Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.34471

Analysis of the Scope of Criminal Liability of Network Platform Under Algorithm Recommendation

Tian Yao

Law School, Zhongnan University of Economics and Law, Wuhan, China
ytian0504@outlook.com

Abstract. The popularity of algorithm recommendation technology has promoted the transformation of network platforms from passive information storage to active content distributors. The secondary dissemination of illegal information through algorithm amplification has posed a severe challenge to the accountability system of traditional criminal law with "content producers" as the core. This paper takes the scope of criminal liability of network platform under algorithm recommendation as the theme, and defines the dissemination behavior, help behavior and omission crime positioning of algorithm recommendation. On this basis, the scope of criminal liability of the platform is classified into three types, namely, active and large-scale, passive and laissez faire, and insufficient risk identification. Suggestions for improving the system are put forward, such as constructing a hierarchical algorithm duty of care system, and clarifying the identification standard of "risk knowledge". The study believes that the criminal law attribution should realize the shift from content producer responsibility to platform risk control responsibility and achieve the dynamic balance between technology governance and the basic principles of criminal law by reasonably defining the scope of attribution.

Keywords: Algorithm recommendation, network platform, technology neutrality principle, imputation of criminal responsibility

1. Introduction

In the digital age, algorithmic recommendation technology has emerged as the core mechanism for content distribution on online platforms. Platforms such as Tiktok, Kuaishou, and Xiaohongshu leverage technologies like collaborative filtering, user profiling, and content tagging to achieve precise content delivery, thereby significantly enhancing the efficiency of information dissemination and the user experience. However, at the same time, the optimization logic of the algorithm recommendation, which focuses on the length of user stay, interaction rate and business income, objectively forms a propagation amplification effect on illegal information such as extreme speech, false information and infringement content. After being pushed by the algorithm, the propagation range of such information increases geometrically, causing a series of social problems such as chaos in cyberspace and damage to citizens' rights and interests.

The traditional criminal liability system is built around the "content producer", positioning the network platform as a "neutral technical service provider", and its responsibility is mostly

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2026.34471

determined by the behavior of the content producer, which makes it difficult to respond to the new problem of the platform actively interfering with the content dissemination in the scenario of algorithm recommendation. When the algorithm has the functions of independent selection, enhancement and recommendation, can the platform still claim exemption on the grounds of "technology neutrality"? How should algorithm recommendation be positioned in criminal law? How to reconstruct the identification standard of platform subjective sin? These problems are not only related to the judgment of platform crime and non-crime in the case, but also touch the underlying logic of criminal liability structure in the network era, which has become a difficult problem to solve in criminal law theory and judicial practice.

Existing research has carried out in-depth discussion on the platform civil liability under algorithm recommendation. Many scholars pointed out that algorithm recommendation has transformed the platform liability from "passive response" to "active prevention". People should build a duty of care system based on technical ability and break through the shackles of the traditional "technology neutrality" principle [1]. In the criminal field, some studies focus on the performance of the information network security management obligations of the network platform and propose that the risk prevention and control responsibility of the platform should be strengthened. However, the research on the criminal attribution of the technical characteristics of the algorithm recommendation is still relatively scattered, and has not yet formed a systematic framework. In particular, there are research gaps in the behavioral attributes of the algorithm recommendation, the determination of subjective guilt, and the criminal application of the principle of technology neutrality.

Based on this, this paper takes the imputation scope of criminal responsibility of network platform under algorithm recommendation as the research theme, and carries out a systematic analysis from the dimensions of technical logic, constitutive requirements, subjective guilt, and the application of technology neutrality principle, trying to reconstruct the platform criminal imputation system under the algorithm scenario, providing ideas for the improvement of criminal legislation of algorithm governance, filling the blank of criminal evaluation of platform algorithm behavior in judicial practice, and achieving the dual goals of technological innovation and legal interest protection.

2. Determination of subjective fault: the difficulty in proving the platform's "knowledge"

Algorithm recommendation technology makes the platform an active content distributor, and its flow-oriented logic is easy to amplify illegal information, which has an impact on the traditional criminal liability system. Algorithm recommendation is not neutral technology, but an extension of the will of the platform. The platform can control the content through data, models and distribution rules. It is predictable and controllable for risk communication and constitutes the factual basis of criminal responsibility [2]. From the perspective of criminal law, algorithmic recommendation can be identified as three types of behavior: first, the dissemination behavior in criminal law, which essentially expands the scope of illegal information and infringes on legal interests equivalent to traditional dissemination [3]. The second is the helping behavior in joint crime, and the platform knowingly provides communication support; Third, the platform's refusal to perform its network security management obligations under specific circumstances may constitute a corresponding crime. Clarifying the nature of behavior is the premise of imputation.

