Journal of Humanities and Social Sciences Studies
ISSN: 2663-7197
DOI: 10.32996/jhsss
Journal Homepage: www.al-kindipublisher.com/index.php/jhsss

JHSSS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

An Analysis of Legal Duty of Care for Social Platforms in Telecom Froud Matching Recommendations: A Perspective Paper

Dazhi Tian[1a] ✉ Jiayuan Wang[1b] and Mengjia Huang[1c]
[1a]Tongji University, Shanghai 200000, China
[1b]North China Institute of Science and Technology, Langfang 065201, China
[1c]Central South University of Forestry and Technology, Changsha 410018, China
Corresponding Author: Dazhi Tian, **E-mail**: tian.dazhi@foxmail.com

| ABSTRACT
Based on the traditional four-element theory and the discussion of social platform duty, this paper analyzes the source of the obligation of recommending matching social platforms involved in telecommunication network fraud. Through case analysis, this paper analyzes whether the subjective fault and objective measures of social platform cases fully fulfill the duty of care. On the negation of the reasonable duty of care on the crime of refusing to fulfill the management obligation, subjective and objective methods are used to discuss whether the platform constitutes the crime of refusing to fulfill the management obligation. The result of the study has revealed the reasonable obligation of care involved in telecommunication network fraud involving recommending matching social platforms so as to urge the relevant departments to strictly supervise such platform cases and the platform to fully fulfill the duty of care in form and substance.

| KEYWORDS
SNS, Telecom Network Fraud, Recommended Matching Social, Platform Duty of Care.

| ARTICLE INFORMATION
ACCEPTED: 21 March 2024 **PUBLISHED:** 03 April 2024 **DOI:** 10.32996/jhsss.2024.6.4.6

1. Introduction:

1.1 Defining the Duty of Care for the Recommended Matching Social Platform in Telecom Fraud

In June 2023, the number of Internet users in China reached 1.079 billion, and the number of users of instant messaging, online videos, short videos and other social platforms ranked among the top 3 Internet applications (China Internet Network Information Center, 2023). Among all kinds of network security problems, the most serious one is that the proportion of Internet users who encounter personal information leakage is the highest, accounting for 23.2%, followed by Internet users who encounter network fraud, accounting for 20.0%. The report of the 20th National Congress of the Communist Party of China pointed out that China should improve the comprehensive network governance system and promote the formation of a good network ecology (Yin & Zhuang, 2024). On the one hand, the emergence of recommended matchmaking social networking meets the personalized needs of users, but on the other hand, it also brings risks such as passive filtering of information, the loss of Socio-linguistic norms, the disclosure of personal privacy and the emergence of new telecommunication fraud means. Some recommended matching dating social platforms represented by Soul do not need real-name authentication and can be used after binding mobile phone numbers and setting gender and age. The anonymity of social identities and the privacy of interactions undermine the ability of users to address their concerns about the flow of personal information to the virtual public space, personality testing before use, setting personalized labels, and other platform features encourage social networking subjects to shorten the interpersonal social distance by presenting themselves, seek each other's identity, and reduce the ability of individuals to grasp and control their own information.

The social platform is an important part of the network ecology. Accurately dividing the obligation of care of social platforms in helping network information crime plays a key role in determining whether the social platform is a criminal offence. The definition of the duty of care of recommendation matching social platforms is still in a dilemma. On the one hand, there are a large number of false accounts among the users of the matching recommendation social platforms, such as Soul, Momo, Tantan, etc., and related fraud cases occur frequently, with victims often suffering huge economic losses; on the other hand, the duty of care of recommendation matching social platforms is overemphasized, while the relevant power (benefit) and incentive mechanism are rarely stipulated, and the compliance governance tools such as the special compliance mechanism for the duty of care of telecom fraud on the recommended matching social platform have not yet been activated by the policy documents, and the platform lacks the internal driving force for the active governance of cybercrime. In addition, there is a fierce controversy in judicial practice about the conditions under which the related acts of telecommunication network fraud and telecommunication network fraud constitute a joint crime. Even when cases are similar, different courts may employ different methods in handling such cases, both identified as separate. Crimes are also identified as joint crimes (Hao, 2023).

