



International Journal of New Approaches to Law and Rationality in
Nationhood, Governance, and Rights Advocacy
Nalarnagara Journal

Vol. 1, No. 3, July 2026 pp. 1264-1273

Journal Page is available at <https://internationaljournal.lppmunsaka.ac.id/index.php/nalarnagara>



Transformation Of Legal Norms Regarding Criminal Defamation Using Artificial Intelligence (Ai) “Between Technological Innovation and Legal Certainty”

Derry Angling Kesuma¹, Rohman Hasyim², Husnaini³, Junaidi⁴

^{1,2,3,4}Sumpah Pemuda School of Law STIHPADA Palembang

Email: Kesumaderry@gmail.com

Abstract

The dissemination of content to accuse or damage the reputation of others will be classified as defamation if it fulfils the above elements using artificial intelligence (AI), namely: disseminating false statements or representations, the intention to make them known to the public, and harm to the victim. This is regulated synergistically in Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions, which emphasises that criminal law applies to content in the digital space in the same way as it does in the real world. Thus, defamation using artificial intelligence (AI) is a criminal offence if it fulfils all of the above elements and can be prosecuted under Article 434(1) of Law No. 1 of 2023 on the Criminal Code in Indonesia.

The investigation and examination process in defamation cases categorised as cybercrimes often reaches a dead end in finding mens rea (malicious intent) due to several complex reasons stemming from the nature of cybercrime itself and the law enforcement conditions in Indonesia: the complexity of digital evidence, Difficulty in Determining the Perpetrator's Intent (Mens Rea), Limited Capacity of Law Enforcement, Dynamic and Cross-Border Modus Operandi, Regulatory and Legal Implementation Challenges, Lack of Coordination and Technical Support.

Indonesia still needs regulatory consistency, training for law enforcement officials and their expertise, and development to increase transparency in the use of AI and improve public trust, such as more open explanations about the mechanisms and benefits of AI. Ethical, privacy, and regulatory challenges must be handled carefully to ensure that these developments provide the greatest possible benefits to society as a whole.

Keywords : Artificial Intelligence, Defamation, Implementation, law enforcement

BACKGROUND

Recent developments in digital technology have brought fundamental changes to various aspects of Indonesian society. Digitalisation has not only affected the way people work, communicate and conduct transactions, but has also created new spaces that were previously unknown to conventional law. This is where two worlds that previously operated separately, namely technology and law, meet. This meeting is not only about how the law adapts to technology, but also how technology is encouraged to develop within ethical and legal boundaries.

The development of artificial intelligence (AI) technology has brought human civilisation into a new era full of complexity and paradoxes that were previously unimaginable (Novrianto, 2025). Artificial Intelligence or AI offers extraordinary efficiency and accelerated productivity in various sectors of life, ranging from industrial automation to precision medical diagnosis (Dharmayanti, 2025). However, on the other hand, this progress has given rise to new modes of crime, including increasingly sophisticated and difficult to detect cybercrime, which is structured and has a high level of anonymity (a state in which a person's identity is unknown or hidden, allowing individuals to act or communicate without being directly detected) that is difficult for law enforcement officials to detect at the scene of the crime (Aryasa, 2022; Febriansyah & SH, 2025).

This phenomenon is no longer merely futuristic discourse or science fiction speculation, but has metamorphosed into a real threat in the form of algorithmic crime operating with a high degree of autonomy. Cybercrime, which was previously carried out manually by humans with physical and cognitive limitations, is now shifting significantly towards full automation and precise synthetic manipulation (Budiyanto, 2025; Naili, 2025). Amidst the rapid growth of interest in AI technology among Indonesians, there is a hidden problem that continues to spread. In the hands of people with malicious intent, the use of AI in Indonesia has led to criminal activity. These cybercriminals have turned AI into a tool for theft, capable of hacking personal data, falsifying identities, and deceiving the public through the manipulation of the voices or faces of public figures.

In Indonesia, the potential for AI abuse is not just an empty prediction. AI-based crimes have emerged in various forms of digital crime that can no longer be taken lightly. Some of the most commonly used methods of using artificial intelligence for criminal acts include deepfake video manipulation, fake voice calls, phishing emails and links, and other forms of social engineering that utilise generative AI technology. Deepfake video or synthetic voice technology has become one of the most prevalent crimes in recent times. Using artificial intelligence devices, perpetrators edit official videos to make it appear as if officials or public figures are promoting fictitious programmes that ask victims to transfer money.

