

Functional Reconstruction of the Safe Harbour Rule for E-commerce Platforms in the Context of Artificial Intelligence and Cloud Computing: A Comparative Study of China and the European Union

Wuling Ying

Zhejiang Vocational College of Special Education, China. Ph.D. Candidate, Law Faculty, Universiti Teknologi MARA, Malaysia. E-mail: 459793221@qq.com.

Abstract: The safe harbour rule is a fundamental rule in the liability regime for online platforms. Its basic function is to prevent platforms from bearing excessive liability for third-party content, product information, or transactional conduct, while requiring them to take necessary measures once they have knowledge of infringement or receive a valid notice. This rule was justified in the early Internet environment. At that stage, platforms mainly provided information storage, transmission, and transactional channels. It was neither realistic nor desirable to require them to conduct comprehensive ex ante review of massive amounts of content and transactions.

However, artificial intelligence (AI) and cloud computing are changing the factual basis on which the safe harbour rule applies to e-commerce platforms. Modern e-commerce platforms do not merely store product information. They also influence transactions through cloud-based data processing, algorithmic recommendation, search ranking, advertising placement, automated review, and dispute resolution mechanisms. Platforms can centralize and process merchant qualifications, transaction records, consumer reviews, complaint data, and abnormal transaction signals. They may also participate in the display, optimization, and dissemination of product information through recommender systems and generative AI tools. Against this background, it is increasingly difficult to describe e-commerce platforms simply as passive intermediaries.

From a comparative perspective between China and the European Union (EU), this article examines the functional reconstruction of the safe harbour rule for e-commerce platforms in the context of AI and cloud computing. EU law retains intermediary liability exemptions, while strengthening platform duties concerning notice and action, statements of reasons, internal complaint handling, trader traceability, recommender-system transparency, and systemic risk governance under the *Digital Services Act* (DSA). Chinese law has developed a more fragmented framework through

the *Civil Code*, the *E-Commerce Law*, rules on algorithmic recommendation, and generative AI regulation. This article argues that the future application of the safe harbour rule to e-commerce platforms should not depend solely on whether the relevant information originates from a third-party merchant. Instead, it should be assessed by reference to the platform's technical capacity, degree of transactional control, algorithmic amplification, commercial benefit, and procedural safeguards.

Keywords: safe harbour rule; e-commerce platforms; artificial intelligence(AI); cloud computing; platform liability; algorithmic governance; China-EU comparison

Introduction

The safe harbour rule is a foundational rule in the liability regime for online platforms. Under this rule, a platform may usually benefit from a limitation of liability where it lacks knowledge of infringement and takes necessary measures after receiving a valid notice. Its core function is to prevent platforms from bearing excessive liability merely because third parties provide content, product information, or transactional services through them.

The rise of AI and cloud computing has, however, changed the factual setting in which the safe harbour rule operates. Modern e-commerce platforms no longer merely store product information or provide transactional channels. Through cloud-based data systems, algorithmic recommendation, search ranking, automated review, and dispute resolution mechanisms, platforms influence product visibility, transaction formation, and risk dissemination. The key question is therefore whether the safe harbour rule should continue to operate on the traditional assumption of platform passivity once the platform's technical capacity has significantly increased.

This article adopts a comparative perspective between China and the EU. It first examines the traditional logic and limits of the safe harbour rule. It then analyses how AI and cloud computing alter the factual basis for assessing platform risk identification, transactional control, and procedural handling. The article further considers the EU path from intermediary liability exemptions towards due diligence and risk governance. It then analyses the connection between safe harbour rules, special platform obligations, and technology-governance rules under Chinese law. Finally, it proposes a functional approach to reconstructing the safe harbour rule for e-commerce platforms.

1. The Traditional Logic and Limits of the Safe Harbour rule

The safe harbour rule is a conditional limitation of liability. Its basic function is to balance platform liability and platform innovation. As a general rule, a platform should not be held liable merely because third-party users publish content, upload product information, or conduct transactions through it. Platform liability may arise only where the platform has knowledge of the relevant infringement or fails to take necessary measures after receiving a valid notice. Section 512 of the US *Digital Millennium Copyright Act* and Articles 12 to 15 of the EU *E-Commerce Directive*

both reflect this basic approach.^[1]

The notice-and-takedown mechanism is the core procedure through which the safe harbour rule operates. When a right holder finds allegedly infringing content or products on a platform, it may submit a notice to the platform. After receiving a notice that satisfies the relevant requirements, the platform should take necessary measures in a timely manner. These measures may include deletion, blocking, disabling access, terminating transactions, or suspending services. If the platform acts in a timely and reasonable way, it can usually limit its own liability. If it refuses to act without justification or delays action in an obvious manner, it may be liable for the expanded harm caused by its failure to act.