In the determination of subjective guilt, the platform often defends with ignorance, which makes the proof of "knowing well" become a judicial difficulty. In this regard, people should reconstruct

DOI: 10.54254/2753-7048/2026.34471

the identification standard combined with the characteristics of the algorithm and introduce the generalized intent theory to accurately identify the subjective fault of the platform.

2.1. Difficulty in identifying "knowledge": causes and manifestations

In the traditional criminal law, the identification of "knowing well" requires the actor to have a clear understanding of the specific illegal facts. This standard is difficult to apply in the scenario of algorithm recommendation, resulting in many difficulties in the proof of subjective "knowing well" on the platform in judicial practice.

On the one hand, the "technology black box" feature recommended by the algorithm makes it difficult to prove the platform's cognition of specific illegal content. Algorithm recommendations relies on the machine learning model for content screening and pushing, and its operation process has strong technicality and complexity. It is difficult for the platform staff to manually review and identify each content recommended by the algorithm. Platforms often deny their "knowledge" of illegal information on the grounds that "algorithms are independently recommended and staff members are unable to know the specific content", while judicial organs are difficult to restore the operation process of algorithms through technical means to prove the platform's cognition of specific illegal content, leading to a deadlock in the proof of "knowledge" [4].

On the other hand, the subjective mentality of the platform is hidden, which is difficult to prove by direct evidence. In practice, in order to pursue commercial interests, the platform often allows algorithms to recommend illegal information but does not make such a decision clearly in writing. Its subjective laissez faire mentality lacks direct evidence to prove it. The judicial organ can only presume through the objective behavior of the platform, but the existing presumptive standard has not yet formed a unified provision, which leads to differences in the determination of the subjective mentality of the platform by different courts, and affects the unity of judicial decisions.

In addition, the traditional "knowing well" standard places too much emphasis on the cognition of specific illegal contents and ignores the platform's general cognition of the risk of algorithm dissemination. In the scenario of algorithm recommendation, although the platform may not know the specific content of illegal information, it can clearly recognize the risk that algorithm recommendation may lead to the proliferation of illegal information through data analysis, but it still allows this risk to occur. The traditional "knowing well" standard cannot evaluate this general cognitive state, which makes it difficult to accurately identify the subjective malignancy of some platforms, and then escape criminal sanctions.

2.2. Application of the dolus evidentius theory in the determination of subjective guilt of platforms

For the proof problem of subjective "knowing" of the platform in the scenario of algorithm recommendation, the generalized intent theory can be introduced to identify it. Generalized intent means that the doer has a general understanding of the harmful results, and still allows the behavior to cause harm, without knowing the specific object and plot [5]. Applying it to the algorithm scenario can effectively solve the dilemma of judicial proof and accurately define the subjective mentality of the platform.

The summary of the platform is deliberately reflected in the recognition and laissez faire of the risk of algorithm propagation. The platform is clear that the algorithm takes traffic as the core, which is easy to amplify illegal and harmful information, and has a general understanding of such risks; However, in pursuit of commercial interests, effective technical prevention and control

DOI: 10.54254/2753-7048/2026.34471

measures and content blocking measures were not taken, and the harmful results were allowed to occur. Even if the platform does not master the specific illegal content, it can still be identified as having subjective intent [6].

Summarizing the intentional theory makes the subjective identification of the platform change from "knowing the specific content" to "knowing the risk of communication", which conforms to the technical characteristics of the algorithm, significantly reduces the difficulty of judicial proof, helps to severely punish the platform for allowing the algorithm to spread illegal information, and realizes the full protection of legal interests.

3. Typified differentiation: specific delimitation of platform criminal liability scope under algorithm-based recommendation

Combined with the behavior attribute recommended by the algorithm, the subjective guilt of the platform and the application limit of the principle of technology neutrality, the criminal imputation scope of the platform under the algorithm recommendation should be classified. According to the different types of platform behavior, different responsibility paths and imputation standards should be divided, so as to realize the principle of proportionality of criminal imputation and avoid the excessive expansion or insufficiency of criminal law evaluation. In this chapter, the criminal imputation scope of the platform under the algorithm recommendation scenario is divided into three types: active enlargement, passive indulgence and insufficient risk identification, and the corresponding imputation standards are set respectively.

