DIPONEGORO
Law Review

Vol. 11, No. 1, April 2026 E-ISSN: 2527-4031
Available online at website: https://ejournal.undip.ac.id/index.php/dlr

ARTIFICIAL INTELLIGENCE, DISINFORMATION, AND LEGAL REFORM IN INDONESIA

[1*] I Gede Widhiana Suarda, [1] Fendi Setyawan, [2] Vicko Taniady, [1] Annas Rashid Musthafa, [1] Natasya Aulia Putri, [3] I Made Putra Arya Wiranata

[1] Faculty of Law, Universitas Jember, East Java, Indonesia
[2] Faculty of Law, Monash University, Australia
[3] Kwangwoon University, Seoul, South Korea
***Corresponding author**: igedewidhiana.suarda@unej.ac.id

Abstract

Artificial intelligence (AI) has transformed the digital information ecosystem by enabling the rapid creation and dissemination of disinformation at an unprecedented scale. Existing legal frameworks, however, remain largely designed to regulate human conduct and conventional digital platforms, creating significant regulatory gaps in addressing AI-generated disinformation. This study examines the adequacy of Indonesia's current legal framework and develops an appropriate regulatory model through a comparative analysis of the legal approaches adopted by the European Union, the United States, and China. This study adopts a doctrinal legal research methodology and employs statutory, conceptual, comparative, and case-based approaches. The analysis draws on theories of legal certainty, legal responsibility, AI sovereignty, and spatial ontology. The findings demonstrate that Indonesia's existing legal framework remains fragmented and does not specifically regulate AI-generated disinformation. Comparative analysis shows that while the European Union adopts a comprehensive risk-based model, China emphasises platform accountability and administrative control, and the United States relies on sector-specific governance, none fully addresses the jurisdictional challenges arising from the transnational operation of AI systems. This study argues that regulating AI-generated disinformation requires moving beyond purely territorial legal approaches towards a post-territorial understanding of jurisdiction. Accordingly, this study proposes a phased regulatory roadmap for Indonesia comprising a Presidential Regulation, amendments to the existing digital regulatory framework, and a comprehensive Artificial Intelligence Act. By integrating comparative legal analysis with emerging theories of AI governance, this study proposes a legislative framework that can address AI-generated disinformation while safeguarding democratic integrity, legal certainty, and fundamental rights.

***Keywords**: Artificial Intelligence; Digital Democracy; Disinformation; Legal Reform.*

Received: 11 January 2026; Revised: 25 April 2026; Accepted: 26 April 2026; Available online: 30 April 2026; Published: 30 April 2026.

***How to Cite**: Suarda*, I Gede Widhiana, Fendi Setyawan, Vicko Taniady, Annas Rashid Musthafa, Natasya Aulia Putri, and I Made Putra Arya Wiranata. "Artificial Intelligence, Disinformation, and Legal Reform in Indonesia." *Diponegoro Law Review* 11, no. 1 (2026): 169–99. https://doi.org/10.14710/dilrev.11.1.2026.169-199.

Copyright © Diponegoro Law Review. Published by Faculty of Law, Universitas Diponegoro. This is an open access article under the CC-BY-NC-SA License. (https://creativecommons.org/licenses/by-nc-sa/4.0/)

1. Introduction

Democracy is a political system based on the principles of popular sovereignty, public participation and transparency of information. As the foundation of free speech and access to truthful information, democracy relies on public trust in the institutions that disseminate information. In this modern era, the presence of technology, especially Artificial Intelligence (AI), has strengthened and accelerated the dissemination of information.[1] However, AI also brings

[1] Marcello M. Mariani et al., "Artificial Intelligence in Innovation Research: A Systematic Review, Conceptual Framework, and Future Research Directions," *Technovation* 122 (2023): 1–25, https://doi.org/10.1016/j.technovation.2022.102623.

new challenges, especially related to the spread of inaccurate information or disinformation.[2] AI currently plays a significant role in filtering and disseminating information through various digital platforms, including social media and search engines. While AI aims to improve the efficiency and accuracy of information, these automated mechanisms often accelerate the spread of disinformation and misinformation. AI, through its ever-evolving algorithms and machine intelligence, can reinforce false or biased narratives in society, directly threatening the quality of democracy.

Democracy relies on the integrity of public discourse, informed participation, and trust in institutions. However, disinformation, particularly when amplified by technology, threatens these democratic foundations. Cass R. Sunstein, a law professor from Harvard Law School in the United States, highlights that the appeal of disinformation lies in its ability to evoke human emotions, such as fear and hope.[3] AI compounds this problem by amplifying content based on engagement rather than accuracy, creating echo chambers and contributing to political polarization, especially during elections.[4] Disinformation has influenced key democratic events across the globe. In 2023 Nigerian election, for instance, political operatives paid influencers to spread fake news targeting opposition candidates.[5] In Indonesia, disinformation in the form of texts and images are used to attack or support certain candidates, creating distrust among voters. For example, in the 2014 election, a photo circulated showing a man resembling the former President of the Republic of Indonesia, Ir. Joko Widodo at a D.N. Aidit campaign event, accusing him of being a stooge of the Indonesian Communist Party (PKI).[6] In addition, there is a false narrative that Prabowo Subianto, a former high-ranking military officer who is now chairman of the Gerindra Party and President of the Republic of Indonesia 2024-2029, was "dishonourably discharged" from the TNI institution, when in fact he was honourably discharged.[7] This dissemination of inaccurate information can greatly influence public sentiment towards candidates.