The safe harbour rule must also be connected with the limiting condition of “knowledge or constructive knowledge.” Where a platform already knows of infringement, or should have known of it on the basis of concrete, obvious, and repeated risk signals, it should not be able to continue relying on liability limitation if it fails to take necessary measures. This condition should not be understood as an independent basis for unlimited expansion of platform liability. Rather, it should be understood as a limitation on the application of the safe harbour rule. Its function is to prevent a platform from remaining passive in the face of obvious risks merely because it has not received a formal notice.

At the same time, this limiting condition must not be expanded without restraint. A platform should not be presumed to know all infringement or unlawful conduct merely because an abstract risk exists. Otherwise, the safe harbour rule would be emptied of its substance, and a general monitoring obligation would re-emerge in another form. The traditional boundary of the safe harbour rule may therefore be summarized in two propositions. First, a platform should not bear a general obligation to conduct continuous, comprehensive, and indiscriminate review of all content, products, and transactions. Second, a platform should still take necessary and proportionate measures when it receives a valid notice or faces concrete, obvious, and repeated risk signals.

The safe harbour rule had a strong factual basis in the early Internet environment. Platforms faced large amounts of third-party content and transactional information. Comprehensive ex ante review was difficult to conduct. This was especially true in intellectual property disputes, where issues such as ownership, scope of authorization, trademark similarity, copyright fair use, and exhaustion of rights often require complex legal assessment. If platforms were required to conduct substantive review before every item of content was published or every product was listed, compliance costs would be excessive. Platforms might also respond by over-removing content and over-blocking transactions. For this reason, traditional safe harbour rules usually reject a general proactive monitoring obligation and instead trigger platform obligations through post-notice procedures.

This structure has not become obsolete in itself. The real difficulty is that artificial intelligence and cloud computing are changing the platform’s ability to identify risks,

^[1] U.S. Copyright Office, *Section 512 of Title 17: A Report of the Register of Copyrights*, 2020; European Parliament and Council, *Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market*, *Official Journal of the European Communities*, L 178, 1–16, 2000.

control transactions, and handle disputes. Traditional rules were based on the assumption that platforms were relatively passive. Modern e-commerce platforms, however, can influence the transaction process through data systems, recommender algorithms, and automated tools. It is in this sense that the safe harbour rule requires functional reconstruction. It should not be simply abolished, but neither should it be mechanically preserved in its traditional form.

2. How AI and Cloud Computing Change the Factual Basis for Applying Safe Harbour to E-commerce Platforms

AI and cloud computing do not, by themselves, exclude the application of the safe harbour rule to e-commerce platforms. E-commerce platforms still deal with massive amounts of product information, complex transactional relationships, and large-scale user activity. If the law required platforms to review all products, merchants, and transactions in advance, compliance costs would remain excessive. Such a requirement could also lead to over-removal, over-blocking, and excessive restrictions on merchants. The real question in the AI era is therefore whether the platform's technical capacity and transactional function have changed the basis on which liability limitations should be assessed.

First, cloud computing increases the possibility that platforms can identify specific risks. Traditional platforms also stored user information, but their capacity for data processing was relatively limited. Modern e-commerce platforms can use cloud-based systems to centralize product information, merchant records, transaction data, payment information, logistics status, consumer reviews, complaint records, and after-sales disputes. These data are no longer merely fragmented pieces of information. They can be continuously recorded, cross-checked, and modelled. Where a merchant has been repeatedly complained about, where a product has continuously generated similar quality problems, or where transactions show abnormal refund rates or negative reviews, the platform may already have the conditions necessary to identify the relevant risk.

This change affects the "lack of knowledge" element in the safe harbour analysis. Under traditional rules, platform obligations are often triggered by a notice from the right holder. In the absence of such notice, a platform may argue that it had no knowledge of the relevant risk. Cloud computing does not mean that platforms should actively discover all infringement or unlawful conduct. It does, however, weaken the platform's ability to rely entirely on a lack of knowledge in specific risk scenarios. In other words, whether a platform can reasonably claim ignorance depends increasingly on whether the risk was concrete, obvious, repeated, and supported by data actually available to the platform.

Second, algorithmic recommendation strengthens the platform's influence over transaction formation and risk dissemination. Modern e-commerce platforms widely use algorithmic systems for product ranking, personalized recommendation, advertising matching, intelligent labelling, and traffic allocation. Which products consumers see, which links they click first, and which promotional information they receive are often shaped by the platform's recommender system. Product-related risks are therefore no longer only the natural result of information uploaded by merchants. They may also be amplified by the platform's recommendation, ranking, and

advertising mechanisms.