3.1. Active amplification type: application of the accessory offender path

Active enlargement means that the platform actively expands the scope of the dissemination of illegal information through algorithm recommendation, and its behavior constitutes an accomplice in joint crime, which is applicable to the imputation path of the accomplice. The core of judgment is whether the platform has positive boosting behaviors such as actively pushing up the weight, weighted recommendation and directional drainage.

Objectively, the platform has actively amplified the dissemination of illegal information, such as adjusting the weight of the algorithm to recommend illegal information, setting up a special recommendation portal for illegal information, and pushing illegal information to a large number of users through the algorithm. There is a direct causal relationship between this behavior and the criminal results of the principal offender, which provides substantive help for the principal offender's behavior. On the subjective side, the platform has a clear intention to help, including both specific knowledge of illegal information and general knowledge of illegal information. The platform knows that its algorithm recommendation behavior will promote the implementation of the principal offender's illegal and criminal behavior, but it still actively implements this behavior and holds a hope or laissez faire attitude towards the occurrence of harmful results. In terms of responsibility determination, the behavior of the active amplification platform establishes the helper in joint crime, and it should bear the corresponding criminal responsibility according to its role in joint crime. If the platform plays a major role in joint crime, it can be identified as the principal offender; If it plays a secondary or auxiliary role, it can be identified as an accessory, and the punishment will be reduced or exempted according to law.

DOI: 10.54254/2753-7048/2026.34471

3.2. Passive laissez-faire type: application of the omission offense path

The negative laissez faire type refers to that the platform knows that algorithm recommendation may lead to the dissemination of illegal information, but does not take effective prevention and control measures, and allows the occurrence of harmful results. Its behavior constitutes the crime of refusing to perform the obligation of information network security management and applies the imputation path of omission crime. The core of the judgment is whether the platform has legal regulatory obligations, has the ability to perform, but refuses to perform obligations.

Objectively, the platform has the legal obligation of information network security management, and has the ability to perform this obligation, but refuses to perform the obligation, resulting in a large number of illegal information being spread by algorithm recommendation, resulting in serious consequences. For example, the platform has not established an illegal information recognition mechanism, has not effectively monitored the operation of the algorithm, and the regulatory authorities refuse to rectify after ordering rectification. On the subjective side, the platform has a generalized intention to the risk of illegal information dissemination, that is, it knows that its omission may lead to the harmful results of illegal information dissemination but allows such results to occur. If the platform fails to recognize such risks due to negligence, or has recognized but credulous enough to avoid, it may constitute a fault. In terms of responsibility determination, the behavior of the passive laissez faire platform constitutes the crime of refusing to perform the obligation of information network security management and should bear criminal responsibility according to the provisions of article 286-1 of criminal law. If the laissez faire behavior of the platform also constitutes the helper of other crimes, it should be punished with a felony according to the punishment principle of imaginative joinder of offenses [7].

3.3. Type of insufficient risk identification: application of fault liability

Insufficient risk identification means that the platform fails to identify the risk of illegal information dissemination in algorithm recommendation due to technical defects, management omissions and other reasons, resulting in a large number of illegal information dissemination and serious consequences. Under this type, the subjective mentality of the platform is negligence, and the corresponding criminal responsibility should be borne according to the degree of negligence. The core of the judgment is whether the platform should foresee the risk and not foresee it due to negligence or foreseeing it but believe it can be avoided.

On the objective side, the platform failed to effectively identify the risk of illegal information dissemination in algorithm recommendation due to technical defects, imperfect management system and other reasons, resulting in harmful results. On the subjective side, the platform is negligent in the occurrence of harmful results, that is, it should foresee the harmful results of its own behavior that may lead to the dissemination of illegal information, but it did not foresee it due to negligence, or it was already foreseen and credulous that it could be avoided. In terms of liability determination, if the behavior of the platform with insufficient risk identification meets the constitutive requirements of relevant negligent crime, it should bear corresponding criminal liability for negligence. However, due to the less subjective malignancy of this type of platform, the punishment should be lighter or mitigated according to law. At the same time, if the platform takes remedial measures in time after the occurrence of harmful results and actively eliminates the harmful consequences, it can be regarded as a discretionary lenient punishment [8].

