binjiang District, Hangzhou, China
chenguangxuan@zjjcxy.cn

[2] The People's Procuratorate of Hangzhou, Zhijiang Road, Shangcheng Distract, Hangzhou, China

[3] Wenzhou Public Security Bureau, Jinqiao Road, Lucheng Distract, Wenzhou, China

Abstract. At present, the structural and irreparable shortcomings of existing laws and regulations in combating and governing underground products have brought a great challenge for the law enforcement agencies. This paper takes the data traffic-threatening underground industries as example, to reveal the state of the typical underground products, analyze the comprehensive ecological chain model of the related illegal activities, and finally proposes operable constructive opinions and countermeasures. This research can provide a certain reference for the legislation of combating underground products, and promote the standardization and improvement of the legal system for governing underground illegal activities.

Keywords: Underground industry · Data traffic threat · Judicial regulation

1 Introduction

Underground cyber industry refers to the use of Internet technology and network platforms to carry out organized, purposeful, division of labor and large-scale network crime, which plays a key role in many cybercrime related illegal activities that undermine network security. The use of Internet platforms to commit cybercrime not only disrupts the normal operation of the market and threatens the stable operation of critical information infrastructure, but also endangers the security of users' personal information and affects the healthy development of the Internet industry. Therefore, it is urgent to improve the existing legal system and implement a variety of measures to precisely combat such crimes and related illegal activities.

However, so far, despite some adjustments to the corresponding legal regulations in China, in the era of Bigdata, data and internet traffic threatening underground crimes are still rampant. Data and internet traffic are an important part of the ecology of the network industry and a key element in the development and fate of Internet enterprises. If the existing legal system is notimproved accordingly, it will not only jeopardise the legitimate

A. Luqman et al. (Eds.): PMIS 2022, AHCS 6, pp. 500–509, 2023.
https://doi.org/10.2991/978-94-6463-016-9_52

rights and interests of Internet enterprises and citizens, but also have an extremely bad impact on the country's economic development. Therefore, this research intends to comb through the relevant legal systems in China and other countries, analyze the main types of cases, and finally build a structural framework of data-flow type underfround industry crimes upstream, midstream and downstream, so as to analyze the existing dilemma at this stage and put forward targeted opinions.

2 Data Traffic-Based Underground Crime

2.1 The Concept of Underground Production

Network underground industry refers to the use of Internet technology and network platforms to carry out organized, purposeful, division of labour and large-scale network illegal crime. In the context of the normalisation of epidemic prevention, the Internet has subsequently become the main way for people to obtain information and communicate, and the Internet economy was then stimulated. Nowdays, new forms of cybercrime have emerged using new Internet technologies, and the network underground industry has also shown the development trend of a underground industry chain. From many cases, it can be found that the network underground industry plays a key role in many cybercrime activities as a "facilitator" and "accomplice".

2.2 "Data Traffic Threatening" Underground Products

The "Regulations on the Ecological Governance of Network Information Content" issued by the State Internet Information Office in 2019 clearly stipulates that artificial methods or technical means shall not be used to implement traffic falsification and traffic hijacking to obtain improper commercial benefits. In an era where "data is king and traffic is paramount", "dark traffic" can be described as a form of data cheating, rather than a voluntary click based on personal preference, and is essentially a fraudulent act. The existing traffic threats include: malicious clicks, traffic hijacking, network water army, illegal acquisition and sale of personal information. The network underground industry through traffic hijacking, malicious clicks, brush single brush volume, theft of data and other illegal means to make illegal profits, not only endanger the legitimate rights and interests of Internet enterprises and citizens, but also on the national economic development has caused a very bad impact.

