Qonun: Jurnal Hukum Islam dan Perundang-Undangan, 9 (2), 2025: 167-198
https://journal.uinsi.ac.id/index.php/qonun/index
DOI: https://doi.org/10.21093/qj.v9i2.13913
E-ISSN: 2774-3209

LEGAL POLICY ON THE EVIDENTIARY STATUS OF IP ADDRESSES IN GOVERNMENT TENDER COLLUSION

Khalid Mustafa*
Universitas Pendidikan Nasional, Denpasar, Bali
I Gede Agus Kurniawan**
Universitas Pendidikan Nasional, Denpasar, Bali
Ruetaitip Chansrakaeo***
Valaya Alongkorn Rajabhat University Under Royal Patronage, Thailand

Abstract

This research aims to analyze the position of IP Address in evidentiary law related to government tender collusion and to formulate the direction of legal policy for its regulation in Indonesia. The research results show that an IP Address has legitimacy as part of electronic evidence based on the Electronic Information and Transactions Law, but it does not have absolute evidentiary power because it only indicates a technical relationship between electronic activities and certain devices or networks. In the case of tender collusion, an IP Address is more accurately classified as circumstantial evidence or corroborative digital evidence that must be supported by metadata, system logs, affiliation relationships, electronic communications, and digital forensic results. This research also found the fragmentation of regulations and the absence of digital evidence standards, which lead to inconsistencies in the application of the law. Therefore, legislative reform is needed thru amendments to Law Number 5 of 1999, strengthening KPPU Regulations, and harmonization with the Electronic Information and Transactions Law, the Personal Data Protection Law, and government procurement regulations. The reform must be based on the principles of integrity, authenticity, chain of custody, due process of law, risk-based enforcement, and digital evidence governance to achieve legal certainty, the effectiveness of competition law enforcement, and transparent, accountable, and integrity-based government procurement governance.

Keywords : Competition Law, Internet Protocol (IP), Tender Conspiracy, Legal Policy.

A. Introduction

* khalidmustafa22@gmail.com
** gedeaguskurniawan@undiknas.ac.id
*** ruetaitip@vru.ac.th

Digital transformation in government administration has fundamentally altered the governance of government procurement of goods and services in Indonesia. The implementation of an electronic procurement system (e-procurement) through the Electronic Procurement Service (LPSE) is an integral part of the bureaucratic reform agenda aimed at enhancing transparency, efficiency, and accountability, as well as preventing practices of corruption, collusion, and nepotism in the utilization of state finances.[1] Digitalization in procurement does not merely transform administrative mechanisms from conventional to electronic systems; it also generates various digital footprints that can be utilized as instruments for oversight and law enforcement.[2] One of the digital footprints increasingly utilized within the law of evidence is the Internet Protocol Address (IP Address), which serves as a unique numerical identifier linking a device to the internet network.[3] Within the context of government procurement, identical or interconnected IP Addresses among tender participants are frequently utilized as indicators of coordination, affiliation, or even collusion during the bidding process. The phenomenon of utilizing IP Addresses as evidence has garnered increasing attention in tandem with the rising number of tender conspiracy cases handled by the Commission for the Supervision of Business Competition (KPPU). In various decisions, identical IP Addresses have been employed as an indicator demonstrating

1 Aji Baskoro, "Combating Corruption In Procurement: The Synergy Of Law Enforcement, Civil Society, And Digital Oversight," *Jurnal Pengadaan Indonesia* 4, No. 1 (April 30, 2025): 24–39, Https://Doi.Org/10.59034/Jpi.V4i1.59.

2 I Gede Agus Kurniawan et al., "The Business Law in Contemporary Times: A Comparison of Indonesia, Vietnam, and Ghana," *Substantive Justice International Journal of Law* 7, no. 2 (December 18, 2024): 114–41, https://doi.org/10.56087/substantivejustice.v7i2.297.

3 Chaerul Shaleh et al., "Human Rights in the Control of Digital Public Space Freedom: A Collaborative Approach Based on Islamic Law Principles," *Jurnal Hukum Islam* 23, no. 1 (June 2025): 1–36, https://doi.org/10.28918/jhi.v23i1.01.

the existence of communication lines or the shared use of electronic facilities among multiple tender participants.[4] Such circumstances create an assumption that the competition did not occur independently, but was instead orchestrated through certain agreements that contravene the principles of fair business competition. Nevertheless, the utilization of IP Addresses as an evidentiary basis still provokes various debates, both from the technical aspect of information technology and from the perspective of the law of evidence. In essence, an IP Address merely indicates the network access point utilized at a specific time and does not automatically prove the existence of an unlawful agreement among market operators. Within information technology practices, the utilization of shared networks, Virtual Private Networks (VPNs), dynamic IPs, Network Address Translation (NAT), cloud infrastructure, or public internet facilities allows multiple users to share the same IP Address without any legal relationship or coordination in the preparation of bidding documents.[5]

These issues demonstrate that developments in digital technology are not always accompanied by adequate advancements in evidentiary regulations.[6] The legal policy of the Indonesian law of evidence remains dominated by a conventional evidentiary paradigm that relies on evidence as regulated under procedural law, whereas the characteristics of electronic evidence develop far more rapidly than the formulation of its

4 Asti Rachma Amalya, "Prinsip Ekstrateritorial Dalam Penegakan Hukum Persaingan Usaha," *Jurnal Ilmiah Mandala Education* 6, no. 1 (2020): 171–85, https://doi.org/10.58258/jime.v6i1.1125.

5 Margaretha Evi Amin Muftiadi, Tri Putri Mulyani Agustina, "Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phisingterhadap Layanan Online Banking," *Hexatech: Jurnal Ilmiah Teknik* 1, no. 2 (2022): 60–65.

6 I Gede Agus Kurniawan et al., "The Business Legal Policy in Indonesia, Ghana, and Vietnam: A Perspective from the Theory of Dignified Justice," *Lex Scientia Law Review* 9, no. 1 (2025): 1535–65, https://doi.org/https://doi.org/10.15294/lslr.v9i1.18096.

legal norms.[7] As a result, uncertainty arises regarding the legal status, evidentiary weight, validity standards, and examination procedures of IP Addresses as evidence in government tender conspiracy cases. This ambiguity potentially leads to inconsistent rulings, both at the KPPU level and during the appeal process in courts, thereby diminishing legal certainty for business actors as well as the effectiveness of competition law enforcement. Normatively, the regulation of electronic evidence has been recognized across various laws and regulations, most notably in the Law on Electronic Information and Transactions along with its amendments, which recognize electronic information and electronic documents as valid legal evidence.[8] On the other hand, Law Number 5 of 1999 concerning the Prohibition of Monopolistic Practices and Unfair Business Competition, along with its implementing regulations, provides space for the utilization of various forms of evidence in the examination of business competition cases. Nevertheless, these regulations have not explicitly governed the technical parameters or evidentiary standards regarding the use of IP Addresses as digital evidence. This normative void leaves law enforcement authorities with an exceptionally wide margin of interpretation in assessing whether an identical IP Address can stand alone as evidence or must be supported by other evidence indicating communication, coordination, or agreement among tender participants.

