Jurnal Ekonomi, Akuntasi dan Manajemen Indonesia
eISSN: 2964-0385

Intellectual Property Rights Protection in the Digital Economy

Muhamad Agung Dharmajaya
STAI YAPATA Al-Jawami, Bandung, Indonesia

ARTICLE INFO

Keywords:
Intellectual Property Rights, Digital Economy, Law Enforcement, Adaptive Regulation.

Email : agungdharmajaya456@gmail.com

ABSTRACT

The rapid development of information technology has transformed the global business landscape into the digital economy era. However, this phenomenon has also brought massive threats to the protection of Intellectual Property Rights (IPR) through various new modes of cyber violations. This study aims to analyze the effectiveness of positive legal regulations in protecting IPR in the digital ecosystem and identify multidimensional obstacles to its enforcement. The research method used is normative juridical with a statutory and conceptual approach through qualitative secondary data analysis. The results indicate that current positive legal regulations are ineffective due to the rigid nature of conventional law and the lag behind the rapid pace of digital technological innovation, thus creating a legal vacuum (rechtvacuum), especially in regulating the generative Artificial Intelligence (AI) ecosystem and the responsibility of digital platforms. Law enforcement in cyberspace is also hampered by structural barriers in the form of cross-border jurisdictional conflicts, technical barriers in the form of manipulation of electronic evidence and the anonymity of perpetrators, and cultural barriers in the form of low public legal awareness that is permissive towards digital piracy. This study concludes that regulatory reforms are needed that adhere to technology-neutral legislation, integrated with cutting-edge technological solutions such as blockchain and smart contracts to automate copyright and royalty tracking, and supported by strengthened international legal diplomacy and digital literacy education to create a safe digital economy ecosystem for innovators

INTRODUCTION

The digital economy has fundamentally transformed all aspects of human life and the global business structure. The massive development of information technology has triggered the emergence of new business models based on data, internet connectivity, and limitless innovation (Suryamizon, 2017). This transformation has shifted economic dependence from commodity-based physical assets to knowledge-based intangible assets. As a result, creativity and innovation have become the primary drivers of a country's economic growth (Mahfuz, 2020).

Within this innovation-driven ecosystem, Intellectual Property Rights (IPR) play a crucial role. IPR serves as the primary legal instrument for protecting the ideas, creative works, and technological innovations of creators and businesses (Chalim, 2011). Strong IPR protection will guarantee legal certainty and equitable financial incentives for inventors. This is crucial for stimulating the sustainability of the innovation cycle in the digital marketplace (Disemadi & Kang, 2021).

However, the borderless nature of cyberspace poses a massive new threat to IPR protection. Digitalization facilitates the illegal duplication, transmission, and redistribution of copyrighted works in a matter of seconds (Suhaeruddin, 2024). Digital content piracy, software plagiarism, and the sale

of counterfeit products on e-commerce platforms are now rampant. This phenomenon significantly harms holders of moral and economic rights (Sianipar & Aisyah, 2022).

These challenges are further complicated by the advent of cutting-edge technologies such as Artificial Intelligence (AI) and Big Data processing. Generative AI is capable of producing new works of art, writing, and program code by absorbing millions of pieces of human-generated data without permission (Manurung, 2022). This has sparked new legal debates regarding the boundaries of copyright infringement and who is entitled to legal liability for machine-generated works (Girindra, 2023).

Conditions on the ground demonstrate that existing positive legal regulations often struggle to keep pace with the pace of technological innovation. Many national IP laws were drafted before the rapid development of the internet, making them no longer relevant to addressing cyber violations (Naufal & Jannah, 2012). This legal lag creates a regulatory vacuum that is often exploited by irresponsible parties for unilateral gain (Agustian & Manik, 2021).

In addition to legal substance issues, cyber law enforcement is hampered by cross-border jurisdictional constraints. Internet IP infringers often operate illegal websites from overseas or use anonymous servers (Asmaul et al., 2023). This unclear jurisdictional boundaries make it difficult for domestic law enforcement officials to effectively pursue enforcement, confiscation, and pursue criminal and civil litigation (Hamdani, 2022).

