The Easta Journal Law and Human Rights
Vol. 3, No. 02, February 2025, pp. 110 - 117
ISSN: 2985-7112, DOI: 10.58812/eslhr.v3i02

Criminal Law Arrangements in Handling the Spread of Social Media Bot-Based False Information in Indonesia

Loso Judijanto[1], Irman Putra[2], Sumarni[3]
[1] IPOSS Jakarta
[2] Sekolah Tinggi Hukum Militer
[3] Sekolah Tinggi Ilmu Ekonomi TRIGUNA Tangerang

Article Info

Article history:

Received Feb, 2025
Revised Feb, 2025
Accepted Feb, 2025

Keywords:

Disinformation
False Information
Indonesia
Legal Framework
Social Media Bots

ABSTRACT

This study examines the legal arrangements in Indonesia for handling the spread of false information through social media bots, employing a normative juridical analysis. The proliferation of disinformation through automated bots has become a significant challenge to public trust, social cohesion, and democratic processes. This paper explores the adequacy of existing legal frameworks, such as the Information and Electronic Transactions Law (ITE Law), the Indonesian Penal Code, and the Election Law, in addressing bot-generated false information. The study identifies key challenges, including technological limitations, legal ambiguities, and jurisdictional issues, and compares Indonesia's regulatory approach with that of the European Union and the United States. The research highlights the need for clear legal definitions, enhanced platform accountability, improved enforcement capabilities, and greater international cooperation to effectively address this issue. The study concludes with recommendations for legal reforms and increased public awareness to mitigate the adverse impact of social media bots on public discourse in Indonesia.

Corresponding Author:

Name: Loso Judijanto
Institution: IPOSS Jakarta
Email: losojudijantobumn@gmail.com

1. INTRODUCTION

The proliferation of social media in Indonesia has significantly transformed communication and information-sharing processes, offering both opportunities and challenges. These platforms have revolutionized communication by creating new channels for information exchange and fostering online communities [1], enabling individuals to connect across distances, share experiences, and participate in collective actions, thus enhancing social unity and engagement [2]. However, the ease of information dissemination on social media has also led to the rapid spread of misinformation and hoaxes, which are prevalent in Indonesia [3], and social media bots further amplify the reach of false information, posing threats to public order and trust in information sources. Despite its crucial role in enhancing political participation and transparency in Indonesian democracy [4], misinformation and political polarization hinder social media's effectiveness, underscoring the need for legal reforms to address these challenges [4]. To mitigate the negative impacts of social media,

promoting digital literacy and mindfulness is essential in addressing issues such as misinformation and mental health concerns [5], while effective regulation and collaboration among government, social media platforms, and the public are crucial to maximizing the positive contributions of social media while minimizing its adverse effects [4].

The Indonesian government's efforts to combat false information, particularly bot-generated misinformation, face significant challenges due to the complexity of detecting and regulating algorithm-driven entities, as the existing legal framework, such as the ITE Law, lacks specificity in addressing the nuances of bot-generated content, complicating enforcement. The integration of advanced machine learning techniques and a comprehensive legal framework could enhance the detection and regulation of such misinformation. Machine learning models, such as the Bidirectional Long Short-Term Memory (BI-LSTM) algorithm, have shown promise in detecting fake news with high accuracy and can be trained on datasets like the Global Fact-Check Database to improve the integrity of information dissemination during elections [6], while other machine learning approaches, including K-Nearest Neighbors and Trigram Models, have been explored for detecting fake news in Bahasa Indonesia, achieving varying degrees of success [7]. However, the current legal framework in Indonesia, including the ITE Law, does not explicitly address the challenges posed by AI technologies like deepfakes and bot-generated misinformation, highlighting the need for specific regulations targeting AI misuse in the political process [8]. A proposed solution is the introduction of a bill focused on AI regulation, which would harmonize existing election laws and address the misuse of AI technologies in elections [9]. Additionally, surveys indicate that a significant portion of the Indonesian population encounters misinformation on social media, with many struggling to differentiate between true and false information, underscoring the need for improved public awareness and education alongside technological and legal measures [10]

This study focuses on the normative juridical analysis of criminal law arrangements in handling the spread of false information propagated by social media bots in Indonesia. It examines the adequacy of existing legal provisions, identifies gaps and challenges in enforcement, and explores potential reforms to strengthen the legal framework. Given the rapid evolution of technology and the increasing sophistication of bots, the law must remain adaptive to effectively mitigate their harmful effects without stifling legitimate digital freedoms.

