

Research Article

Criminal Law Approaches to Protecting IPR in E-Commerce: Implications for Consumer Trust and Market Regulation

Sagar¹, Dr Shilpika Pandey², Mr. Abdul Hajik Ansari³, Ms. Shaliha Bee⁴ and Mr. Yogesh Chandra Gupta⁵

¹Research Scholar, Amity Law School, Amity University, Uttar Pradesh.

²Assistant Professor Grdae-III G. D. Goenka Law School, Goenka University, Gurugram.

³Assistant Professor, Shri Ram Institute of Law, Jabalpur.

⁴Assistant Professor, Shri Ram Institute of Law, Jabalpur.

⁵Assistant Professor, TMCLS, Teerthanker Mahaveer University, Moradabad.

*Corresponding Author

Sagar

Article History

Received: 28.02.2026

Accepted: 22.03.2026

Published: 03.04.2026

Abstract: The explosive growth of e-commerce has revolutionized the global markets in the retailing aspect but has also added the sensitiveness to infringements and misuse of intellectual property laws and rights by much counterfeit, piracy and even violation of trademarks. The impact of these systemic violations is a serious blow of the consumer confidence, competition of the market, and the economic harm to the real businesses. A strict discussion of the criminal law options to protect IPR online markets is identified and a critical analysis of the options relating to how they could enhance confidence among consumers and enhanced market control is given in this paper. The paper disaggregates the enforcement practices, severe criminal sanctions and decentralized approaches of the regulation within big jurisdictions by use of a doctrinal legal approach and a pragmatic added value with the assistance of the secondary statistical materials. The findings show that, with proper protection of crime and responsibility of platforms with advanced technologies to monitor and view them, there will be a notable decrease in the instances of online IPR infringement, and, as a consequence, the trust of consumers will be restored, and more healthy markets within the online environment will be formed. In addition, the paper will focus on the way artificial intelligence is changing and improving the sole intention of detecting and preventing infringement in e-commerce back-ends with regard to its efficiencies and the emerging challenges. Specifically, the paper examines the multidimensionality of the interaction between AI algorithms and intellectual property in the e-commerce setting, in which the personalization of ownership and responsibility of AI-generated content will be ambiguous.

Keywords: Intellectual Property Rights, E-Commerce, Criminal Law, Counterfeiting, Consumer Trust, Market Regulation.

Copyright @ 2026: This is an open-access article distributed under the terms of the Creative Commons Attribution license which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use (NonCommercial, or CC-BY-NC) provided the original author and source are credited.

INTRODUCTION

The international trade has been revolutionized following the widespread digital technology. Online market places have enabled businesses to reach a consumer in any part of the world making it efficient and accessible. Reproduction under the name of faux, computation piracy as well as the abuse of trademarks is so widespread in online platforms due to the anonymity, cross-country transactions and lack of government oversight. This increase in the number of illegal actions is a great threat to the availability and safety of the consumer as well as the overall economic well-being of the legitimate businesses. These holistic issues are compounded by the fact that e-commerce is borderless, which makes traditional geographically confined enforcement modalities to be of little use in fighting transnational violations and assigning accountability [1]. Furthermore, when AI is implemented in e-commerce, in addition to providing improved detection strategies, it also introduces difficulties in connection with the origin of AI-generated contents and the further liability attribution in case of possible IPR violations.

Over the last several years, global e-commerce sales have grown in a very impressive way proving the importance of the

digital markets in the global economy.