If the continued neglect of IP violations in the digital economy continues, the impact will be severely detrimental to the digital investment climate (Novia et al., 2022). Innovators and investors will be reluctant to fund research and development due to the high risk of their products being pirated in the market. For the state, weak IPR protection will reduce national economic competitiveness on the global stage and reduce potential revenue from the digital tax sector (Dharani et al., 2024).

Therefore, in-depth studies are needed to formulate adaptive, progressive, and responsive IPR regulatory reforms. Law enforcement can no longer rely on conventional methods but must adopt modern technological instruments, such as blockchain-based tracking systems. Furthermore, global collaboration between countries is key to addressing cross-border cybercrime that violates the rights of intellectual property owners.

This research aims to fill this academic gap by examining the effectiveness of IPR law amidst the dynamics of the current digital economy. Unlike previous research that focused solely on a single type of IPR, this study comprehensively examines the integration of IPR protection regulations in the era of AI and e-commerce. The primary focus is on finding a legal solution that balances the protection of creators' rights and public access to information.

Based on the above, this research aims to formulate a strategy for strengthening IPR law and enforcement in the digital economy ecosystem. The results of this study are expected to provide theoretical contributions to the development of cyber law and business law. Practically, the recommendations in this study are expected to be material for consideration for policy makers in reforming relevant laws in the future.

METHOD

This research employs a normative juridical approach (literature study) focused on analyzing positive legal norms, legal principles, and the synchronization of laws and regulations related to the protection of Intellectual Property Rights in the digital era. The research is descriptive-analytical, describing current regulations and then analyzing their effectiveness and obstacles to enforcement

in the field (Soekanto, 2007). The data sources used are entirely secondary data, classified into three legal sources. Primary legal sources include relevant laws such as the Copyright Law, the Patent Law, the Trademark Law, and the Information and Electronic Transactions (ITE) Law. Secondary legal sources consist of legal textbooks, scientific journals, previous research results, and relevant academic articles. Meanwhile, tertiary legal sources include legal dictionaries, encyclopedias, and the Great Dictionary of the Indonesian Language, which serve to clarify terminology used in the research.

Data collection techniques were conducted through documentary study, which involved inventorying, reading, recording, and classifying legal sources obtained online and offline. After all secondary data was collected, the data analysis technique used was qualitative analysis using deductive reasoning. The analysis process was conducted in a normative-qualitative manner by interpreting the meaning of the law, comparing legal theory with digital reality, and testing the consistency of IPR regulations with the latest technological developments. The results of the analysis were then synthesized to draw logical and precise conclusions to address the problem formulation regarding the effectiveness and strategies for strengthening IPR protection in the digital economy ecosystem.

RESULT AND DISCUSSION

Effectiveness of Regulation and Barriers to Enforcement of Intellectual Property Rights (IPR) in Cyberspace

The massive development of the digital economy has brought significant disruption to conventional legal systems, particularly within the realm of Intellectual Property Rights (IPR) law. The presence of the internet, e-commerce platforms, and social media has transformed the way people produce, distribute, and consume intellectual works. On the one hand, digitalization opens up limitless market opportunities for creators, inventors, and entrepreneurs to market their creative products globally. However, on the other hand, this phenomenon has opened vast security gaps for the proliferation of IPR infringements using various new methods.

The effectiveness of current positive legal regulations is questionable when confronted with the realities of cyberspace. National legal instruments such as Law Number 28 of 2014 concerning Copyright, Law Number 20 of 2016 concerning Trademarks and Geographical Indications, and Law Number 13 of 2016 concerning Patents appear inadequate. The law was designed with the paradigm of protecting physical or conventional assets in mind. Therefore, when applied to the abstract, dynamic, and fluid digital ecosystem, many articles lose their relevance and are difficult to implement effectively.