This point is particularly important for the application of safe harbour. Traditional rules mainly ask whether the information was uploaded by a third party and whether the platform acted after receiving notice. In an algorithmic e-commerce environment, however, it is also necessary to examine whether the platform expanded the transactional opportunity of the relevant product through recommendation, ranking, advertising, or promotion. If the platform merely stores product information, the justification for liability limitation remains strong. If, however, the platform actively increases the visibility of a high-risk product, or continues to promote a product after repeated complaints, its claim to be a neutral intermediary becomes less persuasive. Sharkey argues, in the context of products liability in the digital age, that online platforms may in certain transactional settings be better placed to prevent risks, because they possess transaction data, control the transaction interface, and influence consumer choice.^[2] Although this argument arises from the context of US law, it is instructive for the safe harbour analysis of e-commerce platforms. It suggests that platform liability should not be assessed solely by asking whether the product was supplied by a third party. It should also consider whether the platform actually influenced the relevant transactional risk.

Third, generative AI blurs the boundary between third-party content and platform tools. Traditional safe harbour rules usually assume that the relevant content originates from third parties. Since the platform does not create the content, it may claim liability limitation if the legal conditions are satisfied. In e-commerce platforms, however, product titles, product descriptions, advertising copy, customer-service responses, livestreaming scripts, product images, and even review content may be generated or optimized by generative AI tools. If a merchant independently uses an external AI tool to generate product information, the platform can still, to a considerable extent, be treated under the traditional third-party content framework. If the platform takes necessary measures after receiving a valid notice, safe harbour protection may still be available.

The situation is different where the platform itself provides generative AI tools and actively helps merchants generate, optimize, or promote product content. In that case, the connection between the platform and the relevant content becomes stronger. The platform cannot simply attribute all related risks to third-party merchants. Henderson, Hashimoto, and Lemley argue that liability for harmful AI outputs is closely related to system design, deployment choices, and safety mechanisms, and cannot be addressed simply by applying traditional content-liability rules.^[3] This argument is also relevant to e-commerce platforms. Where a platform embeds generative AI tools into its transaction system, it should assume clearer governance duties concerning the boundaries of tool use, risk warnings, complaint handling, and error correction.

Finally, automated review changes the operation of the notice-and-takedown mechanism. Traditional notice-and-takedown procedures usually assume that, after a right holder submits an infringement notice, the platform reviews the notice and decides whether to delete, block, or disable access. Modern e-commerce platforms

^[2] Sharkey, C. M., *Products Liability in the Digital Age: Online Platforms as “Cheapest Cost Avoiders,”* *Hastings Law Journal*, 73, 1327–1390, 2022.

^[3] Henderson, P., Hashimoto, T., & Lemley, M. A., *Where’s the Liability in Harmful AI Speech?*, *Journal of Free Speech Law*, 3, 589–629, 2023.

may instead use automated systems to process intellectual property complaints, identify repeated infringement, screen unlawful products, assess consumer refund requests, and decide whether to penalize merchants. Automated review can improve efficiency and help platforms identify obvious violations or repeated infringement more quickly. Yet it may also amplify the effects of erroneous notices, malicious complaints, and system mistakes.

For this reason, safe harbour rules in the AI era should not focus only on whether the platform acted quickly. They should also examine whether the platform acted reasonably. If an automated system removes a product without providing the merchant with an effective explanation, appeal, or correction opportunity, procedural fairness may be weakened. The *DSA* offers an important reference in this respect. While retaining intermediary liability exemptions, it requires platforms to establish notice-and-action mechanisms, provide statements of reasons, set up internal complaint-handling systems, and improve the transparency of recommender systems.^[4] These rules show that modern platform governance is not only a question of whether content is removed. It is also a question of whether platform decisions are transparent, appealable, and correctable.

In sum, AI and cloud computing do not eliminate the safe harbour rule, but they change the factual basis for its application. Cloud computing increases the possibility of identifying specific risks. Algorithmic recommendation strengthens the platform's influence over transaction formation and risk dissemination. Generative AI blurs the boundary between third-party content and platform tools. Automated review changes the procedural structure of notice-and-takedown and dispute handling. The future application of safe harbour to e-commerce platforms should therefore focus more on the platform's technical capacity, risk visibility, degree of transactional involvement, and procedural safeguards in the specific transaction, rather than relying solely on whether the relevant content or product originated from a third party.