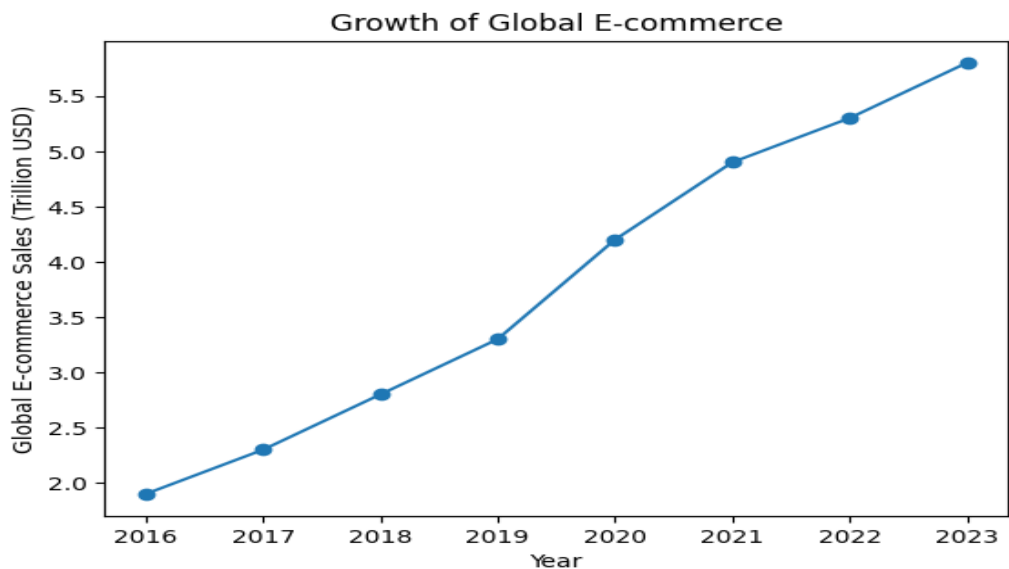


Figure 1: Growth of Global E-Commerce Sales (2016–2023) (Source: UNCTAD E-Commerce Statistics Database, 2023).

The fast rise of online markets has also promoted the existence of fake products and online illegal vendors. The challenge with online platforms is that it has an issue with tracking the millions of product listings online thus letting counterfeit products get into the hands of consumers before the enforcement methods can intervene. This will require a rigorous assessment both of the legal frameworks that are already in place and new technological intervention like the application of AI-based detection systems to protect intellectual property rights in this dynamic world. The growing complexity of e-commerce fraud, frequently enhanced by artificial intelligence and subversive measures developed by fakers, proves the severe necessity of responsive legal provisions and an escalation of international collaboration in order to provide algorithmic clarity and responsibility. It has been shown that the amount of global trade in counterfeit products exceeds \$4.5 trillion, about 3.3 percent of the global trade, and online distribution has contributed greatly to this boom by providing a direct consumer-supplier link that may not always be transparent as to the origin of the products.

Studies by global agencies suggest that counterfeit goods are a significant percentage of world trade and a serious threat to the legitimate stakeholders in businesses, consumers, and governments.