From the perspective of legal policy (politik hukum), these circumstances reflect the necessity to reassess the direction of legislative policy regarding digital evidence law in Indonesia. Legal policy is inherently the state's fundamental policy in

---

7 Mustalim Lasaka, "Ius Constituendum of Electronic Evidence Arrangement in Criminal Procedure Law," *JURNAL LEGALITAS* 16, no. 2 (June 2023): 154–66, https://doi.org/10.33756/jelta.v16i2.20306.

8 Henry Aspan et al., "Cyber Notary Issues Authority Certificate to Provide Legal Protection in Online Selling," *Journal of Law and Sustainable Development* 11, no. 10 (2023): e1801, https://doi.org/10.55908/sdgs.v11i10.1801.

determining the direction of the formulation, application, and reform of law to achieve national objectives. Therefore, the state must be capable of balancing two equally important interests: the effectiveness of eradicating tender conspiracies as a form of business competition violation, and the protection of the rights of business actors through the application of the principles of due process of law, the presumption of innocence, and legal certainty.

Developments in digital technology also present new challenges in the form of the increasing complexity of collusive methods in government procurement. The practice of tender conspiracies is no longer conducted through direct communication, but instead utilizes various digital platforms, the internet network, automated software, and electronic identities that are difficult to trace. Under such conditions, the use of digital evidence has indeed become an unavoidable necessity. However, each piece of digital evidence possesses characteristics distinct from conventional evidence due to its vulnerability to alteration, manipulation, or misinterpretation if it is not examined using digital forensic methods that are scientifically accountable.[9] Therefore, the legal policy of evidence must integrate developments in digital forensic science into the evidentiary system so that the assessment of IP Addresses is not merely based on an administrative approach, but also satisfies the standards of scientific validity and procedural legality.

Research regarding the direction of legislative policies governing evidentiary standards for IP Addresses as digital evidence remains relatively limited. This void indicates a significant research gap that needs to be addressed through a normative legal approach analyzing the interconnectedness among legal policy theory, the law of evidence, business

[9] Surjanti Surjanti et al., "Digital Counter Terrorism: Legal Policy for Countering the Spread of Terrorist Content on Social Media," in *Proceedings of the First International Cyber Law Conference, ICL-C 2023, 11 November 2023, Jakarta, Indonesia* (EAI, 2025), 1–4, https://doi.org/10.4108/eai.11-11-2023.2351348.

competition law, administrative law, and developments in information technology. This study also possesses high practical relevance. The procurement of government goods and services constitutes one of the sectors with the largest budget allocations in state financial management, rendering it highly vulnerable to tender conspiracy practices.

Based on these various issues, this study considers that the legal policy of evidence concerning IP Addresses requires a more comprehensive reconstruction through the formulation of regulations that provide certainty regarding the definition, characteristics, acquisition procedures, authentication, forensic examination, presentation, and evaluation of the evidentiary weight of IP Addresses in government tender conspiracy cases. Such regulations also need to accommodate the principles of modern procedural law, developments in information technology, and best practices in digital forensics, thereby striking a balance between the effectiveness of competition law enforcement and the protection of the parties' constitutional rights. On the basis of the aforementioned description, this study is directed toward analyzing the underlying legal policy governing the proof of IP Addresses in government tender conspiracy cases, identifying the weaknesses in currently applicable regulations, and formulating the direction for statutory reforms capable of providing legal certainty, guaranteeing the validity of digital evidence, and strengthening the integrity of the government procurement system in the era of digital transformation.

This study constitutes normative legal research oriented toward the analysis of positive legal norms, legal concepts, and legislative policies governing the proof of IP Addresses in government tender conspiracy cases. Normative legal research was selected because the issues under study do not focus on societal behavior or the empirical implementation of a regulation, but rather on the construction of legal norms, the consistency of statutory regulations, and the direction of legal

policy in accommodating the development of digital evidence within the government procurement system.[10]

The legal materials utilized in this study consist of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials comprise all statutory regulations related to the law of evidence, business competition, electronic transactions, personal data protection, and government procurement of goods and services. Secondary legal materials include academic books, reputable national and international journal articles, research findings, dissertations, academic commentaries, and expert doctrines regarding digital evidence law, business competition law, and legal policy. Meanwhile, tertiary legal materials consist of legal dictionaries, legal encyclopedias, and other reference sources that support the understanding of the analyzed legal concepts.

The technique for collecting legal materials was conducted through library research by inventorying, identifying, classifying, and reviewing all legal materials in accordance with the focus of this study.[11] Subsequently, these legal materials were systematically arranged based on the normative relationships between regulations, conceptual interconnectedness, and their relevance to the issue of IP Address evidence in government tender conspiracy cases. The inventory process was also conducted to identify potential conflicts of norms, legal vacuums, and regulatory inconsistencies affecting legal certainty in the practice of competition law enforcement. The analysis of legal materials was performed qualitatively using a prescriptive method. The analytical phase commenced with the

---

10 I Gede Agus Kurniawan et al., "Intellectual Property Law and Ethics Creating Space for Ethical Innovation from the Perspective of Dignified Justice," *Negara Hukum: Membangun Hukum Untuk Keadilan Dan Kesejahteraan* 16, no. 1 (2025): 1–18, https://doi.org/10.22212/jnh.v16i1.4647.

11 Achmad Irwan Hamzani et al., "Legal Research Method: Theoretical and Implementative Review," *International Journal of Membrane Science and Technology* 10, no. 2 (2023): 3610–19.

interpretation of legal norms through grammatical, systematic, and teleological interpretations to understand the legislature's intent in regulating electronic evidence. Furthermore, horizontal and vertical synchronization analyses were carried out to assess the compatibility among the statutory regulations governing digital evidence and government procurement of goods and services. The results of this normative analysis were then integrated with a conceptual analysis to evaluate whether the currently applicable regulations satisfy the principles of legal certainty, justice, utility, and the effectiveness of law enforcement.[12] Based on the results of the evaluation, this study formulates the ideal construction of legal policy along with recommendations for statutory reforms concerning the legal status, validity standards, and evidentiary weight of IP Addresses as digital evidence in government tender conspiracy cases, thereby providing an adaptive legal foundation for information technology developments while simultaneously guaranteeing the protection of the parties' rights within the law enforcement process.