3. The EU Path: Retaining Safe Harbour While Adding Due Diligence and Risk Governance

EU law provides an important reference for reconstructing the safe harbour rule for e-commerce platforms in the context of AI and cloud computing. Its regulatory path is to retain the basic structure of safe harbour while gradually adding platform duties of due diligence, transparency, and risk governance. This path shows that modern platform liability is no longer confined to the simple logic of "remove after notice." It increasingly focuses on the platform's actual functions in information ranking, transaction organization, risk dissemination, and procedural safeguards.

The traditional EU safe harbour framework was mainly established by the *E-Commerce Directive*. Articles 12 to 14 of the Directive provide liability exemptions for mere conduit, caching, and hosting services, while Article 15 expressly rejects a general monitoring obligation for intermediary service providers. The hosting rule is particularly important for e-commerce platforms. Under Article 14, a hosting service provider may benefit from a limitation of liability where it does not have knowledge

^[4] European Parliament and Council, *Regulation (EU) 2022/2065 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)*, arts. 16, 17, 20, 27, *Official Journal of the European Union*, L 277, 1–102, 2022

of illegal activity or information. Once it obtains actual knowledge, it must act expeditiously to remove or disable access to the relevant information.^[5]

This rule was suited to the characteristics of early Internet services. Platforms mainly provided information transmission, storage, and hosting functions. It was not appropriate to require them to review all user content. Modern e-commerce platforms, however, are no longer identical to early hosting services. They do not merely display product information. They also influence transactions through search ranking, advertising, recommender systems, merchant ratings, and dispute resolution mechanisms. In the age of AI and cloud computing, platforms can further identify specific risks through data analysis and automated systems. For this reason, understanding e-commerce platforms only as “hosts” no longer adequately explains their role in digital markets.

The Court of Justice of the European Union addressed this issue at an early stage in *L’Oréal SA v. eBay International AG*. The case concerned allegedly trademark-infringing goods sold on eBay. The Court held that whether an online marketplace operator could rely on the hosting exemption under Article 14 of the *E-Commerce Directive* depended on whether it played a neutral role. Where the platform’s conduct is merely technical, automatic, and passive, so that it has neither knowledge of nor control over the stored data, the liability exemption may apply. By contrast, where the platform plays an active role that gives it knowledge of or control over the relevant data, it cannot automatically enjoy the hosting safe harbour.^[6]

The significance of this case lies in the fact that the Court did not rely solely on whether the product information was uploaded by third-party sellers. It further examined the platform’s actual role in the transaction. The Court specifically observed that an online marketplace operator may fall outside the scope of a neutral hosting role where it provides assistance that optimizes the presentation of offers for sale or promotes them.^[7] This reasoning has direct implications for algorithmic e-commerce platforms. Today, recommender systems, personalized advertising, search ranking, and traffic support may constitute more complex forms of presentation optimization and sales promotion. Where a platform uses AI systems to target consumers with specific products, or expands transactional opportunities through advertising and promotion, its role differs from that of a service that merely stores product information.

The *DSA* further develops this approach. It does not abolish intermediary liability exemptions. Instead, it retains liability limitations and the prohibition of general monitoring obligations while adding more detailed platform due diligence duties. Article 8 continues to prohibit the imposition of a general monitoring obligation on intermediary service providers. At the same time, Article 16 requires hosting service providers to establish notice-and-action mechanisms. Article 17 requires platforms to provide statements of reasons when they remove, block, demote, suspend, or

^[5] European Parliament and Council, *Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market*, arts. 12–15, *Official Journal of the European Communities*, L 178, 1–16, 2000.

^[6] Court of Justice of the European Union, *L’Oréal SA and Others v. eBay International AG and Others*, Case C-324/09, Judgment of 12 July 2011.

^[7] Court of Justice of the European Union, *L’Oréal SA and Others v. eBay International AG and Others*, Case C-324/09, Judgment of 12 July 2011.

otherwise restrict content or services. Article 20 requires online platforms to establish internal complaint-handling systems. Article 27 requires online platforms to explain the main parameters used in recommender systems. Article 30 imposes trader traceability duties on online marketplaces. Articles 34 and 35 require very large online platforms and very large online search engines to conduct systemic risk assessments and adopt risk mitigation measures.^[8]

These rules show that EU law has changed the institutional environment in which safe harbour operates. Platforms are no longer merely required to remove content after receiving notice. They must also establish governance mechanisms that are transparent, appealable, traceable, and capable of risk assessment. For e-commerce platforms, trader traceability is particularly important, because product-related risks on platforms are often closely connected with merchant identity, qualifications, and transaction records. Recommender-system transparency is also significant, because whether a product is seen by consumers often depends on search ranking and recommendation logic. Internal complaint-handling mechanisms provide merchants and users with a procedural route to challenge platform decisions.