2. Legal Foundations of the Duty of Care in Telecom Fraud

Based on the traditional Penal Code theory, whether the recommendation of matching social platforms in telecom network fraud constitutes a crime should be analyzed from both subjective and objective perspectives. Furthermore, on the one hand, we should analyze the source of negative crime defined in the traditional Penal Code, and on the other hand, we should take into consideration the theory of accomplice in the traditional Penal Code (Lai, 2022).

2.1 Criminal Law Perspective on Social Platform Responsibilities

As for the source of obligation of negative crime, it can be divided into four types: first, the act obligation expressly stipulated by law. The second is the duty or business requirements of the act. The third is the obligation arising from the legal act. The fourth is the obligation of the act caused by the antecedent act (Liu, 2012). The recommended matching social platforms use laws, such as The Data Security Law of the People's Republic of China, The Cyber Security Law of the People's Republic of China, The Personal Information Protection Law of the People's Republic of China, The State Security Law of the People's Republic of China, Civil Code of The People's Republic of China, Regulation on Protecting the Security of Critical Information Infrastructure, Cyber Security Review Measures of China, Measures on the Administration of Data Security in the Industrial and Information Technology Sector (Trial), Provisions on the Administration of Internet Users' Account Information, as the multi-in-one management pattern based on the Management Regulations. The duty of recommendation matching social platforms shall be based on Article 9 of the Regulations on the Management of Internet User Account Information when examining user registration information. When an Internet information service provider provides services such as information release and instant messaging for Internet users, it shall authenticate the real identity information of the users who apply for registration of relevant account information using mobile phone number, ID card number or unified social credit code. To users who do not provide real identity information or illegally use the identity information of an organization or other people when they register, relevant services shall not be provided for them (State Internet Information Office, 2022). Therefore, when telecom network fraud involves recommending matching social platforms, based on the traditional theory of four elements, it is necessary to consider whether the platform objectively checks the user's identity information in detail. In addition, based on the safe harbor principle and the red flag principle, which are Article 1194, Article 1195, Article 1196 and Article 1197 of the Civil Code, the liability for network tort is stipulated. Therefore, when telecom network fraud involves recommending matching social platforms, these platforms should fulfill the obligation of full prompt when discovering suspected fraud of Internet users and should be able to carry out the technical treatment when finding obvious keywords such as transfer, financial management and gambling. In the first civil case of personal rights infringement disputes caused by an algorithmic risk control system in Beijing Internet Court, the platforms should be able to carry out technical treatment. The court held that there was no subjective fault in the defendant's adoption of algorithmic wind control and decided to reject the plaintiff's claim. In this case, the defendant, or the operator of the marriage and dating platform, had made sure that in the early stage of registration and login, the process of submitting real photos as avatars and real-name authentication mobile phone numbers was set up, which to some extent increased the cost of fraudsters' first entry fraud and provided a higher threshold of protection and authenticity for users on the platform. Secondly, in the process of use, the platform algorithm wind control system was detected many times in a short period, such as finance, fund, WeChat and other so-called pig-killing fraud cases involving high-frequency expression, timely handling of accounts, reflecting its responsibility and obligation to fulfill the main supervision for the public interest according to the law (Zhang, 2022). Although this case is a civil one, the court has fully discussed whether the platform has fulfilled its duties, and the court emphasizes the duties that the social platform should undertake in daily supervision. Therefore, when determining the duty of care in social platform cases, whether there is a subjective fault and whether the duty of care has been fully fulfilled objectively should be considered. First, this note is a reasonable prompt. Based on current technology, social platforms can complete the intelligent analysis of user chat records using algorithms. Second, in terms of violations and telecom fraud accounts, whether the platform has handled related problems in a timely and adequate manner is important. With the current technology, social platform companies have the ability to intelligently identify such keywords through

algorithms and timely freeze and shield related accounts. In such cases, when carrying out business, social platforms should observe legal requirements defined in the traditional penal law theory.