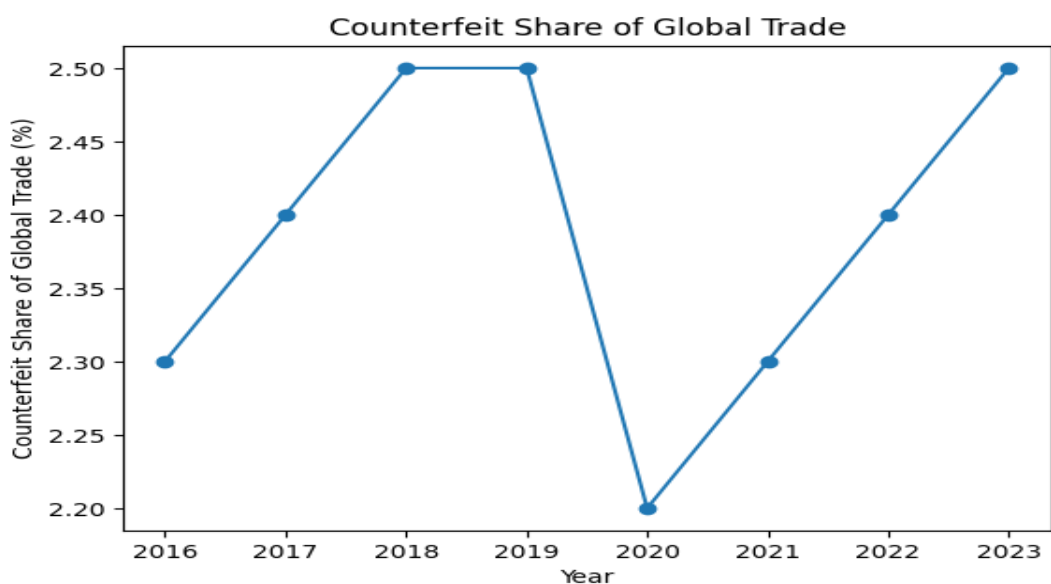


Figure 2: Counterfeit Goods as a Share of Global Trade (2016–2023) (Source: OECD & EUIPO Reports on Illicit Trade, 2023).

The availability of counterfeiters sabotages consumer confidence in the online market and puts fair businesses at a disadvantage. Consequently, this has necessitated the use of criminal law enforcement in the protection of intellectual property rights in the digital economy. The paper will discuss the existing situation in the criminal law practice, where international co-operation and uniform legislation play their role in addressing online IPR cases and how effectively they curb the illicit business and creation of a safe e-commerce market. Analysis will provide a critical evaluation of whether existing responses (legal and technological) are sufficiently adequate to counteract the ever more advanced digital counterfeiting operations, especially those that employ AI.

LITERATURE REVIEW

The links between the protection of intellectual property and online commerce have been generally studied by scholars. Some sources stress that the expansion of the e-commerce has brought a lot of exposure to fake markets and cyber-piracy. In particular, the anonymity of online resources and the universal applicability of the internet to the rights to intellectual property complicate the implementation of protection attempts at any stage, as it is difficult to suspect and punish copyright offenders across national borders. This difficulty is also aggravated by the ongoing development of digital technologies and AI, which require less stable legal frameworks that would be able to adjust to the novel nature of infringement and attribution challenges.

According to economic studies, counterfeit trade adversely affects innovation, brand value, as well as government tax collection. More so, consumers are likely to buy counterfeits unknowingly which do not hold safety or quality standards. It is true that counterfeit and pirated goods represented up to 2.3 percent of world trade in 2021 and a large 4.7 percent of imports to the European Union, which highlights the extensive economic effect of the illicit nature of the practice.

It is also emphasized by the legal researchers that criminal penalties play a crucial role in preventing intellectual property crimes. The criminal law is an effective deterrence, as it imposes some penalties to those engaging in extensive counterfeiting of goods including fines, imprisonment, and seizure of their assets. The success of these remedies, however, in the online situation has been the topic of debate, with some analyses hinting that they can be ineffective or even retrogressive to the online situation of Internet infringement in some cases [2]. These discussions also deal with the application of digital technologies and especially block chain analysis and artificial intelligence that are currently under consideration to improve the observation and control of crypto currency operations and the identification of fake products in the market.

These mechanisms notwithstanding, there are still challenges in enforcement owing to the jurisdictional issue and the international nature of online trade. These issues are even escalated by the fact that digital goods can be copied and transported across borders with a low transaction cost and that; therefore, the copyright owners can be more challenged [1]. There is a pressing need therefore to have strong international collaboration and coherence in laws in order to fight transnational operation of intellectual property crimes successfully.

NATURE OF IPR VIOLATIONS IN E-COMMERCE

E-commerce cases of intellectual property violations are in a number of types. The most common form of violation is counterfeit products in which fraudsters produce imitation of brand products and sell them online through the sites. These illicit activities do not only ruin this market base of original items, but also leave the consumer with poor or even unsafe commodities, only deteriorating consumer confidence in online markets. Besides the physical goods, the digital piracy that involves copying and distributing copyrighted digital works (software, music and movies) illegally is a significant menace to owners of intellectual property.