B. Research Outcome and Discussion

1. The Legal Status of IP Addresses within the Law of Evidence Regarding Government Tender Conspiracies

The Developments in information technology have transformed the characteristics of evidence within the law enforcement process, including in business competition cases, cybercrimes, and civil disputes based on electronic transactions.[13] Proving tender conspiracies constitutes one of the

12 Cynthia Hadita Eka N.A.M. Sihombing, *Penelitian Hukum*, 1st ed. (Malang: Setara Press, 2022).

13 Caroline B Ncube, "Access to Science, Technology, and Innovation: Intellectual Property, Human Rights, and Sustainable Development," in *The Elgar Companion to Intellectual Property and the Sustainable Development Goals* (Edward Elgar Publishing, 2024), 522–36.

most complex aspects of competition law enforcement, as collusive practices are generally conducted in a covert, systematic manner, and are designed to avoid directly identifiable traces.[14] Unlike conventional offenses, which often leave evidence in the form of written documents or confessions from the parties involved, tender conspiracies are more frequently proven through patterns of conduct, communication lines, identical actions among tender participants, or digital evidence demonstrating coordination between business actors. Within the context of the digital transformation of the government procurement system through e-procurement, the existence of the Internet Protocol (IP) Address has become an increasingly vital digital instrument in uncovering relationships between tender participants.[15] Therefore, the analysis regarding the legal status of IP Addresses must be placed within the framework of business competition law as regulated under Law Number 5 of 1999 concerning the Prohibition of Monopolistic Practices and Unfair Business Competition, along with the Regulations of the Commission for the Supervision of Business Competition (KPPU) regarding case-handling procedures. Article 22 of Law Number 5 of 1999 explicitly prohibits business actors from conspiring with other parties to orchestrate or determine tender winners, thereby resulting in unfair business competition.[16] From the formulation of these norms, there are

14 Mira A. Zhumadilova et al., "Civil Legal Handling of Electronic Transactions: The Essence and Modern Realities," *Revista de Direito, Estado e Telecomunicacoes* 15, no. 1 (2023): 160–76, https://doi.org/10.26512/lstr.v15i1.43829.

15 Marie J. Dela Rama, Michael E. Lester, and Warren Staples, "The Challenges of Political Corruption in Australia, the Proposed Commonwealth Integrity Commission Bill (2020) and the Application of the APUNCAC," *Laws* 11, no. 1 (2022): 2–12, https://doi.org/10.3390/laws11010007.

16 Varial Ashari Djafar, "Competition Law Perspective on The Assessment of Conglomerate Merger in Indonesia (Case Study: PT. Aplikasi Karya Anak Bangsa (Gojek) with PT. Tokopedia)," *Legal Brief* 11, no. 5 (2022): 3444–55, https://doi.org/10.35335/legal.xx.xx.

several key elements that must be proven, namely the existence of business actors, the existence of cooperation or agreements with other parties, a process of orchestrating or determining tender winners, and the resulting consequence of unfair business competition. The element of "conspiring" (bersekongkol) is not always manifested in the form of written agreements or explicit communication. In practice, conspiracies are more frequently carried out through informal coordination, the division of roles among tender participants, the utilization of affiliated companies, the manipulation of bid pricing, and the distortion of administrative documents. These circumstances mean that proof cannot rely solely on direct evidence, but also requires an analysis of circumstantial evidence which, when interconnected, forms a legal construction establishing the existence of collusion.[17]

One form of digital evidence that is increasingly utilized is the Internet Protocol (IP) Address, which is a numerical identity assigned to every device connected to the internet network. Technically, an IP Address functions as a logical address that enables the data communication process between devices within a network.[18] From a legal perspective, an IP Address not only serves a technical function for device identification, but also holds potential as digital evidence capable of demonstrating the connection between an electronic activity and a specific device at a particular time.[19] Therefore, the legal status of IP Addresses

17 Brahim Bergougui and Ousama Ben-Salha, "The Impact of Environmental Governance on Energy Transitions: Evidence from a Global Perspective," *Sustainability* 17, no. 19 (September 2025): 8759, https://doi.org/10.3390/su17198759.

18 Guillaume Nibert et al., "Preventing WebRTC IP Address Leaks," in *Risks and Security of Internet and Systems*, 2025, 365–81, https://doi.org/10.1007/978-3-031-89350-6_22.

19 Anya Degenshein, "Finding the Criminal within: The Use and Meaning of Digital Evidence at Trial," *Information, Communication & Society* 27, no. 14 (October 2024): 2514–29, https://doi.org/10.1080/1369118X.2024.2352627.

within the Indonesian evidentiary system needs to be analyzed through the lens of the law of evidence, particularly based on the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP). As digital evidence, an IP Address possesses characteristics distinct from conventional evidence. Digital evidence is inherently electronic information that is stored, sent, received, or processed through an electronic system.[20] In this context, an IP Address is part of the electronic metadata that records the internet connection identity of a device when performing a specific activity. Although it does not directly reveal the personal identity of the user, an IP Address is capable of linking a digital activity to a device, network location, or Internet Service Provider (ISP). Consequently, IP Addresses are frequently utilized in digital forensic processes to reconstruct a sequence of electronic events and identify the connection between perpetrators and the digital activities under examination.

Within the perspective of the Indonesian law of evidence, the legal status of IP Addresses gains legitimacy through the recognition of electronic information as valid evidence. Article 5 paragraph (1) of Law Number 11 of 2008 concerning Electronic Information and Transactions, as last amended by Law Number 1 of 2024, asserts that Electronic Information, Electronic Documents, and their printouts constitute valid legal evidence.[21] This provision expands the national evidentiary system, which previously only recognized conventional evidence as regulated under the Indonesian Criminal Procedure Code (KUHAP). Consequently, an IP Address can be positioned as part of

---

20 Y Katsoulacos and G Makri, "Economics and Antitrust Enforcement at the EU: An Update," *Journal of Antitrust Enforcement* 1, no. 1 (July 2024): 4–8, https://doi.org/10.1093/jaenfo/jnae039.

21 Andrew Christian Banjarnahor and Hana Faridah, "Tinjauan Yuridis Dalam Proses Pembuktian Cyber Pornography Yang Dilakukan Melalui Media Sosial Berdasarkan Hukum Positif Indonesia," *Jurnal Analisis Hukum* 6, no. 1 (2023): 33–47, https://doi.org/10.38043/jah.v6i1.3998.

electronic information that possesses evidentiary value, provided that it is acquired through an electronic system that is reliable and accountable, and satisfies the principles of data integrity, authenticity, and completeness.

The KPPU Regulations regarding case-handling procedures in business competition acknowledge various types of evidence that can be utilized during examinations, including letters or documents, witness testimonies, expert testimonies, circumstantial evidence (petunjuk), confessions of business actors, and electronic evidence in accordance with developments in information technology. The recognition of electronic evidence demonstrates that the evidentiary system in business competition law has evolved in alignment with the digitalization of economic activities.[22] Electronic evidence does not merely consist of electronic mail (e-mail), electronic messages, or digital documents, but also encompasses metadata, system activity logs, digital communication recordings, and IP Addresses that indicate the connection origin of a device when accessing the electronic procurement system. Consequently, an IP Address can be positioned as a part of electronic information relevant to tracing technical relationships between tender participants.