The importance of this research lies in its potential to contribute to the development of a robust legal framework that addresses the complexities of regulating digital spaces. By examining the intersection of technology and law, this study seeks to provide actionable insights and recommendations for policymakers, legal practitioners, and technology experts. It emphasizes the need for collaborative efforts among stakeholders to achieve a balance between protecting societal interests and upholding individual freedoms in Indonesia's digital landscape. Through this investigation, the study aims to answer key questions: What are the limitations of Indonesia’s current legal framework in addressing bot-based false information? How can the law be reformed to effectively tackle this issue? What role can technology and international cooperation play in strengthening enforcement mechanisms?

2. LITERATURE REVIEW

2.1 False Information and Its Impact

False information, including misinformation and disinformation, poses global challenges, particularly in Indonesia, where it fuels political polarization, social unrest, and public health crises. Its rapid spread is driven by sensationalism, which attracts more attention than verified news, amplified by social media platforms. False information influences public perception and political

beliefs, threatening national security and societal stability [11], with platforms like Facebook, Instagram, and TikTok contributing significantly to its dissemination [12]. In India, financial motives often drive fake news creation, impacting journalism integrity [13]. Addressing these issues requires critical thinking skills to recognize misinformation [11] and automated tools using natural language processing to detect patterns like negative sentiment and recurring themes [12]. Fact-checking datasets like Factrix aid in training models to identify false information [14], while news literacy interventions, especially those using mixed framing, enhance resistance to misinformation without undermining trust in accurate news [15]

2.2 Social Media Bots and Their Role

Social media bots in Indonesia have significantly shaped public discourse, particularly during electoral and disinformation campaigns, by mimicking human behavior and making it difficult to distinguish between bot-generated and human-generated content. The increasing sophistication of bot technology enables them to manipulate public opinion through content amplification and the creation of echo chambers that reinforce specific narratives. Social bots profoundly impact public sentiment by engaging in discussions and altering perceptions, negatively affecting users with favorable or neutral stances on topics such as climate activism [16], while AI-generated content disseminated by bots influences public trust and user behavior on social media [17]. Bots also play a central role in spreading misinformation, amplifying echo chambers, and manipulating public sentiment, as seen on platforms like Sina Weibo [18], where they contribute significantly to misinformation dissemination and reinforce specific agendas, limiting access to unbiased information [18]. Detecting social media bots, especially those involved in political campaigns, remains challenging, prompting the development of advanced machine learning models to improve detection accuracy through various features and techniques [19], while unsupervised detection methods have been proposed to identify coordinated fake-follower campaigns, revealing irregular following patterns indicative of bot activity [20].

2.3 Legal Frameworks for Addressing False Information

Indonesia's regulation of false information, primarily through the ITE Law, seeks to balance public order and freedom of expression but faces criticism for vague definitions and potential misuse. Alongside the Penal Code and Election Law, it criminalizes false information causing public harm, yet its broad language has led to selective enforcement, often targeting political dissent [21]. While these laws address defamation and disinformation, they lack provisions for bot-generated misinformation [22]. Critics call for clearer definitions and proportional enforcement to prevent overreach [23]. Compared to Malaysia’s cooperative regulatory approach, Indonesia’s penal-driven policy is more rigid [24]. Emerging technologies and digital forensics offer solutions for tracing false information, emphasizing the need for legislative adaptation [24]. Scholars suggest revising the ITE Law to address digital misinformation threats and considering international models like Germany’s Network Enforcement Act for a more effective framework [25]

