

The Duty of Care Owed by Algorithmic Recommendation Platforms in Relation to Copyright in Micro-short Dramas: A Two-Tier, Four-Step Framework for Liability

Chengyi Lyu

*Faculty of Law and Justice, The University of New South Wales, Sydney, Australia
lyuchengyi162@gmail.com*

Abstract. Algorithmic recommendation has not displaced the fault-based doctrines governing platform secondary liability for online copyright infringement, but it has materially altered a platform's capacity to detect infringement, control its spread, and prove compliance. Scholarly views range from technological neutrality to mandatory filtering, while judicial practice has moved incrementally from notice-and-takedown toward work-specific filtering, repeat-infringer measures, and adjustments to recommendation logic. Taking Articles 1195 and 1197 of the Civil Code and Article 23 of the Regulations on the Protection of the Right of Communication through Information Networks as its normative starting point, this article analyses six recent Chinese cases from *Story of Yanxi Palace* to *Lost You Forever*, drawing comparatively on Article 17 of the EU Copyright Directive, the Digital Services Act, and Section 512 of the US Digital Millennium Copyright Act. Algorithms neither forfeit safe-harbour protection nor guarantee immunity; they are better treated as risk-amplifying factors and evidence of control capacity. The article proposes a two-tier framework: baseline governance duties independent of any individual infringement, and a special duty of care once a risk becomes specific, within which alone the four steps of identification, triggering, matching, and verification operate. A limited re-uploading prevention duty is justified for identified popular micro-short dramas with recurrent infringement, without general monitoring.

Keywords: algorithmic recommendation, micro-short dramas, copyright duty of care, right of communication through information networks

1. Introduction

The commercial value of micro-short dramas is heavily concentrated in their initial-release and paid-conversion periods. Once complete episodes, consecutive clips, or screen recordings are uploaded to short-video platforms, recommendation systems can distribute them within a very short period to users with similar viewing preferences. For right holders, item-by-item detection, evidence preservation, and notification often lag behind the speed at which content is copied, renamed, cropped, and re-uploaded. For platforms, recommendation algorithms both generate traffic and advertising revenue and provide the ability to cease recommending content, identify similar

material, and control accounts. The controversy has therefore shifted from whether a platform uses algorithms to the extent of algorithmic involvement, the point at which a platform must act, and the measures it should take.

The analysis of platform liability must begin by asking whether the platform directly provides the work. In a case concerning the unauthorised reposting of a micro-short drama published by the Wuhan Hongshan District People's Court ([2024] E 0111 Zhi Min Chu No. 164), the defendant renamed a drama produced by another party, placed it in its own mini-program, and charged users for later episodes. This constituted a direct act of communication through information networks, and liability did not require analysis under the duty-of-care doctrine. Where the work is uploaded by a user and the platform merely stores, indexes, or directs users to it—including through recommendations—the relevant liability instead concerns a failure to take affirmative steps to prevent infringement. Xiong Qi accordingly argues that although algorithmic recommendation is automated and individualised, those technical characteristics neither negate platform neutrality nor justify a mandatory *ex ante* review obligation [1]. This is the starting point of the present article: the duty of care applies only to secondary infringement and cannot replace the prior identification of direct conduct.

At the same time, technological neutrality does not mean that liability remains static. Existing scholarship has observed that algorithmic filtering, algorithmic correction, and algorithmic explanation must be assessed by reference to the degree of platform involvement, the specificity of the content, and the risk of erroneous restriction [2]. This article therefore rejects a binary choice between preserving safe harbours and imposing comprehensive filtering. It instead addresses three more specific questions: first, which functions of hybrid recommendation platforms fall within Article 23 of the Regulations on the Protection of the Right of Communication through Information Networks (the Regulations); second, how "knows or ought to know" and "necessary measures" should be differentiated by tier; and third, how a replicable domestic framework capable of preventing over-filtering can be derived from divergent recent decisions in comparable cases. The preliminary conclusion is that algorithmic recommendation neither automatically heightens liability nor necessarily preserves platform neutrality. The duty of care should intensify as a general risk becomes a risk associated with a particular work, account, or mode of dissemination, and as the platform's actual capacity for control increases.

