International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Liability of E-Commerce Platforms for Cybercrimes: A Critical Analysis of Legal Framework

Ms. Nikhitha N[1], Prof. Dr. Nagaraja V[2]

[1]Student, School Of Legal Study, Reva University
[2]Professor, School Of Legal Study, Reva University

Abstract
The rise of e-commerce platforms has transformed international commerce, offering consumers ease of access, convenience and variety in goods and services. The growth of e-commerce platforms in India has been supported by rising internet connectivity, online payments, and government initiatives like Digital India. But it has also opened up opportunities for cyber offences such as identity theft, phishing, data breaches, fake listings and fraudulent transactions. E-commerce platforms, as the middlemen between buyers and sellers, are often the focal point in disputes related to these cyber crimes.

Introduction

The rise of e-commerce platforms has transformed international commerce, offering consumers ease of access, convenience and variety in goods and services. The growth of e-commerce platforms in India has been supported by rising internet connectivity, online payments, and government initiatives like Digital India. But it has also opened up opportunities for cyber offences such as identity theft, phishing, data breaches, fake listings and fraudulent transactions. E-commerce platforms, as the middlemen between buyers and sellers, are often the focal point in disputes related to these cyber crimes.

The role of e-commerce platforms in cybercrime cases has raised complex liability issues. Historically, platforms have relied on the doctrine of "intermediary liability" to maintain that they only offer a technological platform for transactions, and not an active role in them. But the nature of cybercrimes has evolved, making it difficult to distinguish between the roles of intermediary and active participant, and with it, questions over liability.[1]

In India, the Information Technology Act, 2000 (IT Act) offers some safe harbor protections to intermediaries under Section 79. These safeguards are not absolute and depend on the intermediary not being complicit in any illegal activities. The recent Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, have raised the compliance obligations for intermediaries, requiring them to have a grievance redressal mechanism, monitor content, and take more stringent measures.

However, there remains uncertainty in defining liability. Indian courts have taken diverging views on intermediary liability, particularly in intellectual property infringement, fraudulent transactions and user-generated content. This leads to confusion among businesses and consumers, eroding confidence in online

[1] Reed Chris, Internet Law: Text and Materials (Cambridge Univ. Press 2012).

commerce.[2]

Internationally, countries like the United States and the European Union have taken contrasting approaches to intermediary liability. While the United States adopts a more permissive approach under Section 230 of the Communications Decency Act (CDA), the European Union has shifted towards a more stringent regime with the Digital Services Act (DSA). Such global approaches underline the importance for India to balance innovation and responsibility.[3]

Additionally, the functions of e-commerce platforms have evolved beyond mere hosting. They actively participate in activities like marketing, financial transactions, supply chain management, and support services. This reinforces the call for platforms to take a greater role in preventing and combating cybercrimes.

In this regard, it is necessary to critically examine the laws on the liability of e-commerce platforms. This research seeks to explore the laws, their limitations and propose improvements to ensure proper regulation, while supporting digital development and consumer welfare.

Keywords: Cybercrime, E-commerce Liability, Intermediary Liability, Safe Harbor, IT Act 2000, Digital Platforms ,Consumer Protection, Data Breach, Online Fraud, Cyber Law, Platform Accountability, Legal Framework

Research Questions

1. What are the levels of liability of e-commerce platforms for cybercrimes committed using their services under the current Indian law?
2. To what extent are intermediary liability provisions of the IT Act, 2000 and the rules thereunder effective to combat cybercrimes?
3. What changes are needed to bolster accountability without stunting the e-commerce industry's growth?

Nature of Liability of E-commerce Platforms

Liability in e-commerce is about whether platforms should be recognised as intermediaries or active parties to transactions. Historically, platforms have been viewed as intermediaries bringing together sellers and buyers without intervening in their activities. But this role is becoming more complicated as they become more actively engaged in commerce.