Digital piracy can be defined as distribution of copyrighted content such as software, movies and music without permission of the owner or producer through or using digital medium. A second common infringement is cyber squatting or where a domain is registered which contains confusingly similar terms with another trademark and is planned as a way of capitalizing on the reputation of the brand or selling the domain to the trademark owner. The IPR enforcement environment is also complicated by the fact that trademark infringement, such as the use of registered marks in unrelated online advertisements or product listing, is a problem.

Trademark infringement arises when the marketers abuse logos, brand names or product designs to deceive the consumers about the goodness of goods. The spread of such violations requires the development of a complex strategy that requires both serious legal frameworks as well as innovations in the field of technologies, especially due to the ambiguity of online transactions and the national level of online platforms. Domain abuse and cyber squatting is the use of a domain name that is structurally related to an existing brand, like a trademark or generic, to defraud consumers or to capitalize on brand equity. Not only are these practices undermining brand equity, but there is also a diversion of legitimate businesses to gain access to this traffic, making it urgently important that mechanisms are put in place to implement effective policing of the digital setting. Anonymity made available by the internet also makes it more difficult to identify the infringers, it may be

necessary to use some means to identify them like, checking the information of the operator or the domain owner of the specific sites and use sample purchases to collect intelligence [3].

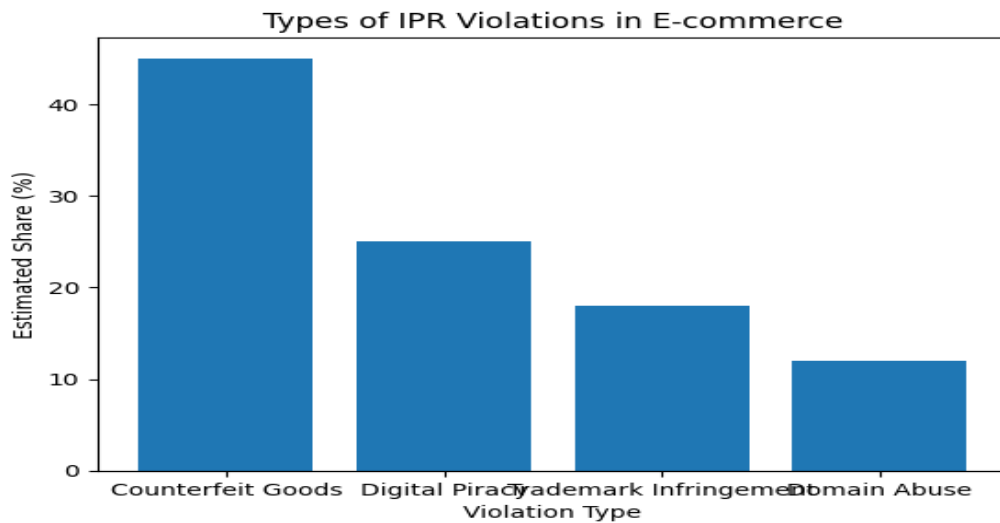


Figure 3: Types of Intellectual Property Violations in E-Commerce (Source: OECD, 2023; WIPO Intellectual Property Statistics, 2023).

The figure illustrates that counterfeit goods account for the largest share of online intellectual property violations, followed by digital piracy and trademark infringement.

CRIMINAL LAW FRAMEWORK FOR PROTECTING IPR

Intellectual property is a significant area of law that is able to be addressed through the criminal law. A lot of jurisdictions make such activities as massive fake production, trademark abuse, and commercial piracy offenses. Such statutory measures can offer harsh punishment; both jail time and huge financial fines, as a result of the rejection of such illegal behavior by society, and to instill fear in would-be criminals. As an example, certain legal means such as submitting cases to law enforcing institutions in order to bring criminal charges are put in place as extra protection against intellectual property rights violations.

The international agreements like the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) compel the member states to establish appropriate enforcement tools that are used in the protection of intellectual property. But, due to the principle of territoriality, the effectiveness of such international structures is frequently constrained because the impact of the national IP law and enforcement measures is limited to certain geographical area to the fact that online infringement is borderless. This disconnect offers the need to have supranational coordination of the legal regulations and more cross-border cooperation in proactive prosecution of intellectual property offenses in e-commerce platform. It necessitates a paradigm shift in the current state of laws to add that transnational element to the internet based intellectual property theft by perhaps enhancing the extradition conventions and mutual legal assistance models.

