WEP Warwick Evans Publishing

Transactions on Social Science, Education and Humanities Research
ISSN: 2960-1770, eISSN: 2960-2262 | Volume 12
LHPPR 2024

Effectiveness Improvement of the "Secondary Authorization" Rule in Criminal Law from the Perspective of Consequentialism

Zhelin Wang

School of Business, Northwest University of Political Science and Law, Shaanxi, China

2664839083@qq.com

Abstract. Human flesh search engine accounts for a large proportion of cyber violence crimes, but a certain lag exists in the current criminal law regulations. There are some defects in regulating the subject of crime with deficiencies in the legislative provisions on the criminal behavior of personal information and the application of the "secondary authorization" rule. Hence, it is difficult to effectively exert the deterrent force that the criminal law should have. From the perspective of consequentialism, focusing on actively and passively disclosed personal information in human flesh search incidents, it can be found that passively disclosed personal information has a higher risk of cyberbullying and greater harm. In this regard, a public opinion identification mechanism should be put in place first to identify the tendency to cyberbullying in a timely manner. Before cyber violence makes a huge difference, all departments will jointly step down for rectification in accordance with relevant regulations. Secondly, criminal law is used to regulate, with the crime of "infringing on citizens' personal information" mainly applicable. At the level of judicial practice, to avoid the dilemma of subjective knowledge, the "presumption and counter-evidence model" with lower cost and higher efficiency is used. Under this model, combined with the reasonable handling principle that "within a reasonable range, there is no major impact on personal rights and interests, and individuals do not choose to refuse", all evidence and information are exhausted to solve problems that exceed the scope of fair use with a major impact and without having been authorized twice. Based on this model, it can effectively identify criminal suspects in human flesh search engines and improve the efficiency of criminal law regulation.

Keywords: Human Flesh Search; Secondary Authorization; Criminal Law Regulation; Consequentialism; Reasonable Treatment.

1. Introduction

Under the current legal system, cyber violence cannot be more precisely regulated. First, due to the relatively light punishment imposed by the law on cyber violence, the deterrent effect is not enough, which makes it difficult to exert long-term governance effects. For example, in criminal punishment cases, the punishment for cyber violence crimes is not sufficiently strong. In cases where the victim's major personal rights and interests are seriously damaged, the victim's physical and mental health is greatly endangered, causing adverse social consequences. Meanwhile, the perpetrator is only sentenced to 3 years with fixed-term imprisonment for the following years. Secondly, it is difficult to pinpoint the responsibility to the individual. The irrational dilemma of network group polarization has led to the irrational "crowds" of netizens gathered on various platforms. The emergence of "crowds" means that the discussion has lost its rationality and is moving towards an out-of-control situation [1] [2], which is the main force of cyber violence. However, it is often thorny to divide responsibilities because of its huge size. As "gatekeepers", large online platforms are obliged to check whether there are violent speeches or videos that violate individual rights on their platforms, and simultaneously take active management and technical measures, while the regulatory rules and mechanisms of most platforms are useless. Both of the above two situations have triggered the implementation dilemma of law enforcement officers in judicial practice [3]. Based on the above-mentioned legal dilemma to be resolved, legislators can think in reverse. Before the law intervenes, the consequences of cyber violence have already produced a series of butterfly effects, which have seriously affected victims and even endangered social stability. Therefore, since the cyber violence

that has already occurred cannot be effectively dealt with, the preventive function of the law can be strengthened. Before cyber violence makes a huge difference, the identification function of the law must intervene in advance to monitor potential cyber violence crimes in advance. In the risk society theory [4], cyber violence is regarded as a high-risk behavior and is hidden with major network platforms hard to detect [5]. The "secondary and passive" situation is the most frequent cyber violence crime as the hardest-hit areas that need special attention from legislators. On this basis, legislators need to take preventive measures, build a pre-governance system to effectively identify potential cyber violence crime risks, and take corresponding measures to regulate them.