Indonesia itself already has regulations that protect user data on social media. Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions covers crucial aspects such as defamation through electronic media, illegal access, and electronic transactions that are legal according to the law. Meanwhile, Law No. 27 of 2022 concerning Personal Data Protection establishes a legal basis for individuals as data subjects, including the right to know, change, and delete their personal data. However, there are still many gaps that need to be bridged, mainly because the pace of technological development is often faster than the legislative process. Often, existing regulations are unable to anticipate the emergence of new technological phenomena such as fintech lending, the Internet of Things, or biometric processing technology.

This is what attracted the author's interest to explore this topic in greater depth and produce an academic paper entitled **“TRANSFORMATION OF LEGAL NORMS REGARDING CRIMINAL DEFAMATION USING ARTIFICIAL INTELLIGENCE (AI) 'Between Technological Innovation and Legal Certainty'”**.

ISSUES

In this scientific paper, the author seeks to address and discuss issues surrounding the transformation of legal norms regarding criminal defamation using Artificial Intelligence or AI. Can AI be considered a legal subject or merely a tool, meaning that responsibility remains with the developer/user in the era of artificial intelligence, in relation to existing regulations in Indonesia, including Law No. 1 of 2023 concerning the Criminal Code Criminal Code, and why the investigation and prosecution of defamation cases that constitute cybercrime often encounter dead ends or difficulties in establishing mens rea?

SCOPE OF RESEARCH

In this scientific paper, the author hopes to find answers to the issues raised, namely the transformation of legal norms regarding criminal defamation using Artificial Intelligence or AI, whether AI can be considered a legal subject or merely a tool, so that responsibility remains with the developer/user in the era of artificial intelligence, in connection with existing regulations in Indonesia, including Law No. 1 of 2023 concerning the Criminal

Code, and why the investigation and examination of defamation cases that constitute cybercrime often reach a dead end or encounter difficulties in finding mens rea.

RESEARCH METHODOLOGY

By using and applying a normative legal research construct (juridical-normative) that is systematically designed to examine the coherence of legal principles, vertical and horizontal synchronisation of legislation, and legal history. This method was chosen based on the nature of the issue being examined, namely the transformation of legal norms regarding criminal defamation using Artificial Intelligence or AI, whether AI can be considered a legal subject or only a tool, so that responsibility remains with the developer/user in the era of artificial intelligence, in connection with existing regulations in force in Indonesia, including Law No. 1 of 2023 concerning the Criminal Code Criminal Code, and why the investigation and examination of defamation cases that constitute cybercrime often encounter dead ends or difficulties in finding mens rea.

DISCUSSION

I. Transformation of Legal Norms Regarding Criminal Defamation Using Artificial Intelligence or AI

Current law is not only limited to formal rules issued by state institutions, but also includes values, norms, and customs that live and develop within society, reflecting the spirit that shapes the character of a nation and is rooted in the lives of its people. Legal pluralism recognises the diversity of legal systems that exist in various countries and cultures, and respects this diversity as a valuable asset. This concept emphasises that no single legal system can be universally applied throughout the world due to differences in culture, history, and socio-political contexts between countries. (Ayu et al. in file:///C:/Users/ACER/Downloads/3690-Article%20Text-6017-1-10-20240614.pdf, accessed on 1 January 2025).

Legal adjustments to technological developments formulate a relevant and effective legal framework while remaining true to traditional legal principles that are essential to interpret and apply in the context of new technologies. These principles include justice, freedom of speech, and human rights, all of which must be adapted to address the challenges and opportunities presented by digital technology. Legal Culture Transformation in the Digital Age should improve the legal system and be able to develop adaptively and responsively to changes from a legal perspective in order to support innovation and sustainable technological development in the fields of science and law. (Rajagukguk n.d.)