Criminal penalties including fines, conviction, and seizure of fake products are other criminal penalties of most countries that have them stipulated in the laws of the nation. Web-based marketplaces can also collaborate with the implementation officers to spot and remove the pirated advertisements. However, these national pursuits have a great concern over the disparity in the criminal laws across the various jurisdictions; in the context of the European Union, civil litigation is uniform, yet, criminal intellectual property matters remain in the majority of cases within national jurisdiction school [4]. Such absence of supranational harmonization in criminal implementation poses the jurisdictional problems especially with regard to identification and prosecution on cross border offenders.

However, these efforts have not succeeded to stop enforcement issues because of e-commerce transactions that are often worldwide and the challenge in tracking anonymity online sellers. Therefore, there is a pressing need to adopt stronger international cooperation instruments, such as the formalized mutual legal assistance treaties and intelligence sharing regime to fill these jurisdictional loopholes and empowering effective inter-jurisdictional prosecution of IP offenders. In particular, although there are some transnational enforcement systems (especially in industrial property rights within the EU), there are still major differences, namely in criminal enforcement of copyright and other copyright-related rights.

5. Impact of IPR Violations on Consumer Trust

The issue of consumer trust is a crucial determinant of success of online marketplaces. In the cases where the consumers

buy counterfeit or fraudulent products, they will base on the platform and the brand less. This undermining of trust not only discourages future buying but also reflects on the validity of the entire e-commerce architecture in that it serves as a ripple effect as it may undermine market integrity and may deter legitimate companies that may not want to get involved. Moreover, the popularity of the contraband could create a perception of the danger among the consumers and motivate them to try different shopping methods or to avoid internet purchase altogether.

There are also risks related to safety of counterfeit goods, especially in such areas as pharmaceuticals, electronics, and automotive parts. These dangers underscore the importance of the application of the criminal intellectual property laws in a very strict manner to ensure the safety and health of the population [5].