2. Identification: Public Opinion Monitoring Mechanism with Priority

The Internet is a place for gathering online public opinion. To identify valuable online public opinion more accurately and quickly, we should grasp emerging and trend information, and then respond to cyber violence crimes predictably. It is necessary to establish a set of efficient and pre-emptive public opinion monitoring mechanisms.

The judgment principle is that "it is within a reasonable range without major impact on personal rights and interests, and individuals do not choose to refuse." From the perspective of consequentialism, a set of public opinion monitoring mechanisms are formulated. Based on the tendency and orientation of cyber violence crimes that continue to emerge, there is continuous dynamic identification and monitoring of the situation, which is combined with artificial intelligence technology for public opinion monitoring, so that speech and information with signs of cyber violence are always monitored in real time, lowering the identification threshold [6]. At the same time, various management departments cooperate to rectify situations that have not become disaster with a tendency to cyberbullying in a timely manner. Horizontally and vertically, they will give full play to the advantages of multi-departmental joint monitoring and create a monitoring mechanism with full coverage, dynamic adjustment, and joint cooperation., so that the network public opinion monitoring mechanism can hit the nail on the head. Taking the social media TikTok as an example, its network public opinion monitoring mechanism has extensive reference significance. With the development of integrated media, large-scale social media is no longer a simple social tool, but also acts as a "gatekeeper" for public opinion monitoring. TikTok has established a human-machine censorship mechanism for short video content screening and traffic control. The machine mainly uses text sentiment analysis, image and video content analysis, keyword monitoring, social network analysis and machine learning algorithms to capture big video content and delete waste of information. Artificially, it further identifies information that is value-oriented and influenced by national policies and public opinion. When negative public opinion occurs, the platform can intervene and guide it as soon as possible by the above means to resolve negative public opinion.

3. Implementation: Post-Regulation of Criminal Law

3.1 Regulatory Behavior of Criminal Law

The manifestations of cyber violence are mainly divided into human flesh search engines and verbal violence, with different charges applied according to various links and specific situations of cyber violence. Here we mainly discuss the relevant legal interpretations of infringing on citizens' personal information, which also include the crimes of defamation, insult, and illegal use of information networks.

The harm of human flesh search engines lies in the unlimited mining of personal information and secondary processing, which seriously damages the major personal rights and interests of citizens. On this basis, the relevant laws and regulations on the crime of infringing on citizens' personal information are roundabout applicable to human flesh search behavior [7]. Article 10 of the *Personal Information Protection Law* stipulates the prohibition of personal information processing, including illegal collection, use, processing, transmission, trading, provision, and disclosure of other people's

personal information, as well as all personal information processing activities that endanger national security and public interests. However, Article 253-1 of the *Criminal Law* only includes the link of illegal acquisition and provision, which only punishes illegal sale, illegal provision, theft or illegal acquisition of personal information by other means [8]. Article 3 of the *Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringement of Citizens' Personal Information* stipulates that providing citizens' personal information to specific persons, releasing citizens' personal information through information networks or other channels, and legally collecting citizens' personal information to others without the consent of the person being collected shall fall into the category of illegal provision [9]. Thus, "illegal collection" in the *Personal Information Protection Law* corresponds to "theft" and "illegal acquisition by other means" in the criminal law, and "illegal trading", "illegal provision", "illegal disclosure" and "illegal transmission" correspond to "illegal sale" and "illegal provision". "Illegal use", "illegal processing" and "illegal transmission" are not subject to regulation for the crime of infringing on citizens' personal information. Such a crime is basically limited to the collection and provision of personal information, and the subsequent use of personal information cannot be directly applied to this crime. In practice, a large number of "abuse" of personal information cannot become the object of regulation of this crime.