2. Doctrinal disagreement and the structure of existing law

2.1. The four positions are not simply opposed

Views on whether algorithms should increase the copyright duty of care may be grouped into four approaches. First, the technological-neutrality approach treats the algorithm's ability to distinguish authorisation, lawful use, and infringement as the fundamental criterion. If the relevant determination cannot be made through technology alone, a platform should not be deemed to have constructive knowledge or to bear heightened liability merely because it uses an algorithm. Second, the limited-duty approach balances actual risk, available information, and the cost of measures, and imposes localised duties in relation to particular works, users, or modes of dissemination. Third, the systemic-reconstruction approach proposes a tiered duty of care beyond notice-and-takedown, based on the platform's role, capacity for control, method of profit, and procedural safeguards. Fourth, the mandatory-filtering approach relies on the probability of infringement and the availability of identification technologies to require active monitoring or prevention of re-uploading in circumstances such as trending content, complete copying, and repeated uploads. The true

disagreement among these approaches is not whether copyright deserves protection, but when a duty arises, whom it targets, how technological errors should be corrected, and how costs should be allocated.

Xiong Qi argues that the automated nature of an algorithm does not deprive platform services of their neutrality and therefore cannot justify prior review in all circumstances [1]. The Research Group of the Shanghai Intellectual Property Court separately examines algorithmic filtering, correction, and explanation, taking the platform's actual role and the particular risk as the basis for selecting measures [2]. Ma Yide and Zhao Diya characterise a "special review duty" as the link between notice-and-takedown and special risks, while proposing that the content of the duty be confined by the principle of proportionality [3]. Ren Anqi further argues that algorithmic platforms should not be regarded as mere conduits; rather, their technical capabilities should be analysed in conjunction with their obligations to review or filter infringing content [4]. This article favours a combination of the limited-duty and systemic-reconstruction approaches. Positively, it neither treats the algorithm alone as the object of attribution nor permits purposeless general monitoring. Negatively, once the risk has become specific, necessary measures that are proportionate rather than excessive should be arranged by reference to function, knowledge, control, and procedure.

2.2. Constructive knowledge is the trigger: necessary measures constitute the duty

Article 1195 of the Civil Code is triggered by a valid notice from the right holder, whereas Article 1197 is triggered when the platform knows or ought to know of a specific infringement. Both provisions attach liability to a failure to take necessary measures. It follows that constructive knowledge is not an abstract duty of proactive inspection, but a condition that activates the platform's obligation to address an individual case. Deletion, blocking, disabling links, terminating recommendations, restricting accounts, and other loss-prevention measures constitute the specific content of the duty of care. Equating constructive knowledge with a review duty produces circular reasoning: the platform ought to have known because it failed to review, and it must review because it ought to have known.

Accordingly, this article divides platform obligations into two tiers. The first comprises baseline governance duties addressing general risks, such as maintaining accessible complaint channels, preserving action logs, publishing and enforcing a repeat-infringer policy, and periodically assessing algorithmic risks. The second comprises case-specific measures directed at a particular work, account, or infringement pattern. Baseline governance duties may exist before the platform becomes aware of a specific infringement, but their breach ordinarily serves only as an auxiliary factor in assessing fault and allocating the burden of proof. The platform may incur corresponding liability for failure to adopt necessary case-specific measures only after the risk has become concrete and the second-tier duty has been triggered.

2.3. Article 23 must be applied by reference to service function

Article 23 of the Regulations specifically governs search and linking services. A platform that disables a link to an infringing work upon receipt of notice may qualify for limited liability; one that knows or ought to know that linked content is infringing bears joint liability. The provision should not be extended to every recommendation merely because a "link" button appears on the page. If the micro-short drama at issue is stored on the platform's servers and can be played directly, the principal provisions are Article 22 of the Regulations and Articles 1195 and 1197 of the Civil Code. Article 22 establishes the safe harbour for hosting services. A hosting platform may benefit from

limited liability only if it lacks actual or constructive knowledge of the infringement and promptly removes or disables access to the infringing content after receiving a valid notice. Once the platform knows or ought to know of the infringement but fails to take necessary measures, the safe harbour no longer applies and liability is determined under Articles 1195 and 1197 of the Civil Code. Article 23 directly applies only where the platform directs users to cloud storage, an external mini-program, or a third-party piracy website.