This institutional change is important for the functional reconstruction of the safe harbour rule. If a platform merely stores third-party product information, the justification for liability limitation remains relatively strong. If, however, it actively increases the visibility of a product through a recommender system or expands transactional opportunities through advertising, its connection with the relevant risk becomes stronger. In particular, where infringing, counterfeit, or unsafe products are repeatedly recommended by algorithms, the platform cannot fully return to the traditional claim that it “merely hosts information.” Of course, recommender-system transparency does not mean that platforms should bear strict liability for all recommendation results. A more reasonable approach is to require platforms to establish appropriate risk identification, recommendation restriction, and complaint-and-correction mechanisms for high-risk products, repeatedly non-compliant merchants, and abnormal transactions.

Although the EU *Artificial Intelligence Act* is not a law specifically governing safe harbour for e-commerce platforms, it further reflects the risk-based orientation of technology governance. Adopted in 2024, the Act establishes a unified regulatory framework for AI systems. Through rules on prohibited AI practices, high-risk AI systems, transparency obligations, and general-purpose AI models, it promotes the allocation of responsibilities in the development and use of AI systems.^[9] Its relevance is that platform liability assessment will increasingly be difficult to separate from the technical systems used by platforms. Where e-commerce platforms use AI for product recommendation, advertising placement, customer-service responses, fraud detection, or complaint handling, they must also consider transparency, risk control, and human oversight mechanisms.

In sum, the EU path can be summarized in three points. First, the safe harbour rule remains necessary. A platform should not be held liable merely because of third-party

^[8] European Parliament and Council, *Regulation (EU) 2022/2065 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)*, arts. 8, 16, 17, 20, 27, 30, 34–35, *Official Journal of the European Union*, L 277, 1–102, 2022.

^[9] European Parliament and Council, *Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, *Official Journal of the European Union*, OJ L, 2024/1689, 12 July 2024.

content or transactional conduct. Second, the safe harbour rule should not operate in isolation. It should be connected with notice and action, statements of reasons, internal complaints, trader traceability, recommender-system transparency, and systemic risk governance. Third, the more active the platform's function becomes, the more its liability limitation must be examined in light of the specific facts. The active-role analysis in *L'Oréal v. eBay* and the duties concerning recommender-system transparency and risk governance under the *DSA* are logically consistent. Together, they show that the more deeply a platform influences transactional display, risk dissemination, and market order, the less it can rely solely on the third-party origin of information as a basis for exemption.

4. Chinese Law: Connecting Safe Harbour Rules with Platform Technology-Governance Duties

Chinese law does not define the safe harbour rule as a unified legal concept. Instead, it has developed a fragmented set of liability limitations and platform-governance rules through the *Civil Code*, the *E-Commerce Law*, and regulations on algorithmic recommendation and generative AI. The basic approach is that a platform is not automatically liable for third-party conduct. However, it must take necessary measures where it receives a valid notice, knows or should know of an infringement risk, or bears specific platform-management duties. The problem in Chinese law is therefore not the complete absence of rules. It is that these rules have not yet been clearly connected. This issue is particularly important in the context of artificial intelligence and cloud computing, where notice handling, product recommendation, content generation, data storage, and risk identification increasingly depend on technical systems.

Articles 1195 and 1197 of the *Civil Code* provide the general rules on online tort liability in Chinese law. Article 1195 provides that where a right holder finds that an online user has infringed its civil rights through online services, it may notify the network service provider to take necessary measures, such as deletion, blocking, or disabling access. After receiving the notice, the network service provider must promptly forward the notice to the relevant online user and take necessary measures according to the preliminary evidence and the type of service involved. Article 1197 further provides that where a network service provider knows or should know that an online user is infringing another person's civil rights through its service, but fails to take necessary measures, it shall bear joint and several liability with that user.^[10]

Together, these two provisions reflect a general liability-limitation structure in Chinese law. Article 1195 focuses on post-notice procedures, while Article 1197 makes clear that liability limitation is not unconditional. Xue Jun argues that the notice-and-takedown and counter-notice rules in the *Civil Code* should be understood as auxiliary rules for determining whether a network service provider is at fault, rather than as a basis for imposing an unconditional removal duty on a platform once it receives notice.^[11] This view helps clarify that safe harbour is not a mechanical “notice means removal” rule. Platform liability should still be assessed by reference to fault, risk visibility, and whether necessary measures were taken.

^[10] National People's Congress, *Civil Code of the People's Republic of China*, arts. 1195, 1197, 2020.