2.4 Challenges in Enforcement

The enforcement of laws against false information faces significant challenges due to technological advancements in bot development, jurisdictional complexities, and a lack of expertise among law enforcement agencies. Sophisticated bots are increasingly difficult to detect, enabling the spread of disinformation and

cybercrimes such as DDoS attacks and click fraud [26], while bot farms, as seen in Ukraine, complicate efforts to combat foreign-coordinated disinformation [27]. Jurisdictional challenges arise as cybercrimes often originate from servers in different countries, complicating enforcement and highlighting the need for international legal harmonization [28]. Law enforcement agencies also struggle with expertise gaps, as rapid technological advancements outpace legal adaptation, making specialized training and global collaboration essential [28]. Addressing these issues requires transnational cooperation between nations, international organizations, and technology companies [29], with innovative solutions such as Microsoft's combination of legal and technical strategies to dismantle botnet operations demonstrating the potential of public-private partnerships in countering disinformation and cybercrime [26].

2.5 Theoretical Framework

This study adopts a normative juridical approach, focusing on the analysis of legal norms and principles. The approach examines the adequacy of Indonesia's legal provisions in addressing bot-based false information and proposes reforms grounded in international best practices. The theoretical underpinnings draw on the balance between freedom of expression, as enshrined in Article 28E of the 1945 Constitution, and the protection of public order, as mandated by Article 28J. While existing literature provides a broad understanding of false information and its regulation, limited studies focus specifically on bot-generated false information in Indonesia. This study seeks to fill this gap by analyzing the legal, technological, and enforcement challenges posed by social media bots. By proposing targeted legal reforms, the research aims to contribute to the development of a more effective framework for combating false information in Indonesia.

3. RESEARCH METHODS

3.1 Research Approach

The normative juridical approach involves the study and interpretation of legal norms and their application. This method is chosen because it provides a comprehensive framework for analyzing the legal provisions that govern the dissemination of false information through social media bots. It also facilitates the identification of gaps and inconsistencies in the legal framework, offering insights into potential reforms.

3.2 Data Collection

The data used in this study is primarily secondary, sourced from primary, secondary, and tertiary legal materials. Primary legal sources include the 1945 Constitution of the Republic of Indonesia, Law Number 11 of 2008 on Information and Electronic Transactions (ITE Law) and its amendments, the Indonesian Penal Code (KUHP), and other relevant regulations such as the Election Law and sector-specific legislation. Secondary legal sources consist of legal commentaries, scholarly articles, and journals discussing the regulation of false information and the role of social media bots, as well as case law and judicial decisions relevant to false information dissemination. Tertiary legal sources include legal encyclopedias, dictionaries, and other reference materials that help clarify legal concepts and terminologies.

3.3 Data Analysis

The collected data is analyzed using qualitative techniques, focusing on the interpretation of legal norms and their application in real-world scenarios. The analysis involves three stages: normative analysis, which examines the adequacy of existing legal provisions in addressing challenges posed by social media bots, including their clarity, specificity, and enforceability; comparative analysis, which evaluates Indonesia's legal framework against those of other jurisdictions, such as the European Union

and the United States, to identify best practices and potential adaptations; and critical analysis, which identifies gaps, ambiguities, and inconsistencies in the legal framework by assessing its alignment with Indonesia's constitutional principles and international standards.

4. RESULTS AND DISCUSSION

4.1 Legal Framework for Regulating False Information in Indonesia

The legal framework in Indonesia comprises several laws and regulations aimed at addressing false information. Key provisions include the Information and Electronic Transactions Law (ITE Law), which under Article 28 prohibits the dissemination of false information that causes public harm, imposing criminal penalties such as imprisonment and fines. However, the law lacks specificity in defining false information and does not explicitly address content generated by social media bots. The Indonesian Penal Code (KUHP) contains provisions on defamation and public disorder that can be applied to cases involving false information, but its general nature makes it less effective in tackling bot-generated disinformation. The Election Law specifically targets false information during electoral campaigns, penalizing individuals or groups disseminating misleading content to influence voter behavior. However, social media bots used for disinformation during elections often evade enforcement due to technological complexities.

