

Legal Liability Of Marketplaces For IPR Infringements On MSME Products Following The ITE Law Amendment

Marthen Alnoldus Rehabean Manongga
Universitas 17 Agustus 1945 Jakarta, Indonesia
e-mail: Marthenmanongga7354@gmail.com

Received [28-06-2026]

Revised [20-08-2026]

Accepted [21-08-2026]

Abstract. Indonesia's rapid e-commerce growth has made User-Generated Content (UGC) marketplaces central to the digital economy, while also increasing civil cyber infringements of intellectual property rights (IPR) affecting Micro, Small, and Medium Enterprises (MSMEs). Counterfeit trademarks and copied industrial designs sold through predatory pricing threaten brand goodwill and business sustainability. This study analyzes the shift in marketplace legal liability from passive Safe Harbor immunity toward risk-based liability after Law Number 1 of 2024, the Second Amendment to the ITE Law. Using normative legal research with statutory, conceptual, and comparative approaches, including comparison with the European Union's Digital Services Act (DSA), the study finds that the phrase “reliable and responsible” in Article 15(1) reconstructs a Statutory Duty of Care. Marketplaces may no longer rely solely on reactive Notice and Take Down mechanisms where passive omission or gross negligence toward recurring IPR infringements is established. Implementing regulations should adopt Notice and Action and Notice and Stay Down mechanisms, Trusted Flagger criteria, and vicarious liability to strengthen legal certainty and Indonesia's digital economic sovereignty.

Keywords: *Marketplace; Intellectual Property Rights; MSMEs; Risk-Based Liability; 2024 ITE Law.*

INTRODUCTION

Micro, Small, and Medium Enterprises (MSMEs) constitute the principal foundation of Indonesia's economic structure. Based on national economic data, the MSME sector contributes more than 60% of Gross Domestic Product (GDP) and absorbs approximately 97% of Indonesia's total workforce (Disemadi, 2021). Over the past decade, the acceleration of digital transformation has driven the massive integration of MSME actors into the e-commerce ecosystem. Major marketplace platforms—such as Tokopedia, Shopee, Lazada, and TikTok Shop—provide commercial infrastructure that shortens conventional distribution chains, enabling local MSME products to reach national and regional markets efficiently (Budhijanto, 2021).

However, the success of digitalization has also created significant structural vulnerabilities. The marketplace ecosystem relies on a User-Generated Content (UGC) business model, in which users are free to independently upload product listings. This model has been exploited by irresponsible parties to commit digital unlawful acts (Perbuatan Melawan Hukum/PMH) (Permata, 2023). IPR infringements in the form of counterfeit goods, unauthorized use of registered trademarks, and imitation of industrial designs belonging to MSMEs are increasingly prevalent in the digital black market.

This phenomenon creates a pronounced unequal bargaining position:

1. Information and Resource Asymmetry: Local MSMEs generally lack dedicated legal units or sufficient budgets to monitor millions of online storefronts every day (Disemadi, 2021).
2. Reputational Damage (Brand Dilution): The sale of low-quality counterfeit goods at very low prices (predatory pricing) not only reduces potential sales (loss of profit) but also erodes consumer trust in authentic brands that were built with limited capital (Ramli, 2010).
3. Misuse of the Safe Harbor Doctrine: Marketplace platforms frequently attempt to avoid legal liability by relying on the Safe Harbor Policy as regulated in the Minister of Communication and Informatics Circular Letter Number 5 of 2016. The reactive Notice and Take Down mechanism applied to date has been shown to trigger a hydra effect: when one infringing store is closed following a report by an IPR owner, ten new stores offering the same counterfeit products may immediately register and resume sales (Sitompul, 2012).

At the same time, marketplace platforms receive direct financial benefits from these activities through transaction commissions (take rates), promotional fees (promoted listings), and the use of logistics and payment facilities integrated into the platform (Makarim, 2015). The tolerance of imitation MSME products, combined with the platform's extraction of economic gains, indicates an accountability gap in the existing legal framework.