Such pattern is not unique to Indonesia. In Belarus, for example, research by Kravets and colleagues revealed how manipulated search engine results, particularly from Yandex, were used to influence public perception during the COVID-19 pandemic. Their findings highlight how algorithmic curation of information can subtly shape political opinion, even outside the context of traditional social media platforms.[8] In the context of elections, the potential impact of AI in exacerbating the spread of disinformation could threaten democratic stability by deepening social polarisation and undermining the integrity of the electoral process. This points to the need for strategic measures to address the challenge of disinformation amplified by modern technologies, in order to protect the democratic order and maintain public trust in information.

While earlier disinformation campaigns were largely driven by humans and traditional media manipulation, current threats are increasingly powered by generative AI, especially large language models (LLMs). These models are capable of producing coherent and persuasive

---

2 Noémi Bontridder and Yves Poullet, "The Role of Artificial Intelligence in Disinformation," *Data & Policy* 3 (2021): 1–21, https://doi.org/10.1017/dap.2021.20.

3 Arif Perdana, "AI dan disinformasi: bagaimana kecerdasan buatan dapat memperparah penyebaran hoaks jelang Pemilu 2024," *The Conversation*, 2023, http://theconversation.com/ai-dan-disinformasi-bagaimana-kecerdasan-buatan-dapat-memperparah-penyebaran-hoaks-jelang-pemilu-2024-212254.

4 Perdana, "AI dan disinformasi: bagaimana kecerdasan buatan dapat memperparah penyebaran hoaks jelang Pemilu 2024."

5 Olusegun Fariudeen Liadi, Musediq Olufemi Lawal, and Olawale Olufemi Akinrinde, "Fake News and Hate Speech in Nigeria's Development and Security Trajectory: A Qualitative Assessment," *Jurnal Pertahanan: Media Informasi Tentang Kajian Dan Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism Dan Integrity* 10, no. 1 (2024): 1, https://doi.org/10.33172/jp.v10i1.19369.

6 Luthfia Ayu Azanella and Bayu Galih, "Penjelasan Soal Foto Kampanye PKI DN Aidit Yang Terdapat Pria Mirip Jokowi," Kompas.com, 2018, https://nasional.kompas.com/read/2018/11/23/15185081/penjelasan-soal-foto-kampanye-pki-dn-aidit-yang-terdapat-pria-mirip-jokowi.

7 Edna Caroline Pattisina, "Prabowo Subianto, Pernah Dipecat atau Tidak?," kompas.id, 2024, https://www.kompas.id/baca/polhuk/2024/02/29/prabowo-pernah-dipecat-atau-tidak.

8 Daria Kravets et al., "Different Platforms, Different Plots? The Kremlin-Controlled Search Engine Yandex as a Resource for Russia's Informational Influence in Belarus during the COVID-19 Pandemic," *Journalism* 24, no. 12 (December 2023): 2762–80, https://doi.org/10.1177/14648849231157845.

narratives that imitate credible sources, making fabricated information more believable and more likely to be shared widely. Simultaneously, LLMs are increasingly being used in content moderation frameworks to identify and mitigate the spread of such disinformation. However, their effectiveness is inconsistent. A recent cross-lingual analysis of ChatGPT, Google Bard (now Gemini), and Bing Chat demonstrated that these platforms often reproduce false information or exhibit political bias, especially in underrepresented languages or politically sensitive contexts.[9] This inconsistency reflects the limitations of existing AI guardrails and filtering mechanisms. Moreover, the intentional manipulation of LLM behavior, such as through prompt injections or training data poisoning, has been identified as a growing tactic used by malicious actors to skew outputs toward false or politically motivated narratives.[10] Furthermore, actors intending to spread disinformation have already begun experimenting with prompt injections and LLM "poisoning" techniques, which manipulate model behaviour or training data to produce outputs that align with specific political agendas or falsehoods.[11] These trends highlight the need to distinguish between generative AI systems, which autonomously produce content, and non-generative systems, such as search engines, which amplify existing content through algorithmic ranking. Both types play a significant role in the spread of disinformation but require different legal and technical interventions to mitigate their impact.

Despite the scale of the threat, Indonesia's regulatory framework is not yet equipped to handle AI-generated disinformation. The existing regulations mostly focus on the ethical use of technology in general and have not touched on specific aspects related to AI-induced disinformation. When examined in the regulations governing the dimensions of information dissemination, Law Number 11 of 2008, which was updated with Law Number 19 of 2016 and lastly updated with Law Number 1 of 2024 on Electronic Information and Transactions (hereinafter referred to as 'ITE Law'), regulates the unlawful dissemination of information, including disinformation and fake news, which focuses on sanctions for disseminators of information (*natuurlijk persoon*) that are deemed to disturb the public or mislead, especially through digital media. However, the ITE Law does not specifically regulate the role of algorithms or AI technology in information dissemination. Furthermore, Minister of Communication and Information Regulation No. 5/2020 on Private Sphere Electronic System Operator ('Permenkominfo 5/2020') stipulates the responsibility of digital platforms in dealing with negative content, including fake news. However, there is no specific regulation to require digital platforms to directly monitor or moderate AI-generated content.