Despite these legal instruments, Indonesia's framework struggles to effectively manage false information, particularly bot-generated content. While the ITE Law prohibits false information dissemination, its vague definitions lead to selective prosecution that often targets political dissent rather than effectively combating disinformation [30]. Similarly, the broad provisions in the KUHP are inadequate for addressing digital-age challenges, and the Election Law's enforcement is hindered by the difficulty of identifying and regulating bot-generated content [31]. To strengthen this framework, legal definitions in the ITE Law should be refined to better address false and bot-generated content [32], enforcement mechanisms—especially in elections—should be improved [33], and false information regulations should be aligned with personal data protection laws for a more comprehensive approach [25]

4.2 Challenges in Regulating Bot-Generated False Information

The challenges posed by social media bots in spreading false information are multifaceted, encompassing technological, legal, jurisdictional, and enforcement issues. Technologically, bots have become increasingly sophisticated, using machine learning algorithms to mimic human behavior and bypass detection mechanisms, complicating enforcement efforts [34]. Despite explicit policies against bot activity, major social media platforms continue to have vulnerabilities in their enforcement mechanisms, allowing bots to operate undetected [34]. Legally, current frameworks lack explicit provisions addressing the role of bots in spreading false information, leading to inconsistencies in law enforcement [35]. Additionally, ambiguous definitions of terms such as "false information" and "public harm" further complicate legal enforcement, as seen in varying interpretations across jurisdictions [36]. Jurisdictional challenges arise as bots often operate across borders, making it difficult to identify and prosecute perpetrators due to legal complexities [28]. Limited international cooperation further weakens enforcement against cross-border disinformation campaigns, highlighting the need for stronger global collaboration [28]. Meanwhile, enforcement capacity remains inadequate, as law enforcement agencies often lack the technical expertise and

resources needed to effectively combat bot-generated false information [37]. The absence of specialized units to address cybercrimes related to social media exacerbates the problem, underscoring the necessity of developing dedicated cybercrime units [37]. Addressing these issues requires an integrated approach that combines technological solutions, legal reforms, international cooperation, and enhanced enforcement mechanisms.

4.3 Comparative Insights

The regulation of social media platforms in the European Union and the United States presents distinct approaches to managing harmful content and bot activity. The EU's Digital Services Act (DSA) mandates that platforms implement robust mechanisms for detecting and removing harmful content, including bot-generated disinformation. It also introduces a Transparency Database to enhance accountability, though platform discretion remains a challenge [38]. The General Data Protection Regulation (GDPR) enforces strict data protection standards, requiring platforms to prioritize user accountability and transparency, which indirectly curtails bot activity [39]. However, while the DSA aims to balance content moderation with fundamental rights, the lack of specificity in reporting requirements can hinder effective compliance [34]. In contrast, the United States follows a platform-centric approach, relying heavily on self-regulation. The Communications Decency Act (Section 230) grants platforms immunity from liability for user-generated content, encouraging them to develop their own moderation policies. However, recent Supreme Court rulings have highlighted the need for legislative updates to balance free expression with content control [40]. At the state level, California has enacted laws targeting bot disclosure and accountability, demonstrating a more proactive stance in addressing bot-related issues [41]. While both the EU and the U.S. emphasize transparency and user protection, their approaches differ in enforcement, with the EU prioritizing regulatory oversight and the U.S. relying on market-driven self-regulation.

4.4 Discussion

Indonesia should amend the ITE Law to explicitly define and criminalize the use of bots for spreading false information, ensuring clear definitions and specific penalties to enhance legal certainty and enforcement. Strengthening platform accountability is also crucial, requiring social media platforms to implement detection mechanisms for bot activity and report such instances to authorities, with regulations modeled after the EU's Digital Services Act (DSA). Additionally, investing in technology and training for law enforcement agencies is essential to improve detection and investigation capabilities, while partnerships with cybersecurity firms and international organizations could provide technical support. Given the cross-border nature of bot activity, Indonesia should enhance international cooperation by collaborating with global organizations and adopting treaties addressing cybercrime and disinformation. Lastly, public awareness campaigns should be prioritized to educate users on identifying bot-generated content and the risks of false information, with collaborative efforts involving the government, civil society, and private sector playing a vital role in mitigating its impact.