^[11] Xue, J., A Study on the Online Tort Provisions of the Civil Code: Centered on the Reconstruction of the Framework of Legal Interpretation, *Journal of Comparative Law*, 2020(4).

The *Civil Code* rules, however, are general rules. They are not specifically designed for e-commerce platforms. E-commerce platforms do not merely host third-party product information. They also organize product display, search ranking, transaction matching, payment arrangements, after-sales services, and complaint handling. Compared with ordinary information storage services, e-commerce platforms exert greater influence over the transaction process. It is therefore insufficient to explain e-commerce platform liability solely through general online tort rules. The special obligations under the *E-Commerce Law* must also be considered.

Article 27 of the *E-Commerce Law* requires platforms to verify and register the identity, address, contact information, and administrative licences of platform operators, and to update such information regularly. Article 29 requires platforms, upon discovering unlawful information concerning products or services on the platform, to take necessary measures in accordance with law and report to the competent authorities. Article 38 provides that where a platform knows or should know that products sold or services provided by operators on the platform fail to meet personal or property safety requirements, or otherwise infringe consumers' lawful rights and interests, and fails to take necessary measures, it shall bear liability in accordance with law.^[12]

Articles 42 to 44 of the *E-Commerce Law* provide specific rules on notice, declaration, and publication in intellectual property disputes. Where an intellectual property right holder believes that its rights have been infringed, it may notify the platform to take necessary measures, including deletion, blocking, disabling access, terminating transactions, or suspending services. After receiving the notice, the platform must take necessary measures in a timely manner and forward the notice to the operator on the platform. Where the operator considers that no infringement exists, it may submit a declaration. The platform must forward the declaration to the right holder and inform the right holder that it may complain to the competent authority or bring an action before a people's court. If the right holder fails to notify the platform within the statutory period that it has filed a complaint or brought an action, the platform must promptly terminate the measures taken. The platform must also publish the notices, declarations, and handling results in a timely manner.^[13] This notice, declaration, and publication mechanism establishes an exchange procedure among the right holder, the platform, and the operator on the platform. It helps address problems such as malicious notices, unclear standards for platform review, and imbalances between the protection of right holders and the interests of platform operators.^[14] In this sense, the *E-Commerce Law* does not adopt a simple "notice means takedown" model. It sets up a procedural mechanism that includes notice, forwarding, declaration, termination of measures, and publication of results. Whether a platform may rely on liability limitation should therefore depend not only on whether it removes or blocks content quickly, but also on whether it complies with these procedural safeguards.

Rules on algorithmic recommendation further change the normative context in which safe harbour applies. Article 2 of the *Provisions on the Administration of Algorithmic*

[12] National People's Congress, Electronic Commerce Law of the People's Republic of China, arts. 27, 29, 38, 2018.

[13] National People's Congress, Electronic Commerce Law of the People's Republic of China, arts. 42–44, 2018.

[14] Wen, Y., Study on the Application of "Notice and Counter-Notice" Rules in Electronic Commerce Law, *E-Commerce Letters*, 13(4), 3828–3834, 2024.

Recommendation in Internet Information Services defines algorithmic recommendation technologies to include generation and synthesis, personalized pushing, ranking and selection, search filtering, and scheduling and decision-making. Article 4 requires algorithmic recommendation services to comply with laws and regulations and to follow the rules of fairness, openness and transparency, scientific reasonableness, and good faith.^[15] For e-commerce platforms, product search ranking, personalized recommendation, advertising, intelligent labelling, and traffic allocation may all involve algorithmic recommendation technologies.

Algorithmic recommendation rules do not directly cancel safe harbour protection. Recommender systems are now basic functions of modern e-commerce platforms. The key issue is whether the platform has amplified the risk of a particular product, merchant, or transaction through algorithms. Where a product has already generated repeated complaints, high-risk labels, or abnormal transaction signals, and the platform continues to recommend or advertise it, the connection between the platform and the relevant transaction becomes stronger. Zhang Yang argues, in relation to copyright filtering obligations under algorithmic recommendation, that although platforms using algorithmic recommendation technologies remain network service providers, technological development distinguishes them from traditional network service providers, and safe harbour rules should not apply automatically. Algorithmic recommendation improves platforms' information-management capacity and also brings traffic-based economic benefits. Platforms should therefore bear obligations corresponding to these capacities and benefits.^[16] This view supports the proposition that algorithmic recommendation does not automatically increase platform liability, but it may affect the specific assessment of the platform's duty of care.