Indonesian society now relies heavily on digital platforms in carrying out daily activities, whether for education, work, or health services. However, there is sometimes a lack of awareness about the personal data rights of others, and this is often exploited by certain parties for their own gain. The Tokopedia data leak case and the alleged sale of data from BPJS Kesehatan show how weak the data protection system was before the enactment of the PDP Law in 2022. Nevertheless, this law will only be effective if accompanied by consistent law enforcement and adequate public education. In an ideal situation (Das Sollen), criminal law should function as an ultimum remedium or a last resort and a dynamic social defence instrument that is able to adapt to the dialectics of the times. As emphasised in the principles of modern criminal law and the mandate of the constitution, the state has an absolute obligation to guarantee legal certainty, a sense of security, and protection for its citizens from all forms of threats, including hybrid threats originating from the digital realm that transcend physical jurisdictional boundaries.

Law No. 27 of 2022 concerning Personal Data Protection has adopted global data protection principles, such as transparency, accountability, and data minimisation. In practice, entities that manage large amounts of data, such as e-commerce, ride-hailing applications, and digital financial companies, are required to appoint a Data Protection Officer and prepare a Data Protection Impact Assessment (DPIA) if there is a high risk to personal data. However, challenges also arise from the rise of cybercrime. Activities such as phishing, digital fraud, ransomware, and social media account hacking are becoming more frequent, even targeting government agencies and educational institutions. Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions does regulate illegal access, system interference, and the dissemination of negative content. However, its effectiveness is highly dependent on law enforcement officials' understanding of digital evidence and relevant forensic procedures. Many officials still lack technical competence in cyber forensics, which often leads to dead ends in cyber case investigations.

A *conditio sine qua non* requires irrefutable evidence that the perpetrator's actions were the direct cause (proximate cause) of the prohibited outcome. However, the modern AI development ecosystem involves a very long and fragmented supply chain, ranging from initial dataset providers, foundation model trainers, computing infrastructure providers, to end users who perform fine-tuning. When an AI agent commits a crime, the 'invisible hands' of these various actors contribute to each other, creating The Problem of Many Hands. (Dian Juniorso in <https://rivierapublishing.id/jii/index.php/>; accessed on 1 January 2026)

The second revision of the ITE Law through Law No. 1 of 2024 and the enactment of the New Criminal Code through Law No. 1 of 2023 are expected to provide a robust and responsive legal framework. The hope is that these legal instruments will be able to cover every unlawful act that harms society without exception in order to create public order and substantive justice amid the uncertainty of the digital era. However, legal reality (*Das Sein*) shows that there is a wide and fundamental gap between these normative expectations and the capabilities of existing positive regulations. Indonesian national criminal law is still very much stuck in a conventional anthropocentric paradigm that places biological humans (*natuurlijke persoon*) as the only main legal subjects who can be held accountable. (Dian Juniorso in <https://rivierapublishing.id/jii/index.php/>; accessed on 1 January 2026).

Defamation using AI has been described in greater depth and has illustrated and presented a new, more complex form of defamation, namely:

1. Deepfake videos: AI creates fake videos that make it appear as if someone has committed a despicable act;
2. Synthetic audio (voice cloning): AI imitates a person's voice to convey false accusations;
3. Automated text manipulation: AI bots spread false accusations massively on social media.

Regulations governing defamation were previously stipulated in Law No. 1 of 1946 concerning the Criminal Code, and were later amended by Law No. 1 of 2023 concerning the Criminal Code. We can see the differences in the wording of the articles in the aforementioned laws:

Article 311 paragraph (1) of the Criminal Code	Article 434 paragraph (1) of Law 1/2023
If the person committing the crime of defamation or written defamation is allowed to prove that the accusation is true, fails to prove it, and the accusation is contrary to	If any person referred to in Article 433, namely a person who verbally attacks the honour or reputation of another person by accusing them of something with the

what is known, then he or she shall be punished for slander with a maximum imprisonment of 4 years.	intention of making it known to the public (defamation), is given the opportunity to prove the truth of the accusation but is unable to do so, and the accusation is contrary to what they know to be true, they shall be punished for defamation with a maximum imprisonment of 3 years or a maximum fine of Category IV, which is Rp200 million.
---	--

Then, the elements of the defamation clause must refer to the provisions on defamation in accordance with Article 310 paragraph (1) of the Criminal Code in conjunction with Constitutional Court Decision No. 78/PUU-XXI/2023 and Article 433 paragraph (1) of Law 1/2023 as follows:

Article 310 paragraph (1) of the Criminal Code in conjunction with Constitutional Court Decision No. 78/PUU-XXI/2023	Article 433(1) of Law No. 1 of 2023
Any person who deliberately attacks the honour or reputation of another person by making an accusation verbally, with the clear intention of making it known to the public, shall be punished for defamation with a maximum imprisonment of nine months or a maximum fine of Rp4.5 million.	Any person who verbally attacks the honour or reputation of another person by making an accusation, with the intention of making it known to the public, shall be punished for defamation with a maximum imprisonment of 9 months or a maximum fine of category II, which is IDR 10 million.