The characteristics of tender conspiracies dictate that an IP Address cannot be understood as standalone evidence. In KPPU examination practice, proof relies heavily on a circumstantial evidence or indirect evidence approach. Circumstantial evidence consists of a series of facts which, individually, might not prove an infringement, but when analyzed collectively, demonstrate a pattern of conduct that is highly unlikely to have occurred by coincidence. This approach has developed because conspiracy

[22] M Afif Hasbullah, "Linking Anti-Trust Laws With Industrial Development: Highlighting The Prevalence of Anti-Trust Laws Within The Indonesian Manufacturing Sector," *International Journal of Criminal Justice Sciences. Criminal Justice Sciences (IJCJS)-Official Journal of the South Asian Society of Criminology and Victimology* 17, no. 1 (2023): 274–86, https://doi.org/10.5281/zenodo.4756105.

perpetrators almost never leave explicit evidence of an agreement. Therefore, the KPPU constructs proof through a combination of various indicators, such as identical bidding document formats, the use of the same physical address, corporate ownership ties, shared telephone numbers, identical price bidding patterns, close intervals in document upload times, and the use of the same IP address during the tender document uploading process.

Within this perspective, an IP Address holds evidentiary value as an indicator demonstrating a technical relationship between tender participants. If multiple participating companies upload their documents through identical IP Addresses or from the same internet network within a close timeframe, such a condition can raise a presumption that the drafting and uploading of the documents were conducted from the same location, device, or network. This fact can strengthen indications that the participants did not act independently in accordance with the principles of fair business competition. Nonetheless, the use of the same IP Address does not automatically prove that a conspiracy has occurred. A shared IP Address can also be caused by the use of a shared internet network, shared office facilities, public internet services, the use of Virtual Private Networks (VPNs), or specific network configurations that generate identical IP addresses for multiple users.[23] Therefore, IP Addresses must be analyzed cautiously and correlated with other evidence to avoid premature conclusions.

KPPU examination practice demonstrates that IP Addresses are generally utilized as supporting evidence to reinforce the existence of other indicators of collusion. In a number of electronic tender conspiracy cases, the Commission Panel (Majelis Komisi) does not merely consider the shared IP address,

[23] Mohammad A. Karim, Hye Chung Kum, and Cason D. Schmit, "A Study of Publicly Available Resources Addressing Legal Data-Sharing Barriers: Systematic Assessment," *Journal of Medical Internet Research* 24, no. 9 (2022): 3, https://doi.org/10.2196/39333.

but also connects it with document metadata similarities, computer operator identities, file creation timestamps, communication patterns between participants, affiliated relationships among directors or shareholders, and the exchange of information prior to the tender process. This evidentiary approach reflects the application of the convergence of evidence principle, whereby the more interconnected indicators there are, the stronger the conviction that coordination in violation of Article 22 of Law Number 5 of 1999 has occurred. Consequently, an IP Address derives its evidentiary value not from its standalone existence, but from its capacity to strengthen the logical connection with other evidence.

From the perspective of the theory of evidence, the legal status of IP Addresses in KPPU practice is more accurately qualified as part of circumstantial evidence (alat bukti petunjuk / indirect evidence) that supports the formulation of the Commission Panel's conviction.[24] This aligns with the nature of business competition law, which does not always require direct evidence of an agreement, but instead provides room for the utilization of economic analysis, market conduct analysis, and indirect evidence to prove anti-competitive practices. This approach has also evolved across various international competition law regimes, where the proof of cartels and bid rigging relies more heavily on a combination of economic and behavioral evidence rather than the confessions of the perpetrators.

Nevertheless, the utilization of IP Addresses as a basis of proof must still satisfy the principles of reliability, authenticity, integrity, and proportionality.[25] IP Address data must be acquired through lawful mechanisms, verifiable through digital forensic

24 Delvino Aldy Djiwandono et al., "Prinsip Exclusionary Rules of Evidence Dalam Pembuktian Tindak Pidana Narkotika" 6, no. 4 (2024): 12066–80.

25 William Harrison Clarke, *The Civil Service Law: A Defense of Its Principles, With Corroborative Evidence From the Works of Many Eminent American Statesmen* (London: Legare Street Press, 2021).

audits, and derived from electronic systems that guarantee data integrity. Furthermore, its utilization must take into account the principles of personal data protection and due process of law to avoid violating the rights of business actors. Consequently, within the evidentiary system for tender conspiracies under Law Number 5 of 1999 and KPPU Regulations, an IP Address holds a strategic position as digital evidence in the form of circumstantial evidence, which functions to reinforce the legal construction of proof regarding coordination among tender participants; however, it does not possess absolute evidentiary value unless supported by a chain of other mutually corroborating evidence. This approach reflects a balance between the effectiveness of competition law enforcement and the protection of the principles of legal certainty and procedural justice.

An IP Address cannot be viewed as standalone evidence in proving a person's guilt or legal liability. Technically, an IP Address only indicates that an activity originated from a specific device or network, but it does not automatically prove which individual operated the device. The use of shared networks, Virtual Private Networks (VPNs), proxy servers, dynamic IP addresses, and spoofing practices allows for discrepancies between the device identity and the actual user identity. Therefore, from the perspective of the law of evidence, an IP Address is more accurately qualified as circumstantial evidence or indirect evidence that must be correlated with other evidence, such as server logs, user authentication data, system activity records, electronic communications, expert digital forensic testimonies, and other electronic evidence. This approach aligns with evidentiary principles that require harmony and mutual reinforcement among pieces of evidence to generate an objective conviction in the judge.

An analysis of the UU ITE demonstrates that the validity of electronic evidence is determined not only by the form of the information but also by the quality of the electronic system that produced the evidence. Article 16 of the UU ITE stipulates that

electronic system operators must guarantee the reliability, security, and integrity of the electronic systems utilized. Consequently, an IP Address only possesses evidentiary value if the data is derived from an electronic system that meets reliability standards and can be audited through digital forensic mechanisms. Thus, the aspect of the chain of custody, data authenticity, and the procedures for acquiring electronic evidence become vital factors in determining the evidentiary value of an IP Address before the court.

On the other hand, the utilization of IP Addresses as evidence must also take into account the personal data protection regime as regulated under Law Number 27 of 2022 concerning Personal Data Protection. In international practice and data protection doctrine, an IP Address is categorized as electronic personal data if it can be linked, either directly or indirectly, to a specific individual. This means that the collection, storage, processing, and disclosure of IP Addresses must be executed based on a lawful legal basis, clear objectives, the principle of proportionality, and with due regard for the rights of the data subject. While law enforcement authorities do possess the power to acquire such data for the purpose of law enforcement, this authority must still be exercised in accordance with legal procedures, the principle of legality, and the principles of human rights protection to prevent any abuse of power or infringement upon the right to privacy.

The status of IP Addresses within the Indonesian legal system constitutes a form of recognition toward the evolution of digital evidence, which is increasingly relevant in the era of digital transformation. However, its evidentiary value is relative and not absolute, as an IP Address only indicates a technical link between an electronic activity and a specific device or network, rather than the direct identity of the perpetrator. Therefore, the effectiveness of utilizing IP Addresses as evidence heavily relies on professional digital forensic application, integration with other electronic evidence, compliance with the provisions of the

UU ITE regarding the reliability of electronic systems, and respect for personal data protection principles as regulated under the Personal Data Protection Law. This approach will foster a balance between the interests of law enforcement, legal certainty, and the protection of privacy rights in the utilization of digital evidence in Indonesia.