2.3 Status of Related Research

In recent years, some scholars have conducted more research on blackmail, however, most of the research focuses on the analysis of the current trend and the handling of specific cases in the area of data traffic threatening graymail. In the article "The Criminal Law Protection of Data Credit—Taking "Traffic underground" as an Example", Gao Yandong and Li Ying proposed that "the crime of obstructing data credit" is the primary task to maintain the basic order of the digital economy. Chen Juan et al. put forward the idea of "technology neutrality" in "A Preliminary Study on the Criminal Law Regime

of Network Technology underground Production". In his article "A preliminary study on the criminal law regime of cyber technology blackmail", Chen Juan and others put forward the idea of "technology neutrality". He proposes that establishing the concept of proactive defence, establishing a governance structure with multi-body collaboration and constructing an all-round collaborative governance mechanism is an effective mechanism for managing the cyber blackmail supply chain. Su Daojing, in "An analysis of the governance of cyber underground products from the perspective of the rule of law", proposes to strengthen the real-name system, form a preventive alliance and improve the legal system in order to contribute to the governance of cyber underground products. The proper and effective solution to crack the special operating structure of the network blackmail supply chain is to establish multiple entities. However, Li Shiyang in "It is advisable to strengthen the criminal protection of credit" said, "China has not yet established a set of operational and universal credit protection and evaluation mechanism, and although there is the principle of honesty and credit in civil law, there is no credit as a universally protected legal benefit in criminal law.

In the article "U.S. Social Media Cleans Up Traffic Fraud", Xin Jia discusses that data traffic-type crimes also exist abroad, but due to the relatively well-developed credit system in the U.S., such behaviour can generally be solved by means of credit discipline and civil compensation. Gao and Li found that explicit protection of credit is also found in the criminal laws of Korea, Japan and Switzerland, yet there is no corresponding legal regulation in China. In The New Interventionism, American scholar Richard N Haas suggests that data sovereignty should not exist because the institution of sovereignty itself has become an obstacle to historical development. In contrast, Russian author Gachev Ilya Igorevich, in "International Legislation on Cybercrime Needs to Keep Up with the Times", talks about how "direct cross-border access to another country's data without the consent of its data authorities makes it impossible to safeguard national sovereignty and leaves open the possibility of violating human rights and freedoms and infringing on users' privacy rights". As can be seen, effectively combating the data traffic threatening underground industry and safeguarding data sovereignty and effective jurisdiction is an important issue for countries to maintain national sovereign dignity and national security.

3 Analysis of Existing Legal Regulation

3.1 Legislation in China

The "Network Security Law of the People's Republic of China" issued in 2016 and the "Measures for the Administration of Internet Group Information Services" issued in 2017 both involve legal provisions for platforms providing information on Internet group services and group users, and there are also provisions in China's criminal law such as "the crime of refusing to fulfill the obligations of information network security management" and "the crime of illegal use of information network". "These laws and regulations came into being along with the booming development of Internet groups, and have also played a role in purifying the Internet environment. In China's current criminal law provisions, there are three main crimes that punish the provision of technical support for cybercrime, namely: the crime of providing programs and tools for intrusion into and

Table 1. Summary of existing legal regulation to combat underground crime in China.

Legal documents	Year
Criminal Law of the People's Republic of China	1997
Decision of the Standing Committee of the National People's Congress on Safeguarding the Security of the Internet	2000
Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases Endangering the Security of Computer Information Systems	2011
Law of the People's Republic of China on Electronic Commerce	2013
Opinions on Several Issues Concerning the Application of Criminal Procedures in Handling Cybercrime Cases	2014
Law of the People's Republic of China on Network Security	2016
Measures for the Administration of Internet Group Information Services	2017
Law of the People's Republic of China on Anti-Unfair Competition	2019
Provisions on the Ecological Governance of Network Information Content	2019
Law on Data Security	2021
Measures on Network Security Censorship	2022

illegal control of computer information systems; the crime of illegal use of information networks; and the crime of helping criminal activities in information networks. These three offences have three things in common. And the subjective "knowledge" of the suspect is an element of all three offences. Meanwhile, all the three offences are based on "aggravating circums blackmail stances" as an element of the crime. At present, the "Two High Courts" has already stipulated the "seriousness of the circumstances" for the crime of providing programs and tools for intrusion into or illegal control of computer information systems, while the crime of unlawful use of information networks and the crime of assisting information networks have been defined as "seriousness of the circumstances". In judicial practice, there is controversy over what constitutes "aggravating circumstances" for the crimes of illegal use of information networks and assisting criminal activities in information networks, and further improvement is needed in the relevant interpretations (Table 1).