Article 310 paragraph (1) of the Criminal Code in conjunction with Constitutional Court Decision No. 78/PUU-XXI/2023 has the following elements:

1. anyone;
2. who intentionally;
3. attacks the honour or reputation of another person;
4. by accusing them of something;
5. verbally;
6. with the intention that it be made known to the public.

Furthermore, R. Soesilo, in his book *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentari-Komentarnya Lengkap Pasal Demi Pasal* (The Criminal Code and Its Complete Article-by-Article Commentary) (p. 225), explains that Article 310 of the Criminal Code defines 'insulting' as attacking a person's honour and reputation. Then, the person attacked usually feels ashamed. Meanwhile, the 'honour' that is attacked here only concerns honour in terms of reputation, not 'honour' in the sexual sphere or honour that can be tarnished because of an offence to one's genitals in the context of sexual desire. Regarding the 'alleged act' in Article 310 of the Criminal Code, S.R. Sianturi, in his book *Tindak Pidana di KUHP (Criminal Acts in the Criminal Code)*, argues (p. 560) that the allegation can be in the form of news that actually happened or it can also be mere 'fabrication'.

According to the Explanation of Article 433 paragraph (1) of Law 1 of 2023 concerning the Criminal Procedure Code, the nature of defamation is when an insulting act is committed by accusing, either verbally, in writing, or with images, which attacks the honour and

reputation of a person, thereby causing harm to that person. The act of defamation does not necessarily have to be a criminal offence. The object of a criminal offence under this article is an individual. Meanwhile, defamation against government institutions or groups of people is not covered by this article.

Artificial intelligence (AI) technology, blockchain, and deepfake have expanded new dimensions in the relationship between law and technology. To date, there is no law that specifically regulates the standards, audits, and legal responsibilities of AI systems. Meanwhile, the misuse of deepfakes to spread hoaxes or identity fraud has caused concern, but there is no explicit legal framework in place. This legal vacuum not only jeopardises citizens' privacy but also threatens social stability and public trust in digital media.

The impasse faced by the Indonesian criminal justice system in responding to defamation crimes in AI-based cyber media, as described above, essentially stems from the dominance of an excessive legalistic positivism paradigm. Legal positivism, which views law solely as a set of logical and autonomous written rules, tends to reduce the complexity of social issues, including technological disruption, into rigid boxes of legal syllogisms. From a positivist perspective, judges are positioned merely as 'mouthpieces of the law' (*la bouche de la loi*) whose main task is to match the facts of the trial with the wording of the articles.

Law No. 1 of 2023 concerning the Criminal Code (KUHP) contains the latest provisions regarding the elements that must be fulfilled in order for an act to be categorised as defamation, including defamation using artificial intelligence (AI), as follows:

1. The Perpetrator, namely that the act was committed by a person who is a legal subject and can be held legally responsible for what they have done, and for perpetrators who are minors, there is a mechanism of representation by parents or guardians;
2. The act attacks the honour or reputation of a person, namely the perpetrator accuses or disseminates information that can damage the honour or reputation of a person, and this can be done verbally or orally, in writing, or through other media, including digital artificial intelligence (AI) media;
3. The existence of allegations or statements, whereby the perpetrator accuses someone of doing something, whether true or false, and specifically in the case of defamation, the allegations can be proven to be false or disseminated in a manner contrary to the facts;
4. Intentional and public knowledge, namely that the accusation or statement was deliberately disseminated so that it would be known by many people, and this element emphasises the aspect of *Mens Rea*, namely the intention to harm or attack someone's reputation;
5. Causality of Loss, namely that there must be a connection between the act of spreading slander and the material or immaterial loss suffered by the victim;
6. Medium or Means of Dissemination, namely that defamation can be carried out directly or indirectly or using an intermediary, including digital technology and if carried out with artificial intelligence (AI, e.g. deepfake, generative content), the act can still be criminalised as stipulated in Law No. 1 of 2023 and the ITE Law (Article 27a);
7. No proof of truth, namely where the perpetrator cannot prove that the accusation is true, thus fulfilling the element of defamation, and if the accusation can later be proven or is true, and if it can be proven that it was for the public interest or in self-defence, then the perpetrator may not be punished.