The enactment of Law Number 1 of 2024 concerning the Second Amendment to the ITE Law introduced a fundamental change in cyberspace governance. Article 15 paragraph (1) of the 2024 ITE Law stipulates that Electronic System Providers (PSEs) must operate electronic systems in a "reliable and responsible" manner. This phrase requires a radical reinterpretation, shifting from purely technical reliability toward legal governance liability based on a proactive duty of care.

LITERATURE REVIEW

Development Law Theory (Grand Theory)

This study is grounded in the Development Law Theory developed by Prof. Mochtar Kusumaatmadja. The theory holds that law functions not only as an instrument of order or social stability, but also as a means of social renewal (law as a tool of social engineering) and as a directive instrument in economic development (Kusumaatmadja, 1986).

In the context of the digital economy:

1. Regulatory and Protective Functions: Law must intervene in unequal free-market relations, constrain excessive concentrations of digital capital within private platform governance, and protect economically weaker groups, particularly MSMEs (Kusumaatmadja, 1986).
2. Avoiding Legal Paralysis: Law must not remain passive or allow cyberspace to become a legal vacuum that merely trails technological development (law always limps behind technology). Reinterpreting the norms of the 2024 ITE Law represents legal renewal intended to direct technological development in line with national economic sovereignty (Budhijanto, 2021).

Legal Liability Theory and the Typology of Cyber Liability (Middle-Range Theory)

Legal liability defines the extent to which a legal subject must bear the consequences of losses caused to another party (Agustina, 2003). In cyberlaw doctrine, intermediary liability can be classified into four principal categories:



Figure 1. Four Types of Liability

Figure 1 shows that cyber-intermediary liability is divided into four categories:

1. Direct Liability (the platform creates illegal content itself): This is the most stringent form of liability. In this scenario, the platform provider, as a cyber intermediary, is no longer merely a passive intermediary. It is actively involved in creating, manipulating, or providing unlawful content or goods.
2. Vicarious Liability (benefiting from users' misconduct): This form of liability arises because a cyber intermediary has a particular legal relationship with the primary wrongdoer. The intermediary exercises control or authority over the system and receives material benefits from the infringement.
3. Contributory Liability (knowingly facilitating IPR infringements): This form of liability applies when a cyber intermediary is aware of an Intellectual Property Rights (IPR) infringement but knowingly provides assistance or facilities that make the infringement easier to commit. The key elements are "knowledge" and "contribution."
4. Risk-Based Liability (independent management of systemic risk): This is a more proactive and prevention-oriented approach. Platforms are responsible for conducting systemic risk assessments and taking the mitigation measures necessary to prevent future harm or infringements.

The shift from fault-based liability, which is based on conventional wrongdoing, toward risk-based liability becomes unavoidable when digital platforms function as the principal gatekeepers of commercial traffic (Makarim, 2015).

Legal Discovery Theory and Teleological Interpretation (Applied Theory)

1. Legal Discovery Theory (Rechtsvinding)

From the perspective of conventional private law, including the Indonesian Civil Code (KUHPerdata), legal rules were developed in an era when digital technology was not yet envisaged. As transactions and business operations move into cyberspace, a fundamental problem emerges: conventional legislation does not explicitly regulate cyberlaw norms, or, where such norms exist, they remain abstract and vague.

Where a legal vacuum (*rechtsvacuüm*) or vague norm exists, the principle applies that judges or law-enforcement officials may not refuse to decide a case (*non liquet*). This is where Legal Discovery Theory (*Rechtsvinding*) operates.

Rechtsvinding emphasizes that lawmaking does not end when legislation is enacted. Judges and legal practitioners are given active intellectual space to explore, formulate, and “discover” new legal norms from existing positive law in order to bridge the gap between dynamic cyberlaw facts (sein) and abstract written legal rules (sollen).

2. Teleological/Sociological Interpretation as an Applied Theory

When legal-discovery instruments are used to examine ambiguous norms, Teleological/Sociological Interpretation functions as the applied theory.