Through the above classification, people can reasonably delimit the scope of criminal liability according to the different characteristics and subjective sins of the platform behavior, and realize the

DOI: 10.54254/2753-7048/2026.34471

accuracy, hierarchy and proportion of criminal liability, which can not only effectively combat the illegal and criminal acts of the platform, but also avoid the excessive expansion of criminal law evaluation, taking into account the dual goals of technological innovation and legal interest protection.

4. Institutional improvement: reconstructing the path of criminal imputation for algorithmic recommendation from the perspective of interest balancing

The core of improving the system of criminal liability fixation of network platform in the scenario of algorithm recommendation is to balance the interests of platform, users' rights and interests and network public interests with refined rules, avoid excessive inclination of single interests, and realize the synergy of technological innovation and legal interest protection. Next, the specific system design scheme is proposed from three aspects: the platform compliance system, the judicial identification standard and the legal coordination mechanism.

4.1. Establishing a platform algorithm compliance system oriented to interests

The design of platform algorithm compliance system should become the legal carrier of interest measurement and realize the pre balance between commercial interests and public interests by clarifying the legal obligations and responsibility boundaries of the platform. According to Professor Liang Shangshang's interest hierarchy theory, the formulation of legal rules is itself a process of interest measurement at the legislative level. It is necessary to take into account the specific interests of the parties, group interests, institutional interests and social and public interests , and build a compliance rule system of "legal obligations - hierarchical responsibilities - incentive compatibility" [9].

At the level of legal obligation, the mandatory obligation of algorithm compliance of the platform is clarified through legislation, and the obligation to review the conflict of interest of the algorithm is added. The platform is required to specially review the conflict between commercial interests and public interests and keep a written report when designing and modifying the algorithm. At the same time, the filing standard was refined in the regulations on the administration of Internet information service algorithm recommendation, and the weight of algorithm flow and risk prevention and control was clarified, so as to eliminate the pure optimization goal of commercial income.

At the level of responsibility stratification, people should follow the principle of proportionality in criminal law and set differentiated criminal responsibility according to the degree of interest damage. The active amplification platform intentionally enlarges illegal information and ignores public interests, and is severely punished according to law; If the passive and laissez faire platform fails to fulfill its management obligations, it can be given a lighter punishment if it is remedied in time afterwards; If the platform with insufficient risk identification causes minor damage due to technical limitations, administrative responsibility shall be applied first and criminal law shall be strictly observed.

At the incentive compatibility level, learn from the non-prosecution system of enterprise criminal compliance, and establish a platform initiative leniency mechanism. For the platform that has established and improved the system of conflict of interest review, risk monitoring and emergency response, and has been certified by a third party, if it has remedied and recovered the loss in time after violating the law, it can apply non prosecution or lighter punishment, and guide the platform to actively balance public interests and commercial interests.

DOI: 10.54254/2753-7048/2026.34471

4.2. Establishing legal standards for interest balancing in judicial application

The clarification of the judicial identification standard is the key link of interest balancing, which needs to provide a clear basis for the judge to weigh interests through the refinement of judicial interpretation and Adjudication Rules, so as to avoid the arbitrariness and subjectivity of judicial discretion. The judge should comprehensively identify and weigh the interests of all parties in the judgment and construct the judicial application rules of "interest identification result demonstration" [10].

At the level of interest identification, it defines the types of core interests of judicial review, including platform commercial interests, user group interests, and cyberspace public interests, and establishes the priority rule of giving priority to social public interests and giving consideration to reasonable individual interests. When the commercial interests of the platform are at the cost of damaging the rights and interests of unspecified users, its claim for exemption from liability will not be supported, and the public interests and group interests will be protected first.

At the level of result argumentation, the judge should strengthen the interpretation of interest measurement of judgment reasoning, and the judge should specify the interest identification, basis of balance and balance results in the judgment documents. When determining that the platform constitutes an accomplice, clarify the assistance of algorithm recommendation to the principal offender and the reason why commercial interests cannot oppose public interests; When finding no responsibility, it indicates that the platform has fulfilled its reasonable duty of care and the basis for non-imputable damage, so as to enhance the credibility and unity of the referee.

4.3. Establishing the interest balance mechanism of multiple legal coordination

Algorithmic governance requires the coordinated efforts of criminal law, administrative law and civil law to form a multi-level legal system of interest protection.