The dissemination of content to accuse or damage the reputation of others will be classified as defamation if it fulfils the above elements using artificial intelligence (AI), namely:

1. Disseminating false statements or representations.
2. The intention to make it known to the public.
3. Damage to the victim.

This is regulated synergistically in Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions, which emphasises that criminal law applies to content in the digital space in the same way as it does in the real world. Thus, defamation using artificial intelligence (AI) constitutes a criminal offence if it meets all the above elements and can be prosecuted under Article 434(1) of Law No. 1 of 2023 on the Criminal Code in Indonesia.

II. The Investigation and Examination Process of Defamation Cases Categorised as Cybercrime Often Reaches a Dead End or Fails to Find Mens Rea.

In facing the challenges of AI technology misuse, collaboration between AI and law needs to be realised in the form of computer technology that harmonises existing rules, such as the legal culture of a country. This will enable the application of AI, which is a technology-based legal system convention, to be more easily understood, managed, used, accessed, or predicted. The concept used to explore ideas applied to law focuses on information representation and rule-based legal systems (Andriyani et al. n.d.).

The application of progressive law in the realm of defamation, which is categorised as a cybercrime, is also relevant to Nonet and Selznick's theory of responsive law, which emphasises that good law is competent, fair, and capable of responding to social needs. Today's digital society needs certainty that they are protected from the threat of autonomous algorithms. If criminal law remains adamant about the rigid principle of formal legality (*nullum delictum*), then the law will lose its authority and relevance and become an obsolete historical artefact amid the rapid pace of digital civilisation. Progressive law offers a way out by placing the 'conscience of the law' above the 'technicalities of the law'. Judges are encouraged to explore the values of justice that live within society (living law), where society demands that technology creators cannot simply wash their hands of the chaos created by their creations, even if technically 'it's just code' at work.

The investigation and examination process in defamation cases categorised as cybercrime often reaches a dead end in finding mens rea (malicious intent) due to several complex reasons stemming from the nature of cybercrime itself and the law enforcement conditions in Indonesia:

1. The complexity of digital evidence, where:
 - a. Evidence in cyber defamation cases is usually digital, such as social media posts, emails, or instant messenger messages, WhatsApp messages, and so on. Digital footprints can be altered with sophisticated technology, deleted, or quickly hidden by the perpetrator.
 - b. Digital artefacts often still require in-depth forensic analysis to identify their origin, which requires special expertise and a long time to find the elements of a criminal act.
2. The difficulty of determining the perpetrator's intent (mens rea)
 - a. Mens rea in the context of defamation using cyber media is difficult to prove because perpetrators can disseminate information without the direct intent to cause harm, sometimes disguised as opinion in podcasts or satire;

- b. Evidence of digital behaviour can be ambiguous: for example, retweets, shares, or comments may be made without realising the defamatory impact on others. This complicates the legal determination of malicious intent.
3. Limitations of Law Enforcement Capacity
 - a. This is linked to the limited number of police personnel who understand and master information technology, with the number of cyber unit members being very disproportionate and inadequate compared to the number of cases received;
 - b. The lack of budget and infrastructure for data protection and investigation technology hinders the collection of valid digital evidence.
4. Dynamic and Transnational Modus Operandi
 - a. Cybercriminals can be anonymous, using false identities, VPNs, or transnational servers, making it difficult to gain direct access to them;
 - b. International cooperation to track down perpetrators often takes a long time due to multinational legal procedures.
5. Regulatory Challenges and Law Enforcement
 - a. The Electronic Information and Transactions Law provides a legal basis, but it is abstract and often inconsistent with other regulations, leaving room for interpretation in determining the intent and responsibility of perpetrators;
 - b. The investigation process requires at least two pieces of evidence to elevate the status of a suspect, which is sometimes difficult to fulfil due to the volatile and easily manipulated nature of digital evidence.
6. Lack of Coordination and Technical Support

Investigations require collaboration between the police, PPNS, the Ministry of Communication and Information Technology, and other institutions. Lack of coordination can slow down the flow of information and evidence, making it very difficult to establish mens rea.