One key indicator of the ineffectiveness of this regulation is the slow legal response to keep pace with technological innovation. Law is inherently static and rigid, while digital technology moves exponentially within a matter of days. This lag creates a legal vacuum that is often exploited by irresponsible parties to exploit others' intellectual works without permission for unilateral financial gain, while simultaneously harming the original creators both morally and economically.

This regulatory challenge is further complicated by the emergence of cutting-edge technologies such as generative artificial intelligence (AI) and data scraping. Current AI platforms are capable of producing new works of art, writing, and program code in an instant by absorbing millions of human-created data sets on the internet without permission and without compensation. Existing IPR regulations fail to provide legal certainty regarding the limits of copyright infringement by learning machines, or who should bear legal responsibility for such violations.

In addition to the weaknesses in the law's substance, IPR enforcement in cyberspace is hampered by a highly complex structural obstacle: cross-border jurisdictional conflicts. The internet has essentially eliminated the geographical barriers between countries that have historically been the basis for the implementation of the rule of law. A website providing pirated film content or illegal software can be operated by a perpetrator in country A, using a server rented in country B, and accessed by millions of consumers in country C.

This cross-border situation creates serious legal complications when domestic law enforcement officials attempt to take action. A country's national law strictly adheres to the principle of territoriality, where the authority of police, prosecutors, and judges is limited by the country's borders. Law enforcement officials cannot simply seize servers, block international domains, or arrest perpetrators outside their jurisdiction without going through a lengthy and bureaucratic process of international cooperation and extradition.

Another obstacle weakening IPR protection in the digital economy is the inherent anonymity of internet users. In cyberspace, anyone can easily disguise their true identity using pseudonyms, fake data, or even using encrypted private networks like Virtual Private Networks (VPNs) and The Onion Router (Tor). This anonymity makes it difficult for police to track down the masterminds behind piracy websites or social media accounts selling counterfeit goods.

This difficulty in identifying perpetrators directly impacts the evidentiary process in the courts. In both criminal and civil procedural law, the clarity of the legal identity of the accused or defendant is an absolute requirement that cannot be ignored. When the physical identity of the perpetrator cannot be reliably established due to digital manipulation, lawsuits or claims filed by legitimate intellectual property rights owners often fail or are inadmissible in court.

Equally complex, electronic evidence in digital IP infringement cases is extremely fragile and easily manipulated. Digital data such as downloaded files, website links, or transaction histories on e-commerce platforms can be deleted, altered, or hidden within seconds by perpetrators who realize they are being monitored. This situation requires law enforcement officers to possess robust digital forensic expertise to ensure the authenticity and integrity of evidence presented in court.

However, in reality, the quality and quantity of technological infrastructure and cyber expertise possessed by law enforcement officers are currently very limited. Not all police units or prosecutors in various regions have adequate digital forensic facilities to handle white-collar cybercrime. This limited technical competence means that handling reports of IP infringement in cyberspace tends to be slow, incomplete, and often only targets lower-level perpetrators or small retailers.

In addition to these structural and substantial barriers, there are deeply rooted cultural barriers within the digital society itself. The current legal culture still exhibits a very low level of awareness of the importance of respecting the intellectual property rights of others. The internet has created a permissive mindset where digital information and content available online are considered public goods that can be freely owned, copied, and distributed without paying royalties.

This comparative culture of favoring cheap or free goods fosters a digital piracy ecosystem across various creative industry sectors, from music and films to e-books and computer software. Digital consumers often feel no guilt when illegally downloading songs or purchasing pirated applications on e-commerce platforms. They view these actions as personal economic efficiency, unaware that their actions are slowly stifling the creativity and economic income of original creators.

This weak protection of intellectual property rights (IPR) in cyberspace is exacerbated by the nature of regulations for the majority of IPR groups in Indonesia, which adhere to a complaint-based offense system (klachtdelict) rather than a regular offense (officialdelict). Under this provision, law

enforcement officials lack the legal authority to conduct spontaneous investigations or take action even if they become aware of actual IPR infringement practices online. Law enforcement must await an official report or direct complaint from the rights owner or injured creator.