2.2 Co-offending Theory and the Duty of Care in Telecom Fraud

The theory of joint crime is mainly determined by whether there is collusion and common practice between the subjects of joint crime (Zhang, 2021). In the analysis of recommendation social platforms, which usually match and recommend friends to network users through algorithms, if the recommended friends are liars, according to the traditional theory of accomplice and if one party commits a negligent crime and the other intentional crime, one does not constitute a joint crime, based on this situation, we should first analyze whether the platform party has criminal intent. At present, social platforms have obviously become hotbeds of criminal behavior. Except for some social apps established without committing crimes, indirect intent is mainly considered when considering whether large matching and recommendation social platforms have intention, which is whether they allow the occurrence of criminal results to occur. Based on the above discussion on the obligations of such social platforms, when a suspected criminal act is found, it should be given an effective reminder in substance rather than just a formal reminder. If such a social platform only gives a simple pop-up reminder, it is difficult to deny its indirect intention to the criminal act. Once a social platform is identified as having indirect intention, the conditions for establishing an accomplice are met in both subjective and objective aspects. Based on the theory of complete criminal association, the conspiracy to establish a joint crime should satisfy sufficient intentional contact, while the simple understanding does not constitute sufficient intentional contact (Yang, 2018). This paper argues that such social platforms should not be indulgent towards cybercrime in the current social background, and their subjective malign reaction to the results of crime is relatively large, and their subjective intention cannot be excluded only by insufficient collusion (Zhang, 2014).

The separation of accomplices based on this establishment should meet the following two aspects: expression of intent and efforts to prevent the occurrence of criminal results (Supreme People's Procuratorate of the People's Republic of China, 2016). The separation of accomplices established by social platforms in joint crimes is analyzed based on actual criminal behavior. First, when fraud is carried out, social platforms should actively and effectively prevent fraud with measures, including the adoption of technical, intelligent monitoring to shield keywords, freezing suspected fraud accounts, fully reminding the risk through the prompt pop-up window, and fully reminding the substantive through intelligent voice customer service calls, smart SMS reminders, etc.; the second situation is when the fraud has been implemented, social platforms will inevitably need to make serious efforts to prevent the outcome of the crime, such as freezing platform fund accounts suspected of fraud, timely cooperating with the Internet police review, reporting the situation to the public security authorities, and even limiting the amount of money transferred to prevent further expansion of the harmful outcome. If such a social platform fails to fulfill its obligation to effectively prevent the occurrence of criminal results from the perspective of the identification of accomplices, it will not only get involved in the crime because it refuses to perform the information network security management obligation, but it may also directly constitute the accomplice of the crime of fraud. The sufficient conditions for constituting the crime of fraud cannot be excluded just because the social platform does not constitute the crime of refusing to perform the information network security management obligation.

3. Analyzing the Current State and Future Directions of Duty of Care for Social Platforms

In recent years, with the emergence of a large number of recommended matching social apps, their application models tend to be homogenized. Under cruel competition, software developers find it difficult to attract users only through homogenized competition. To improve DAU and revenue, some social platforms indulge in the spread of unhealthy information and even illegal information. Some dating apps even intentionally use advertising slogans and detailed page pictures that are vaguely related to pornography to induce users to download, and they do not shield sexually suggestive photos and trading methods in users' personal space or albums, or encourage live broadcasting to make illegal profits, providing a hotbed for crimes such as pig killing, online whoring and online gambling. Although relevant departments are now calling on social platforms to promote multi-dimensional and multi-level capacity building, including pre-prevention, in-process monitoring and timely prevention, there are still several black industrial chains in social platforms, and their duty of care should, therefore, meet higher requirements.

The first paragraph of Article 6 of the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on several issues related to the application of Law to criminal cases, such as Illegal Use of information Networks and Help Information Network Criminal Activities clearly stipulates that the obligation of refusing to perform information network security management is not fulfilled (Supreme People's Court of the People's Republic of China & Supreme People's Procuratorate of the People's Republic of China, 2019).In determining whether the platform constitutes a crime of refusing to perform management obligations, full consideration should also be given to whether it fails to retain the logs of the vast majority of users or fails to implement the authentication of real identity information. However, in various places, the determination of social platforms involving the crime of refusing to perform management obligations varies due to policy reasons, and because of taking into account the development of the industry, it is often handled as appropriate when determining whether social platforms constitute the crime of refusing to perform management obligations. In the process of criminal identification, too much emphasis on the management obligations of social platforms will also affect the development of its industry. In addition, the Anti-Fraud Law sets out the responsibilities and

obligations of Internet platforms in the determination of civil tort cases under current legal norms, even if the online platforms are unable to disclose the true identity information of their users when they fail to fulfill their obligation of real-name registration, thereby rendering the specific infringer unknown, it is incumbent upon the online platforms to assume corresponding supplementary liability for any damages suffered by the victim. However, in reality, very few victims can successfully claim compensation from the platform.