Research combining AI and disinformation has been discussed globally, such as: 1) Research conducted by Katarina Kertysova with the title "*Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation is Produced, Disseminated, and Can Be Countered*".[12] This article discusses the challenges and opportunities of using AI in information operations. It explores how AI can help fight online disinformation, discusses limitations as well as threats such as user profiling, microtargeting, and deepfakes, and reviews potential solutions to curb AI-powered disinformation. Ultimately, the article emphasises that building social resilience is key to dealing with future waves of disinformation; and 2) Research conducted by Noemi Bontridder and

[9] Aleksandra Urman and Mykola Makhortykh, "The Silence of the LLMs: Cross-Lingual Analysis of Guardrail-Related Political Bias and False Information Prevalence in ChatGPT, Google Bard (Gemini), and Bing Chat," *Telematics and Informatics* 96 (January 2025): 102211, https://doi.org/10.1016/j.tele.2024.102211.

[10] Mykola Makhortykh et al., "Stochastic Lies: How LLM-Powered Chatbots Deal with Russian Disinformation about the War in Ukraine," *Harvard Kennedy School Misinformation Review*, ahead of print, August 26, 2024, https://doi.org/10.37016/mr-2020-154.

[11] Jason Lucas et al., "Fighting Fire with Fire: The Dual Role of LLMs in Crafting and Detecting Elusive Disinformation," in *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing*, ed. Houda Bouamor, Juan Pino, and Kalika Bali (Singapore: Association for Computational Linguistics, 2023), 14279–305, https://doi.org/10.18653/v1/2023.emnlp-main.883.

[12] Katarina Kertysova, "Artificial Intelligence and Disinformation : How AI Changes the Way Disinformation Is Produced, Disseminated, and Can Be Countered," *Security and Human Rights* 29 (2018): 55–81, https://doi.org/10.1163/18750230-02901005.

Yves Poullet entitled "*The Role of Artificial Intelligence in Disinformation*".[13] AI systems play a major role in disinformation, exacerbating the problem by making it easier for certain parties to create and spread false content. This raises ethical and human rights issues, especially regarding dignity and freedom of expression. The European Union, through its Digital Services Act proposal, is pushing for transparency and auditing of large platform recommendation systems. The research notes that advertising-based business models on the web are a major cause of disinformation, and changes to these models could reduce their impact.

Based on previous research and creating a state of the art in this field, this research will discuss the regulation and problems faced in Indonesia, especially related to AI and disinformation in the context of digital democracy today. For this reason, there are two problem formulations that will be studied, namely: 1) How is AI regulated in relation to disinformation in Indonesia?; 2) How do legal frameworks compare across different jurisdictions?; and 3) What is the ideal legal construction to regulate AI that spreads disinformation in digital democracy? In this research framework, there are three discussions that will be studied. First, the author will analyse the algorithm used by AI and the author will analyse the regulations governing AI and disinformation in Indonesia. Furthermore, in the second discussion, the author will examine regulations in the European Union, the United States and China regarding AI and its relation to disinformation. In the third discussion, the author will propose the legal construction needed in regulating AI to prevent disinformation, so as to strengthen the foundation of digital democracy.

2. Method

This research uses a doctrinal legal method with a comprehensive approach, including a statutory approach, comparative study, and case analysis. The statutory approach is used to analyse the regulations governing AI and disinformation under positive law in Indonesia, with particular attention to the impact on democracy. In this analysis, emphasis is placed on legal aspects relating to responsibility, ethics, and protection of human rights, as well as evaluating the effectiveness of regulations in protecting the integrity of the democratic process from the spread of disinformation.

Further, a comparative study approach compares the applicable regulations in the European Union, the United States, and China with existing laws in Indonesia, focusing on identifying similarities and differences in the regulation of AI and disinformation and their impact on democracy. Finally, illustrative examples of AI-related disinformation approach is used to explore the social phenomena arising from disinformation provided by AI, which can affect public opinion and political participation. Secondary data used includes primary legal materials such as applicable laws and secondary legal materials such as journals and books, to create a structured, systematic, and comprehensive analysis, while strengthening the position of democracy amidst the challenges of disinformation.

3. Results and Discussion

3.1. Regulation of AI in the Spread of Disinformation in Indonesia

3.1.1. Artificial Intelligence Collecting Data: Learn More about Algorithm System

Artificial intelligence (AI) technology has various types of developments, one of which is Deep Learning. Deep learning provides the possibility to perform computations composed of several layers of processes to learn data representations from an abstract form.[14] Broadly defined, the analogy is that a human goes from having no knowledge of a concept to understanding it better when confronted with relevant data. Based on how the data is used, deep learning can be divided into three: supervised learning, unsupervised learning, and reinforcement learning. In particular, many commercial AI applications are modelled on supervised learning and some reinforcement learning. Supervised learning is a way of learning an AI model by providing

[13] Bontridder and Poullet, "The Role of Artificial Intelligence in Disinformation."