4.5 Balancing Freedom of Expression and Public Order

The regulation of false information must balance the constitutional right to freedom of expression with the need to protect public order. Overly restrictive laws risk stifling legitimate dissent and critical discourse. A rights-based approach, emphasizing proportionality and necessity, is essential for ensuring that legal measures align with democratic principles.

4.6 Proposed Legal Reforms

Based on the findings, the study proposes the following legal reforms:

1. Amending the ITE Law to include specific provisions targeting bot-generated disinformation.
2. Introducing a regulatory framework that holds platforms accountable for monitoring and reporting bot activity.
3. Establishing specialized cybercrime units to handle cases involving social media bots.
4. Promoting international agreements to facilitate cross-border cooperation in addressing disinformation.

5. CONCLUSION

The spread of false information via social media bots presents significant legal and societal challenges in Indonesia. Despite the existence of relevant laws such as the ITE Law, the current legal framework is insufficient to address the complexities of bot-generated disinformation effectively. Key issues such as vague legal definitions, technological limitations, and cross-border jurisdictional challenges hinder the enforcement of laws aimed at curbing disinformation. Drawing on comparative insights from the European Union and the United States, this study underscores the need for clear legislative measures that explicitly address the use of bots for spreading false information. Additionally, enhancing platform accountability, strengthening technological capabilities for law enforcement, and fostering international cooperation are crucial steps toward mitigating the negative impact of disinformation. The proposed legal reforms, along with public awareness campaigns, are essential to protect the integrity of public discourse and promote democratic values in the digital era.

REFERENCES

[1] Y. Sanjaya and R. R. Phahlevy, "Social Media's Crucial Role in Shaping Indonesian Democracy," *Indones. J. Law Econ. Rev.*, vol. 19, no. 3, pp. 10–21070, 2024.

[2] C. S. Cagatin, "The societal transformation: The role of social networking platforms in shaping the digital age," *Interdiscip. Soc. Stud.*, vol. 3, no. 3, pp. 103–107, 2024.

[3] Barge Gul Khalili, Tamanna Quraishi, and Fatana Dayan, "Evaluating the Impact of Social Networks on Human Communication in the Digital Era," *Socio-Economic Humanist. Asp. Townsh. Ind.*, vol. 2, no. 1, pp. 152–163, 2024, doi: 10.59535/sehati.v2i1.252.

[4] B. W. Setyawan, S. Pd, M. Pd, U. I. N. Sayyid, A. Rahmatullah, and H. Kistanto, "Tulungagung Dan Sekitarnya agama , ras , suku , etnis yang beragam teori Roland Barthes yang dikutip dari buku memiliki sebuah makna yang bisa dilihat tanda . Fokus penelitian membahas digemari oleh anak-anak muda yang sudah," vol. XVIII, no. 2017, pp. 30–36, 2024.

[5] T. D. Handayani, "Bijak Menggunakan Media Sosial pada Masyarakat Digital," *Akad. J. Mhs. Humanis*, vol. 4, no. 3, pp. 741–752, 2024, doi: 10.37481/jmh.v4i3.1011.

[6] D. K. S. Sekarhati, "Combating Hoax and Misinformation in Indonesia Using Machine Learning What is Missing and Future Directions," *Eng. Math. Comput. Sci. J.*, vol. 6, no. 2, pp. 143–150, 2024.

[7] C. T. Noerman and A. L. Ibrahim, "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara," *J. USM Law Rev.*, vol. 7, no. 2, 2024.

[8] H. Armiwulan, R. A. Rahman, V. N. Prabowo, and J. Hajdú, "Artificial Intelligence and Its Challenges To Elections In Indonesia: A Legal Analysis," *Jambura Law Rev.*, vol. 6, no. 2, pp. 264–285, 2024.