On 1 September 2021, the Data Security Law came into force, which clearly stipulates that the State shall establish a data security review system. According to the Data Security Law, data processing activities include the collection, storage, use, processing, transmission, provision and disclosure of data. The latest revision of the Network Security Review Measures also came into effect on 15 February 2022, which incorporates situations where data processing activities carried out by network platform operators affect or may affect national security into the scope of network security review. The Cybersecurity Review Measures focus on situations where the above-mentioned data processing activities carried out by network platform operators affect or may affect national security (Table 2).

Table 2. Summary of existing legal regulation to combat black and white crime abroad.

Document	Country	Time	Remarks
Criminal Code	Japan	1907	Article 233: A person who damages the credit of another or obstructs his business by spreading a false rumour or using a false scheme shall be punished by……
Criminal Code	Korea	1953	Article 313: Anyone who spreads falsehoods or otherwise deceives to the detriment of another's credit shall be punished by……
Swedish National Data Protection Law	Sweden	1973	Provides penalties for the criminalisation of unauthorised access, collection, processing, copying, storage, transmission, use, modification, destruction of data, etc.
Computer-crime Law	US	1978	Act specifies penalties for offences such as intellectual property rights, infringement of computer devices and equipment, and infringement of computer users
Data Protection Law	UK	1984	Sets out the principles, measures, etc. for the protection of personal computer data
Computer Abuse Act	U.S.	1986	Clarifies fraud and abuse offences in federal computer crimes.
Criminal Law Amendment(Second Economic Crime Prevention Act)	Germany	1986	Inserted several provisions dealing with computer security and crime.
Computer Misuse Act	UK	1990	Closes gaps in existing legislation to deal with hacking attacks
Information, Informationization and Information Protection Law	Russia	1995	This law regulates information resources, their use, informatization, information systems, technologies and their means of protection, as well as the protection of information and the rights and interests of subjects in the field of information and informatization.
Criminal Code of the Russian Federation	Russia	1996	This law regulates computer-related crimes under the title of "Crimes in the field of computer information".

(*continued*)

Table 2. (*continued*)

Document	Country	Time	Remarks
Federal Computer Systems Protection Act (FCPA)	US	1997	Computer systems were brought under the protection of the law for the first time.
Law on Personal Data	Russia	2000	This law regulates the access, freezing, unfreezing and deletion of personal data by personal data subjects.
Convention on Cybercrime	30 countries	2001	Chapter II: Art. 2, Art. 4, Art. 8.
Federal Information Security Management Act	US	2002	More detailed provisions on information security for government agencies.
Act on the Promotion of Information and Communication Network Use and Protection of Information	Korea	2006	Major portals are required to record and verify information such as the real name and ID number of individual netizens before accepting their messages, posting photos and videos, and other operations, failing which the website will be fined up to 30 million KRW.
Swiss Federal Criminal Code	Switzerland	1996 Revised	Article 160: Anyone who maliciously violates his or her conscience, by stating or spreading falsehoods that materially damage or seriously endanger the credit of another person, upon complaint, is liable to……

3.2 Legislation in Other Countries

The criminal law of many countries or regions protects the credit of persons…….”; the Swiss Penal Code provides that “a person who, with malice against his conscience, materially damages or seriously endangers the credit of another person by stating or spreading falsehoods, shall be punished on complaint…”….”. The criminal law protection of contractual credit is reflected in the offences of contractual fraud and letter of credit fraud. It can be seen that, although there are already relatively complete legal provisions on credit in the field of private law, the protection of credit has not been neglected in the criminal law of various countries. The crime of data-flow type of underground industry is a kind of dishonest behavior on data.

With data fraud becoming a cancer threatening the development of the digital economy, more and more countries and regions are strengthening the criminal law protection of data credit. As one scholar has pointed out, “computer forgery-type crimes are inherently contrary to the public trust, and as an aspect of the novelty of criminal law, at least in Romanian criminal law, falsification of data is also one of the substantive objects of such crimes”. At the international level, the Convention on Cybercrime (hereinafter referred

to as "the Convention") was signed in Budapest in November 2001 by 26 member states of the Council of Europe and 30 other countries, including the United States, Japan and Canada.