Etymologically, teleological derives from telos, meaning purpose. This method of interpretation does not focus solely on grammatical or literal meaning (the letter of the law); rather, it seeks the societal purpose and legislative spirit (the spirit of the law or ratio legis). The method adjusts the meaning of older or rigid legal texts so that they remain aligned with contemporary needs, justice, and sociological realities.

3. Case Application: Examining the Phrase “Reliable and Responsible” in Article 15 of the 2024 ITE Law

Article 15 of Law Number 1 of 2024 (the Second Amendment to the ITE Law) requires every Electronic System Provider (PSE) to operate its electronic system in a “reliable and responsible” manner. Yet what are the concrete indicators of “reliable” and “responsible” when hacking, server downtime, or data leakage occurs? This is where the vagueness of the norm becomes apparent.

Through Teleological/Sociological Interpretation, the substantive meaning of the phrase can be identified by considering three principal pillars:

a. Consumer Protection Objectives

1. Teleological Application: The central telos of the ITE legal regime and data-protection framework is to prevent an imbalance of bargaining power between cyber-platform owners and users or consumers.
2. Meaning Identified: Teleologically, the word “reliable” means that a platform must maintain standardized cybersecurity systems, guaranteed uptime, and mature risk-mitigation arrangements. If the system goes down without notice and causes losses to users, the platform may be regarded as having failed to meet the reliability criterion.

b. Legal Certainty

1. Teleological Application: Law is created to provide predictable processes for business actors and society.
2. Meaning Identified: The word “responsible” requires the availability of transparent Service Level Agreement (SLA) mechanisms, fully functioning complaint channels, and readiness to comply with risk-audit requirements. Without clear accountability, legal certainty in electronic transactions cannot be achieved.

c. Restoration of MSME Actors' Intangible Rights

1. Teleological Application: Sociologically, disruptions to cyber platforms, such as e-commerce services or payment gateways, most severely affect vulnerable groups, particularly MSMEs. Losses caused by platform errors include not only lost transaction value (material loss), but also loss of business reputation, customer trust, and a sense of security (intangible loss) (Sitompul, 2012).
2. Meaning Identified: Teleological legal discovery broadens the scope of the phrase “responsible” in Article 15 of the 2024 ITE Law so that it is not limited to direct financial compensation, but also includes a platform obligation to restore the reputation and intangible losses of MSME actors affected by system failures.

By integrating Legal Discovery Theory (Rechtsvinding) and Teleological Interpretation as an applied theory, the vague phrase “reliable and responsible” in Article 15 of the 2024 ITE Law

is no longer treated as mere technical jargon. It is transformed into a measurable standard of legal obligation: the reliability of a system and the responsibility of a cyber platform are assessed according to the extent to which the platform can guarantee consumer protection, create legal certainty, and restore the intangible rights of business actors, particularly MSMEs whose livelihoods depend on the digital ecosystem.

METHODS

Research Typology and Nature

This study is normative legal research (doctrinal legal research) that examines law as an autonomous, coherent, and hierarchical system of norms. It is prescriptive-analytical in nature, seeking to critically assess the adequacy of positive legal norms and to propose formulations for legal reform (*ius constituendum*).

Research Approaches

1. Statute Approach: Examining the interrelationship of norms in Law Number 1/2024 (the Second ITE Law Amendment), the Indonesian Civil Code, Law Number 20/2016 on Trademarks and Geographical Indications, Law Number 31/2000 on Industrial Designs, Government Regulation Number 71/2019, and Minister of Trade Regulation Number 31/2023.
2. Conceptual Approach: Analyzing cyberlaw doctrines such as Statutory Duty of Care, Constructive Knowledge, Willful Blindness, and Notice and Stay Down (Ramli, 2010).
3. Comparative Legal Approach (Internal & External Comparative Approach): Comparing Indonesia's positive-law framework with the European Union legal instrument through the 2024 Digital Services Act (DSA).