2. Future Regulation of IP Address Evidence in Government Tender Conspiracies: A Legal Policy Perspective

Legal policy (politik hukum) constitutes the fundamental policy of the state in determining the direction of the formulation, reform, and application of law to achieve national objectives as mandated in the Preamble to the 1945 Constitution of the State of the Republic of Indonesia.[26] In the context of information technology developments, Indonesia's legal policy faces new challenges in the form of the need to accommodate various types of digital evidence that were unknown when the conventional evidentiary legal system was established..[27] One form of digital evidence that is increasingly vital is the Internet Protocol (IP) Address, particularly in government tender conspiracy cases conducted through electronic procurement systems. Although various laws and regulations have recognized electronic information as valid evidence, to date there are no specific regulations governing the legal status, evidentiary standards, acquisition procedures, or evidentiary value of IP Addresses within the law enforcement process. This condition indicates that Indonesia's legal policy on digital evidence remains partial and is

---

26 Fradhana Putra Disantara et al., "Prophetic Law in Modern Business: Integration of Humanization, Liberation, and Transcendence in Commercial Contracts," *Batulis Civil Law Review* 6, no. 3 (December 2025): 185, https://doi.org/10.47268/ballrev.v6i3.3364.

27 Puti Priyana Rika Srihastuti, "Criminological Review Of Planned Killing In The Region Karawang Polres Law (Study Of Decision Number 155/Pid.B/2022/Pn Kwg)," *Jurnal Ilmiah Wahana Pendidikan* 10, no. 4 (2024): 766–80.

not yet fully capable of anticipating increasingly complex developments in information technology.[28]

The development of the electronic-based government procurement system for goods and services has shifted the evidentiary paradigm in business competition cases, particularly regarding tender conspiracies. The digitalization of procurement processes through the Electronic Procurement Service (LPSE) generates various forms of digital footprints, including Internet Protocol (IP) Addresses, document metadata, system activity logs, and user authentication data. Nevertheless, the currently applicable legal framework has not provided a comprehensive regulation regarding either the legal status or the evidentiary standards for such digital evidence. Law Number 5 of 1999 concerning the Prohibition of Monopolistic Practices and Unfair Business Competition was drafted within the context of conventional transactions, and thus has not anticipated the characteristics of electronic proof developing in the digital era. Consequently, the utilization of IP Addresses in KPPU examination practice relies heavily on institutional interpretation and evidentiary practices rather than explicit legal norms.[29] This condition demonstrates the necessity of legal reconstruction that not only accommodates the developments of information technology, but also guarantees legal certainty, the protection of business actors' rights,[30] and the effectiveness of business competition law enforcement.

---

28 Jhonatan Mulyana Nababan, Ismansyah Ismansyah, and Aria Zurnetti, "Law Enforcement Using the Electronic Traffic Law Enforcement (ETLE) System Against Traffic Violations in Jurisdiction Jambi Polresta," *International Journal of Multicultural and Multireligious Understanding* 10, no. 2 (2023): 558–67.

29 Rika Azizah et al., "Fungsi Dan Peran Lembaga KPPU Dalam Praktek Persaingan Usaha," *Karimah Tauhid* 2, no. 3 (June 2023): 697–707, https://doi.org/10.30997/KARIMAHTAUHID.V2I3.8789.

30 I Gede Agus Kurniawan et al., "The Philosophical Approach to the Existence of Business Law: Comparison of Indonesia, Vietnam, and Ghana," *Jurnal Hukum Bisnis Bonum Commune* 8, no. 1 (2025): 55–76, https://doi.org/https://doi.org/10.30996/jhbbc.v8i1.12382.

From the perspective of legislative legal policy, the recognition of electronic evidence indeed represents a progressive step in responding to digital transformation. This is reflected in the Electronic Information and Transactions Law (UU ITE), which expands the national evidentiary system by recognizing Electronic Information and Electronic Documents as valid legal evidence. Similarly, the Personal Data Protection Law (UU PDP) introduces a framework for protecting electronic data that is increasingly relevant in the digital era. However, both regulations remain general in nature, as they only govern the basic principles of electronic information without providing specific regulations regarding the characteristics of particular digital evidence, including IP Addresses. Consequently, the interpretation of the legal status of IP Addresses still depends on the interpretation of law enforcement officials, judges, and institutions such as the Commission for the Supervision of Business Competition (KPPU), which potentially creates disparities in evidentiary practices.

In government tender conspiracy cases, this condition becomes increasingly crucial because the procurement system has become completely reliant on electronic platforms, such as the Electronic Procurement Service (LPSE). All activities of tender participants leave digital footprints that can be recorded by the system, including IP Address data, document metadata, activity logs, and user authentication information. Nevertheless, to date, Presidential Regulation Number 16 of 2018, as amended by Presidential Regulation Number 12 of 2021, focuses more heavily on procurement governance and has not regulated in detail the utilization of digital footprints as evidence in the law enforcement process. Similarly, Law Number 5 of 1999 concerning the Prohibition of Monopolistic Practices and Unfair Business Competition and various KPPU Regulations have not yet provided normative standards on how IP Addresses should be acquired, verified, analyzed, and assessed as evidence in tender conspiracy cases. This norm vacuum causes the utilization of IP

Addresses to develop more through examination practices rather than through regulatory certainty within laws and regulations.

The weaknesses of the currently applicable regulations are also evident in the absence of uniform digital evidentiary standards. Laws and regulations have not provided boundaries regarding when an IP Address can be deemed to possess evidentiary value, what the evidentiary mechanism is when the use of dynamic IPs, Virtual Private Networks (VPNs), Network Address Translation (NAT), or shared networks is discovered, and how digital audit procedures must be conducted to satisfy the principles of data authenticity and integrity. In fact, the characteristics of internet technology mean that a single IP address does not necessarily indicate a user's identity with certainty. Without clear standards, there is a risk that IP Addresses may be overutilized as a basis of proof, or conversely, neglected due to being deemed lacking in legal certainty.[31] Both conditions are equally potential to reduce the effectiveness of business competition law enforcement.

Furthermore, existing regulations have not yet comprehensively governed the relationship between digital proof and the protection of citizens' constitutional rights. The utilization of IP Addresses as evidence directly correlates with the right to privacy and personal data protection, given that under certain conditions, an IP address can be categorized as electronic personal data. Therefore, an evidentiary legal policy must not solely orient toward the effectiveness of law enforcement, but must also guarantee a balance between the interest of the state in eradicating tender conspiracies and the protection of the rights of individuals and business actors. The absence of regulations concerning access procedures to IP Address data, the authority of institutions entitled to acquire it,

---

31 I. Gede Widhiana Suarda, Moch Marsa Taufiqurrohman, and Zaki Priambudi, "Limiting the Legality of Determining Suspects in Indonesia Pre-Trial System," *Indonesia Law Review* 11, no. 2 (2021): 137–53, https://doi.org/10.15742/ilrev.v11n2.2.

data retention periods, and oversight mechanisms for the utilization of such data potentially gives rise to abuses of power and violations of the principle of due process of law.