The Convention sets out nine categories of cybercrime offences punishable under criminal law in Chapter II, Articles 2 to 10, of which three are closely related to data traffic-based underground crimes: (1) Illegal interception: This type of conduct includes the illegal interception of computer data of a "non-public nature" transmitted by a computer. According to the European Council Directive, computer data is "non-public" if it is transmitted without the intention of making the information public, even if it is transmitted using a public network; (2) Data interference: includes any intentional destruction, deletion, damage, alteration or concealment of computer data, which is intended to ensure the authenticity of computer data and the availability of computer programs; (3) Computer-related fraud: includes any data entry, alteration, deletion or concealment of any computer data with fraudulent intent, or interference with the normal operation of a computer system, for the purpose of personal gain and causing damage to the property of another person. It is an offence punishable by criminal penalties.

The Convention on Cybercrime is the world's first international convention against cybercrime and will certainly have an important impact on the corresponding legislation of most countries in the world. Following the Convention on Cybercrime can establish a wider international judicial cooperation to jointly combat cybercrime, which has an important role in combating transnational cybercrime and reflects a special protection to ensure the authenticity and validity of data information on the Internet.

4 Existing Flaws and Challenges

According to the data provided by Yongan Online, malicious diversion is still a underground scenario, they generally use script tools, using the platform's private messages, comments, messages and other functions, bulk release diversion information; there will also be underground industry in the social networking platform, issued "collect powder", "pull group" task, they often ask ordinary users to pull friends into the group, after reaching a certain number of people, then a certain amount of money to collect the group, and then transfer the group to the downstream fraud gang, etc..

According to data released by China Internet Information Center in August 2021, as of June 2021, the size of China's Internet users reached 1.011 billion, an increase of 21.75 million compared to December 2020, and the Internet penetration rate reached 71.6%, an increase of 1.2 percentage points compared to December 2020. However, in the process of increasing the number of Internet names, the number of websites in China has been declining year by year, from a peak of 5.44 million in 2018 to 4.22 million in June 2021, and the number of APPs has also dropped from 4.52 million in 2018 to 3.59 million. Against this backdrop, many companies are facing the dilemma of "traffic topping out" and disappearing traffic dividends, and are feeling the crisis like never before. In the face of the predicament, some enterprises through the sinking market, diversified operations and other ways to overcome the sad, but there are also some enterprises through the evil ways of a few unscrupulous elements desperate, trying to rely on traffic hijacking and other improper means to seize illegal benefits, the use

of "traffic hijacking" means to attack competitors, to obtain illegal benefits. In addition to external attacks, Internet companies will more or less buy a certain amount of user traffic through various channels, while paying traffic purchase fees to the channels. Some traffic channels, in order to increase their own income, hijack the natural traffic of the purchasing company into channel traffic through technical means, adding additional traffic purchase fees to the purchasing company. This shows that data traffic threatening underground industry, represented by traffic hijacking, is an act that harms people and does not benefit oneself, which not only destroys the authenticity and validity of data, but also seriously disrupts the normal order of production and operation, hinders the development of China's digital economy, and is in urgent need of legal regulation.

At the same time, data leakage problems are frequent and various industries are facing threats. 2021, after Yongan Online's manual operation and expert analysis, a total of more than 1,700 effective data leakage intelligence incidents were monitored, involving nearly 500 enterprises and more than 30 industries. Among them, the number of incidents increased sharply in November, up 2 times compared to October, which was mainly due to a large number of e-commerce online shopping and logistics express information leakage after the Double Eleven shopping festival. The leaked data is usually used for fraud, advertising promotion and peer competition. According to the relevant data from Yongan, the data types leaked in 2021 were mainly focused on platform user information, accounting for 98%; followed by personal information of citizens, database accounts, backend source code information, etc. The leakage of platform user information will most likely be used for various types of marketing promotions, and is also a major cause of frequent frauds. The main channel for trading data assets is still Telegram, with 80% of transactions occurring, followed by the dark web and bats.

