Criminalization of Copyright-Infringing Information Distribution Algorithms

Zihang Lan, Shuhan Yang, Xiao Wang, and Yanru Yan(✉)

Faculty of Law, Macau University of Science and Technology, SAR, Avenida Wai Long,
Taipa 999078, Macau, China
1032026396@qq.com

Abstract. With the rapid emergence of user-generated content, Internet service providers have frequently employed information distribution algorithms that recommend information to users based on use statistics. If the information it actively recommends infringes the copyright of others, it is unclear whether and to what degree the Internet service provider should face criminal charges. In answer to the aforementioned problems, this article examines the criminality of copyright-infringing information distribution algorithms using the social harm theory and makes recommendations for improving Chinese criminal legislation. Based on the balance of interests between cyber-copyright owners and algorithm service providers, this article believes that information distributors should be considered unilateral accessory criminals to the uploaders of copyright infringement works, and relevant laws need to be revised urgently.

Keywords: Information distribution algorithms (IDA) · Internet service providers (ISPs) · unilateral accessory crime · copyright crime · user-generated content (UGC)

1 Introduction

Algorithm is the umbrella word for a finite, rigorous set of mathematical and logical tests for automated decision-making [1]. With the rapid expansion of network users and the rapid emergence of user-generated content (UGC), Internet service providers (ISPs) have increasingly adopted information distribution algorithms (IDA) for customised and personalised content distribution in various sectors, such as audio-visual entertainment [2–4], electronic shopping malls [5–7], information communities [8–10], search engines [11–13], to name a few. IDA collects and analyses vast amounts of user usage data to recommend content that users may enjoy, hence boosting user retention or business conversion efficiency. [14] While the IDA provides users with highly tailored material, it also arouses concerns about the potential infringement of users' privacy rights security [15–16] and safety concerns about the algorithmic ethics of "information cocoons" [17]. Intellectual property infringement issues have also emerged, particularly when an ISP recommends UGC protected by copyright law to others without the consent of the cyber-copyright owners [18–20]. The criminal liability of ISPs in such cases, as well

I. A. Khan et al. (Eds.): HWESM 2023, ASSEHR 760, pp. 284–295, 2023.
https://doi.org/10.2991/978-2-38476-068-8_35

as the extent and nature of criminalization, remains unclear in jurisprudence study and judicial recognition. To remedy the above deficiencies, legal hermeneutics, typology study, historical research, as well as dynamic value balancing and interest measurement will be employed in this dissertation to investigate the criminalization of IDA and to perfect its punishment mechanism in Chinese criminal law.

2 Characterization of IDA

Before discussing the criminalization of IDA, it is necessary to characterize it in criminal law. However, present qualitative research on IDA is primarily restricted to civil law. Lu Haijun believes that the "technology neutrality" criterion must be broken, because the IDA's basic concepts must include the platform's own values and interests [21], such as the mechanism design for the algorithm to identify copyright infringement works, the severity of filtering measures for infringing works, and the content and people to whom IDA recommends content. Therefore, when these values and interest considerations match the subjective requirements stipulated in criminal law, ISPs may be punished by the criminal law. According to Xia Mengying, the technological logic of IDA, which is based on user choices, is "technical hegemony." The IDA regulates the information distribution channel by collecting data, processing it, and suggesting it, as well as directing the user's behaviour, regulating the value impact, and eroding the user's copyright [22]. Therefore, the ISPs should bear criminal responsibility.