Hybrid platforms involving uploading, retrieval, intelligent aggregation, external redirection, and even live streaming should be characterised separately at each stage of content dissemination. Content uploaded through a platform-operated account, curated as part of a platform-produced feature, or placed behind a platform-imposed paywall is directly provided by the platform. User-submitted materials may constitute storage services; the aggregated presentation of third-party resources may constitute search or linking services; and information feeds are generally an additional mode of distributing content within one of the preceding services. An algorithm cannot alter the legal category of a service, although it may affect factual findings as to the obviousness of the risk and the platform's capacity for control.

3. Divergence, convergence, and lessons from recent decisions

3.1. From Story of Yanxi Palace to The Mystic Nine: algorithms as aggravating factors rather than an independent category of conduct

In the Story of Yanxi Palace case ([2018] Jing 0108 Min Chu No. 49421), the court did not equate automated recommendation with dissemination by the platform itself. Instead, considering the prominence of the popular work, the volume of infringing content, the traffic-related benefits generated by feed recommendations, and the platform's capacity to respond, it found reasonable grounds for the platform to know of the infringement and held that its measures were insufficient effectively to halt and prevent obvious infringement. The case did not establish that algorithmic recommendation itself constitutes infringement. Rather, it showed that the risk, benefit, and capacity for control amplified by recommendation may collectively raise the applicable standard of care.

The Mystic Nine case ([2022] Su 02 Min Zhong No. 4040) offered a clearer account of organisational involvement. The platform classified content by episode or feature and systematically processed uploaded material to facilitate continuous viewing. The court therefore concluded that the platform had not merely provided passive storage and may have facilitated infringement. In both cases, the issue was not an error in the algorithmic code itself, but the platform's responsibility for identifying, continuously organising, and repeatedly promoting particular popular works.

3.2. Divergent outcomes in The Mystic Nine and the Ximalaya case

The circumstances of the latter case differed from those above. In Youku v Ximalaya ([2023] Hu 73 Min Zhong No. 287), the Shanghai Intellectual Property Court explained that recommendations generated by a personalised algorithm were not the product of manual editing, screening, or arrangement. The mere fact that recommended audio infringed copyright was therefore insufficient to establish that the platform exercised substantial control over the information or knew of its existence. On its face, the result runs counter to The Mystic Nine, but the facts examined were not identical. In the former case, there was no evidence that the work had been organised through features, lists, or manual intervention; in the latter, intelligent aggregation, classification, and the creation of a complete collection were expressly established as facts. The apparent divergence

should therefore not be understood as an inconsistency in the applicable legal standard, but as the consequence of different findings concerning the nature and degree of platform intervention. A court-published case analysis similarly distinguishes automated personalised recommendation from the active selection, organisation, and classification of particular works when assessing whether a platform knew or ought to have known of the infringement [5].

Whether an algorithm is "neutral" should therefore not be treated as an all-or-nothing judicial proposition. A more appropriate approach distinguishes among types of recommendation. Personalised rankings generated solely from a user's viewing history have a weaker connection to particular content. By contrast, rankings, topics, episode indexes, collections, and live-stream portals created by a platform make the risk specific to a particular work. The divergence between the decisions indicates that an algorithm becomes evidence of constructive knowledge only when combined with content specificity, platform participation, and prior notice.

3.3. From Battle Soul to the high damages awards of 2025: necessary measures move from takedown to limited prevention of re-dissemination

The Battle Soul case ([2021] Zhe 0192 Min Chu No. 5770; [2022] Zhe 01 Min Zhong No. 3098) expressly held that a relatively strict duty of care should apply to algorithmic recommendations used by a platform. Where a right holder supplied a clearly identified work, examples of infringement, and screening criteria, the short videos concerned could be filtered or intercepted on that basis. The boundary was nevertheless limited: the court did not require indiscriminate filtering of all works, but confined prevention to measures responsive to the objects actually identified by the right holder.

The final decisions in the 2025 cases involving Deyun Laughter Club further strengthened this trend. Publicly available materials indicated clustering around relevant topics, live streams and replay resources, a large volume of infringing videos, repeat-infringer users, and continued dissemination after repeated notices. The courts referred both to substantial damages and to remedies such as filtering and interception. In Deyun Laughter Club ([2024] Yue Min Zhong No. 5088, Guangdong High People's Court), item-by-item notice and takedown could not constitute an effective measure after prolonged enforcement efforts and the emergence of numerous repeat accounts. The duty at that point should extend beyond deleting known URLs to identifying works through fingerprint matching, controlling related accounts, disabling recommendations, and preventing the reappearance of manifestly overlapping content.