E-commerce platforms play a variety of roles, such as displaying product listings, facilitating payment processing, providing logistics and customer support services. These roles go beyond neutral intermediary, prompting questions about whether platforms should be liable for illegal and scam transactions on their platforms.[4]

Common cybercrimes on e-commerce platforms include fraudulent listings, phishing, identity theft and fraud. It can be challenging for victims to obtain redress from platforms, which often deflect responsibility to third-party vendors. This leaves a regulatory loophole for consumers.

The intermediary liability principle is based on the notion that platforms should not be liable for third-party content unless they have knowledge or control of the content. But the issues of "knowledge" and

[2] OECD, Consumer Policy Guidance on E-commerce (2016).
[3] Takach George S., Computer Law (Irwin Law 2013).
[4] Ministry of Electronics and Information Technology, Government of India Reports.

"control" are nuanced in the online environment, particularly with algorithms and automation.
Court interpretations have helped shape the concept of platform liability. Courts have considered the degree of control that platforms exercise, how they respond to complaints and whether they meet their due diligence obligations. These considerations affect the ability of a platform to rely on safe harbor.
The other key factor is the doctrine of knowledge, which suggests that platforms can be liable for activities they should have known about. This doctrine raises the standards for platforms to monitor content.
In summary, liability of e-commerce platforms is shifting and is in line with the evolution of e-commerce. It is increasingly recognised that platforms can no longer remain completely passive and need to take more responsibility for cyber crimes.

Liability Framework in India

India's cyber law is mainly governed by the Information Technology Act, 2000. The Act's Section 79 grants safe harbor to intermediaries, protecting them from liability for content posted by third parties, as long as they adhere to due diligence and do not abet any unlawful activities.
The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, have now provided more details on intermediary duties. These require intermediary platforms to appoint grievance officers, establish complaint redressal mechanisms and take down unlawful content within a reasonable period.[5]
E-commerce platforms are also governed by consumer protection laws. The Consumer Protection Act, 2019, and the E-commerce Rules, 2020, mandate that platforms uphold transparency, fairness and accountability in their operations.
However, enforcement is a significant issue. The transnational nature of platforms makes enforcement under domestic laws challenging. Also, the uncertainty around the definition of "due diligence" contributes to compliance uncertainties.
Court rulings have played a role in establishing intermediary liability.

1. Shreya Singhal v. Union of India[6]

This landmark case has defined the liability of intermediaries under Section 79 of the Information Technology Act, 2000. Although the Court was primarily deciding on the constitutional validity of Section 66A, it also made significant interpretations of Section 79 and intermediary liability. It confirmed intermediaries (including e-commerce platforms) are covered by the safe harbor provision and not liable for content from third parties unless they have actual knowledge of wrongdoing. It also mandated that the intermediary's knowledge must be acquired through a court order or by a lawful authority of the government and thus avoids excessive and arbitrary liability on the intermediary.[7]
The ruling is significant in the case of cyber frauds on e-commerce platforms as it sets up a notice-and-takedown system as opposed to active monitoring. Businesses are not expected to monitor or control user content but are expected to act appropriately once notified. This allows freedom of innovation and trade but has been criticised as being reactive because cyber fraud or illegal listings can occur until notice is provided. However, it does serve as a precedent for intermediary liability in India.

[5] Reserve Bank of India, Guidelines on Digital Payments Security Controls (2021
[6] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[7] Reserve Bank of India, Guidelines on Digital Payments Security Controls (2021

2. Myspace Inc. v. Super Cassettes Industries Ltd.

The Delhi High Court discussed the liability of an internet intermediary for copyright infringement in this matter. Super Cassettes Industries Ltd. claimed that copyrighted material was being infringed upon Myspace. The Court found that intermediaries are protected by safe harbor provisions (Section 79 of the IT Act) as long as they do not have actual knowledge of the infringing material and respond promptly to any notice. The Court ruled against the notion of intermediaries being obligated to monitor all content, given the technical and practical difficulties.