[14] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton, "Deep Learning," *Nature* 521, no. 7553 (2015): 436–44, https://doi.org/10.1038/nature14539.

data to the model and then training it until it is able to represent the trained data. That way, when faced with inputs that are similar (not the same) to the data, the AI model will output accordingly. With many publicly open datasets, this method is often practised for commercial AI models. Meanwhile, reinforcement learning is a method that trains the model based on the feedback received, in the form of reward and punishment. The model is set up in such a way that it will maximise the reward and minimise the punishment. This concept is generally used when developers want to give their side and users the opportunity to provide feedback. So that over time, the AI model will increasingly understand what output the user actually wants.

To simplify the explanation, an example of a commonly used AI product, such as ChatGPT will be used. For other models, it will have a similar concept and only a different algorithm configuration. However, it is important to clarify that GPT-like large language models (LLMs), such as ChatGPT, represent only one category of generative AI. These models are based on transformer architectures optimized for language processing, whereas other generative models, such as image-generation systems like DALL·E or Stable Diffusion, utilize distinct mechanisms. For instance, diffusion models work by learning to iteratively denoise random noise into a coherent image, a process fundamentally different from the token-by-token prediction in LLMs. Multi-modal models, such as GPT-4o or Google Gemini, also integrate architectures tailored to combine visual, textual, and sometimes auditory data, often incorporating cross-modal attention and vision-language pretraining strategies. These architectural differences reflect the varied goals and modalities of generative AI, making it inaccurate to generalize the GPT-like architecture as the standard for all AI-generated content.[15]

Based on the developer's statement, data collection is done by using all publicly accessible information on the internet, as the developers do not search for information through paid sites or the 'dark web'. They also use filters and remove unwanted information for their training model, such as blasphemy, adult content, sites that collect personal data, and spam.[16] Regarding the use of personal data, the amount of data available on the internet is often related to a person's personal data. Thus, the model also uses it for the learning mode. However, they state that the use of the collected data is only limited to the model training process, such as for prediction, reasoning, and problem solving.

ChatGPT claims that the process of training the model is basically providing associations between words and concepts. Through these associations, the model updates weights so that it is able to understand the relationship between words contextually. This approach utilises the transformer algorithm, which is a key framework in many modern language models. Transformers rely on the multi-head attention module, a sophisticated technique for capturing relationships between elements in sequential data such as words in a sentence.

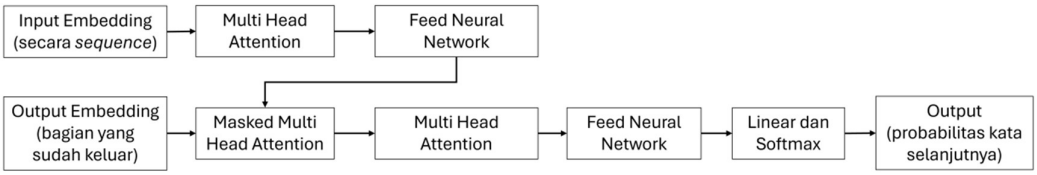


Figure 1. Flowchart of the attention module process in the transformer

Basically, grounding is done by directly associating two or more concepts. For example, to help models understand human language, words must be converted into numerical representations that are meaningful to computers, i.e. embedding. These embeddings are vector representations of words, which allow computers to understand the semantic relationships

[15] Chitwan Saharia et al., "Photorealistic Text-to-Image Diffusion Models with Deep Language Understanding," arXiv:2205.11487, preprint, arXiv, May 23, 2022, https://doi.org/10.48550/arXiv.2205.11487.

[16] OpenAI, "How ChatGPT and Our Foundation Models Are Developed | OpenAI Help Center," 2024, https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-foundation-models-are-developed.

between words. For example, the relationship between the words king and queen is represented as a vector relationship similar to the relationship between man and woman.

On the encoder side, each word in the input is converted into an embedding, which is then processed through the multi-head attention module. This module is designed to capture the relationship between words, even if the words are far apart in order. Multi-head attention works by:

A. Creating Query, Key, dan Value

Each embedding is projected into three separate spaces: query (Q), key (K), and value (V).

$$Q = XW_Q, \quad K = XW_K, \quad V = XW_V$$

With, W_Q, W_K, W_V are trainable weight matrices (containing trainable weights).

B. Calculating Attention Score

Attention score is calculated using the dot product between query and key, which is then normalised with SoftMax:

$$Attention(Q, K, V) = \mathbf{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V$$

Where d_k is the key dimension. This score indicates how strong the relationship between words in the input context is.

C. Head Multiple

Multiple parallel 'heads' (multi-heads) are used to allow the model to capture different types of relationships between words simultaneously. The result of the attention module is passed to the feed-forward network (FFN), which is a linear layer applied to each embedding position independently. This FFN allows the model to learn richer representations. The process is as follows:

$$FFN(x) = ReLU(xW_1 + b_1)W_2 + b_2$$

After passing through the FFN, the result is completed with residual connections (summation of initial inputs) and layer normalisation. As the stage after the encoder, the decoder has a similar structure to the encoder, but includes causal attention to ensure the model only looks at the previous words when predicting the next word. The main processes in the decoder are:

A. Masked Multi-Head Attention

This attention ensures that when generating the next word, the model does not 'see' the words that have not yet been generated. Masking is applied to the attention by assigning infinitely negative values to elements in the future.