In judicial practice, the crimes of insult, defamation, infringement of citizens' personal information and illegal use of information network crimes are all aimed at regulating cyber violence, but they are different in the protection objects and emphases of rights. The crime of insult and defamation emphasizes the protection of the right of reputation, while the crime of infringing on the protection of personal information emphasizes the protection of the right of information privacy [10]. Both the crime of illegally using information networks and the crime of infringing on citizens' personal information involve the illegal use of information technology, but the former focuses on combating the illegality of network dissemination content, while the latter focuses on the protection of personal data.

Verbal violence is a vital part of cyber violence, which mainly involves the application of defamation and insult [11]. Article 246 of the *Criminal Law* stipulates that openly insulting others by violence or other methods constitutes the crime of insult if the circumstances are serious [12]. Insulting behavior directly belittles the individual's sense of honor and self-esteem, which may cause the victim's respect to decline in his social circle. To strengthen the punishment of online insults, according to Article 3 of the *Guiding* Opinions *of the Supreme People's Court*, the *Supreme People's Procuratorate*, and the *Ministry of Public Security on Legally Punishing Cyber Violence and Crimes*, "Whoever blatantly insults others by means of wanton abuse, malicious slander, and disclosure of privacy on the information network, if the circumstances are serious and comply with the provisions of Article 246 of the *Criminal Law*, shall be convicted and punished for the crime of insult." Article 246 of the *Criminal Law* stipulates that fabricating facts to slander others constitutes the crime of defamation if the circumstances are serious [13]. Defamation may cause victims to suffer damage in social evaluation through the public dissemination of specific false information. Compared with several other methods of cyber violence, cyber defamation is the easiest to identify, and cyber violence that constitutes defamation also accounts for the vast majority of relevant criminal judgments.

3.2 Criminal Standards for Disclosed Personal Information

Personal information has been disclosed. Since anyone can obtain it, there is no problem of illegal acquisition. There is only the question of whether the act of reselling or providing disclosed personal information to others or obtaining disclosed personal information from others constitutes a crime.

3.2.1 Meet the "Reasonable Handling Standard" and Prevent Violations

As long as it complies with the "principle of reasonable handling", if it does not exceed the reasonable purpose, reasonable use, and reasonable range at the time of initial disclosure to sell or provide personal information without heavy impact on personal rights and interests, it is in line with the

"reasonable range of personal information without no significant impact on the rights and interests of individuals and individuals do not choose to refuse", which is a reasonable handling behavior and prevents criminal illegality.

The criminal suspect Xiao Wu downloaded and disclosed the industrial and commercial registration information of enterprises in various places on websites such as Tianyancha and Qichacha. After sorting out and classifying, he sold more than 18,000 pieces of information and made a profit of more than 10,000 yuan. He was transferred to the procuratorate by the public security organ on suspicion of infringing on citizens' personal information [14]. Although according to Article 3 of the *Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringement of Citizens' Personal Information*, "Providing citizens' personal information legally collected to others without the consent of the person being collected falls under the provisions of Article 253-1 of the *Criminal Law*", it is determined that Xiao Wu's behavior is suspected of the crime of infringing on citizens' personal information, but the procuratorate uses Article 1036 of the *Civil Code* that "when processing personal information under any of the following circumstances, the perpetrator shall not bear civil liability... (2) Reasonably deal with the natural person's self-disclosed or other legally disclosed information, except that the natural person expressly refuses or processes the information that infringes on his major interests..." Based on the above-mentioned grounds, it is believed that since there is no evidence to prove that Wu's behavior of selling legally disclosed information has been rejected by the obligee or infringes on his major interests, it should not be determined as a crime of infringing on citizens' personal information. Besides, it should not be deemed to constitute a crime of infringing on citizens' personal information.

3.2.2 Not Conform to the Initial Public Purpose and Use, Necessary to Further Judge the Criminal Illegality

Obviously violating the purpose and use at the time of initial disclosure may constitute a crime. When the information processor exceeds the initial public purpose and use, whether it is criminally illegal needs to further analyze whether the behavior is necessary for criminal punishment. It mainly judges whether there is a "fundamental" change from the initial purpose and use, whether it has a major impact on personal rights and interests, and whether the collection, provision, and sale of information have been "secondary authorized" by the person whose information is processed.