Another issue is the lack of harmonization among regulations governing electronic evidence. Currently, provisions regarding electronic evidence are scattered across various regulations, such as the KUHAP, the UU ITE, the UU PDP, the Competition Law, and various sectoral regulations concerning government procurement of goods/services. This fragmentation of regulations causes evidentiary standards to vary according to the characteristics of each respective legal regime. In practice, this condition can generate uncertainty when a case simultaneously involves aspects of business competition law, state administrative law, and criminal law. Therefore, national legal policy needs to be directed toward the harmonization of the electronic evidentiary system so that uniform standards exist regarding the legal status, evidentiary weight, and procedures for utilizing digital evidence, including IP Addresses.

Legislative reform also needs to strengthen institutional aspects through the drafting of technical guidelines that integrate the KPPU, the LKPP, LPSE operators, law enforcement agencies, and digital forensic experts into a standardized evidentiary mechanism. Strengthening human resource capacity, certifying digital forensic experts, standardizing electronic audit software, and ensuring data interoperability among agencies constitute essential components of a legal policy direction oriented toward technology-based law enforcement effectiveness. Consequently, proof will no longer depend solely on the individual interpretations of law enforcement officials, but will instead be based on procedures that are objective, transparent, and scientifically as well as legally accountable. The legal policy direction for regulating IP Address evidence in Indonesia should be aimed at establishing a digital evidentiary legal system that is adaptive to technological developments while remaining steadfast in upholding the principles of legal certainty, justice,

and utility. This legal policy must be capable of integrating the interests of business competition law enforcement, government goods/services procurement governance, personal data protection, and respect for human rights into a comprehensive regulatory framework.[32] Through harmonious legislative reform rooted in information technology developments, an IP Address will not only serve as a technical instrument in the investigative process but will also acquire a clear legal standing as digital evidence that can support the realization of a government procurement system that is transparent, accountable, competitive, and free from tender conspiracy practices.

Reconstruction needs to be directed toward substantive amendments to Law Number 5 of 1999 through provisions that explicitly recognize digital evidence as part of the evidentiary system in business competition cases. Thus far, the recognition of electronic evidence has relied heavily on provisions within the Electronic Information and Transactions Law (UU ITE), whereas the Competition Law has not provided detailed regulations regarding the types, characteristics, or evidentiary weight of electronic evidence. The reform of the law should expand the definition of evidence by incorporating electronic information, metadata, system activity logs, network data, and IP Addresses as part of valid electronic evidence. However, this recognition needs to be accompanied by a clarification that an IP Address is not evidence possessing absolute evidentiary value (full proof), but rather digital evidence that must be assessed alongside other evidence in accordance with the principle of free evaluation of evidence (vrije bewijswaardering).[33]

---

32 Fradhana Putra Disantara, "Perspektif Keadilan Bermartabat Dalam Paradoks Etika Dan Hukum," *JURNAL LITIGASI (e-Journal)* 22, no. 2 (2021): 205–29, https://doi.org/http://dx.doi.org/10.23969/litigasi.v22i2.4211.

33 Ajoy P. B, "Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis," 2022, https://doi.org/10.36348/sijlcj.2022.v05i02.005.

Reconstruction also needs to be carried out through the strengthening of KPPU Regulations as technical instruments governing the procedures for examining business competition cases. Thus far, KPPU Regulations have provided room for the utilization of electronic evidence, but have not regulated operational standards concerning the acquisition, verification, analysis, and evaluation of IP Addresses. Therefore, more detailed guidelines are required regarding digital forensic procedures, examination standards for LPSE system logs, electronic metadata verification methods, and procedures for evaluating the relationship between a shared IP Address and indications of coordination among tender participants. Such regulations also need to determine objective parameters regarding conditions that can diminish the evidentiary value of an IP Address, such as the use of dynamic IPs, Virtual Private Networks (VPNs), Network Address Translation (NAT), proxy servers, or shared networks. With these parameters in place, the evidentiary process will no longer depend on the subjectivity of the examiner, but will instead be based on technical standards that are uniform and scientifically accountable.

Within the framework of reconstructing the law of evidence, an IP Address should be positioned as corroborative digital evidence, which is digital evidence that functions to reinforce or confirm the existence of other evidence. This concept is more appropriate than positioning an IP Address as primary evidence because, technically, an IP address only indicates a relationship between an electronic activity and a specific device or network, rather than individual identity or the existence of an agreement among business actors. Therefore, the evidentiary weight of an IP Address must be constructed through the principle of corroboration, namely the existence of mutual reinforcement with other evidence, such as bidding document metadata, close intervals in document upload times, corporate ownership ties, electronic communication patterns, system audit results, and expert digital forensic testimonies. This approach

reflects a balance between the need for effective proof and the protection of the presumption of innocence, thereby preventing criminalization or the imposition of administrative sanctions based solely on a shared IP address.

The reconstruction also needs to adopt a risk-based digital evidence approach, which positions an IP Address as one of the risk indicators for the occurrence of tender conspiracies, rather than as a sole indicator. This approach enables the KPPU and law enforcement agencies to conduct risk-based analyses on the behavioral patterns of tender participants by utilizing big data technology, artificial intelligence (AI), and network analysis. Consequently, the IP Address functions as a trigger mechanism to conduct further investigations, while the final proof remains dependent on the accumulation of mutually correlated evidence. Such a reconstruction will generate an evidentiary system that is more adaptive to technological developments without disregarding the principles of legal certainty and procedural justice.

Future legal policy concerning IP Address evidence must be directed toward the establishment of a regulatory system that is responsive to digital technology developments without neglecting the principles of a constitutional state (negara hukum). Legislative reform needs to commence through amendments to Law Number 5 of 1999 by incorporating provisions that explicitly recognize digital evidence, including IP Addresses, electronic metadata, system logs, and network information, as part of electronic evidence in business competition cases.[34] These amendments must also be accompanied by provisions concerning evidentiary standards, the classification of evidentiary weight as corroborative digital

[34] I Gede Agus Kurniawan, Lourenco de Deus Mau Lulo, and Fradhana Putra Disantara, "IUS Constituendum of Expert Advisor in Commodity Futures Trading: A Legal Certainty," *Jurnal IUS Kajian Hukum Dan Keadilan* 11, no. 1 (2023): 31–45, https://doi.org/https://doi.org/10.29303/ius.v11i1.1170.

evidence, digital forensic procedures, and the obligation to utilize more than one piece of electronic evidence to prove the existence of a tender conspiracy. Consequently, Indonesian business competition law will possess normative certainty in line with the development of the digital procurement system.