B. Cross-Attention

In addition to masked attention, the decoder also has cross-attention to connect information from the encoder output with the decoder input. This process allows the decoder to understand the global context of the input.

C. Feed-Forward Network

Just like the encoder, the result of cross-attention is passed through FFN.

D. SoftMax Output

The final result of the decoder is a score that is passed to SoftMax to generate probabilities for all words in the vocabulary. The word with the highest probability is selected as the next output token.

The attention mechanism helps language models understand the relationships between words in context. By analyzing word embeddings and their meanings, the transformer architecture enables the model to recognize how a word's meaning can change depending on its use, for example, bank as in riverbank or bank as a financial institution. This ability to interpret words based on context is key to the accuracy of models like ChatGPT. While generative AI like ChatGPT creates content on its own, non-generative systems like search engines also influence the spread of disinformation. They don't produce content, but they often promote results that get more clicks, favoring emotional or attention-grabbing content over accurate information. This behavior is similar to social media algorithms and can reduce the visibility of reliable sources.[17] Empirical studies support this, showing that search engines like Yandex and Google tend to surface emotionally charged or politically biased content, especially during sensitive events.[18]

3.1.2. Indonesia Regulations on AI Related to Disinformation

Advances in AI technology have had a profound impact on various aspects of human life, especially in the way information is produced, disseminated, and consumed.[19] Amidst the easy access to information offered by digital technology, a serious new challenge has emerged, namely the spread of disinformation.[20] Disinformation, defined as false or misleading information spread deliberately to achieve a specific goal, is becoming increasingly easy to produce and spread through AI-based tools. In Indonesia, where democracy relies heavily on informed public participation, the spread of this disinformation can threaten the integrity of the political process, manipulate public opinion, and create distrust in institutions that are supposed to be the pillars of democracy.[21]

One of the most striking and worrying forms of AI-based disinformation is deepfake technology.[22] Deepfakes are capable of creating video or audio that appears very realistic yet is completely manipulated. For example, a video showing a political leader behaving inappropriately or saying things that were never said can easily influence public perception and create a negative stigma. When this kind of information spreads virally on social media platforms, the impact is not only limited to the individuals involved, but can also extend to damaging the reputation of institutions and exacerbating political dynamics, including influence on election results. Therefore, it is important to understand how AI technology plays a role in the spread of disinformation and what the implications are for democratic structures and social stability. Empirical research demonstrates that disinformation campaigns can measurably shift public sentiment during

[17] Axel Bruns, *It's Not the Technology, Stupid: How the 'Echo Chamber' and 'Filter Bubble' Metaphors Have Failed* Us, n.d.

[18] "Search Engine Manipulation to Spread Pro-Kremlin Propaganda | HKS Misinformation Review," accessed July 13, 2025, https://misinforeview.hks.harvard.edu/article/search-engine-manipulation-to-spread-pro-kremlin-propaganda/.

[19] Vicko Taniady and Steven Theonald Siahaan, "Artificial Intelligence and the Constitutional Court: A Newpath of Making Independent Decisions?," *Jurnal Kajian Pembaruan Hukum* 3, no. 2 (2023): 2, https://doi.org/10.19184/jkph.v3i2.41726.

[20] Botambu Collins et al., "Trends in Combating Fake News on Social Media – a Survey," *Journal of Information and Telecommunication* 5, no. 2 (2021): 247–66, https://doi.org/10.1080/24751839.2020.1847379.

[21] Yujitia Ahdarrijal and Dian Eka Rahmawati, "The Role of Digital Media in Determining the Direction of Indonesia's Democracy in 2023," *The Journal of Society and Media* 8, no. 1 (2024): 144–64, https://doi.org/10.26740/jsm.v8n1.p144-164.

[22] Felipe Romero Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content," *International Review of Law, Computers & Technology* 38, no. 3 (2024): 297–326, https://doi.org/10.1080/13600869.2024.2324540.

elections. For example, a study reported in SciELO Brazil revealed that 33% of X accounts discussing Rodrigo Duterte's ICC arrest in the Philippines were fake, responsible for over 1,300 posts, 7,000 engagements, and 11.8 million views and up to 45% of election-related conversation was driven by these inauthentic accounts.[23] In Brazil's 2018 presidential race, more than 90% of the population used WhatsApp, where marketing groups invested approximately R$12 million (~US$3 million) to send coordinated disinformation in private chats; one study found that 85% of Bolsonaro voters saw the false "gay kit" narrative, and 56% believed it.[24]

The ITE Law is the main legal basis for regulating the use of information technology, including the dissemination of digital content.[25] Previously, Article 27 paragraph (3) of the ITE Law regulated electronic defamation by prohibiting the intentional dissemination or transmission of electronic information or documents containing allegations that attacked another person's honour or reputation. Following the entry into force of Law No. 1 of 2023 on the Criminal Code on 2 January 2026, however, this provision is no longer applicable, and electronic defamation is principally regulated under Article 433 of the Criminal Code. By contrast, Article 28 paragraph (1) of the ITE Law, as amended by Law No. 1 of 2024, remains relevant to the dissemination of false or misleading electronic information that causes material loss to consumers in electronic transactions. Although the ITE Law does not explicitly regulate AI-generated content, its applicable provisions may still be used to address certain forms of false or misleading electronic information disseminated through AI-assisted systems. However, the main limitation in the Law is that it applies to the user (*natuurlijk persoon*) as a legal subject, without regulating AI algorithms or systems that operate automatically in spreading negative content.