The nature of this complaint-based offense often becomes a stumbling block because many creators or rights holders are reluctant to report the violations they experience. The main reasons are the cost of litigation, bureaucratic complications, and the uncertainty of the final outcome in court, which is often disproportionate to the value of the losses they suffer. Due to this passive attitude of victims, perpetrators of IPR infringements in the digital world can continue to operate their illegal businesses without fear of legal action.

The impact of this ineffective IPR protection is highly destructive for the sustainability of the digital economy ecosystem at a macro level. When intellectual works are no longer guaranteed legal security, innovators, designers, and investors will lose the incentive and motivation to research and develop new innovations. Why should they spend significant time, energy, and capital creating something if, in the end, that work can be easily plundered and commercialized by others without strict legal sanctions?

Ultimately, the state's failure to provide optimal IPR protection in cyberspace will reduce the national economic competitiveness at the global level. Foreign investors bringing high-tech and substantial capital will be reluctant to invest in countries with weak IPR enforcement due to the high risk of product piracy. Therefore, mapping the portrait of regulatory ineffectiveness and the intertwined barriers to law enforcement is a crucial foundation for formulating the direction of future legal reform.

Adaptive Regulatory Reform Strategy and Technology-Based Solutions

Facing the complex legal impasse in the cyber ecosystem, conventional law enforcement can no longer be maintained as the sole shield protecting Intellectual Property Rights (IPR). The state must immediately take progressive steps through a dual approach that combines substantive legal reform and the adoption of cutting-edge technological instruments. Rigid conventional approaches must be replaced with a legal paradigm that is flexible, responsive, and adaptive to digital dynamics to address the various new legal loopholes exploited by transnational infringers.

A fundamental step that policymakers must take is to adopt the principle of technology-neutral legislation. This principle emphasizes that the formulation of articles in IPR laws should not be limited to a specific type of existing technological platform or medium. Regulations must be designed using broad yet precise legal language so that when new technologies emerge in the future, the laws retain the legal reach to prosecute perpetrators without having to wait for a lengthy amendment process.

This legal reform must also address the regulatory gaps regarding ownership and commercial use within the generative Artificial Intelligence (AI) ecosystem. The government needs to clarify the boundaries of the fair use doctrine in the context of mass data scraping by machine learning. There must be standard regulations requiring AI developers to seek permission and pay fair compensation to original creators whose work is used to train algorithms, and clarify the legal copyright status of new works automatically generated by machines.

Beyond AI issues, legal reforms must target strengthening the legal responsibility of digital platform providers, known as the Intermediary Liability doctrine. Currently, user-generated content and e-commerce platforms often seek refuge behind the safe harbor principle, which absolves them of responsibility for illegal content or products uploaded by users. New adaptive regulations should

require these digital platforms to implement proactive filtering systems based on artificial intelligence technology to automatically detect and block pirated content or goods before they appear on the internet.

This step also needs to be supported by stricter sanctions for digital platforms proven negligent or allowing illegal accounts to operate freely within their ecosystems. When platforms are subject to secondary civil and administrative legal liability, they will be financially compelled to strengthen their internal curation systems. This way, the burden of law enforcement will no longer rest solely on the police, but rather on self-governance mechanisms by tech giants.

However, strengthening regulations at the domestic level will never be sufficient without a transformation of law enforcement from conventional methods to a cybersecurity approach. One of the most promising technological innovations that can be adopted as a systemic solution is blockchain technology. Blockchain's key characteristics—transparent, decentralized, and immutable—make it an ideal instrument for building a global-scale digital intellectual property rights (IPR) recording and tracking system that is far more secure than conventional databases.

Through the integration of IPR into a blockchain network, every digital work—from music and design to software patents—can be assigned a unique digital identity in the form of a valid digital ownership certificate. When a work is uploaded to the internet, its creator's origins, ownership history, and changes in economic rights can be tracked in real time by anyone around the world. This instantly eliminates the anonymity that has historically served as a shield for pirates, as any replication of a work without blockchain validation is immediately detected as illegal.