These decisions do not mean that China has adopted comprehensive upload filtering of the EU model. Their convergence may be summarised in three propositions. First, there must be a particular work or infringement pattern, rather than a general industry risk. Second, the right holder should in principle provide copyright samples and information sufficient to enable identification. Third, the intensity of the duty is determined collectively by the platform's scale, technical capacity, direct financial benefit, repeated notices, and the effectiveness of its measures.

3.4. Progressive comparison of representative cases

The cases above can be examined under a common framework in which platform participation has a progressive relationship with constructive knowledge. In Story of Yanxi Palace, the initial broadcast period, number of infringements, traffic-derived benefits, and absence of an adequate response all indicated an algorithmic amplification effect; both the prominence of the work and the overall volume of infringement could therefore raise the standard of care. The Mystic Nine went further by treating classification, intelligent aggregation, and episode compilation as examples of structural

content arrangement and adopted a broader understanding of active platform involvement. By contrast, *Youku v Ximalaya* took a cautious position: in the absence of manual editing, feature design, or a specifically identified work, it declined to infer constructive knowledge merely from recommendation. Taken together, the three cases demonstrate that automated ranking alone is weak evidence. Only where recommendation coincides with content specificity, organisational involvement, and notice can the algorithm support a heightened standard of care.

As to the evolution of necessary measures, *Battle Soul* allowed a right holder to identify a definite work, examples of infringement, and screening targets, thereby recognising filtering or interception of a category of works as a possible response. *The Knockout*, *Deyun Laughter Club*, and *Lost You Forever* focused further on repeated notices, recurrent infringing accounts, concentrated or converging topics, and live streams and their replays. They accordingly pressed platforms to move beyond simple link deletion toward fingerprint analysis, suspension of recommendations, control of relevant accounts, and prevention of repeated dissemination of obvious variants. The central question in these cases was plainly not whether the platform used an algorithm, but whether the risk had materialised, whether the content had been systematically arranged, whether existing measures had remained ineffective over time, and whether the proposed new measure was both feasible and proportionate.

4. Lessons from foreign legal regimes

4.1. European Union: specific-information-driven prevention of re-uploading and procedural safeguards

Article 17 of the EU Directive on Copyright in the Digital Single Market establishes a special liability regime for online content-sharing service providers. In the absence of authorisation, a platform must demonstrate that it made best efforts to obtain permission and, once the right holder has supplied "relevant and necessary information" or sufficiently substantiated notice, made best efforts to ensure the unavailability of particular works, expeditiously removed them, and prevented future uploads. Geiger and Jütte observe that automated filtering may create tension among copyright protection, platforms' freedom to conduct a business, and users' freedom of expression, and that an overbroad filtering duty may become general monitoring in practice [6]. Quintais and others further emphasise that implementation of Article 17 must safeguard lawful uses such as quotation, criticism, and parody, while complaint procedures and human review should reduce erroneous restrictions produced by automated identification [7].

In the joined *YouTube/Cyando* cases (C-682/18 and C-683/18), the Court of Justice of the European Union continued to distinguish between a platform that merely provides facilities and one that actively intervenes beyond the intermediary role, requiring a fact-specific assessment of the connection among concrete knowledge, the manner of participation, and available measures [8]. In *Poland v Parliament and Council* (C-401/19), the Court confirmed that although Article 17 may in practice require the use of recognition tools, platforms may not block content whose illegality requires a complex legal assessment, and must provide complaint and human-review mechanisms. Article 8 of the Digital Services Act maintains the prohibition on imposing a general monitoring obligation, while recommendation-system transparency, systemic-risk assessment, and risk mitigation extend platform responsibility from individual responses to an auditable governance process. Quintais and Schwemer note that the Digital Services Act and Article 17 are not wholly separate: where the copyright-specific regime is incomplete, the former's procedural and due-diligence rules may operate supplementarily [9].

This specific-information-driven approach is particularly relevant to micro-short dramas because right holders generally possess complete master copies and can readily provide representative infringing samples and other information necessary for content identification. Accordingly, requiring platforms to prevent the re-uploading of specifically identified works may offer a more targeted response to repeated dissemination than either passive notice-and-takedown or unrestricted general monitoring.