Legal Materials and Analytical Technique

1. Primary Legal Materials: The 1945 Constitution, the Indonesian Civil Code, the 2024 ITE Law, the Trademark Law, Government Regulation on Electronic System and Transaction Operations (PP PSTE), and the 2024 EU DSA.
2. Secondary Legal Materials: Textbooks on private law and cyberlaw, accredited scientific journals, academic manuscripts, and legislative records.
3. Analytical Technique: All legal materials are processed qualitatively using a deductive syllogistic method, connecting the Major Premise (Duty of Care and PMH norms) with the Minor Premise (platform tolerance of counterfeit goods) in order to produce a rational legal conclusion.

RESULTS AND DISCUSSION

Reinterpretation of PSE Status and Liability Following Law Number 1 of 2024

Transformation of the Marketplace's Legal Status

Under Indonesia's positive legal system, marketplace platforms are expressly classified as Private-Scope Electronic System Providers (PSEs) under Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions (PP PSTE). As legal subjects operating digital ecosystems for corporate interests, marketplaces bear responsibility for ensuring that their systems are secure, lawful, and trustworthy (Makarim, 2015). Historically, marketplace liability has been limited by Minister of Communication and Informatics Circular Letter Number 5 of 2016 concerning Guidelines on the Responsibilities of User-Generated Content Platform Providers. Circular Letter 5/2016 adopts the Safe Harbor doctrine, which grants platforms legal immunity for illegal content or products uploaded by sellers, provided that the platform implements a reactive Notice and Take Down mechanism (Permata, 2023).

Teleological Reinterpretation of Article 15 Paragraph (1) of the 2024 ITE Law

The enactment of Law Number 1 of 2024 (the Second Amendment to the ITE Law) marks a paradigm shift from permissive-liberal regulation toward risk-based accountability. Article 15 paragraph (1) of the 2024 ITE Law states:

“Electronic System Providers shall operate Electronic Systems in a reliable and responsible manner and shall be responsible for the proper operation of such Electronic Systems.”

A teleological interpretation of the phrase “reliable and responsible” produces new legal consequences:

1. Technical Reliability vs. Legal Reliability: System reliability is no longer measured only by server availability (uptime) or protection against hacking (cybersecurity), but also by the system's capacity to mitigate the risks of cybercrime, including IPR counterfeiting (Budhijanto, 2021).
2. The Emergence of the Statutory Duty of Care Doctrine: Platforms bear a legal obligation to apply professional standards of due care. Allowing a system to remain repeatedly vulnerable to misuse by counterfeiting accounts may be classified as a failure to meet the system-safety standards required by law (Permata, 2023).
3. Narrowing of Safe Harbor Immunity: The Safe Harbor doctrine in Ministerial Circular Letter 5/2016, which is hierarchically subordinate to legislation, can no longer serve as an absolute legal shield where a platform remains passive toward infringements that it reasonably should have known about (constructive knowledge) (Sitompul, 2012).

Reconstruction of Digital Unlawful Acts (PMH) Arising from Marketplace Negligence

To claim compensation for losses suffered by MSMEs due to the circulation of counterfeit products on marketplaces, civil actions rely on Article 1365 in conjunction with Article 1367 of the Indonesian Civil Code. The reconstruction of the elements of digital PMH is set out below:



Figure 2. Reconstruction of the Elements of Digital Unlawful Acts

Figure 2 illustrates the legal construction for reconstructing the elements of Digital Unlawful Acts (PMH) under Article 1365 of the Indonesian Civil Code. The framework identifies five principal elements:

1. Act (Gedraging): Passive omission in relation to the Duty of Care imposed by the 2024 ITE Law.
2. Unlawfulness (Onrechtmatig): Violation of written legislation, propriety, and the principle of professional due care.
3. Fault (Schuld): Demonstrated Constructive Knowledge and Willful Blindness in pursuit of profit margins.
4. Loss (Schade): Material Loss (Lucrum Cessans) and Intangible Loss (Brand Dilution and Reputation).
5. Causation (Causaliteit): The platform functions as the “Main Enabler” that expands the reach of losses arising from infringements of MSME IPR.