Furthermore, Article 45A Paragraph (1) of the ITE Law stipulates criminal sanctions for perpetrators who spread misleading information and can cause polemics. However, although this regulation focuses on individual or group responsibility, the dissemination of information supported by AI is an area that is difficult to monitor, given the complexity of technology and the ease of access provided by digital platforms. The absence of regulations that directly target the use of AI technology in spreading negative content makes it difficult for the government to take action against perpetrators who use AI anonymously or automated systems to spread disinformation. One important regulation that also needs to be considered is Permenkominfo 5/2020. This regulation regulates the responsibility of electronic system operators (PSEs) to remove or moderate illegal content. However, Permenkominfo 5/2020 focuses more on the general aspects of negative content and does not provide specifications related to content generated or distributed by AI; hence, weaknesses in its implementation still occur.

Law No. 27 of 2022 on Personal Data Protection ('PDP Law') provides an essential legal framework in the context of the use of personal data, especially in relation to AI. In an era where personal data is used to target content specifically to users, the PDP Law serves to protect individuals from political manipulation that can occur through the use of data without consent. This is crucial to maintaining the integrity of democracy, where the public must be protected from misuse of data that can be used to spread misinformation or manipulate public opinion. By ensuring that data is treated ethically, the PDP Law contributes to efforts to build public trust in the political system and democratic institutions.

In another regulatory framework, Electronic System Operators (ESOs) have significant responsibilities in regulating and ensuring information security, especially in the context of using AI Chatbots as Electronic Agents.[26] This is explicitly regulated in Article 36 paragraph (1) of

[23] "Exclusive: Fake Accounts Drove Praise of Duterte and Now Target Philippine Election | Reuters," accessed July 13, 2025, https://www.reuters.com/world/asia-pacific/fake-accounts-drove-praise-duterte-now-target-philippine-election-2025-04-11/?utm_source=chatgpt.com.

[24] Gustavo Ferreira Santos, "Social Media, Disinformation, and Regulation of the Electoral Process: A Study Based on 2018 Brazilian Election Experience," *Revista de Investigações Constitucionais* 7 (January 2021): 429–49, https://doi.org/10.5380/rinc.v7i2.71057.

[25] Deni Achmad et al., "Legal Protection Against Victims of Doxing Crime in Indonesia," *Jurnal Bina Mulia Hukum* 8, no. 1 (2023): 92–105, https://doi.org/10.23920/jbmh.v8i1.1062.

[26] Gio Arjuna Putra, Vicko Taniady, and I. Made Halmadiningrat, "Tantangan Hukum: Keakuratan Informasi Layanan AI Chatbot Dan Pelindungan Hukum Terhadap Penggunanya," *Jurnal Rechts*

Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions ('PP PSTE'), which states that a PSE can organise its own electronic system or use an Electronic Agent. In this context, AI Chatbot functions as an intermediary that provides conversation-based services to the public, making it easier for them to access information.[27] As part of a PSE, AI Chatbot is also bound by the obligations set out in Article 3 paragraph (1) of PP PSTE, which asserts that PSEs must organise electronic systems in a reliable and convenient manner, and be responsible for the operation of these systems. This obligation becomes even more important when considering that disinformation can spread rapidly through AI, and that the public has the right to accurate and reliable information. As such, Article 8 of PP PSTE emphasises the importance of security, reliability and service continuity of the software used by PSEs. If the AI Chatbot cannot be relied upon to provide correct information, then the potential for the spread of disinformation will increase, which could be fatal to society and the democratic process.

Furthermore, Article 39 paragraph (1) of PP PSTE underlines the importance of public protection in the implementation of electronic systems, which is a crucial aspect in the use of AI Chatbots. In this context, the rights of the public must be fulfilled, including the right to obtain accurate information. When AI Chatbots spread false or misleading information, this not only harms individuals but can also disrupt the democratic process by shaping public opinion based on inaccurate data. In an era where disinformation can spread virally, the reliability of information provided by AI becomes increasingly important to maintain public trust in political institutions and processes.

Further, the Minister of Communication and Informatics Circular Letter No. 9 of 2023 on Ethics of Artificial Intelligence aims to ensure that the development and utilisation of AI in Indonesia is ethical, responsible, and safe for society.[28] Some of the key principles outlined include transparency, accountability, and fairness in the use of AI.

The principle of transparency demands that data processing by AI be understood by the public, especially if it involves personal data, so that people have an understanding of how AI works and what it is used for. The principle of accountability requires the developer to be responsible for the decisions or results produced by the AI, as well as providing a review mechanism in case of error or bias. Fairness emphasises the importance of avoiding bias and discrimination in AI design so that the technology functions fairly for all groups of society. This is particularly relevant in the era of digital democracy, where information spreads rapidly through technology, including AI, which can inadvertently or deliberately spread disinformation. When AI is used in digital information management, there is a high risk of it being used to spread misleading content or negatively influence public opinion, which may jeopardise democratic principles, public trust, and social stability.