Criminal law and administrative law work together to build a cohesive mechanism of administrative compliance and criminal accountability. The administrative law is responsible for daily supervision and timely correcting minor interest imbalance through rectification and punishment; As a last resort, criminal law only regulates acts that seriously damage public interests. The regulatory authorities first ordered the platform to rectify, and if it refused to rectify or caused serious consequences, it will be transferred to the judicial organ for criminal responsibility, taking into account the efficiency of regulation and the modesty of criminal law.

Criminal law and civil law are coordinated, and criminal accountability and civil compensation are implemented in parallel. The victim can claim compensation through criminal incidental civil action or separate civil action. Criminal law clearly stipulates that criminal accountability does not affect the bearing of civil liability. At the same time, an inversion of the burden of proof for algorithm infringement is added to prove that there is no causal relationship between algorithm behavior and damage by the platform, which can reduce the burden of proof of the victim and comprehensively compensate for the loss of individual interests.

Cross-regional legal collaboration, recommending typical criminal imputation cases by the supreme law release algorithm, and unifying judicial judgment standards; Establish a cross regional algorithm compliance information sharing platform, realize the exchange of regulatory and judicial information, eliminate the imbalance of interest protection caused by regional differences, and ensure the fairness of law application.

To sum up, the proposed criminal imputation system based on the reconstruction algorithm with interest measurement as the core can not only accurately crack down on the behavior of illegal

DOI: 10.54254/2753-7048/2026.34471

information dissemination assisted by the algorithm, but also reserve a reasonable space for technological innovation, ultimately realize the dynamic balance between the commercial development of the platform, the protection of users' rights and interests and the maintenance of cyberspace order, and promote the legalization and standardization of algorithm governance.

5. Conclusion

Algorithm recommendation technology promotes the network platform from information storage to active distribution, profoundly changes the traditional criminal liability structure centered on content producers, and brings new challenges to criminal governance. The algorithm is not a neutral technology, but an extension of the will of the platform and business choice. It is predictable and controllable and is the factual basis for the platform to bear criminal responsibility.

At the level of criminal law, algorithm recommendation can be evaluated as spreading behavior and helping behavior, which constitute omission crime under specific circumstances and provide a normative basis for imputation. Aiming at the problem of "knowing well" proof of the platform, the theory of generalized intent is introduced to shift the subjective identification from "knowing the specific content" to "cognitive communication risk" and solve the dilemma of black box proof of algorithm. When the platform has subjective faults, it is not allowed to claim technology neutral exemption.

The classification of criminal liability of the platform can be divided into three types: active enlargement, passive laissez faire and insufficient risk identification, which correspond to the path of aiding offender, omission offender and fault liability respectively, so as to achieve accurate and proportional liability.

In order to balance technological innovation and legal interest protection, people should build a layered algorithm duty of care system, clarify the "risk aware" standard, improve the system with the measurement of interests as the core, clarify the compliance obligations through legislation, unify the judicial rules, strengthen the coordination between the criminal law and the people, realize the collaborative balance between technology development, platform responsibility and cyberspace order, and promote the legalization of algorithm governance under the premise of abiding by the modesty of criminal law.

References

[1] Wan, Y. (2025) Research on the duty of care in algorithm recommendation on network platform. Doctoral dissertation, Tutor: Ying, D., Beijing University of Posts and Telecommunications.
[2] Lu, C. and Song, W. (2024) Determination of joint tort liability of short video platform in algorithm recommendation mode. People's Justice, (20), 113.
[3] Sun, Q. (2025) Ethical dilemma and solutions of news communication under algorithm technology. Southeast Communication, (06), 25-29.
[4] Sun, P. (2025) The duty of care of algorithm recommendation service providers -- Taking "the first case of algorithm recommendation" as the starting point. Theory and Practice of Law, 1.
[5] Hong, C. (2026) Reflections on the theory of crime constitution in China. Dispute Settlement, 12, 1.
[6] Wang, X. (2025) Research on the presumption of "knowing well" in the crime of information network crime. Advances in Social Sciences, 14, 476.
[7] Wang, Y. (2026) On the boundary of criminal regulation of cyber violence. Dispute Settlement, 12, 15.
[8] Tang, Q. (2026) Research on the boundary between network platform and user security obligation rules. Frontiers of Law, 1.
[9] Liang, O. (2002) The hierarchy of interests and the development of interest measurement -- Also on the interest measurement theory of Ichiro Kato. Legal Research, (01), 52-65.
[10] Liang, O. (2017) Public interest and interest measurement. Social Science Abstracts, (01), 77-79.