The principles of new regulations must be built upon several core pillars, namely legal certainty, technological reliability, proportionality, accountability, personal data protection, due process of law, and algorithmic transparency in the utilization of digital technology. Regulations must also adopt the principle of technology-neutral regulation, ensuring that legal norms remain relevant despite future technological developments. Through this approach, the law no longer rigidly regulates specific types of technology, but instead governs general principles regarding the validity of digital evidence, electronic data governance, and the protection of the parties' rights, which can be applied to various technological innovations. The development of a digital evidence governance concept is also necessary, encompassing digital evidentiary governance that integrates legal, technological, institutional, and ethical aspects into a single, unified system. This concept positions digital evidence as an information source that must be managed based on a clear lifecycle, starting from the processes of data creation, collection, storage, analysis, utilization, to data erasure in accordance with legal provisions. Digital evidence governance also mandates national standardization regarding the chain of custody, system interoperability among agencies, information security audits, and independent oversight mechanisms for the utilization of electronic data by law enforcement officials. In the context of government goods and services procurement, this concept enables the creation of a digital evidentiary ecosystem that not only supports the law enforcement process, but also enhances the quality of governance, strengthens the integrity of the LPSE system, and builds public trust in the government procurement process

C. Conclusion

The status of the Internet Protocol (IP) Address within the law of evidence regarding government tender conspiracies in Indonesia possesses legitimacy as a component of electronic evidence under the UU ITE; however, its evidentiary weight is not absolute as it merely demonstrates a technical relationship between an electronic activity and a specific device or network, rather than direct user identity or the existence of an agreement. In KPPU examination practice, an IP Address is more accurately qualified as circumstantial evidence or indirect evidence that must be correlated with other evidence—such as document metadata, system logs, affiliated relationships, communication patterns, and digital forensic results—to construct a comprehensive framework of proof regarding the existence of a tender conspiracy. Therefore, the utilization of an IP Address as evidence must be executed based on the principles of integrity, authenticity, chain of custody, due process of law, and personal data protection in order to foster a balance between the effectiveness of business competition law enforcement, legal certainty, and the protection of human rights within transparent, accountable, and high-integrity government procurement governance.

Future regulations concerning IP Address evidence in government tender conspiracy cases must be directed toward the establishment of a comprehensive, adaptive, and integrated digital evidentiary legal system aligned with information technology developments. Legislative reform needs to be carried out through amendments to Law Number 5 of 1999, the strengthening of KPPU Regulations, and harmonization with the Electronic Information and Transactions Law, the Personal Data Protection Law, and government procurement regulations to generate legal certainty regarding the status, acquisition procedures, evidentiary standards, and utilization of IP Addresses as digital evidence. An IP Address should be positioned as corroborative digital evidence functioning to reinforce a chain of other evidence through the application of digital forensics, chain of custody, and evidentiary standards based on risk-based enforcement; thus, its utilization will not

only be effective in uncovering tender conspiracy practices, but will also guarantee the protection of personal data, due process of law, and the presumption of innocence. Consequently, the direction of digital evidentiary legal reform in Indonesia must orient toward the establishment of digital evidence governance that integrates legal, technological, institutional, and governance aspects, thereby realizing a government procurement system that is transparent, accountable, competitive, and provides legal certainty in business competition law enforcement in the era of digital transformation.

BIBLIOGRAPHY

Amalya, Asti Rachma. "Prinsip Ekstrateritorial Dalam Penegakan Hukum Persaingan Usaha." *Jurnal Ilmiah Mandala Education* 6, no. 1 (2020): 171–85. https://doi.org/10.58258/jime.v6i1.1125.

Amin Muftiadi, Tri Putri Mulyani Agustina, Margaretha Evi. "Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phisingterhadap Layanan Online Banking." *Hexatech: Jurnal Ilmiah Teknik* 1, no. 2 (2022): 60–65.

Aspan, Henry, Abdi Setiawan, Irawan, Etty Sri Wahyuni, Ari Prabowo, and Ami Natuz Zahara. "Cyber Notary Issues Authority Certificate to Provide Legal Protection in Online Selling." *Journal of Law and Sustainable Development* 11, no. 10 (2023): e1801. https://doi.org/10.55908/sdgs.v11i10.1801.

Azizah, Rika, Rika Azizah, Dr. Jacobus Jopie Gilalo, and R. Yuniar Anisa. "Fungsi Dan Peran Lembaga KPPU Dalam Praktek Persaingan Usaha." *Karimah Tauhid* 2, no. 3 (June 2023): 697–707. https://doi.org/10.30997/KARIMAHTAUHID.V2I3.8789.

B, Ajoy P. "Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis," 2022. https://doi.org/10.36348/sijlcj.2022.v05i02.005.

Banjarnahor, Andrew Christian, and Hana Faridah. "Tinjauan Yuridis Dalam Proses Pembuktian Cyber Pornography Yang Dilakukan Melalui Media Sosial Berdasarkan Hukum Positif Indonesia." *Jurnal Analisis Hukum* 6, no. 1 (2023): 33–47. https://doi.org/10.38043/jah.v6i1.3998.

Baskoro, Aji. "Combating Corruption in Procurement: The Synergy of Law Enforcement, Civil Society, and Digital Oversight." *Jurnal Pengadaan Indonesia* 4, no. 1 (April 2025): 24–39.

https://doi.org/10.59034/jpi.v4i1.59.

Bergougui, Brahim, and Ousama Ben-Salha. "The Impact of Environmental Governance on Energy Transitions: Evidence from a Global Perspective." *Sustainability* 17, no. 19 (September 2025): 8759. https://doi.org/10.3390/su17198759.

Clarke, William Harrison. *The Civil Service Law: A Defense of Its Principles, With Corroborative Evidence From the Works of Many Eminent American Statesmen*. London: Legare Street Press, 2021.

Degenshein, Anya. "Finding the Criminal within: The Use and Meaning of Digital Evidence at Trial." *Information, Communication & Society* 27, no. 14 (October 2024): 2514–29. https://doi.org/10.1080/1369118X.2024.2352627.

Disantara, Fradhana Putra. "Perspektif Keadilan Bermartabat Dalam Paradoks Etika Dan Hukum." *JURNAL LITIGASI (e-Journal)* 22, no. 2 (2021): 205–29. https://doi.org/http://dx.doi.org/10.23969/litigasi.v22i2.4211.

Disantara, Fradhana Putra, Ade Sathya Sanathana Ishwara, Geraldha Islami Putra Disantara, and Dinara Abdunayimova. "Prophetic Law in Modern Business: Integration of Humanization, Liberation, and Transcendence in Commercial Contracts." *Batulis Civil Law Review* 6, no. 3 (December 2025): 185. https://doi.org/10.47268/ballrev.v6i3.3364.

Djafar, Varial Ashari. "Competition Law Perspective on The Assessment of Conglomerate Merger in Indonesia (Case Study: PT. Aplikasi Karya Anak Bangsa (Gojek) with PT. Tokopedia)." *Legal Brief* 11, no. 5 (2022): 3444–55. https://doi.org/10.35335/legal.xx.xx.

Djiwandono, Delvino Aldy, Felicia Tanalina Ylma, Diqa Qothrunnada, and Amanda Nur. "Prinsip Exclusionary Rules of Evidence Dalam Pembuktian Tindak Pidana Narkotika" 6, no. 4 (2024): 12066–80.