In practice, the court tends to determine the crime of infringing on citizens' personal information if the acquisition, provision, and sale of information that exceeds the use of personal information, limited use, and scope without the procedure of "secondary authorization". According to Prosecution Case No. 140 of the *Supreme People's Procuratorate Bulletin*, "obtaining information with a limited scope of use requires the consent and authorization of the information subject. The information that the information subject voluntarily and actively discloses to the public can be determined to agree to others to obtain without infringing on its legitimate interests, which can be used legally and reasonably. However, the use and scope of information are limited [15].

Defendant Li used his computer to search the Taobao seller's store information on the Alibaba website, copied the seller's Wangwang name, and entered the default password to log in through Qianniu.com, so as to obtain the good-quality accounts of the Taobao store and sell them to Zeng and Li, which was later used for fraudulent activities. The court held that "Citizens' personal information is protected by law. Even if individual citizens voluntarily disclose it to the public, others are not allowed to sell or rent it out without authorization."

In the above-mentioned case, the defendant exceeded the initial disclosed use and purpose when processing the information, and his sale and rental behavior did not have the second authorization of the person whose information was processed, so it constituted the crime of infringing on citizens' personal information.

Combined with the relevant provisions of the *Personal Information Protection Law* and *Criminal Law*, the crime of infringing on citizens' personal information is basically limited to the collection

and provision of personal information, with the subsequent use of personal information not applied to this crime. The behavior of personal information cannot be the object of regulation of this crime. Under the framework of doctrinal jurisprudence, it emphasizes the application of law in practice through normative doctrine to protect interests and prevent them from being violated by criminal acts. Hence, from the perspective of normalism, only the above-mentioned liberal and logical explanations can be made for relevant laws. However, under the contradiction between limited laws and infinite behaviors, various rules are derived by liberal and logical explanations for limited laws. To apply the current law to more situations, the cost of pursuing formal justice remains high. Meanwhile, because normalism emphasizes the theory of legal interests and constitutive elements, it will be difficult to put into implementation in some practical problems. For example, it is impossible to distinguish between intentional homicide and indirect homicide purely from the perspective of the norm. It is also difficult to identify the subjective elements of its behavior. For another example, drinking and driving itself does not infringe on legal interests, but there is a potential risk of hitting people while drinking and driving, so the law cannot excessively condone it and must regulate it. However, if the theory of legal interests is too adhered to at this time, it will be difficult to constitute a crime for drunk driving [16]. The consequentialism of law and economics is different. Consequences are the anchor to challenge the traditional identification of the constituent elements of crimes. In the past, practice was often in trouble because of the need to see identification. Today, the "presumption-counter-evidence model" with lower cost and higher efficiency replaced it. Combined with the judgment basis of "within a reasonable range, there is no significant impact on personal rights and interests, and individuals do not choose to refuse". This circular process can cover all evidence and information and solve the problems beyond the scope of fair use, major impact and non-compliance. Issues about secondary authorization should avoid the above-mentioned dilemma.

Considering legal issues from the perspective of consequentialism can first greatly improve the efficiency of criminal law regulation [17]. Consequentialism believes that criminal law norms must directly promote the realization of public interests, and the implementation of criminal law must be conducted within the necessary limits without exceeding this limit. Through the way of thinking of consequentialism, more attention can be paid to the effect of punishment, thereby promoting the enforcement efficiency of criminal law. Secondly, the perspective of consequentialism is more vital to judicial improvement than simply enacting new laws. Considering the issue of punishment from the perspective of consequentialism can emphasize whether the general preventive function that the legislature cares about can be realized, so that it is easier to obtain the legislature with more room for communication. In this way, judicial improvement can be more in line with the basic values of the public, avoid arbitrary interpretation of judicial personal preferences, and better protect the realization of social public interests.