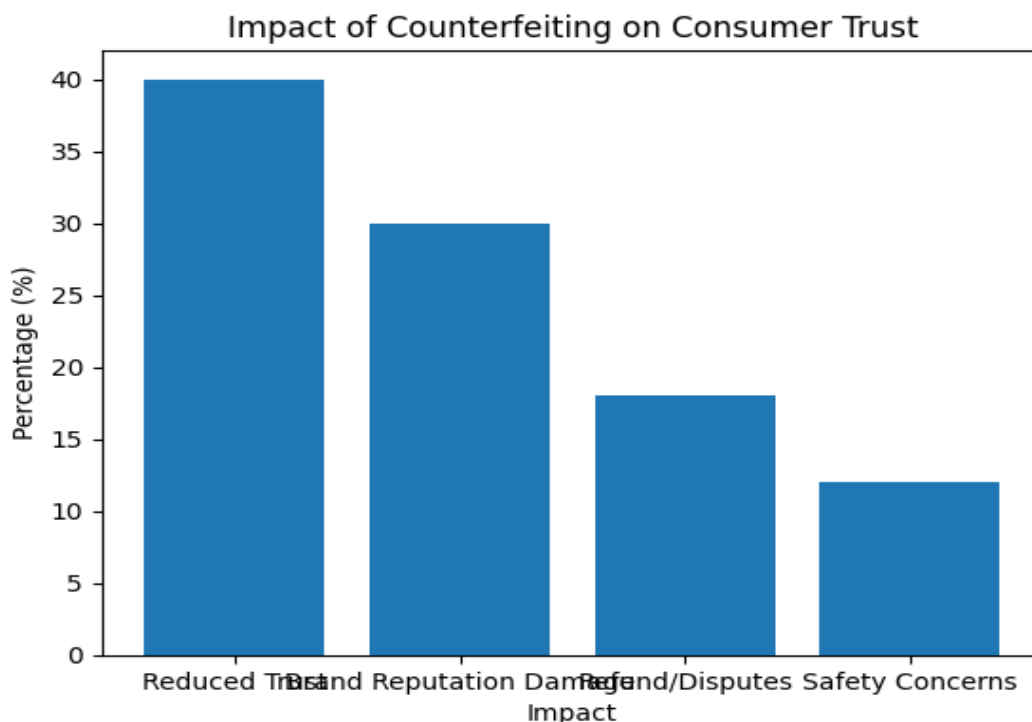


Figure 4: Impact of Counterfeiting on Consumer Trust in Online Marketplaces (Source: OECD Consumer Survey on Counterfeit Goods, 2023).

The Figure shows that the greatest effect of fake products is the loss of consumer confidence in the online services, and the next most important factors are the negative reputation of the brand and the elevated deceptive conflicts and restitution demands.

These conditions eventually influence the sustainability of online marketplaces and the readiness of consumers to use online transactions. There is a natural increase in the spread of fake products propelled by e-commerce which is enabled by organized crime syndicates that involved numerous illegal operations. This spread is enhanced by the international dispensation capabilities provided by online stores and social networking, which make it difficult to trace and stop illegal trade.

6. Role of Criminal Enforcement in Market Regulation

Online market enforcement also helps to control healthy competition and preserve the protection of intellectual property rights by means of criminal enforcement. Criminal law serves to protect the lawful business by suppressing illegal acts like infringement of trademarks, selling fake goods and services, and providing a level field and consumer trust in the authenticity of goods and services [6]. This penalty is an essential instrument, since it imposes excessive fines on the offenders and thereby preventing possible offenders with the help of this, besides making the trading climate safer.

Various measures to curb online counterfeiting are taken by governments and other control agencies. These consist of prosecuting counterfeit sellers in courts, reimbursement of counterfeit products, and collaborating with digital platforms to get illegal listings removed. Moreover, the regulatory authorities are actively expanding their use of sophisticated analytical software and artificial intelligence to detect the trends of illegal trade and, accordingly, attempt to disrupt the illegal chains of counterfeit production, which enhance the standard enforcement options with the abilities of the technology.