There are three main problems with governance: Firstly, it is difficult to assess the strength of the criminalisation process and it is easy to be "exploited". At present, although the social hazards of "Data-flow Type of Underground Industry" have led to extensive thinking in the academic community, the Criminal Law of the People's Republic of China expressly provides for data traffic threatening underground crimes, although some data traffic underground crimes to a certain extent meet the crime of illegal business, false advertising, damage to computer systems, illegal use of information networks, illegal use of computer systems, illegal use of information networks and illegal use of computer systems. Although some of the data flow-based illegal activities satisfy to a certain extent the constituent elements of the crimes of illegal business operation, false advertising, damage to computer systems, illegal use of information networks and other crimes, contrary to the provisions of the Anti-Unfair Trade Law and other relevant laws, it is usually difficult to criminalize the above crimes. But the above crimes are unable to fully cover all the people in the whole data traffic illegal industry chain, and cannot well judge the nature of their infringement of legal interests.

Secondly, it is difficult to obtain evidence. The data flow threat type of underground production has the characteristics of anonymity and hidden behavior, if the lack of support and cooperation of relevant enterprises and departments, it is difficult to trace and forensic "flow underground production" malicious brush volume behavior. On the other hand, compared to the huge amount of revenue generated by the "Data-flow Type of Underground Industry", the penalties for malicious fraud are minimal under the existing

laws and administrative regulations in China. The Network Security Law of the People's Republic of China stipulates that the act of fabricating or spreading false information to disturb the economic and social order can be punished in accordance with the relevant laws and administrative regulations. But even with reference to the relevant provisions of the E-Commerce Law of the People's Republic of China and the Anti-Unfair Competition Law of the People's Republic of China, the fines imposed by the administrative authorities on the "Data-flow Type of Underground Industry" shall not exceed 2 million yuan. In the face of the lure of huge profits, it is difficult to effectively stop the unchecked spread of the "Data-flow Type of Underground Industry industry" with such a low administrative fine.

Third, it is difficult to prosecute and the cost of litigation is high. On the one hand, the anonymity of "Data-flow Type of Underground Industry" makes private prosecution extremely difficult, and without the help of the state public authorities, many cases cannot even find a suitable defendant. On the other hand, civil litigation is based on the principle of proof by those who claim, requiring victims to collect relevant evidence on their own. This makes litigation more difficult for the victim companies and individuals, and not only does it take a long time and is costly, but the compensation obtained is not proportional to the cost of litigation.

5 Conclusion

This paper analyzes the status, constituent factors and common characteristics of data-traffic-threating underground industries and related illegal activities, analyzes the defects and loopholes of existing relevant domestic and foreign laws and regulations in combating and governing the above-mentioned illegal industries and related cybercrimes, and finally targeted opinions and suggestions were put forward on the crackdown and governance of data-traffic-threating productions. The purpose of this article is to provide reference advice and decision-making basis for relevant law enforcement agencies.

Acknowledgment. This work was supported by the National Social Science Foundation of China under Grant No. 21BSH051.

References

1. Ji GH (2021) The judicial proof of the amount of crime of cyber Underground from the perspective of guiding cases. J State Prosecutor's Coll 29(01):55–71
2. Liu XQ (2021) Criminal regulation of upstream crimes of cyber underground. J State Prosecutor's Coll 29(01):3–17
3. Zhang LX, Jiang MK (2021) Analysis of the situation of underground crime and exploration of investigation and prevention strategies - taking the public accounts as an example. Public Secur J (J Zhejiang Police Coll) 2021(05):39–42
4. Yu C (2021) Classification and criminal response of new telecommunication network fraud crime. 2021(14):42–45
5. Shen L, Qu YM (2021) Analysis and countermeasures of telecommunication network fraud industry chain. China Crim Police 2021(04):51–55

6. Sun CH, Bao JY (2020) Research on anti-unfair competition related issues of online game underground. Legal Soc 2020(35):54–56
7. Su DJ (2020) Analysis on the governance of internet underground products from the perspective of rule of law. Legal Expo 22:46–48
8. Pi Y (2021) Empirical study on the regulation of internet underground production criminal law. J State Prosecutor's Coll 29(01):18–40
9. Hai S (2021) The pattern and regulation of the black-and-grey industrial chain of cybercrime. J State Prosecutor's Coll 29(01):41–54
10. Guo C, Cui W (2020) Research and analysis of internet underground industry chain. Infn Netw Secur 2020(S1):6–9
11. Gao YD, Li Y (2020) Criminal law protection of data credit – take 'traffic underground production' as an example. J Zhejiang Univ 50(03):63–78