However, the effectiveness of the implementation of this Circular Letter is very limited due to its non-legally binding nature and has no consequences or sanctions as stipulated in Law Number 12 Year 2011 on the Formation of Laws and Regulations ('P3 Law').[29] This makes the circular merely a moral guideline or advice that does not have sufficient execution power to regulate AI practices in the field. In the context of the threat of disinformation spreading in the era of digital democracy, the weak enforcement of AI ethics through this circular letter is a challenge. Without strict sanctions, the development and use of AI may continue to be carried out with disregard for the expected aspects of transparency, accountability, or fairness, including in cases where AI is used to spread disinformation quickly and widely.

Vinding: Media Pembinaan Hukum Nasional 12, no. 2 (2023): 2, https://doi.org/10.33331/rechtsvinding.v12i2.1258.

[27] Putra, Taniady, and Halmadiningrat, "Tantangan Hukum: Keakuratan Informasi Layanan AI Chatbot Dan Pelindungan Hukum Terhadap Penggunanya."

[28] Ferinda K. Fachri, "CEO Hukumonline Soroti Beberapa Peraturan Terkait AI di Indonesia," Hukumonline.com, 2024, https://www.hukumonline.com/berita/a/ceo-hukumonline-soroti-beberapa-peraturan-terkait-ai-di-indonesia-lt66c4ccd9763ce/.

[29] Cholida Hanum, "Analisis Yuridis Kedudukan Surat Edaran Dalam Sistem Hukum Indonesia," *Humani (Hukum Dan Masyarakat Madani)* 10, no. 2 (2020): 2, https://doi.org/10.26623/humani.v10i2.2401.

The existence of ethical regulations is actually important in dealing with the negative potential of AI, especially those that affect public opinion and social stability. However, without reinforcement through binding legal rules, it is difficult for the government to guarantee the implementation of AI ethics in Indonesia. As a result, these regulations, although well-intentioned, tend to be ineffective in minimising the risks of AI misuse in the digital era, especially in counteracting disinformation that can undermine the foundations of a healthy democracy.

The challenge of disinformation through AI in the context of Indonesian democracy is very important to note. AI algorithms have the potential to create what is known as an echo chamber, where users are only exposed to information that supports their own views.[30] This phenomenon contributes to the extreme polarisation of public opinion and erodes the quality of democracy, as it becomes increasingly difficult for people to obtain diverse and accurate information. A clear example can be seen in previous elections in Indonesia, where disinformation content was often utilised to spread misleading narratives, exacerbating tensions between communities. With the inability to effectively regulate AI, digital platforms may continue to distribute harmful content, negatively impacting public trust in democratic institutions, including the electoral process.

Amidst these challenges, it is important for Indonesia to develop regulations that are more comprehensive and responsive to the spread of AI-based disinformation. This includes increasing collaboration between the government, private sector and civil society to create an effective framework for combating disinformation. Public education is also key to building resilience against disinformation by improving individuals' ability to recognise and respond to inaccurate information. With these measures, it is hoped that democracy in Indonesia can be maintained and public participation can be enhanced, creating a healthier environment for public discourse and informed decision-making.

3.2. The European Union (EU), The United States (US), and China Regulations on AI Related to Disinformation

3.2.1. The European Union (EU)

The EU's regulation of AI and disinformation reflects a serious attempt to deal with the challenges arising from technological developments in the digital age. With the increasing use of AI in the production and distribution of information, the risk of spreading disinformation is heightened, which can threaten the integrity of society, democratic processes, and public trust in institutions. Disinformation can take many forms, such as fake news, image and video manipulation, and personalised content designed to reinforce a particular point of view.[31] Therefore, the European Union is committed to creating comprehensive regulations to address this issue.

The regulation proposed by the European Union, specifically through the framework of the European Union Artificial Intelligence Act ("EU AI Act"),[32] seeks to provide clear guidelines for the use of AI technology, especially in preventing the spread of disinformation that has the potential to undermine democracy. The EU AI Act aims to set high standards for the development and use of AI systems, with a focus on protecting society and ensuring the responsible use of technology.[33] One important aspect of this law is the classification of AI systems based on risk.

---

[30] Virani Wulandari, Gema Rullyana, and Ardiansah Ardiansah, "Pengaruh Algoritma Filter Bubble Dan Echo Chamber Terhadap Perilaku Penggunaan Internet," *Berkala Ilmu Perpustakaan Dan Informasi* 17, no. 1 (2021): 1, https://doi.org/10.22146/bip.v17i1.423.

[31] Esma Aïmeur, Sabrine Amri, and Gilles Brassard, "Fake News, Disinformation and Misinformation in Social Media: A Review," *Social Network Analysis and Mining* 13, no. 1 (2023): 30, https://doi.org/10.1007/s13278-023-01028-5; Ali Khan, Kathryn Brohman, and Shamel Addas, "The Anatomy of 'Fake News': Studying False Messages as Digital Objects," *Journal of Information Technology* 37, no. 2 (2022): 122–43, https://doi.org/10.1177/02683962211037693.