[9] S. G. Arkaan, A. R. Atmadja, and M. D. Firdaus, "Fake news detection in the 2024 Indonesian general election using Bidirectional Long Short-Term Memory (BI-LSTM) algorithm," *Fake news Detect. 2024 Indones. Gen. Elect. using Bidirectional Long Short-Term Mem. algorithm*, vol. 21, no. 2, pp. 22–30, 2024.

[10] A. F. Nugraha, Y. Pristyanto, R. Setiani, S. A. H. Bahtiar, A. D. Putra, and R. F. A. Aziza, "A Comparative Study of Machine Learning Models for Detecting Fake News Content in Bahasa Indonesia Online Media," in *2024 International Conference on Smart Computing, IoT and Machine Learning (SIML)*, 2024, pp. 43–48.

[11] P. F. A. van Erkel, P. Van Aelst, J. Van Nieuwenborgh, C. H. de Vreese, M. Hameleers, and D. N. Hopmann, "Combating Disinformation With News Literacy Interventions: An Experimental Study on the Framing Effects of News Literacy Messages," *Int. J. Press.*, p. 19401612241279536, 2024.

[12] O. Bhanushali *et al.*, "Towards Mitigating Misinformation: A Structured Dataset of Fact-Checked Claims from News Media," in *2024 IEEE Region 10 Symposium (TENSYMP)*, 2024, pp. 1–6.

[13] R. Bala and M. Muhammed, "An Empirical Study on Fake News Menace and Misinformation with Special Reference to India," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 285–294, Nov. 2024, doi: 10.48175/IJARSCT-22154.

[14] E. J. Schlicht, "Characteristics of Political Misinformation Over the Past Decade," *arXiv Prepr. arXiv2411.06122*, 2024.

[15] D.-I. Călin, A. BARCAN, and C. Constantin, "Fake News," in *International Conference on Cybersecurity and Cybercrime*, 2024, vol. 11, pp. 56–60.

[16] Z. Ellaky and F. Benabbou, "Political social media bot detection: Unveiling cutting-edge feature selection and engineering strategies in machine learning model development," *Sci. African*, vol. 25, p. e02269, 2024.

[17] H. Wan, M. Luo, Z. Ma, G. Dai, and X. Zhao, "How Do Social Bots Participate in Misinformation Spread? A Comprehensive Dataset and Analysis," *arXiv Prepr. arXiv2408.09613*, 2024.

[18] M. M. Rahman, A. A. Tutul, A. Nath, L. Laishram, S. K. Jung, and T. Hammond, "Mamba in vision: A comprehensive survey of techniques and applications," *arXiv Prepr. arXiv2410.03105*, 2024.

[19] Y. Zouzou and O. Varol, "Unsupervised detection of coordinated fake-follower campaigns on social media," *EPJ Data Sci.*, vol. 13, no. 1, p. 62, 2024.

[20] L. Li, O. Vásárhelyi, and B. Vedres, "Social bots spoil activist sentiment without eroding engagement," *Sci. Rep.*, vol. 14, no. 1, p. 27005, 2024.

[21] N. Shah, G. Khandhadai, S. K. Prasad, K. Kim, and D. Lewis, "思 米 沙".

[22] F. Sidiq, A. S. Azahra, and D. I. Pirdaus, "Implications of Changes in the Criminal Procedure Law of the ITE Law on Individual Rights in the Indonesian Legal System," *Int. J. Humanit. Law, Polit.*, vol. 2, no. 2, pp. 56–61, 2024.

[23] S. Supanto, Y. Saefudin, N. Ismail, R. Susanti, and L. K. Adi, "Regulating Fake News and Hoaxes: A Comparative Analysis of Indonesia and Malaysia," *J. Hum. Rights, Cult. Leg. Syst.*, vol. 3, no. 3, pp. 656–677, 2023.

[24] A. Afisa, Z. Qodir, A. Habibullah, and U. Sugiharto, "Analysis of the ITE Law on Digital Rights and Democratic Values in Indonesia," *J. Soc. Media*, vol. 8, no. 2, pp. 424–444, 2024.