Analysis of the Fault Element: Willful Blindness and Constructive Knowledge

Under conventional private law, fault (schuld) is assessed through intent (dolus) or negligence (culpa) (Agustina, 2003). In cyberspace, platform fault may be established through two doctrines:

1. Constructive Knowledge: A platform is deemed to “reasonably have known” about transactions involving counterfeit goods based on objective anomaly indicators, such as an implausible selling price (for example, a registered MSME-branded product sold at only 5% of its official price), suspicious product descriptions, or a surge in buyer reports (Permata, 2023).
2. Willful Blindness: Where a platform possesses search-engine and artificial-intelligence (AI) capabilities capable of personalizing product recommendations for advertising revenue, but deliberately fails to use those technologies to filter counterfeit goods, the platform may be considered to have engaged in willful blindness (culpa lata) (Ramli, 2010).

Intangible Losses and the Decline of Brand Reputation (Brand Dilution)

MSME losses arising from IPR infringements on marketplaces are not limited to material losses in the form of lost potential profits (lucrum cessans) and research or trademark-registration costs (damnum emergens). The most damaging losses are intangible losses in the form of brand dilution, namely the erosion of the uniqueness, distinctiveness, and exclusivity of registered MSME trademarks due to the circulation of low-quality counterfeit products (Disemadi, 2021). Misled consumers may post negative reviews on digital storefronts, permanently damaging the MSME's business reputation.

Application of the Vicarious Liability Doctrine (Article 1367 of the Indonesian Civil Code)

Under Article 1367 of the Indonesian Civil Code, a person or legal entity is responsible not only for losses caused by its own actions, but also for losses caused by persons under its supervision or by objects under its control (Agustina, 2003).

A marketplace acts as the primary ecosystem controller by providing:

1. Digital storefronts and search facilities;
2. Payment-processing services (payment gateways);
3. Partner delivery and logistics services; and
4. Paid promotional features.

Because platforms control transaction infrastructure and derive financial benefits in the form of commissions from each sale of counterfeit goods, the doctrine requires them to bear vicarious liability for negligent supervision of illegal sellers (Makarim, 2015).

Comparative Study: Indonesian Regulation and the European Union's 2024 Digital Services Act (DSA)

The European Union adopted Regulation (EU) 2022/2065, known as the Digital Services Act (DSA), which became fully applicable in 2024. The DSA has become a new global benchmark (gold standard) for regulating digital intermediary platforms (EU Commission, 2022).

Table 1. Comparative Matrix of Legal Norms

Comparison Indicator	Indonesian Positive Law	European Union Digital Services Act (DSA) 2024
Philosophical Paradigm	Passive-Reactive (Safe Harbor) based on Ministerial Circular Letter 5/2016	Proactive-Risk-Based (Risk-Based Liability)
Immunity Approach	Uniform immunity for platforms of all sizes	Asymmetric responsibility (additional obligations for very large platforms/VLOPs)
Enforcement Mechanism	Notice and Take Down (no definite time standard)	Standardized Notice and Action + transparency of reasons (Statement of Reasons)
Prevention of Recurrence	Not specifically regulated (triggers the Hydra Effect)	Mandatory Notice and Stay Down (prevention of re-uploading)
Status of Reporters	All reporters are verified individually through bureaucratic procedures	Recognition of Trusted Flagger status (MSME associations/experts)
Algorithmic Transparency	Algorithms are tightly protected as trade secrets	Mandatory independent algorithm audits and opening of the recommendation black box
Compliance Sanctions	Limited administrative sanctions and conventional civil remedies	Administrative fines of up to 6% of total annual global turnover

Lessons from Trusted Flaggers and Notice and Action Mechanisms

The European Union's DSA introduces the concept of Trusted Flaggers, namely institutions, industry associations, or independent entities with specialized expertise in detecting illegal content or goods (EU Commission, 2022). Reports submitted by Trusted Flaggers must be prioritized and acted upon by platforms without bureaucratic delay.

In the Indonesian context, adopting a Trusted Flagger mechanism would significantly benefit MSMEs. MSME associations or IPR-assistance consortia could be registered as trusted reporters with the Ministry of Communication and Digital Affairs (Kemenkomdigi) or the Directorate General of Intellectual Property (DJKI), enabling reports of counterfeit MSME products to be acted upon immediately by marketplaces.