This blockchain implementation can be further optimized through the use of smart contracts. Smart contracts are computer program codes that run automatically on a blockchain network to execute digital agreements without the need for third-party intermediaries. In the context of IPR protection, creators can embed licensing rules and royalty rates directly into their digital works through smart contracts.

When an internet user accesses, downloads, or uses the work for commercial purposes, a smart contract will automatically deduct the licensing fee from the user's digital wallet and deposit it directly into the creator's account within seconds. This mechanism not only creates transparent economic justice for innovators but also cuts through the often-sluggish bureaucracy of collective management institutions, while simultaneously reducing the scope for illegal platforms to monetize works without permission.

Furthermore, the adoption of advanced digital watermarking technology should be mandatory for commercially distributed visual and audio content. This technology embeds hidden ownership data into the file's binary code, making it irremovable even if the file is compressed, re-recorded, or formatted. The combination of watermarking and blockchain tracking will make it easier for rights owners to gather valid electronic evidence for litigation purposes.

From an institutional perspective, the establishment of a dedicated cybercourt unit for intellectual property rights (IPR) needs to be considered to expedite the resolution of legal disputes in the digital economy era. Conventional courts often lack the technical capacity to understand the intricacies of digital evidence, resulting in sometimes inaccurate decisions. The presence of judges certified in cyber law and information technology will ensure that the judicial process is more objective, precise, and based on legal certainty.

In addition to domestic reform and technology adoption, resolving cross-border jurisdictional conflicts requires aggressive legal diplomacy through strengthened international cooperation. Given the transnational nature of digital intellectual property crimes, countries must agree on harmonized

digital evidence standards and a more streamlined cyber extradition mechanism. The establishment of an international cyber law enforcement forum specifically for intellectual property rights needs to be initiated to facilitate coordination between countries in simultaneously blocking illegal servers worldwide.

Existing international agreements, such as the TRIPS Agreement, also need to be updated to include specific clauses regarding law enforcement in cyberspace and the digital circular economy. This cross-border law enforcement cooperation must include the exchange of cyber intelligence on global piracy syndicates. With solid collaboration, no region in the world will be a safe haven for intellectual property violators.

Finally, this strategy must conclude with efforts to reconstruct society's legal culture through massive and structured digital literacy education. The government, academics, and creative industry associations must collaborate, utilizing digital platforms themselves, to campaign for the importance of respecting intellectual property rights as a form of investment in the nation's future. Changing the public mindset from a culture of hunting for freebies to one that values originality is key to creating a healthy and secure digital economic ecosystem.

Through the synergistic integration of adaptive regulations, advanced technology-based protection, competent courts, global cooperation, and public legal awareness, the digital economic ecosystem will grow conducively. Innovators will no longer be haunted by the fear of theft of their works, while the public will still have equitable access to information. Ultimately, the resilience of the digital IPR system will be a key pillar supporting national sovereignty and economic competitiveness on the global stage.

CONCLUSION

Based on all the research findings and discussions outlined above, it can be concluded that current positive legal instruments have not effectively protected Intellectual Property Rights amidst the rapid growth of the digital economic ecosystem. This ineffectiveness stems from the rigid and static nature of conventional law, which often lags behind the exponential pace of digital technological innovation. This lag has resulted in various new legal vacuums (rechtvacuum) that have not been addressed by national laws, particularly regarding the clarity of legal accountability for mass data compilation by generative Artificial Intelligence (AI) technology and the definition of the legal liability of online shopping platform providers.

This ineffectiveness of conventional law is further exacerbated by multidimensional structural, technical, and cultural barriers to law enforcement in cyberspace. Structurally, domestic law enforcement officials are hampered by cross-border jurisdictional conflicts due to the borderless nature of the internet, while national legal authority is limited by the principle of territoriality. Technically, cybercriminals' use of anonymity and network encryption makes tracking them extremely difficult, compounded by the fragile and easily manipulated nature of electronic evidence. Culturally, law enforcement is hampered by the low legal awareness of digital communities, which still maintain a permissive mindset toward piracy and the free download of illegal works.