CONCLUSION

In this highly advanced era, where social media can be used by irresponsible individuals, social media remains a tool for them to facilitate their malicious intentions, one of which is committing the criminal act of defamation. In this case, law enforcement agencies play an important role in interpreting the law, ethics, and social values so that regulations that enforce the law governing AI as a whole, including standards, management, ethics, licensing, data protection, and legal responsibility for its use in Indonesia, are in line with the laws and principles of Pancasila of the Unitary State of the Republic of Indonesia.

The combination of easily manipulated digital evidence, perpetrator anonymity, limited technical capabilities of law enforcement, and abstract regulations with suboptimal implementation makes the process of establishing mens rea in cyber defamation cases extremely challenging. To improve effectiveness, the following are needed: Increased technological and digital forensic capacity for law enforcement officials, ongoing training related to the analysis of intent in digital criminal cases, harmonisation of regulations and legal procedures to accommodate the complexity of cybercrime, and cross-agency and international collaboration in investigating multi-layered and transnational cases.

The dissemination of content to accuse or damage the reputation of others will be classified as defamation if it fulfils the above elements using artificial intelligence (AI), namely: disseminating false statements or representations, the intention to make them known to the public, and harm to the victim. This is regulated synergistically in Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions, which emphasises that criminal law applies to content in the

digital space in the same way as it does in the real world. Thus, defamation using artificial intelligence (AI) is a criminal offence if it fulfils all of the above elements and can be prosecuted under Article 434(1) of Law No. 1 of 2023 on the Criminal Code in Indonesia.

The investigation and examination process in defamation cases categorised as cybercrimes often reaches a dead end in finding mens rea (malicious intent) due to several complex reasons stemming from the nature of cybercrime itself and the law enforcement conditions in Indonesia: the complexity of digital evidence, Difficulty in Determining the Perpetrator's Intent (Mens Rea), Limited Capacity of Law Enforcement, Dynamic and Cross-Border Modus Operandi, Regulatory and Legal Implementation Challenges, Lack of Coordination and Technical Support.

Indonesia still needs regulatory consistency, training for law enforcement officials and their expertise, and development to increase transparency in the use of AI and improve public trust, such as more open explanations about the mechanisms and benefits of AI. Ethical, privacy, and regulatory challenges must be handled carefully to ensure that these developments provide the greatest possible benefits to society as a whole.

REFERENCES

- Aan Setiadarma, Ahmad Zaki Abdullah, Priyono Sadjijo, And Dwi Firmansyah. 2024. 'Tinjauan Literatur Transformasi Sosial Dalam Era Virtual'. Khatulistiwa: Jurnal Pendidikan Dan Sosial Humaniora 4(1): 232–44. Doi:10.55606/Khatulistiwa.V4i1.2930.
- Amelia, Nabila Fitri, Diva Maura Marcella, Hening Jiwa Semesta, Sabrina Budiarti, And Saskiana Fitra Usman. 2024. 'Implementasi Artificial Intelligence (Ai) Dalam Pembentukan Peraturan-Undangan Di Indonesia'. Ural Ilmu Hukum Dan Administrasi Negara 2, No. 1: 56–70.
- Andriyani, Widyastuti, Rian Sacipto, Deby Susanto, Cory Vidiati, Reza Latifaturahmah, Aline Kurniawan, Nugrahani Editor Gratika, Riani Santi, And S Wahyuddin. Technology, Law And Society Penulis Tohar Media. <https://Toharmedia.Co.Id>.
- Amelia, Y. F., Kaimuddin, A., & Ashsyarof, H. L. (2024). Pertanggungjawaban Pidana Pelaku Terhadap Korban Penyalahgunaan Artificial Intelligence Deepfake Menurut Hukum Positif Indonesia. *Dinamika Jurnal Ilmiah Hukum*, 30(1), 67–76. <https://Penerbitgoodwood.Com/Index.Php/Jihham/Article/View/3937>
- Aryasa, K. B. (2022). *Ainomics—Economic Artificial Intelligence*. Elex Media Komputindo.
- Badan Siber Dan Sandi Negara. (2024). *Lanskap Keamanan Siber Indonesia 2023*. Direktorat Operasi Keamanan Siber Bssn. <https://Educsirt.Kemendikdasmen.Go.Id/Portal/Berita/197>
- Budiyanto, S. H. (2025). *Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia*. Sada Kurnia Pustaka.
- Dharmayanti, Y. P. (2025). *Kebijakan Hukum Pidana Dalam Upaya Menanggulangi Artificial Intelligence (Ai) Dalam Cyber Crime*. Universitas Islam Sultan Agung Semarang.
- Dupont, B., Fortin, F., & Leukfeldt, R. (2024). Broadening Our Understanding Of Cybercrime And Its Evolution. *Journal Of Crime And Justice*, 47(4), 435–439. https://Www.Researchgate.Net/Publication/378613280_Broadening_Our_Understanding_Of_Cybercrime_And_Its_Evolution
- Hartiwi Ningsih. *Peran Transformasi Digital Dalam Meningkatkan Demokrasi Yang Berkepastian Hukum*.
- Irawan, Hengki, And Zainudin Hasan. 'Dampak Teknologi Terhadap Strategi Litigasi Dan Bantuan Hukum: Tren Dan Inovasi Di Era Digital.' *Innovative: Journal Of Social Science Research* 4, No. 2 (2024): 4600-4613. '4600-4613'.