Reconstruction of a Risk-Based Liability Model (Risk-Based Liability Framework)

Based on a synthesis of positive law following the 2024 ITE Law and the comparative analysis of the EU DSA, this study proposes a reconstructed Risk-Based Liability framework for marketplaces that balances the protection of MSME IPR with the sustainability of technological innovation.



Figure 3. Risk-Based Marketplace Liability Reconstruction Framework

Figure 3 shows the reconstruction framework for risk-based marketplace liability. The framework requires Electronic System Providers (PSEs) to implement proactive legal governance pursuant to Article 15 paragraph (1) of the 2024 ITE Law.

To mitigate the risk of IPR infringement, platforms combine two principal approaches:

Technical Measures (Technology Assistance)

1. AI Filtering / Image Detection: An intelligent system automatically scans and rejects images of counterfeit products before they can be successfully uploaded.
2. Notice and Stay Down: Once a counterfeit product is removed because an infringement has been established, the system blocks similar products from being uploaded again.
3. Real-Time DJKI API Integration: The platform system connects directly to the government's copyright and trademark database (DJKI) to automatically verify brand authenticity.

Procedural Measures (Rules & Services)

1. Trusted Flaggers: Trusted reporters, such as official trademark owners or associations, receive a “fast track” so that their reports are processed immediately without waiting in the ordinary queue.
2. Dedicated MSME Channel: A simpler and faster assistance channel enables small-business actors to report counterfeiting of their products.
3. IPR ODR (Online Mediation): An in-application online dispute-resolution feature is provided where buyers, sellers, and trademark owners are involved in a dispute.

The synergy between technology and procedure is expected to create accountability and digital sovereignty, protect MSME IPR, and establish a fair and secure cyber ecosystem.

Technical Approach Pillar

1. Automated Content Filtering & Computer Vision: Marketplace platforms must integrate image-recognition and automated character-recognition technologies to detect visual similarities between registered trademark logos and the forms of industrial designs owned

by MSMEs when sellers upload product listings during merchant onboarding (Permata, 2023).

2. Notice and Stay Down Mechanism: Platforms must adopt content-fingerprinting technology. Once a product listing is determined to infringe IPR and is removed, the product's digital data must be archived so that the system automatically rejects attempts by other accounts to re-upload the counterfeit product (Sitompul, 2012).
3. Cross-Sector Data Integration via API: Real-time system connectivity should be established through an Application Programming Interface (API) between the trademark and industrial-design databases of the Directorate General of Intellectual Property under the Ministry of Law and Human Rights and marketplace seller-verification systems.

Procedural Approach Pillar

1. Strict Seller Verification (Know Your Merchant/KYM): The proliferation of anonymous sellers should be prevented by requiring identity verification based on NIK/NPWP and business-legality documents before a store is permitted to activate transaction features (Disemadi, 2021).
2. IPR Online Dispute Resolution (ODR): Platforms must provide an independent, rapid, affordable, and transparent internal cyber-dispute resolution mechanism, including an obligation to provide a Statement of Reasons where an IPR report is accepted or rejected (EU Commission, 2022).
3. Digital Reversal of the Burden of Proof (Shifting Burden of Proof): Given the information asymmetry in which digital log data and algorithms are entirely controlled by the platform, the burden of proof in civil litigation should be shifted. The platform should be required to demonstrate that its security and risk-filtering systems have operated to the fullest extent of an active duty of diligence (Agustina, 2003).

CONCLUSION

Transformation of the Legal Paradigm Following the 2024 ITE Law: The enactment of Law Number 1 of 2024 reconstructs the meaning of system reliability under Article 15 paragraph (1), shifting it from technical-operational reliability to legal governance liability. Marketplace platforms can no longer rely absolutely on passive Safe Harbor Policy immunity under Ministerial Circular Letter 5/2016 where they allow IPR infringements to occur repeatedly (repetitive infringement).