4 Conclusion

The report of the 20th National Congress of the Communist Party of China proposed to improve the comprehensive network governance system and promote the formation of a good network ecology. Building cyber power has become the core and strategic issue of China's modernization [18]. The modernization of the network security legal system is not only the proper meaning of protecting the legitimate rights and interests of netizens as well as the development of the network economy, but also a necessary condition for safeguarding national network sovereignty and national defense security. Undoubtedly, the improvement of personal information protection discussed in this paper is also to improve the network security governance system. To maintain the ultimate goal of Chinese network security, China still needs to cover data security, personal information protection, artificial intelligence, special products for network security, commercial encryption, etc. In January 2023, 16 departments including the Ministry of Industry and Information Technology, the State Cyberspace Administration of China, the National Development and Reform Commission, and the Ministry of Public Security jointly issued the *Guiding Opinions of 16 Departments including the Ministry of Industry and Information Technology on Promoting the Development of the Data Security Industry*,

focusing on the data security protection and related data resource development and utilization needs. In December 2023, the Cyberspace Administration of China issued the *Administrative Measures for Reporting Cybersecurity Incidents (Draft for Comment)*, which stipulates that operators should promptly activate emergency plans for handling cybersecurity incidents. By issuing relevant policies and formulating relevant laws to improve the Chinese security governance system, China has continuously enhanced its capabilities of guaranteeing network security through system construction, so that network security work has laws to follow and evidence to check, making contributes to the development of the network security industry and the digital economy.

References

[1] Yuan, G. F. & Liu, Z. P. (2022). Defining "the masses": A sociological survey of knowledge on the spread of The Crowd: A Study of the Popular Mind in China. Studies of Journalism and Communication, (1): 29.

[2] The mind of crowds mentioned by Gustav Le Bon in The Crowd: A Study of the Popular Mind refers to the fact that under certain conditions, individuals are affected by factors such as group atmosphere and emotions, which have a different psychological state from when they are alone. This phenomenon is particularly obvious in collective events and social movements.

[3] Zhang, X. B. (2021). Research on the setting of special obligations for personal information protection of Internet ecological "gatekeepers". Social Science Abstracts, (8).

[4] Jiang, F. B. (2011). Cyber violence: Concept, roots and countermeasures—An analytical perspective based on risk society. Zhejiang Academic Journal, (6).

[5] Liu, J. H. & Ke, H. X. (2018). The tension of public opinion in moral psychology: A study on the evolution pattern from Internet rumors to Internet violence and its influencing factors. International Journalism, (7): 40.

[6] Yan, X. F. (2021). The difficulties and countermeasures of network public opinion monitoring under the background of mobile Internet. Communication, (8).

[7] Yu, H. S. (2023). Regulation model of cyber violence from the perspective of criminal integration. Legal Science (Journal of Northwest University of Political Science and Law), (5): 41.

[8] Same as the 21st note sourced from Criminal Law of the People's Republic of China.

[9] Same as the 20th note sourced from Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringement of Citizens' Personal Information.

[10] Sun, D. C. (2023).

[11] Zhou, J. H., Yu, H. S. & Li, Z. H. (2023). Cyber violence crime: A normative analysis of criminal law. Chinese Applied Law, (5).

[12] Same as the 21st note sourced from Criminal Law of the People's Republic of China.

[13] Same as the 21st note sourced from Criminal Law of the People's Republic of China.

[14] The first case of procuratorial organs applying the Civil Code to determine that the perpetrator did not constitute a crime of infringing on citizens' personal information.

[15] Bulletin of the Supreme People's Procuratorate, No. 140.

[16] Guo, Z. L. (2023). Interpretive principles of criminal law governance of cyber violence. Jianghan Tribune, (5).

[17] Chen, H. (2018). Value and position of consequentialism in judicial adjudication. Jurist, (4).

[18] Xi, J. P. (2022). Hold high the great banner of socialism with Chinese characteristics and work together to build a modern socialist country in an all-round way—Report at the twentieth national congress of the Communist Party of China. Beijing: People's Publishing House, 66.