4.2. United States: specific knowledge, repeat-infringer policies, and no general monitoring

Section 512 of the US Digital Millennium Copyright Act (DMCA) continues to make notice-and-takedown and specific knowledge central to safe-harbour protection, while requiring service providers to adopt and reasonably implement policies for terminating the accounts of repeat infringers. Section 512(m) expressly provides that eligibility for limited liability is not conditioned on monitoring services or affirmatively seeking facts indicating infringement. The institutional strength of this approach lies in its separate treatment of knowledge of specific infringement, governance of repeat infringement, and the absence of a general monitoring duty. It avoids inferring knowledge of every specific infringement merely because a platform is aware that piracy is generally present online. Elkin-Koren's review of online intermediary liability shows that the core function of safe harbours is to incorporate both platform cooperation in enforcement and safeguards against excessive expansion of private censorship into the institutional design [10].

For China, the US model supports the baseline requirement that risk be made specific, while the EU model provides tools for preventing repeated dissemination once that has occurred. The comparative study by Frosio and Mendis shows that proactive monitoring and filtering have become an international trend in platform governance, but are legitimate only where their objects are specific, their measures proportionate, and rights adequately protected [11]. Keller's analysis of EU filtering case law likewise indicates that platforms may be required to identify specific or equivalent content, but should not be compelled automatically to block content requiring an independent legal assessment [12]. The shared lesson is that platform duties may be heightened, but must be organised around specific objects, professional diligence, and procedural safeguards; commercialisation and automated recommendation cannot themselves be decisive.

4.3. Limited transplantation into Chinese law

China should not directly transplant the liability structure of Article 17, under which certain platforms are treated as communicating content to the public, because Articles 1195 and 1197 of the Civil Code and Articles 22 and 23 of the Regulations continue to rest on direct infringement by network users and secondary liability of platforms. China may nevertheless adopt its remedial sequence: necessary information supplied by the right holder, prevention of re-uploading of a specific work, and complaint and review procedures. The US rules further suggest that repeat-infringer account policies and the exemption from general monitoring should both form part of the judicial standard. Micro-short dramas are particularly suited to such limited transplantation. Their commercial value is concentrated shortly after release; complete episodes, consecutive instalments, and screen recordings of paid content ordinarily have relatively stable audiovisual features; and re-uploads involving renaming, cropping, or slight changes in playback speed are more readily identifiable through sample comparison than scattered user-generated material. Once the right holder has supplied an authorised sample, episode list, and confirmed infringing content, a time-limited,

threshold-based, and appealable obligation to prevent re-uploading of a specified micro-short drama is therefore both more necessary and more feasible.

In addition, Articles 7 and 8 of the Provisions on the Administration of Algorithm-Generated Recommendations for Internet Information Services require platforms to review algorithms, assess security, and conduct periodic verification. These process obligations under administrative law do not constitute elements of civil infringement, but may be used to assess whether a large platform has the capacity to verify, record, or modify its models. Administrative compliance is, in other words, evidence of capacity rather than a direct basis of civil liability.

5. A domestic two-tier, four-step framework for liability

5.1. Baseline governance duties

At the baseline-governance level, platforms should establish four mechanisms. First, both copyright complaints and counter-notices should be easy to submit and track. Second, platforms should record notices, responsive actions, disabling times, and fingerprint matches. Third, they should articulate and implement policies addressing repeat-infringer accounts. Fourth, they should periodically examine risks arising from the recommendation system itself, including whether it repeatedly directs known infringing material into trending, related, or similar-content areas. These duties serve to determine whether a platform possesses the basic governance structure of a prudent administrator; they do not require item-by-item review of every upload.

The legal consequences of baseline governance duties should be assessed through rules of evidence and fault. If a platform lacks a complaint mechanism, fails to produce action records, or has not applied its repeat-infringer policy, a court may relax the evidentiary burden on the right holder in proving fault. Conversely, complete logs, a clear complaint process, and validated technologies constitute evidence that due care has been exercised. This approach neither imposes liability solely because infringement occurred nor allows algorithmic governance to remain an unauditable and unverifiable black box.