Qualification of Digital Unlawful Acts (PMH): Passive omission by a marketplace regarding the circulation of counterfeit MSME goods satisfies the elements of an unlawful act under Article 1365 in conjunction with Article 1367 of the Indonesian Civil Code. Platform fault may be established through the doctrines of Constructive Knowledge and Willful Blindness, where platforms disregard their technological capabilities in order to preserve transaction commissions. Platforms bear vicarious liability for material losses and brand dilution suffered by MSMEs.

Need for a Risk-Based Liability Model: Comparison with the European Union's 2024 Digital Services Act (DSA) shows that Indonesia requires stronger regulation, shifting from a reactive Notice and Take Down model toward Risk-Based Compliance Liability. This model requires proactive AI filtering, Notice and Stay Down mechanisms, recognition of Trusted Flaggers for MSME associations, and transparency in algorithmic governance.

LIMITATION AND FUTURE RESEARCH

1. Research Limitations

This study has several methodological and substantive limitations:

Dominance of the Normative-Dogmatic Approach: The study focuses on doctrinal legal research and comparative regulatory analysis and therefore does not yet present quantitative empirical data on the financial losses suffered by MSMEs or the percentage of counterfeit listings successfully included in field samples.

Limited Accessibility of Algorithmic Log Data: The researcher has limited access to the internal ownership criteria of artificial intelligence and algorithmic log data held by private marketplace platforms because such information is protected under the trade-secret doctrine. This limitation restricts an objective technical evaluation of the precision of the filtering engines currently used by platforms.

Commercial Compliance Costs Not Yet Measured: The study has not examined in depth the economic impact of implementing Risk-Based Liability on the sustainability of medium- and small-scale marketplace businesses, including local start-ups that may struggle to bear the cost of expensive AI-filtering technology investments.

2. Suggestions for Future Research

To enrich cyberlaw scholarship and IPR protection in the digital economy, future studies are encouraged to examine the following aspects:

Juridical-Empirical Study (Socio-Legal Research): Empirical research should measure the effectiveness of enforcing digital PMH claims brought by MSMEs before the Commercial Court and assess the level of cyberlaw literacy and the readiness of law-enforcement officials, including judges and investigators, to process digital evidence and digital forensics.

Legal-Formulation Research Using Economic Analysis of Law: Quantitative analysis should examine the return on investment (ROI) and compliance costs associated with the Risk-Based Compliance Liability model so that future implementing regulations under the 2024 ITE Law do not undermine Indonesia's technology start-up investment climate.

Interdisciplinary Research on Algorithmic Governance & AI Law: Future research should develop a legal framework for independent algorithmic-transparency audits capable of examining the black box of e-commerce recommendation algorithms without undermining companies' trade-secret rights.

REFERENCES

- Agustina, Rosa. (2003). *Perbuatan Melawan Hukum*. Jakarta: Penerbit Pascasarjana Fakultas Hukum Universitas Indonesia.
- Budhijanto, Danrivanto. (2021). "Hukum Telekomunikasi, Penyiaran, & Teknologi Informasi: Digitalisasi dan Konvergensi". *Jurnal Hukum Siber*, 3(2), 112-128.
- Disemadi, Hari Sutra. (2021). "Locus de Statu: Perlindungan HKI bagi UMKM di Era Perdagangan Elektronik". *Jurnal Komunikasi Hukum*, 7(1), 89-104.
- European Commission. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act). Brussels: Official Journal of the European Union.
- Kusumaatmadja, Mochtar. (1986). *Hukum, Masyarakat, dan Pembinaan Hukum Nasional*. Bandung: Binacipta.
- Makarim, Edmon. (2015). *Pengantar Hukum Informatika dan Pasarnya*. Jakarta: RajaGrafindo Persada.

- Permata, Rika Ratna. (2023). "Kewajiban Kehati-hatian Penyelenggara Platform E-Commerce dalam Perlindungan Merek Terdaftar". *Jurnal Kekayaan Intelektual*, 4(2), 201-218.
- Ramli, Ahmad M. (2010). *Cyber Law dan HKI dalam Sistem Hukum Indonesia*. Bandung: Refika Aditama.
- Sitompul, Josua. (2012). *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Hukum Pidana*. Jakarta: Tatanusa.