Generative AI regulation further affects the assessment of the source of product information. The *Interim Measures for the Management of Generative Artificial Intelligence Services* apply to services that use generative AI technologies to provide text, images, audio, video, and other content generation services to the public.^[17] On e-commerce platforms, generative AI may be used to produce product titles, product descriptions, advertising copy, customer-service responses, livestreaming scripts, and product images. If the platform merely hosts content independently uploaded by merchants, traditional safe harbour rules may still apply. If, however, the platform provides AI tools and actively generates, optimizes, or promotes product content, its role is no longer limited to information storage. In such circumstances, whether the platform participates in content formation should become an important factor in assessing whether it can rely on liability limitation.

The core issue under Chinese law is therefore how to connect the general online tort rules in the *Civil Code*, the special platform obligations in the *E-Commerce Law*, and the rules on algorithmic and generative AI governance. A feasible interpretive path is to connect platform liability limitations with the platform's technology-governance

^[15] Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, & State Administration for Market Regulation, Provisions on the Administration of Algorithmic Recommendation in Internet Information Services, arts. 2, 4, 2021.

^[16] Zhang, Y., The Construction of Copyright Filtering Obligations under Algorithmic Recommendation, *Modern Law Science*, 45(4), 75–89, 2023.

^[17] Cyberspace Administration of China, National Development and Reform Commission, Ministry of Education, Ministry of Science and Technology, Ministry of Industry and Information Technology, Ministry of Public Security, & National Radio and Television Administration, Interim Measures for the Management of Generative Artificial Intelligence Services, art. 2, 2023.

capacity. Platforms should still benefit from liability limitation when they provide basic intermediary services. However, where a platform deeply participates in transaction governance through algorithmic recommendation, generative AI tools, automated review, and cloud-based data processing, the application of safe harbour should be assessed by reference to the platform's control capacity, risk visibility, compliance with statutory procedures, and the need for consumer protection. As Xue Jun observes, the core issue of platform liability under the *E-Commerce Law* is how to understand the platform's special function in transaction organization and the boundaries of its liability.^[18] E-commerce platform liability should therefore not be assessed solely by asking whether product information originates from a third party. It should also be analyzed in light of the platform's actual function in organizing transactions.

5. Functional Reconstruction: From Formal Exemption to Functional Review

AI and cloud computing do not deprive the safe harbour rule of its value for e-commerce platforms. On the contrary, the rule remains necessary. E-commerce platforms process massive amounts of product, merchant, and transaction information every day. If platforms were required to conduct comprehensive proactive review of all products and transactions, compliance costs would be excessive. Such a requirement could also lead to over-removal, over-blocking, and barriers to market entry. The purpose of functional reconstruction is therefore to reinterpret the conditions under which liability limitation applies.

First, attention should be paid to the platform's technical capacity. Traditional safe harbour rules often assume that platforms cannot promptly discover all third-party infringement or unlawful conduct. Under conditions of cloud computing and AI, however, platforms can centralize merchant information, transaction records, complaint data, consumer reviews, and abnormal transaction signals. The enhancement of technical capacity does not mean that platforms should bear a general monitoring obligation. It does, however, affect the platform's reasonable duty of care in specific risk scenarios. Where there are repeated complaints, high-risk products, obvious abnormal transactions, or risk signals already identified by the system, it becomes difficult for the platform to rely entirely on lack of knowledge as a basis for liability limitation.

Second, attention should be paid to the platform's degree of transactional control. E-commerce platforms differ from ordinary content-hosting services. They not only display product information, but also participate in transaction matching, payment arrangements, logistics-information integration, after-sales rule-making, and complaint handling. The deeper the platform's control over the transaction process, the narrower the space for it to claim a purely neutral intermediary role. Where a platform merely provides basic transaction space and takes necessary measures after receiving a valid notice, liability limitation should still apply. Where it deeply participates in product display, transaction rules, and after-sales handling, it should demonstrate that it has established corresponding risk-governance and procedural-safeguard mechanisms.

^[18] Xue, J., The Connotation and Application Model of Platform Liability under the E-Commerce Law, *Science of Law (Journal of Northwest University of Political Science and Law)*, 41(1), 57–68, 2023.

Third, attention should be paid to algorithmic amplification. Recommender systems, search ranking, advertising, and traffic allocation have become important functions of modern e-commerce platforms. A platform should not lose safe harbour protection merely because it uses algorithms, since recommender systems are basic components of e-commerce operations. However, where repeated complaints, high-risk labels, or abnormal transaction signals already exist, and the platform still continues to recommend or promote the relevant product through algorithms, the connection between the platform and risk dissemination becomes stronger. Algorithmic amplification should therefore become an important factor in assessing the platform's duty of care.