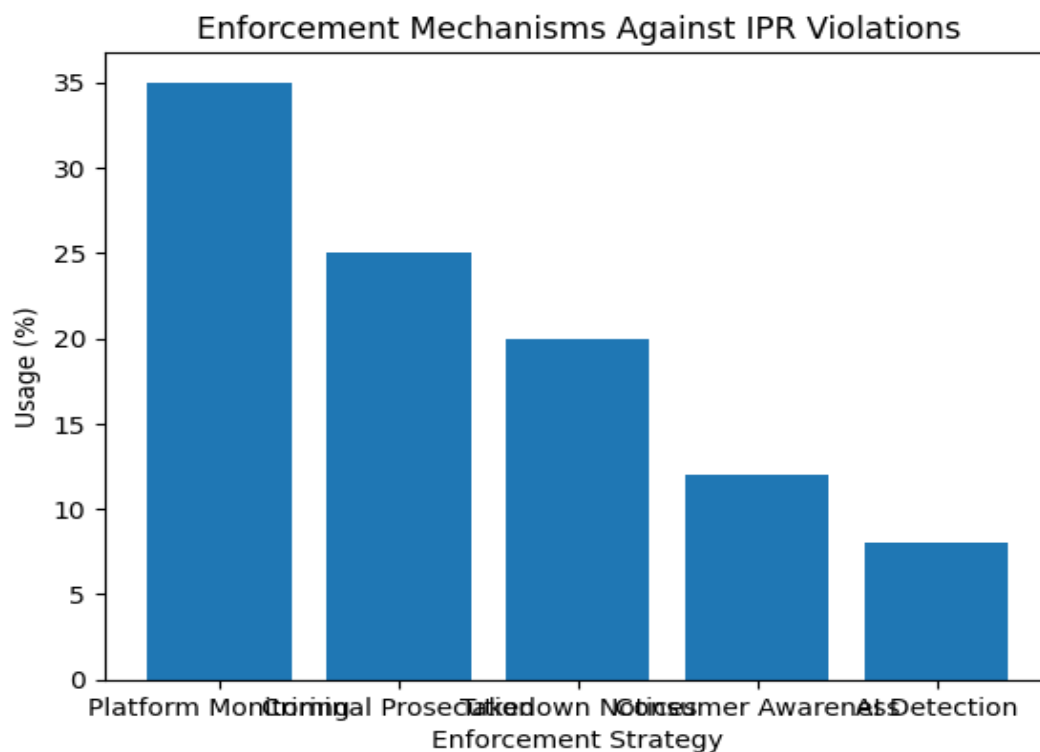


Figure 5: Enforcement Mechanisms against Online Intellectual Property Violations (Source: WIPO Global Enforcement Report, 2023).

The figure shows that platform monitoring and criminal prosecution are among the most widely used enforcement strategies.

Artificial intelligence and automated monitoring tools are also just starting to be applied to discover suspicious listings and identify counterfeit products as technological solutions. These innovations are vital towards enhancing the evidentiary foundation needed to prosecute criminals successfully in the digital world especially when it comes to handling the dynamics of online intellectual crime infringements and the liability of e-commerce online platforms. This involves the need to tackle the secondary liability of the online market regarding fake products where the various interpretations of the law set in different jurisdictions, including the EU and the US, present a hindrance to its full application. Furthermore, the police work within that right widely recognized by people, which is usually carried out through proactive surveillance and reactive legal measures, becomes indeed requisite in the view of these enforcement complicates since product counterfeiting is not necessarily a priority area of law enforcement agencies [7].

7. Challenges in Criminal Enforcement

Although it is essential to enact criminal law, it is facing a number of challenges that are restricting its efficiency. To start with, the jurisdictional problems across the borders mean that it is hard to prosecute online sellers who are in other countries. Second, the anonymity of online spaces enables pirates to generate several personalities and avoid being detected. Third, the infringing material and the fast development of ways to counterfeit the content can commonly overwhelm the enforcement bodies and thus, the investigative strategies and legal regulations must keep changing in order to efficiently counter the dangers that these intricate attacks represent.

Third, enforcement agencies are commonly afflicted with resource constraints and technologies to trace down more intricate online fraud networks. These issues are also aggravated by different national legal frameworks and these enforcement priorities that may prove to be a barrier to international cooperation and the further enforcement of intellectual protection of various jurisdictions.

Also, the blockchain technology has promising opportunities to advance intellectual property protection, by providing immutable registration and visible verification of the good, which will deter the creation and distribution of fake products [8]. Additionally, criminal enforcement must be conducted with a delicate knowledge of the working processes of digital platforms and legal responsibilities of infringement mediated by platforms, including the privacy of private takedown systems, and judicial redress across borders [9]. What is more, the very nature of production and distribution, which is decentralized in current manufacturing processes, especially when a new technology is used such as 3D printing, creates even more headaches when it comes to the origin of contraband goods and assigning responsibility.

CONCLUSION

E-commerce has not only provided old areas of trade a new prospect the world over but has also presented the partaking market with a fresh encounter to violate intellectual property through the mere expansion of online markets and trade services, which have provided organized crime groups with a new avenue to thrive and spread their illicit actions. Fake products, online piracy and copyrights infringements remain one of the major problems facing regulators and companies that degrade consumer confidence and market value.

By preventing criminal acts like trademark infringement and the spread of fake products among others, criminal law continues to play an essential role in ensuring that the illegal actions are discouraged, protecting the legitimate businesses, and promoting consumer trust. Nonetheless, successful enforcement necessitates cooperation among governments, and digital sites as well as intellectual property owners, especially via enforcement tactics such as prosecuting criminals, collaborating with platforms, as well as non-governmental policing in the context of enforcement intricacies.