5.2. Special duty of care

A platform enters the special-duty tier only when a valid notice, actual knowledge, or constructive knowledge makes the risk specific to a work, item of content, account, or mode of dissemination. The object is not permanent monitoring of the entire internet, but prevention of continued expansion of the same harm within an identifiable scope. Specificity can be established through four types of "anchor": a work anchor, such as the title, authorised file, and episode list; a content anchor, such as an audiovisual fingerprint and a confirmed infringing sample; an actor anchor, such as repeat-infringer and associated accounts; and a scenario anchor, such as live streaming during the initial-release period, a collection of complete episodes, or a screen recording of paid content. The clearer the anchor, the stronger the justification for automated measures.

5.3. Functional identification

A court should first determine the platform's actual function in the dissemination process. Where the platform uploads content itself, charges for viewing, or assigns content-production tasks, direct infringement rules apply. Merely providing technical storage for users' videos does not itself constitute infringement. Entrances to external cloud storage, mini-programs, and piracy websites

should be governed by Article 23 of the Regulations. Rankings, curated features, and intelligent collections are facts relevant to control and participation. Functional identification prevents two forms of misclassification: concealing self-operated content behind the label of a "technology platform," and treating on-platform playback as falling within Article 23 merely because the page contains a hyperlink.

5.4. Risk trigger

Risk triggering should be governed by a standard of "specific knowledge plus a holistic assessment." A valid notice may directly trigger duties under Article 1195 or Article 23. In the absence of notice, constructive knowledge under Article 1197 should be assessed by considering the work's popularity and initial-release period, the completeness of the infringement, platform-created features or collections, repeated complaints, account history, direct financial benefit, and the technical difficulty of identification. An algorithm carries significant evidentiary weight in only two circumstances: first, where the platform actively organises content by reference to the work's title, cover image, plot, and rankings; and second, where the platform already possesses copyright samples or has confirmed infringement but continues recommending highly similar content. Personalised ranking alone is insufficient to establish constructive knowledge.

5.5. Matching measures to risk

Necessary measures should be combined progressively in accordance with the infringement risk. For low-risk excerpts potentially involving lawful use, appropriate measures include pausing recommendations, forwarding notices, and conducting human review. A confirmed individual infringement should be deleted, blocked, or delinked. Where the same popular micro-short drama is repeatedly uploaded, the platform should add fingerprint comparison, disable keyword associations, and stop autoplay of similar content. Where an account repeatedly infringes, the platform should reduce its visibility, suspend monetisation, restrict live-streaming, or terminate the service. If the platform creates an infringing feature or live-stream portal, or directly shares the resulting revenue, its conduct may fall outside the scope of secondary liability.

This article characterises the resulting obligation as a "limited continuing duty." It is continuing because each re-upload of a confirmed work or an obvious variant should not require a fresh notice. It is limited because the objects of filtering, identification thresholds, and applicable period must be jointly confined by information supplied by the right holder, the work's commercial cycle, technical accuracy, and the risk of false positives. For example, after a right holder has supplied an authorised sample of a micro-short drama and sent repeated notices, a further upload of the same episode with only a changed title, cropped image, or slightly altered playback speed should not allow the platform mechanically to await another item-specific URL notice. It should use audiovisual fingerprinting, cease recommendations, and restrict repeat-infringer accounts. Conversely, content involving works with the same title, criticism, parody, trailers, or authorised promotion must not be blocked automatically on the basis of keywords or a low-similarity match alone.

5.6. Procedural verification

Whether a technical measure is "necessary" cannot be assessed solely by asking whether some infringing content ultimately remained available; the process must also be verified. A platform should explain the basic grounds for restrictions to affected users and provide counter-notice, appeal,

and human-review procedures. Right holders should be required to warrant the authenticity of supplied samples and bear responsibility for erroneous notices. Platforms should preserve records of filtering thresholds, the proportion of human reviews, and model adjustments. Where trade secrets are involved, limited disclosure may be achieved through court investigation orders, confidentiality orders, or third-party audits.

Procedural verification should also affect the burden of proof. Once the right holder proves a specific work, repeated infringement, continuing notices, and platform recommendation, the platform should explain the measures adopted and their effects. An adverse inference may be drawn if the platform refuses without justification to disclose action logs. A platform that demonstrates the use of reasonable thresholds, timely model correction, and an appeal process for lawful content should not incur strict liability merely because isolated infringing items evaded detection. The copyright duty of care is thereby transformed from an unverifiable inquiry into whether the platform "did its best" into a form of process-based liability capable of judicial examination.