Therefore, this study concludes that IPR protection in the digital economy era can no longer rely on conventional methods but must transform through modern, integrative strategies. The government must immediately implement legal reforms by drafting regulations that adhere to technology-neutral legislation so that laws can continue to adapt to current dynamics without the need for repeated amendments. This adaptive regulation must then be combined with the use of cutting-edge cyber technology such as blockchain to build a global, unmanageable digital IPR

registration system, as well as the use of smart contracts to automate the distribution of royalties to creators. This comprehensive strategy must ultimately be supported by strengthened international legal diplomacy to disrupt transnational criminal networks, as well as massive digital literacy education to reconstruct a legal culture in the digital community that places greater value on the originality of works.

REFERENCES

1. Suryamizon, A. L. (2017). Pengaruh Teknologi Terhadap Perkembangan Hukum Hak Kekayaan Intelektual di Indonesia. *Pagaruyuang Law Journal*, *1*(1), 58-75.
2. Mahfuz, A. L. (2020). Problematik Hukum Hak atas Kekayaan Intelektual (HAKI) di Indonesia. *Jurnal Kepastian Hukum Dan Keadilan*, *1*(2), 47-59.
3. Chalim, M. A. (2011). Pengaruh perkembangan iptek terhadap permasalahan haki. *Jurnal Dinamika Hukum*, *11*, 47-58.
4. Disemadi, H. S., & Kang, C. (2021). Tantangan Penegakan Hukum Hak Kekayaan Intelektual dalam Pengembangan Ekonomi Kreatif di Era Revolusi Industri 4.0. *Jurnal Komunikasi Hukum (JKH)*, *7*(1), 54-71.
5. Suhaeruddin, U. (2024). Hak Kekayaan Intelektual Dalam Era Digital: Tantangan Hukum Dan Etika Dalam Perlindungan Karya Kreatif Dan Inovas. *Jurnal Hukum Indonesia*, *3*(3), 122-128.
6. Sianipar, E. A., & Aisyah, P. (2022). Perlindungan Hak Kekayaan Intelektual dalam Era Digital: Tantangan dan Solusi Hukum. *Judge: Jurnal Hukum*, *3*(02), 62-65.
7. Manurung, E. A. P. (2022). Karya Digital Dan Perlindungan Hak Kekayaan Intelektual Di Era Digital. *Verdict: Journal of Law Science*, *1*(1), 30-36.
8. Girindra, I. A. V. (2023). Potensi penggunaan blockchain dalam manajemen hak kekayaan intelektual di Indonesia: Peluang dan hambatan. *Esensi Hukum*, *5*(1), 82-98.
9. Naufal, M. M., & Jannah, H. S. (2012). Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif Dan Hukum Islam. *Al-Mawarid Journal of Islamic Law*, *12*(1), 42565.
10. Agustian, R. A., & Manik, J. D. N. (2021). Tindak Pidana Informasi Elektronik Dalam Kerangka Hukum Positif. *PROGRESIF: Jurnal Hukum*, *15*(1), 92-111.
11. Hamdani, J. A. (2022). Perlindungan Hukum Hak Cipta Lagu Terhadap Pelanggaran Melalui Download Pada Website Penyedia Lagu Gratis. *Fiat Iustitia: Jurnal Hukum*, 79-92.
12. Asmaul, A., Karim, K., & Adhilia, L. T. F. (2023). Perlindungan hukum terhadap pelanggaran hak cipta melalui internet. *Jurnal Litigasi Amsir*, 239-253.
13. Novia, A. A., Rahmadani, D. A., & Hidayati, M. N. (2022). Pelanggaran hak cipta melalui situs streaming ilegal.
14. Dharani, L. I. C., Idayanti, S., & Rahayu, K. (2024). *Perlindungan Hukum terhadap Tindakan Phishing di Media Sosial*. Penerbit NEM.
15. Soekanto, S. (2007). Penelitian hukum normatif: Suatu tinjauan singkat.