ByteDance, the pioneer of IDA, said in the introduction that it is not manual editing and that the platform is neither accountable for the generation of material nor does it have a position or set of values [23]. Its primary operation consists of a series of code-based algorithms, hence it should not be held criminally liable for copyright infringement. Furthermore, Xiong Qi believes that the content recommended by algorithms reflects the value orientation of network users rather than the value orientation of ISPs, and the content recommended by algorithms is mostly determined by users [24]. According to Xiong Qi, if users prefer some copyright-infringing content, the ISPs will recommend the copyright-infringing content to these users for a long time according to the neutral algorithm, which does not represent the program's fundamental design logic. In accordance with the notion of "technology neutrality," ISPs should not be held criminally liable for any hypothetical copyright infringements caused by IDA. However, the potential errors of users do not impede the ISP's censoring duties. In the meantime, the law cannot impose a strict moral requirement on all users. It is the responsibility of ISPs to incorporate the value notion of copyright infringement prevention into the design of IDA, given that it is certain that some users would be suggested for infringing content, such as unauthorized reposts of well-liked works from other platforms taking advantage of asymmetric information, and short videos of film commentary that enable users to watch copyright-protected movies freely and efficiently while infringing the original work's adaptation rights and information networks' communication rights.

The current IDA may be separated into decentralised and centralised algorithms based on the mechanism for recommending user-generated content [25]. Decentralized IDA allows everyone to be central, whereas centralised IDA distributes material just to the platform's heavyweight hosts or bloggers. Centralized IDA might result in certain illegal works not being viewed, as they are not posted by prominent streamers and hence should be considered impossible attempted copyright infringement. ISPs should not be punished because they impede copyright violations. In contrast, the decentralised IDA is the exact reverse. Each user's uploaded works will be suggested to other users. If the works are suspected of infringing on intellectual property rights, the ISP may be held accountable for them. Hence, the IDA described in this paper is restricted mostly to decentralised algorithms.

The Cyberspace Administration of China issued the Regulations on the Administration of IDA in March 2022, which defined IDA as the use of algorithms to provide information to users, including generation and synthesis, personalised recommendation, sorting and selection, retrieval and filtering, scheduling and decision-making [26]. The preceding algorithms entail scheduling considerations for individualised recommendation and retrieval filtering, and their complexity and adaptability need that the creators of IDA maintain control over them. This study concurs with Lu Haijun's position that IDA should not be viewed as a wholly technology-neutral action. In contrast, they effectively compress the ISPs' value perspective. Based on the above analysis, IDA should be legally defined as "a new communication mode that recommends information to users based on their usage data using an artificial intelligence (AI) recommendation algorithm with a specified value orientation."

3 Penalizability of IDA

This paper holds that the IDA is penalizable by criminal law, because it has serious social harm, and its social harm is mainly reflected in the four elements, including object elements, objective elements, subject elements and subjective elements. Based on the social harm analysis, this paper believes that ISPs should be recognized as unilateral accessory to the uploaders of the copyright infringing works.

Regarding the subject aspects of crime, the defence against IDA's penalty relies mostly on AI's accountability. AI replaces humans in identification and decision-making processes in order to recognise user pictures and copyright violations more accurately. Some AI academics think that although AI does not yet possess total autonomy, it has gained considerable autonomy in matching user-created content and user data through deep learning and generative adversarial network, which transcends its role as a tool for humans [27] ISPs should not accept criminal liability for the action of AI since "algorithmic black box" leads to unpredictable consequences of copyright infringement screening and is not entirely controlled by programmer input information. This argument is insufficient, however, as the development of AI is still at the stage of artificial narrow intelligence, and it has no practical value for AI to carry out human rules such as penalties and jail. Simultaneously, granting AI independent personality at this moment will lower the duty of algorithm creator, operator, and user and blur the line between algorithm and human. Hence, the present criminal legislation should recognise IDA as a tool utilised by ISPs to enhance screening efficiency and product competitiveness, lest no one be held accountable for copyright infringement. In addition, ISPs will be accountable for the design and monitoring of AI, even if AI develops a significant degree of autonomy in the future and is deemed a criminal law subject. Wu Liangjun proposed adding the crime of refusing to conduct AI safety management responsibilities to the Criminal Code, which compels developers, suppliers, and users of AI systems to carry out reasonable safety management obligations under statute [28]. Hence, even if AI are granted legal subjects in the future, ISPs cannot avoid regulatory duties and continue to be the subject of copyright infringement crimes.