[25] S. Muslim and N. Solapari, "The Impact of Hate Speech Regulations on Freedom of Expression an Indonesian Legal Perspective," *Easta J. Law Hum. Rights*, vol. 3, no. 01, pp. 10–19, 2024.

[26] B. Dupont, "Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime," *Crime, law Soc. Chang.*, vol. 67, pp. 97–116, 2017.

[27] O. O. Amoo, A. Atadoga, T. O. Abrahams, O. A. Farayola, F. Osasona, and B. S. Ayinla, "The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system," *World J. Adv. Res. Rev.*, vol. 21, no. 2, pp. 205–217, 2024.

[28] R. Raj and D. Chaudhuri, "Online Privacy and Cyber Security: Challenges and Its Regulations," *Issue 1 Int'l JL Mgmt. Human.*, vol. 7, p. 1408, 2024.

[29] J. Huang, "Chinese private international law and online data protection," *J. Priv. Int. Law*, vol. 15, no. 1, pp. 186–209, 2019.

[30] M. S. Siregar, B. Ananda, and B. Purba, "Analisis Dampak Hukum Perlindungan Konsumen Dalam Perdagangan Online (Menelaah Dampak Perlindungan Hukum Terhadap Konsumen Dalam Transaksi Online)," *AL-MIKRAJ J. Stud. Islam dan Hum. (E-ISSN 2745-4584)*, vol. 5, no. 01, pp. 320–330, 2024.

[31] W. S. Nansi, "Cyberbullying Formulative Problems Against Child Protection in Indonesia," *Const. Law Rev.*, vol. 2, no. 2, pp. 113–128, 2024.

[32] N. M. D. G. Putri, N. L. M. Mahendrawati, and N. M. P. Ujianti, "Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *J. Prefer. Huk.*, vol. 5, no. 2, pp. 240–245, 2024.

[33] F. S. Utama, D. E. Purwoleksono, and T. Rachman, "Data Leakage of the Indonesian Elections Commission in Legal Aspects of Personal Data Protection.," *Media Iuris*, vol. 7, no. 3, 2024.

[34] K. Radivojevic, C. McAleer, C. Conley, C. Kennedy, and P. Brenner, "Social Media Bot Policies: Evaluating Passive and Active Enforcement," *arXiv Prepr. arXiv2409.18931*, 2024.

[35] I. Ilin and A. Kelli, "Natural Language, Legal Hurdles: Navigating the Complexities in Natural Language Processing Development and Application," *J. Univ. Latv. Law*, vol. 17, pp. 44–67, 2024.

[36] A. Vlasov and S. Klymenko, "Peculiarities of the criminal-legal evaluation of public appeals and distribution of materials in social networks," *Uzhhorod Natl. Univ. Herald. Ser. Law*, vol. 3, pp. 291–296, Nov. 2024, doi: 10.24144/2307-3322.2024.85.3.46.

[37] M. Huda, A. Awaludin, and H. Siregar, "Legal Challenges in Regulating Artificial Intelligence: A Comparative Study of Privacy and Data Protection Laws," *Int. J. Soc. Hum.*, vol. 1, pp. 116–125, Nov. 2024, doi: 10.59613/g8dc9v94.

[38] R. Kaushal, J. Van De Kerkhof, C. Goanta, G. Spanakis, and A. Iamnitchi, "Automated transparency: A legal and empirical analysis of the digital services act transparency database," in *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*, 2024, pp. 1121–1132.

[39] G. Gosztonyi and G. F. Lendvai, "Online platforms and legal responsibility: A contemporary perspective in view of the recent US developments," *Masaryk Univ. J. Law Technol.*, vol. 18, no. 1, pp. 125–141, 2024.

[40] A. Lima, J. Montevilla, and L. Santos, "Regulação Legal Das Redes Sociais: Proteção De Dados E Liberdade De Expressão," *Rev. ft*, pp. 37–38, Oct. 2024, doi: 10.69849/revistaft/pa10202410212137.

[41] J. T.-Z. Wei, F. Zufall, and R. Jia, "Operationalizing content moderation 'accuracy' in the Digital Services Act," in *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 2024, vol. 7, pp. 1527–1538.