Eka N.A.M. Sihombing, Cynthia Hadita. *Penelitian Hukum*. 1st ed. Malang: Setara Press, 2022.

Gede Widhiana Suarda, I., Moch Marsa Taufiqurrohman, and Zaki Priambudi. "Limiting the Legality of Determining Suspects in Indonesia Pre-Trial System." *Indonesia Law Review* 11, no. 2 (2021): 137–53. https://doi.org/10.15742/ilrev.v11n2.2.

Hamzani, Achmad Irwan, Tiyas Vika Widyastuti, Nur Khasanah, and Mohd Hazmi Mohd Rusli. "Legal Research Method: Theoretical and Implementative Review." *International Journal of Membrane Science and Technology* 10, no. 2 (2023): 3610–19.

Hasbullah, M Afif. "Linking Anti-Trust Laws With Industrial Development: Highlighting The Prevalence of Anti-Trust Laws Within The Indonesian Manufacturing Sector." *International Journal of Criminal Justice Sciences. Criminal Justice Sciences (IJCJS)-Official Journal of the South Asian Society of Criminology and Victimology* 17, no. 1 (2023): 274–86. https://doi.org/10.5281/zenodo.4756105.

Karim, Mohammad A., Hye Chung Kum, and Cason D. Schmit. "A Study of Publicly Available Resources Addressing Legal Data-Sharing Barriers: Systematic Assessment." *Journal of Medical Internet Research* 24, no. 9 (2022): 3. https://doi.org/10.2196/39333.

Katsoulacos, Y, and G Makri. "Economics and Antitrust Enforcement at the EU: An Update." *Journal of Antitrust Enforcement* 1, no. 1 (July 2024): 4–8. https://doi.org/10.1093/jaenfo/jnae039.

Kurniawan, I Gede Agus, Fradhana Putra Disantara, Mac Thi Hoai Thuong, and Briggs Samuel Mawunyo Nutakor. "The Business Law in Contemporary Times: A Comparison of Indonesia, Vietnam, and Ghana." *Substantive Justice International Journal of Law* 7, no. 2 (December 18, 2024): 114–41. https://doi.org/10.56087/substantivejustice.v7i2.297.

Kurniawan, I Gede Agus, Lourenco de Deus Mau Lulo, and Fradhana Putra Disantara. "IUS Constituendum of Expert Advisor in Commodity Futures Trading: A Legal Certainty." *Jurnal IUS Kajian Hukum Dan Keadilan* 11, no. 1 (2023): 31–45. https://doi.org/https://doi.org/10.29303/ius.v11i1.1170.

Kurniawan, I Gede Agus, Putu Aras Samsithawrati, Fradhana Putra Disantara, and Briggs Samuel Mawunyo Nutakor. "Intellectual Property Law and Ethics Creating Space for Ethical Innovation from the Perspective of Dignified Justice." *Negara Hukum: Membangun Hukum Untuk Keadilan Dan Kesejahteraan* 16, no. 1 (2025): 1–18. https://doi.org/10.22212/jnh.v16i1.4647.

Kurniawan, I Gede Agus, Putu Aras Samsithawrati, Fradhana Putra Disantara, Mac Thi Hoai Thuong, and Briggs Samuel Mawunyo Nutakor. "The Business Legal Policy in Indonesia, Ghana, and Vietnam: A Perspective from the Theory of Dignified Justice." *Lex Scientia Law Review* 9, no. 1 (2025): 1535–65. https://doi.org/https://doi.org/10.15294/lslr.v9i1.18096.

———. "The Philosophical Approach to the Existence of Business Law: Comparison of Indonesia, Vietnam, and Ghana." *Jurnal Hukum Bisnis Bonum Commune* 8, no. 1 (2025): 55–76.

https://doi.org/https://doi.org/10.30996/jhbbc.v8i1.12382.

Lasaka, Mustalim. "Ius Constituendum of Electronic Evidence Arrangement in Criminal Procedure Law." *JURNAL LEGALITAS* 16, no. 2 (June 2023): 154–66. https://doi.org/10.33756/jelta.v16i2.20306.

Nababan, Jhonatan Mulyana, Ismansyah Ismansyah, and Aria Zurnetti. "Law Enforcement Using the Electronic Traffic Law Enforcement (ETLE) System Against Traffic Violations in Jurisdiction Jambi Polresta." *International Journal of Multicultural and Multireligious Understanding* 10, no. 2 (2023): 558–67.

Ncube, Caroline B. "Access to Science, Technology, and Innovation: Intellectual Property, Human Rights, and Sustainable Development." In *The Elgar Companion to Intellectual Property and the Sustainable Development Goals*, 522–36. Edward Elgar Publishing, 2024.

Nibert, Guillaume, Sébastien Tixeuil, Baptiste Polvé, Nana J. Bakalafoua M'boussi, and Xuan Son Nguyen. "Preventing WebRTC IP Address Leaks." In *Risks and Security of Internet and Systems*, 365–81, 2025. https://doi.org/10.1007/978-3-031-89350-6_22.

Rama, Marie J. Dela, Michael E. Lester, and Warren Staples. "The Challenges of Political Corruption in Australia, the Proposed Commonwealth Integrity Commission Bill (2020) and the Application of the APUNCAC." *Laws* 11, no. 1 (2022): 2–12. https://doi.org/10.3390/laws11010007.

Rika Srihastuti, Puti Priyana. "Criminological Review Of Planned Killing In The Region Karawang Polres Law (Study Of Decision Number 155/Pid.B/2022/Pn Kwg)." *Jurnal Ilmiah Wahana Pendidikan* 10, no. 4 (2024): 766–80.

Shaleh, Chaerul, Fauzan Ali Rasyid, Adang Sonjaya, and Manswab Mahsen Abdulrahman. "Human Rights in the Control of Digital Public Space Freedom: A Collaborative Approach Based on Islamic Law Principles." *Jurnal Hukum Islam* 23, no. 1 (June 2025): 1–36. https://doi.org/10.28918/jhi.v23i1.01.

Surjanti, Surjanti, Maisa Maisa, Dicky Eko Prasetio, and Retno Sari Dewi. "Digital Counter Terrorism: Legal Policy for Countering the Spread of Terrorist Content on Social Media." In *Proceedings of the First International Cyber Law Conference, ICL-C 2023, 11 November 2023, Jakarta, Indonesia*, 1–4. EAI, 2025. https://doi.org/10.4108/eai.11-11-2023.2351348.

Zhumadilova, Mira A., Yerkin Sh Dussipov, Gulnar I. Arginbekova, Bolat

Zh Aitimov, and Yelena V. Milova. "Civil Legal Handling of Electronic Transactions: The Essence and Modern Realities." *Revista de Direito, Estado e Telecomunicacoes* 15, no. 1 (2023): 160–76. https://doi.org/10.26512/lstr.v15i1.43829.

*lembar ini sengaja dikosongkan