In the future, for the social platforms involved in telecom fraud, regulatory authorities should have stricter requirements for such platforms, which should not only require them to formally fulfill their duty of care, but also require them to fully fulfill their duty of care when it comes to actual algorithms, and conduct supervision and research with their algorithms. When dealing with such cases, the case handling organs should consider the operation logic of the social platforms' code and whether there is a subjective intention of allowing criminal behavior to occur. Only when the form and substance are satisfied can they be determined to fulfill the duty of care. Case handling organs should be fully aware that the relationship between the crime of refusing to perform management obligations and the crime of fraud is not a competition of legal articles, and whether it constitutes a joint crime of fraud should be considered separately, taking into account the development of related industry and the social responsibility it should perform. The judicial departments should also lower the threshold for criminalization in the identification of criminal crimes and should fully consider whether it constitutes a joint infringement of civil law in civil disputes. Once the victims suffer losses due to the failure of the recommended social platforms to fulfill their duty of care, they can claim part of the economic compensation from the social platforms based on criminal or civil judicial remedies.

4. Conclusion

The determination of duty of care for a recommended matching social platform affects not only whether it constitutes a crime of refusing to perform management obligations but also whether it constitutes a joint crime of fraud. The requirement for its duty of care should not be lowered due to the development of the industry, and whether the rights and interests of victims are relieved should also be considered. On the one hand, every individual social user is a source of traffic for social platforms, supporting the development of enterprises in the industry. On the other hand, each account is not just a storage unit; the users behind the account are individuals who live fresh lives and are part of a family and society. While social platforms gain traffic and benefits from social members, they should also provide security for social users.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] China Internet Network Information Center. (2023, August 8). *The 52nd statistical report on Internet development in China*. https://www.cnnic.net.cn/n4/2023/0828/c199-10830.html

[2] Hao, J. (2023). Judicial determination of joint crime of telecom network fraud and related acts. *Journal of Guangxi Police College, 30*(2), 102-113.

[3] Lai, Z. (2022). Information network security management obligation in the crime of refusing to perform information network security management obligation. *Criminal Law,* (3), 309-340.

[4] Li, Y. (2024). Practical dilemma and breakthrough approach of the crime of helping information network crimes. *Qin Zhi,* (1), 34-36.

[5] Liu, K. W. (2012, November 19). *A brief analysis of the sources of obligations for crimes of omission*. China Court Network. https://www.chinacourt.org/article/detail/2012/11/id/788915.shtml

[6] State Internet Information Office. (2022, June 9). *Internet user account information management regulations*. https://www.gov.cn/zhengce/zhengceku/2022-06/28/content_5698179.htm

[7] Supreme People's Court of the People's Republic of China, & Supreme People's Procuratorate of the People's Republic of China. (2019, October 25). *Interpretation of several issues concerning the application of laws in criminal cases, such as illegal use of information networks and assistance in information network criminal activities*. https://www.spp.gov.cn/spp/xwfbh/wsfbh/201910/t20191025_436138.shtml

[8] Supreme People's Procuratorate of the People's Republic of China. (2016, September 26). *Theory of separation of accomplices is conducive to realizing the compatibility of crime and punishment*. https://www.spp.gov.cn/ztk/dfld/2016dfld/dfld98_3376/ywtt/201609/t20160929_168519.shtml

[9] Yang, C. X. (2018). Typical thinking on the criminal liability of network service providers. *Jurisprudence,* (4), 162-172.

[10] Yin, B., & Zhuang, X. (2024). Effective construction of special compliance mechanism for anti-cyber violence on social platforms. *Jiangxi Social Sciences,* (1), 93-103.

[11] Zhang, M. (2014). Identification method of joint crime. *Law Research,* (3), 3-25.

[12] Zhang, M. (2021). *Penal law* (6th ed.). Law Press.

[13] Zhang, X. (2022, November 30). The platform misjudged the user as a pig-butchering scam swindler and banned him. Beijing internet court ruled that the platform did not constitute infringement. *Rule of Law Daily,* 06.