- Kajian, Jurnal, Hukum Dan, Pendidikan Kewarganegaraan, Abraham Ethan Martupa, And Sahat Marune. 2023. 2 Civilia : Metamorfosis Metode Penelitian Hukum: Mengarungi Eksplorasi Yang Dinamis. <http://Jurnal.Anfa.Co.Id>.
- Mutmainnah, A., Suhandi, A. M., & Herlambang, Y. T. (2024). Problematika Teknologi Deepfake Sebagai Masa Depan Hoax Yang Semakin Meningkatkan: Solusi Strategis Ditinjau Dari Literasi Digital. *Upgrade: Jurnal Pendidikan Teknologi Informasi*, 1(2), 67–72.
<https://Journal.Universitasbumigora.Ac.Id/Index.Php/Upgrade/Article/Download/3702/1604>
- Naili, Y. T. (2025). Optimalisasi Penegakan Hukum Terhadap Kejahatan Siber Berbasis Ai Terhadap Perempuan: Kajian Hukum Pidana Dan Kebijakan Digital. *Jurnal Media Hukum*, 13(2), 207–219.
- Novrianto, M. (2025). Kebijakan Hukum Pidana Terhadap Cyber Crime Berbasis Artificial Intelligence Di Indonesia. *Jurnal Kepastian Hukum Dan Keadilan*, 7(2), 150–170.*
- Olimid, A. P., Georgescu, C. M., & Olimid, D. A. (2024). Legal Analysis Of Eu Artificial Intelligence Act (2024): Insights From Personal Data Governance And Health Policy. *Access To Justice In Eastern Europe*, 7(4), 1–23. https://Ajee-Journal.Com/Upload/Attaches/Att_1731686201.Pdf
- Syaputra, R. (2024). Urgensi Pengaturan Perlindungan Hukum Terhadap Korban Deepfake Melalui Artificial Intelligence (Ai) Dari Perspektif Hukum Pidana Indonesia. *Jurnal Hukum Respublica*, 23(1), 5–12.*
<https://Garuda.Kemdiktisaintek.Go.Id/Author/View/8149235>
- Rajagukguk, Ratna Marselina. *Hukum Dan Teknologi: Menghadapi Tantangan Hukum Di Era Digital*.
- Samekto, Fx Adji, And Ani Purwanti. *Perubahan Tatanan Sosial Dan Transformasi Pemaknaan Pancasila*.
- Sebayang, Ekinia Karolin, Mahmud Mulyadi, And Mohammad Ekaputra. 2024. ‘Potensi Pemanfaatan Teknologi Artificial Intelligence Sebagai Produk Lembaga Peradilan Pidana Di Indonesia’. *Locus Journal Of Academic Literature Review* 3(4): 317–28. Doi:10.56128/Ljoalr.V3i4.311.