Strengthen the law, law enforcement, involving the transnational problem, resource constraint and laying down technological solutions, like artificial intelligence in infringement detection and blockchain technologies that cannot be changed to check IP can immensely safeguard the digital economy. Such measures, along with a higher level of global cooperation, will ensure that online markets are sustainable in the long term, irrespective of the incurring threats like decentralized production through 3D printing.

REFERENCES

1. R. Prasad, "Cyber Borderlines: Exploring the Interplay Between E-Commerce and International Trade Law," *Studies in Law and Justice*, vol. 2, no. 4, p. 1, Oct. 2023, doi: 10.56397/slj.2023.12.01. Available: <https://doi.org/10.56397/slj.2023.12.01> [Accessed: Oct. 2025]
2. R. Adams, "The Evolution of Intellectual Property Rights in the Digital Age," *Journal of Modern Law and Policy*, vol. 3, no. 2, p. 52, Dec. 2023, doi: 10.47941/jmlp.1554. Available: <https://doi.org/10.47941/jmlp.1554> [Accessed: Sep. 2025]
3. T. Ahmad, "Issues of Trademark Infringement in E-Commerce: A Comparative Study of India, China and USA," *SSRN Electronic Journal*, Jun. 2016, Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3177389 [Accessed: Oct. 2025]
4. M. Dhenne, "L'appréciation de la brevetabilité des inventions mises en oeuvre par ordinateur par les juridictions françaises (The Assessment of the Patentability of Computer-Implemented Inventions by the French Courts)," *SSRN Electronic Journal*, Jan. 2019, doi: 10.2139/ssrn.3418886. Available: <https://doi.org/10.2139/ssrn.3418886> [Accessed: Jan. 2025]
5. V. P. Kohli, "Combatting Falsification and Counterfeiting Of Medicinal Products in the European Union : A Legal Analysis," *Research Portal Denmark*, p. 351, Jan. 2018, Available: <https://local.forskningsportal.dk/local/dki-cgi/ws/cris-link?src=cbs&id=cbs-221f344e-6f59-4bec-9585-483af3959af4&ti=Combatting%20Falsification%20and%20Counterfeiting%20Of%20Medicinal%20Products%20in%20the%20European%20Union%203A%20A%20Legal%20Analysis> [Accessed: Aug. 2025]
6. R. Raman and D. Pramod, "A Strategic Approach Using Governance, Risk and Compliance Model to Deal With Online Counterfeit Market," *Journal of theoretical and applied electronic commerce research*, vol. 12, no. 3, p. 13, Aug. 2017, doi: 10.4067/s0718-18762017000300003. Available: <https://doi.org/10.4067/s0718-18762017000300003> [Accessed: Oct. 2025]
7. D. Shepherd, J. M. Wilson, and T. Gaudette, "Brand protection and counterfeit products: An examination of resourcing," *Journal of Economic Criminology*, vol. 11, p. 100202, Nov. 2025, doi: 10.1016/j.jeconc.2025.100202. Available: <https://doi.org/10.1016/j.jeconc.2025.100202> [Accessed: Jan. 2026]
8. M. R. Shetkar, "Fake Product Identification System Using Blockchain Technology," *INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, vol. 7, no. 8, Aug. 2023, doi: 10.55041/ijsrem25212. Available: <https://doi.org/10.55041/ijsrem25212> [Accessed: Oct. 2025]
9. D. Sharma and D. Anand, "Cross-Border Enforcement of Copyright, Patent and Trademark in the Digital Era: Challenges, Litigative Trends, and Emerging Market Perspectives," *International Journal For Multidisciplinary Research*, vol. 7, no. 5, Oct. 2025, doi: 10.36948/ijfmr.2025.v07i05.59407.
10. Available: <https://doi.org/10.36948/ijfmr.2025.v07i05.59407> [Accessed: Mar. 2026]