In terms of subjective factors of crime, ISPs have an indirect intentional state of mind regarding the repercussions of copyright infringement that may be induced by IDA. The Internet platform's user agreement prohibits users from uploading copyright-infringing content [29], therefore it can be assumed that the ISP is aware that copyright-infringing content may emerge on its network platform. Insofar as ISPs are aware that copyright-infringing content may appear on the platform, but do not add corresponding filtering algorithms to the IDA for the purpose of increasing platform traffic, they are indirectly expressing a subjective intent to cause harm through the widespread dissemination of infringing works. If ISPs are aware of a stricter recommendation algorithm for infringing material filtering methods and choose a less stringent one, it can be inferred that they have a permissive attitude regarding the occurrence of damaging effects, which is also an indirect intentional statement of mind. It is worth noting that care must be taken to exclude neglect and loss of expectant possibility. As ISPs construct the IDA, they should anticipate gaps in the algorithm for filtering copyright-infringing content. Nevertheless, they fail to anticipate these loopholes, leading to a substantial volume of copyright-infringing information, whose subjective statement of mind is negligence. This paper argues that the scope of punishment for IDA should be limited to intentional acts because if the criminal law punishes technical negligence in designing algorithms, it will impose unreasonable algorithm design obligations on ISPs, which will lead to a substantial expansion of the scope of criminal law punishment, and the punishment will be excessively severe, which may result in violations of human rights. Only administrative punishments are appropriate for algorithm design errors. Yet, the existing technology of ISPs is incapable of achieving the aim of screening all copyright-infringing materials. According to the criminal law notion of expectant possibility, the law is not inconsiderate. When the requirement of "technical incapacity" is met, it is unreasonable to expect the perpetrator to take legal action to safeguard copyright. Consequently, if criminal penalty is to be applied for IDA, the loss of expectant possibility must be ruled out. That is, we should identify the breadth of the ISP's review and filtering obligations in a way that is consistent with their capabilities and avoid imposing obligations that exceed their capacity.

In terms of object elements of crime, according to the relevant theories of intellectual property law, the determination of copyright infringement by ISPs applies the "safe harbor" principle, and its main content is the "notice-delete" rule [30]. With the rapid development of Internet technology, especially the maturity of IDA based on AI and big data, Internet dissemination of copyright infringing works is becoming the main form of copyright infringement crimes. Compared with traditional piracy, the wide spread, fast speed and large number of infringements have brought great property and spiritual losses to copyright owners that cannot be salvaged by the principle of safe harbor. However, some ISPs gain high traffic benefits and profits through improper cross-platform flow of intangible knowledge achievements, which has serious social harm. Therefore, criminal punishment is necessary and irreplaceable because of its severity. In other words, the criminal punishment of IDA has its basis of justice.

In terms of objective elements of crime, copyright-infringing IDA, which has a certain degree of neutrality, helpfulness and relevance, is a kind of neutral helping behavior. It may seem harmless in appearance, but it objectively promotes the principal offender's behavior and results [31]. Current scholarly consensus about neutral helpful behaviour is the idea of limited punishment, which encompasses subjective attribution, objective attribution, and mixed attribution. The theory of subjective imputation holds that if the ISP is determined to have intentional expansion of possible copyright infringement results caused by IDA, it can be recognized as an accomplice. The theory of objective imputation believes that it should be limited according to the strength of the relationship between the IDA and the principal offender's behavior and results [32]. Both the theories of subjective imputation and objective imputation have their flaws, and the eclectic theory combining the two has become the mainstream view on neutral helping behavior in academic circles, but the eclectic theory is still not specific enough for determining the punitive nature of neutral helping behavior, which does not give a criterion that can be widely and repeatedly applied. Instead, its application requires specific analysis of specific situations. From the paper's perspective, the proportion of IDA used in legal versus illegal situations is critical to its judgement of penalizability. According to the frequency and scope of illegal use of ISPs' behavior, Li Changbing divides helping behaviors into main illegal use, easy illegal abuse, and occasional illegal use [33]. Different types of helping behaviors should adopt different criminalization standards. Some scholars believe that according to this standard, the IDA is a helping behavior that is occasionally illegally used, and it is not criminally punishable according to the general theory of limiting punishment for neutral helping behavior [34]. In contrast, this paper believes that IDA is a helping behavior that is easy to be illegally abused compared to the manual recommendation, and consequently it is punishable by criminal law.