The ruling has broader ramifications for e-commerce websites in dealing with cyber-infringements such as counterfeit products and misleading transactions. It rejected the notion of constructive knowledge, stating that liability only exists in the case of specific knowledge of unlawful content. It also highlighted the need for a robust takedown system in place for redressal of complaints. This case, therefore, reiterates a middle ground, safeguarding the rights of the intermediary and holding it responsible when it fails to take down content upon valid complaints.

In conclusion, while India's legal framework offers a basis for regulating e-commerce platforms, it needs to be fine-tuned to cater to newer issues and ensure compliance.

Comparative Analysis and Emerging Challenges

Comparative studies of legal frameworks worldwide show different approaches to intermediary liability. In the United States, a hands-off approach is taken, granting platforms immunity under Section 230, promoting innovation and freedom of speech.

Meanwhile, the European Union has adopted a more rigorous approach with the Digital Services Act, requiring platforms to moderate content, be transparent and combat illegal conduct. This prioritises responsibility and user safety.

India falls somewhere in between. It offers safe harbours but also requires due diligence. But the lack of specific rules can result in uneven implementation and compliance issues.

The rise of new technologies like artificial intelligence and blockchain adds to the problem. The use of algorithms by platforms can unintentionally aid cybercrime, raising issues of accountability in a machine-driven world.

Multijurisdictional issues are also a major challenge. Cybercrimes can span jurisdictions, complicating enforcement and investigation efforts. This calls for global collaboration and legal harmonisation.

Data protection is also a major issue. The growing data collection and processing by e-commerce sites increase the risk of data theft and identity fraud. Strong data protection legislation is needed to tackle these challenges.

In summary, the dynamic nature of technology and cyber crime requires the law to keep evolving and adapting. Lessons from comparative experiences can assist India in striking the right balance between stimulation of innovation and accountability.

Conclusion

E-commerce platforms' responsibility for cybercrimes is a multifaceted and dynamic topic that demands a delicate balance. Online platforms are essential for enabling e-commerce, but as they become more deeply embedded in transactions, they need to take greater responsibility.

India's legal regime, mainly governed by the IT Act and its rules, offers a framework for dealing with intermediary liability. But enforcement gaps, lack of clarity, and the dynamic nature of cyber risks

undermine its adequacy.

Courts have sought to interpret the liability, but conflicting interpretations have emerged. This suggests a need for legislative clarity and consistency.

International experiences show that too much immunity or too much regulation are not optimal. Striking a balance between innovation and consumer protection is key to fostering digital development.

Finally, a more robust legal framework and improved enforcement measures will be key to tackling cybercrimes in e-commerce.

BIBLIOGRAPHY

1. Information Technology Act, 2000, No. 21 of 2000, India Code.
2. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
3. Consumer Protection Act, 2019, No. 35 of 2019, India Code.
4. Consumer Protection (E-Commerce) Rules, 2020.
5. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
6. Myspace Inc. v. Super Cassettes Industries Ltd., 2016 SCC OnLine Del 6382.
7. Kent RO Systems Ltd. v. Amit Kotak, 2017 SCC OnLine Del 7201.
8. Avnish Bajaj v. State (NCT of Delhi), 150 (2008) DLT 769.
9. Pavan Duggal, Cyber Law in India (LexisNexis 2017).
10. Aparna Viswanathan, Cyber Law: Indian and International Perspectives (LexisNexis 2012).
11. Reed Chris, Internet Law: Text and Materials (Cambridge Univ. Press 2012).
12. Takach George S., Computer Law (Irwin Law 2013).
13. OECD, Consumer Policy Guidance on E-commerce (2016).
14. European Union, Digital Services Act, 2022.
15. U.S. Communications Decency Act, 47 U.S.C. § 230.
16. Reserve Bank of India, Guidelines on Digital Payments Security Controls (2021).
17. Ministry of Electronics and Information Technology, Government of India Reports.
18. NASSCOM, Cybersecurity and E-commerce Report (2022).
19. Journal of Cyber Law & Policy, Various Issues.
20. Harvard Journal of Law & Technology, Various Articles.