6. Conclusion

Copyright liability for algorithmic recommendation platforms cannot be understood solely through the proposition that more advanced technology necessarily entails heavier responsibility. Nor can it be resolved formally by asserting that platforms remain neutral because algorithms operate automatically. Recent decisions show that what truly aggravates liability is the materialised form of the risk: particular works are promoted in large concentrations, warnings from right holders recur, infringing users continue to emerge, and a platform capable of detection and control fails to intervene. In such circumstances, one-notice-one-takedown can no longer fulfil the function of preventing the spread of harm required by Articles 1195 and 1197 of the Civil Code and Article 23 of the Regulations.

Under the "two-tier, four-step" method proposed here, complaint mechanisms, action logs, repeat-infringer rules, and algorithmic assessments form the first tier of baseline governance duties. Only after the risk becomes specific to a work, item of content, account, or dissemination scenario does the platform enter the second tier of special duties of care and proceed through functional identification, risk triggering, matching of measures, and procedural verification. The central proposition is that an algorithm cannot independently serve as the basis for attribution. It should instead be treated as a fact that amplifies risk or demonstrates capacity for control. A platform is not subject to strict liability guaranteeing zero infringement, but to process-based liability proportionate to the actual risk, degree of knowledge, technical capacity, and probability of erroneous restriction.

In the context of micro-short dramas, the short commercial cycle, relative ease of identifying complete unauthorised copies, and speed of repeated uploads make a limited continuing duty for specified works more appropriate than it would be for scattered content generally. Such a duty must nevertheless be conditioned on the right holder's provision of necessary information and bounded by lawful use, complaint and review procedures, and the absence of general monitoring. This approach can both incorporate the delinking rule in Article 23 of the Regulations into the Civil Code's system of necessary measures and translate foreign rules on preventing re-uploading and providing procedural safeguards into workable standards for Chinese courts.

References

- [1] Xiong, Q. (2020). "Algorithmic recommendation" and the rules for determining joint infringement by network service providers. *China Review of Administration of Justice*, 4, 125-136. (in Chinese)

- [2] Research Group of Shanghai Intellectual Property Court. (2024). The duty of care of algorithmic recommendation service providers. *Journal of Law Application*, 7, 24-36. (in Chinese)
- [3] Ma, Y. D., & Zhao, D. Y. (2025). A new interpretation of the duty of care of algorithmic recommendation service providers: Centered on the special review duty. *Intellectual Property*, 2, 3-23. (in Chinese)
- [4] Ren, A. Q. (2023). Rules for determining copyright infringement in algorithmic recommendation by network service platforms. *Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition)*, 36, 190-198. (in Chinese)
- [5] Zong, S. Y. (2026). Study on the duty of care of algorithmic recommendation service providers. *Taizhou Court Network*, 22 May 2026. (in Chinese)
- [6] Geiger, C., & Jütte, B. J. (2021). Platform liability under Article 17 of the Copyright in the Digital Single Market Directive, automated filtering and fundamental rights: An impossible match. *GRUR International*, 70, 517-543.
- [7] Quintais, J. P., Frosio, G., van Gompel, S., Hugenholtz, P. B., Husovec, M., Jütte, B. J., & Senftleben, M. (2019). Safeguarding user freedoms in implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European academics. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 10, 277-282.
- [8] Quintais, J. P., & Angelopoulos, C. (2022). YouTube and Cyando, joined cases C-682/18 and C-683/18 (22 June 2021): Case comment. *Auteursrecht*, 46-51.
- [9] Quintais, J. P., & Schwemer, S. F. (2022). The interplay between the Digital Services Act and sector regulation: How special is copyright? *European Journal of Risk Regulation*, 13, 191-217.
- [10] Elkin-Koren, N. (2014). After twenty years: Revisiting copyright liability of online intermediaries. In S. Frankel & D. Gervais (Eds.), *The evolution and equilibrium of copyright in the digital age* (pp. 29-51). Cambridge University Press.
- [11] Frosio, G., & Mendis, S. (2020). Monitoring and filtering: European reform or global trend? In G. Frosio (Ed.), *The Oxford handbook of online intermediary liability* (pp. 544-565). Oxford University Press.
- [12] Keller, D. (2020). Facebook filters, fundamental rights, and the CJEU's Glawischnig-Piesczek ruling. *GRUR International*, 69, 616-623.