More specifically, ISP should be classified as unilateral accessory to the uploaders of the copyright infringing works. The reasons are as follows: First, the IDA has a strong subjective initiative. ISPs have active actions such as sorting out, editing or recommending content suspected of copyright infringement, so the IDA is relatively proactive and independent, lacking sufficient neutrality, and consequently it has the legal obligation to review user-generated content. Second, the social harm becomes more serious as the IDA attracts more users. IDA is of great significance for improving user stickiness and retention. With the maturity of IDA, more users will be retained on the network platform, and the spread of copyright infringement works will be greater, and the social harm will be greater as well. Therefore, ISPs should undertake a higher duty of care commensurate with information management capabilities for the competitive advantages brought about by algorithmic recommendations, and take effective measures to actively regulate and prevent infringement. If reasonable measures are not taken, criminal responsibility should be assumed. Third, ISPs play a key and major role in the harmful consequences stipulated in the criminal law. The aggregation of a large number of similar minor behaviors in cyberspace may cause serious social harm. The lack of any general illegal subject does not affect the formation of social harm, but only the lack of ISPs will block the formation of social harm. At the same time, the nature of repeated application of IDA to an unspecified majority determines that its infringement cannot occur only once. Instead, once it is designed and used in business activities, it must be a collective crime and business crime carried out many times, which should be "an accumulatively calculated quantity or amount". Furthermore, it is unreasonable to apply the joint principal offender theory. There is no communication between the ISP and the user who uploads the infringing copyright work, so it cannot constitute a joint principal offender. At the same time, although the ISP knows that the uploader's behavior may be illegal, the ISP does not have the right to decide whether to commit the crime and how to commit the crime, so it is unreasonable to identify ISP as the joint principal offender. Based on the analysis above, copyright-infringing IDA should be punished by the criminal law, and the ISPs should constitute unilateral accessory to the uploaders of the copyright infringing works, which should not be identified as the joint principal offender.

4 Governance Path of IDA

4.1 Governance Path Based on Jurisprudence

First, in an era of highly developed 5G technology and broad Internet use, a single general criminal conduct may quickly ferment via the unique combination of digital space, causing damage to legal interests that extends far beyond the initial illegal act. In a nutshell, ISPs' neutral helpful activity can be split into accomplices with primary offenders and accomplices without principle offenders. In certain instances where IDA infringes on copyright, a single illegal act of copyright infringement is not enough to constitute a crime, so it is accomplices without principal offenders. Most nations opt for "treating aiders as perpetrators" in order to combat such technical crimes with more independence and increased societal harm. In terms of legislation technology, it is necessary to make the unilateral accessory the principal offender in this case, and to establish independent legal punishment and constitutive elements, so that the non-execution behaviour can satisfy the requirements of the criminal law's constitutive elements and be transformed into execution behaviour.

Second, whether the subject directly responsible for the unit crime of IDA should be the designer or the operator needs to be analyzed according to the specific situation. With the maturation and growth of algorithm division of labour, an increasing number of algorithm designers are no longer algorithm operators, and algorithm operators can achieve their own technical goals by purchasing algorithm modules and services; therefore, it is necessary to differentiate algorithm designers and algorithm operators based on criminal law standards. In the qualitative component of criminal law, the algorithm designer must differentiate between the unit's outside and inside. If the algorithm is not designed for network services and is only used by the algorithm operator, the algorithm operator should be directly responsible. If the algorithm is designed for ISPs and the algorithm designer is required to include filters for copyright-infringing content, the algorithm designer shall be directly responsible. If the algorithm designer is a member of the unit, both the algorithm designer and algorithm operator are jointly directly responsible for the crime.