Fourth, attention should be paid to procedural safeguards. The safe harbour rule should not ask only whether the platform removed or blocked content quickly. It should also check whether the platform's handling mechanism was reasonable, transparent, and correctable. In intellectual property cases, the platform should handle notices, declarations, termination of measures, and publication of results in accordance with law. In other e-commerce disputes, the law may not expressly establish the same counter-notice mechanism. Even so, platforms may still take measures that affect the rights and interests of merchants or consumers. Such measures include product removal, traffic restriction, account suspension, and refusal of refunds. Where such measures are taken, platforms should provide necessary explanations, complaint channels, and correction mechanisms. The more widely automated review is used, the more important procedural safeguards become. Otherwise, the platform may improve processing efficiency in form while substantively amplifying erroneous notices, malicious complaints, and system mistakes.

On the basis of these factors, the application of the safe harbour rule to e-commerce platforms should move from formal identity-based analysis to functional review. Functional review means that liability limitation should no longer depend only on whether product information comes from a third party, whether the platform received a notice, or whether it removed content in time. It should instead examine the platform's technical capacity, degree of control, algorithmic role, and procedural safeguards in the specific transaction. This approach serves two functions. First, it prevents platforms from bearing excessive liability for third-party conduct. Second, it prevents platforms from relying on "third-party content" or "absence of notice" to avoid reasonable governance duties after their technical capacity has significantly increased.

Developments in both EU and Chinese law show that the safe harbour rule is moving from a pure exemption rule towards a legal structure connected with platform-governance duties. EU law connects intermediary liability exemptions with notice and action, statements of reasons, internal complaints, trader traceability, recommender-system transparency, and systemic risk governance through the *DSA*. Chinese law has developed rules on notice handling, special platform obligations, and technology governance through the *Civil Code*, the *E-Commerce Law*, and regulations on algorithmic recommendation and generative AI. Although the two systems follow different paths, their common trend is clear. Platforms still do not bear a general monitoring obligation. However, closer scrutiny is required in certain situations. This includes cases where specific risks have emerged, where the platform can identify and

control those risks, or where the platform substantively intervenes in transactions through technical systems.

6. Conclusion

The safe harbour rule has provided important institutional space for the development of Internet platforms. It prevents platforms from bearing excessive liability for third-party content and transactional conduct, and it also reduces incentives for platforms to engage in over-removal and excessive restrictions. This institutional value remains important in the era of artificial intelligence and cloud computing. E-commerce platforms continue to deal with massive amounts of product information and complex transactions. They still need liability limitations.

However, the technical capacity and transactional function of modern e-commerce platforms have changed. Cloud computing increases the possibility that platforms can identify specific risks. Algorithmic recommendation strengthens the platform's influence over product visibility and transactional opportunities. Generative AI blurs the boundary between third-party content and platform tools. Automated review changes the procedural structure of notice-and-takedown and dispute handling. For these reasons, continuing to rely entirely on the traditional passive-intermediary narrative can no longer adequately explain the actual role of e-commerce platforms in digital transactions.

This article argues that the safe harbour rule for e-commerce platforms should be functionally reconstructed in the context of AI and cloud computing. Platforms should still enjoy liability limitation when they provide basic intermediary services. They should not incur liability merely because they use cloud computing, algorithmic recommendation, or AI tools. The key issue is not the mere use of technical systems. Rather, the question is how the platform uses those systems in the transaction process. Relevant factors include the platform's degree of participation in transactions, its ability to identify specific risks, its role in amplifying risks through recommendation or advertising, its direct benefits from the relevant transactions, and the procedural safeguards it provides.

The China-EU comparison shows that the more appropriate direction is not to abolish the safe harbour rule, but to place it within a broader framework of platform-governance duties. The EU experience lies in retaining intermediary liability exemptions while limiting passive exemption through due diligence duties, transparency mechanisms, and risk governance. The focus for Chinese law is to further connect the *Civil Code*, the *E-Commerce Law*, and technology-governance rules, and to clarify the platform's duty of care in different risk scenarios. Future judicial interpretations, regulatory guidance, and platform compliance rules in China may further clarify that the platform's technical capacity, degree of transactional control, algorithmic amplification, and procedural safeguards should all be important factors in determining the application of safe harbour.

Accordingly, the safe harbour rule in the AI era should not be understood simply as a tool for platform exemption. Nor should it be expanded into a regime of comprehensive platform liability. It should instead operate as a functional liability-limitation mechanism. Under this mechanism, platforms will not be overburdened with liability for third-party conduct. At the same time, they will not be

able to rely on formal neutrality to avoid reasonable governance responsibilities when their technical capacity and market control have significantly increased.