Thirdly, in the age of algorithms, the types of evidence for copyright infringement have undergone enormous modifications. IDA creates copyright infringing content that is predominantly displayed as "information flow." The current information flow will be altered by a simple refresh or restart, making it harder to retain infringing content. With the use of algorithmic models, a huge number of copyright-infringing content may be distributed rapidly, requiring copyright owners to fix a large quantity of preliminary evidence of infringement in a short period of time, which raises the expense and difficulty of conviction. Moreover, with the help of 5G technology, suspected infringing content may spread exponentially to multiple user ports using IDA, making infringing content easy to spread, harmful, difficult to locate, and unpredictable, and making it impossible for the criminal law to fully investigate crimes that are more socially harmful due to network communication.

The notion of "risk criminal law" should be utilised to resolve this issue. "Risky society" refers to the stage of social evolution in which global dangers generated by human activity predominate in the context of globalisation, which is viewed as the outcome of contemporary technology's reaction to industrial society [35]. Compared to manual recommendation, IDA as an emerging modern technology poses significant diversity threats to industrial civilization. In light of the dangers introduced by IDA, it is challenging to maintain the safety and order of the "risky society" through outcome prevention for an extended period of time. Thus, a dangerous society is in dire need of the requirements of the risk legislation to govern the newly additional societal hazards posed by IDA. The idea of "risk criminal law" asserts that the criminal law punishes the potential infringement of legal interests rather than the actual infringement of legal rights. From the standpoint of the security and preservation of social innovation accomplishments, lawmakers should advance the criminal law defence line to the algorithm stage, which is viewed as the inevitability of historical progression. Applying the theory of "risk criminal law" to the problem of IDA means that as long as there is a risk of escaping copyright protection according to the algorithm's underlying logic, criminal responsibility can be investigated even if the harmful consequences stipulated in the previous criminal law have not been caused or cannot be proven. Allowing the possible violation risk of the IDA to be examined by criminal law can aid in resolving the challenge of evidence gathering, since the IDA can be legally penalised without the necessity for actual harm, for which it is difficult to collect evidence.

Some academics are of the opinion that the "risky society" theory might result in grave concealed hazards for the preservation of human rights and degrade people's individual freedom. In addition, they argue that IDA will be included in the purview of criminal law, even if the harm is unknown and neutral. In contrast, this paper asserts that the early intervention method of punishment through the potential infringement risk of IDA can prevent the risk from evolving into actual damage as much as possible, and that the scope of punishment risk is limited to behaviours that have potential copyright infringement risks based on life experience and factual logic. At the same time, ISPs are viewed as the source of the danger of copyright infringement, necessitating the intervention of criminal law to mitigate hazards and safeguard the creative fervour and sense of security of copyright owners. Comparing the ISPs to the copyright owner in terms of the interest balance, this article concludes that the ISPs are in a stronger position in the legal relationship of service provision. The strong viewpoint is mirrored in the format terms of ISPs, which demand that users approve their copyrights in a demanding manner. Hence, for the purpose of safeguarding vulnerable populations, the criminal law's value orientation should be skewed towards preventing crime rather than preserving human rights. Regarding the duty of ISPs, it is fair to adopt the theory of "risk criminal law".

4.2 Governance Path Based on China's Actual Situation

Copyright-infringing IDA in Chinese criminal law is actually a crime that combines the mode of act and omission. From the perspective of the crime of omission, if the IDA failed to meet the duty of care "commensurate with the information management capabilities", failed to take reasonable preventive measures against infringements, especially repeated infringements, and refused to take reasonable measures even after being notified of deletion in the civil law or ordered to rectify in the administrative law, the ISPs will constitute the crime of refusing to perform the obligation of information network security management in China. This crime is a pure omission crime, based on the ISP's obligation to prevent the mass dissemination of copyright-infringing works. It is worth mentioning that so far, only 4 cases concerning the crime of refusing to perform information network security management obligations can be retrieved on the Chinese Judgment Documents website. Excessively high threshold for conviction, unclear stipulations of obligations, difficulty in clarifying the regulatory responsibilities of the government and ISPs, and poor "convergence mechanism between administrative law and criminal law" have together led to the "zombification" of this crime. From the perspective of a crime of the mode of act, the ISP's active behavior of sorting out, editing, or recommending the suspected infringing content is in line with the first paragraph of the crime of copyright infringement "copying and distributing its written works, music, movies without the permission of the copyright owner, TV, video works, computer software and other works" and the objective elements of the crime of aiding information network criminal activities "knowingly that others use the information network to commit crimes, providing Internet access, communication transmission and other technical support for their crimes, or providing advertising promotion, payment and settlement, etc." Therefore, if the IDA infringes the copyright, it will be threefold imaginative coincidence which includes the crime of refusing to perform the network security management obligations by omission, the crime of helping the information network crime and the crime of copyright infringement by act. Finally, it can only be convicted and punished from one felony, that is, the crime of copyright infringement by act.

In order to improve the criminal regulation of IDA, China's criminal law should make the following adjustments: First, clarify the obligation of ISPs to review and filter copyright-infringing works. At present, China's judicial interpretation is too general and broad, which is not conducive to the conviction of IDA in practice, and it is easy to cause disputes. Second, perfect the convergence mechanism between civil law, administrative law and criminal law. In order to realize the modesty of criminal law, the legislator set the precondition of administrative punishment for the crime of refusing to perform the obligation of information network security management. Such a provision leads to the high threshold of the crime, which is difficult to convict in practice. In order to solve this problem, the criminalization conditions should be diversified, and consequently the pre-criminal conditions of the civil law should be added. For example, it should be amended to read: “If the copyright owner of user-created content sends a notice to the Internet service platform to adjust the filtering algorithm or delete the infringing content, and the Internet service platform refuses to delete it without justifiable reasons, and the circumstances are serious, it shall bear criminal responsibility.” Third, in the objective elements of the crime of refusing to perform the obligation of information network security management in Article 286, Paragraph 1 of the Criminal Law of the People’s Republic of China, “causing the massive spread of illegal information” should be amended to “causing the risk of massive spread of illegal information”. According to the above theory of “risk criminal law”, it is necessary to advance the intervention point of criminal law to the algorithm formulation stage of the ISP, because if the algorithm fails to establish a reasonable filtering mechanism for copyright infringement content, then the operation of the IDA will inevitably lead to dissemination of copyright infringing works. Therefore, rather than applying the criminal law when irreversible harm is created, it is better to impose criminal punishment on the ISP at the algorithm stage. Fourth, clarify whether IDA is a “copy and distribution” stipulated in copyright infringement crime. It is still widely debated whether the IDA can be regarded as “copy and distribution” in the crime of copyright infringement. Therefore, it is urgent to clarify the meaning in judicial interpretations.

5 Conclusion

IDA is a new style of communication that recommends information to users based on their usage statistics by employing an AI recommendation algorithm with a particular ISP value orientation. This paper analyses the limits, conditions, and rationality of the criminalization of IDA using the four elements, refutes the subject theory of AI, and concludes that IDA artificially creates legal risks compared to manual recommendation, and should be subject to a higher duty of care. If ISPs breach this duty of care, they should be held criminally liable. In particular, ISPs should be considered unilateral accomplices to the uploaders of copyright-infringing material because of their significant initiative and substantial social harm. In order to avoid “strangling technology” and preserve the modesty of the criminal law, this paper proposes the addition of the pre-criminal conditions of civil notification and the exclusion of the “technical impossibility” of the IDA applicable to the loss of expectant possibility in the criminal law. To perfect the regulation of Chinese criminal law on IDA, this study offers the theory of “risk criminal law” to address the difficulties of collecting evidence for IDA and to advance the criminal law intervention point to the algorithm design stage. By study and explanation, this research concludes that the copyright-infringing IDA is a combination of acts and omissions. This article argues, based on the current state of China’s criminal legislation, that copyright-infringing IDA is a creative coincidence of numerous crimes and should be punished according to the more serious offence. In conclusion, when governing IDA through criminal law, we should not only consider the economic interests of copyright owners to actively combat crimes, but also protect technological innovation and avoid unreasonable distribution of criminal law obligations to strike a balance between the functions of protecting human rights and combating crime. In addition to preserving the interests of cyber-copyright owners, we must also defend the rights of ISPs in order to preserve a balance between the sustainability of the output of original works and social interests in the growth of IDA.

References

1. Blair, Ann, Duguid, Paul, Goeing, Anja-Silvia and Grafton, Anthony. Information: A Historical Companion, Princeton: Princeton University Press, 2021. p. 247 https://doi.org/10.5860/crl.83.2.343
2. Zhao, Xiaojian, et al. Video recommendation over multiple information sources. Multimedia systems 19.1 (2013): 3–15. https://doi.org/10.1007/s00530-012-0267-z
3. Pyo, Shinjee, Eunhui Kim, and Munchurl Kim. Automatic and personalized recommendation of TV program contents using sequential pattern mining for smart TV user interaction. Multimedia systems 19.6 (2013): 527-542. https://doi.org/10.1007/s00530-013-0311-7
4. Horsburgh, Ben, Susan Craw, and Stewart Massie. Learning pseudo-tags to augment sparse tagging in hybrid music recommender systems. Artificial Intelligence 219 (2015): 25-39. https://doi.org/10.1016/j.artint.2014.11.004
5. Behera, Rajat Kumar, et al. Personalized digital marketing recommender engine. Journal of Retailing and Consumer Services 53 (2020): 101799. https://doi.org/10.1016/j.jretconser.2019.03.026
6. Castro-Schez, Jose Jesus, et al. A highly adaptive recommender system based on fuzzy logic for B2C e-commerce portals. Expert Systems with Applications 38.3 (2011): 2441–2454. https://doi.org/10.1016/j.eswa.2010.08.033
7. Huang, Zan, Daniel Zeng, and Hsinchun Chen. A comparison of collaborative-filtering recommendation algorithms for e-commerce. IEEE Intelligent Systems 22.5 (2007): 68-78. DOI:https://doi.org/10.1109/MIS.2007.4338497
8. Wang, Y., Shang, W.: Personalized news recommendation based on consumers' click behavior. In: Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference on, 2015. IEEE, pp 634–638 https://doi.org/10.1109/FSKD.2015.7382016
9. Shi, B., Ifrim, G.: Hurley N Learning-to-Rank for Real-Time High-Precision Hashtag Recommendation for Streaming News. In: Proceedings of the 25th International Conference on World Wide Web, 2016. International World Wide Web Conferences Steering Committee, pp 1191–1202 https://doi.org/10.1145/2872427.2882982
10. Shu, Jiangbo, et al. A content-based recommendation algorithm for learning resources. Multimedia Systems 24.2 (2018): 163-173. https://cnki.net/
11. Sharma, Dushyant, et al. A brief review on search engine optimization." 2019 9th international conference on cloud computing, data science & engineering (confluence). IEEE, 2019. DOI:https://doi.org/10.1109/CONFLUENCE.2019.8776976
12. Makhortykh, Mykola, Aleksandra Urman, and Roberto Ulloa. How search engines disseminate information about COVID-19 and why they should do better. (2020). https://doi.org/10.37016/mr-2020-017
13. McNally, Kevin, et al. A case study of collaboration and reputation in social web search."ACM Transactions on Intelligent Systems and Technology (TIST) 3.1 (2011): 1–29. https://doi.org/10.1145/2036264.2036268
14. Zhao, Zhengwei. Analysis on the "Douyin (Tiktok) Mania" Phenomenon Based on Recommendation Algorithms. E3S Web of Conferences. Vol. 235. EDP Sciences, 2021. https://cnki.net/
15. Lam, Shyong K., Dan Frankowski, and John Riedl. Do you trust your recommendations? An exploration of security and privacy issues in recommender systems." International conference on emerging trends in information and communication security. Springer, Berlin, Heidelberg, 2006. https://doi.org/10.1007/11766155_2

16. Liu, Desheng, et al. P3OI-MELSH: Privacy Protection Target Point of Interest Recommendation Algorithm Based on Multi-Exploring Locality Sensitive Hashing. Frontiers in Neurorobotics 15 (2021): 660304. https://cnki.net/
17. Sunstein CR. 2006 Infotopia: How many minds produce knowledge. Oxford: Oxford University Press. https://doi.org/10.1353/sof.0.0060
18. ZHOU, LINA, Recommendation Algorithm and Platform's Duty of Care----Iqiyi V. Bytedance Copyright Case in China. https://doi.org/10.2139/ssrn.4284527
19. Beijing Haidian District Court (2018), Beijing 0108 Civil First Instance No. 49421 https://wenshu.court.gov.cn/
20. Yan Shu. Research on Copyright Infringement Duty of Care of Internet Service Providers under the background of Algorithm Recommendation Technology.2022. MA thesis, Yantai University. https://cnki.net/
21. Lu Haijun, Xu Lang, and Youli. Legal Regulation of Internet Platform Algorithm Recommendation. China Publishing.13(2022):22–28. https://cnki.net/
22. Xia Mengying, Xu Jialin. Privacy Risks and Legal Countermeasures of algorithmic Information Distribution. Media Observer.10(2020):14-18. DOI:https://doi.org/10.19480/j.cnki.cmgc.2020.10.002.
23. Liu Bin. Ethical Dilemmas and Solutions of News Client Algorithm Recommendation -- A Case Study of Toutiao. News Communication. 16(2022):34–36+39. https://cnki.net/
24. Xiong Qi. Information Push Algorithms and ISP's Contributory Infringement. Chinese Applied Law.04(2020):125–136. https://cnki.net/
25. Liu Zhengchi, Zhou Sha, and Li Sanxi. Competition of Social Media Platform Based on Flow Distribution——From "Decentralized Social" to "Centralized Media", "China's Industrial Economy. 10 (2022): 99–117. https://doi.org/10.19581/j.cnki.ciejournal.2022.10.012
26. The Chinese Regulations on the Administration of Internet Information Service Algorithm Recommendation. Article 2. http://www.gov.cn/zhengce/2022-11/26/content_5728941.htm
27. Lan, Z. (2022) From Animals to Artificial Intelligence: Non-Human Beings' Intellectual Property Protection by "Judicial Capacity for Copyrights". Beijing Law Review, 13, 697-714. DOI: https://doi.org/10.4236/blr.2022.134045.
28. Wu Liangjun. On the dilemma and solution of copyright criminal law protection in the age of artificial intelligence. Publishing Research.08(2019):44-48. DOI:https://doi.org/10.19393/j.cnki.cn11-1537/g2.2019.08.010.
29. Hu Li, He Jinhai. An Empirical Study on the Mode of Users Data Authorization of User Agreement——A sample of 40 User Agreement of Internet Platform. Hebei Law, 2022, 40(10): 160-180. DOI: https://doi.org/10.16494/j.cnki.1002-3933.2022.10.009.
30. Zhong Sanyu, Zheng Yixin. On the Application of "Safe Harbor Rules" for Internet Service Providers. Cross-strait Legal Science, 2022,24(03):39–48. https://cnki.net/
31. Chen Xingliang. On Neutral Helping Behavior. Oriental Law, 2022, No.88(04): 132–145. https://doi.org/10.19404/j.cnki.dffx.2022.04.008.
32. Wang Yue. Research on Restricted Punishment of Neutral Helping Behaviors. Jilin University, 2022. DOI: https://doi.org/10.27162/d.cnki.gjlin.2022.007438.
33. Li Changbing. A New Discussion on the Boundary of the Criminal Punishment for Neutral Aiding Behavior in Internet. Law Science Magazine, 2020, 41(04): 79-89.
34. MAIMAITI Usman, YANG Limin. Algorithm push and criminal liability normative reconstruction of copyright infringement of internet service providers: From "practical role" to "normative capability". Journal of Chongqing University of Technology (Social Science), 2021(8): 147 -159. https://cnki.net/
35. Zhang Mingkai. Reflections on Several Theoretical Issues of Criminal Law in "Risk Society". Law and Business Research, 2011, 28(05): 83-94. DOI: https://doi.org/10.16390/j.cnki.issn1672-0393.2011.05.014.