[32] Rofi Aulia Rahman, "Artificial Intelligence Regulation on Labour Market: Comparative Perspectives on the European Union Artificial Intelligence Act in the Indonesian Context," *Lex Scientia Law Review* 8, no. 1 (2024): 1, https://doi.org/10.15294/lslr.v8i1.3465.

[33] Celso Cancela-Outeda, "The EU's AI Act: A Framework for Collaborative Governance," *Internet of Things* 27 (2024): 1–11, https://doi.org/10.1016/j.iot.2024.101291.

The EU AI Act divides AI systems into four risk categories: minimal, limited, high, and unacceptable.[34] AI systems that have the potential to spread disinformation, such as algorithms used by social media platforms, are categorised as high-risk.

Article 6 of this regulation provides for the classification of high-risk AI systems. AI is considered high-risk if it is used as a safety component of a product or is a product itself regulated under EU legislation, and the product is required to undergo a conformity assessment by a third party prior to marketing. In addition, this article also covers AI listed in Annex III, with exceptions if the AI does not pose a significant risk to health, safety, or fundamental human rights. Exclusion criteria include AI that only performs narrow procedural tasks, supports the outcomes of human activities, or is used for decision pattern analysis without directly affecting human judgement. AI providers that claim their systems are not high-risk must document such assessments and fulfil registration obligations. Furthermore, Article 8 stipulates the compliance of high-risk AI systems with the requirements set out in the regulation. These AI systems must comply with the requirements by considering their intended use and the latest technological developments in the field of AI.

In addition, the risk management system as stipulated in Article 9 should be used as the basis for ensuring compliance. This Article also stipulates that if a product contains AI systems regulated by both this regulation and EU harmonised legislation (Annex I Part A), then the product provider is responsible for ensuring full compliance with all applicable requirements.

Article 9 of the EU AI Act regulates the risk management system for high-risk AI systems. This system must be designed, implemented, documented, and maintained throughout the system's lifecycle with an iterative process that includes regular review and updates. The main stages in the risk management system include the identification and analysis of known or foreseeable risks, evaluation of risks in the intended use or reasonably foreseeable misuse, analysis of data from post-market monitoring systems, and adoption of appropriate risk mitigation measures.

Article 9 of the EU AI Act related to risk management systems for high-risk AI is particularly relevant in preventing disinformation caused by AI. Risk identification and analysis, as outlined in Article 9(2)(a), can be used to detect potential disinformation arising from AI system usage, such as biases in datasets or algorithm designs that facilitate the spread of false information. Furthermore, risk evaluation for misuse, as stated in Article 9(2)(b), enables developers to predict scenarios where AI systems might be misused to generate or disseminate disinformation. Additionally, Article 9(6) of the EU AI Act mandates periodic audits and evaluations of high-risk AI systems. These audits aim to ensure that algorithms do not disseminate misleading content or violate applicable laws and that their operations are sufficiently transparent. This obligation reflects the European Union's commitment to addressing disinformation issues using a data-driven and evidence-based approach, providing assurance to the public that the AI systems employed have undergone rigorous evaluation processes. Stakeholder involvement is also emphasized in the EU AI Act.

Article 15 specifies that high-risk AI systems must be developed and designed to meet high standards of accuracy, resilience, and cybersecurity while performing consistently throughout their lifecycle. This aims to ensure the systems deliver reliable outputs under various conditions and are not prone to errors or defects that may arise. At every stage, from development to implementation, these systems need to be optimized for stable and robust performance.

In assessing the accuracy and reliability of high-risk AI systems, the European Commission collaborates with relevant parties, including metrology institutions and benchmarking organizations, to promote the development of benchmarks and appropriate measurement methodologies. This effort aims to establish objective guidelines and standards that can be widely applied across the industry, ensuring that developed AI systems have clear and measurable performance metrics. Moreover, Article 15(2) stipulates that accuracy levels and other relevant accuracy metrics must be included in the system's instructions for use. This ensures that users

[34] Claudio Novelli et al., "Taking AI Risks Seriously: A New Assessment Model for the AI Act," *AI & Society* 39, no. 5 (2024): 2493–97, https://doi.org/10.1007/s00146-023-01723-z.

have complete information about the expected accuracy levels of the system and can evaluate its performance in real-world environments.

The resilience of high-risk AI systems is another key concern. These systems must be able to withstand various disruptions, such as errors, defects, or inconsistencies that may occur in their operational environments. Technical and organizational measures must be implemented to enhance system resilience against potential disturbances. Resilience can be improved through the application of technical redundancy, such as backup plans or additional safeguards, ensuring uninterrupted operation even in challenging conditions. If the AI system continues to learn after deployment, its design should minimize the risk of biased outputs caused by feedback loops influencing inputs for subsequent operations and implement appropriate mitigation measures to manage such loops.

In addition, Article 15(5) requires high-risk AI systems to be protected from unauthorized third-party attempts to alter their use, output, or performance by exploiting system vulnerabilities. Cybersecurity solutions must be tailored to the relevant risks and specific situations of the system. Technical measures to address AI-specific vulnerabilities include prevention, detection, mitigation, and control of potentially harmful attacks, such as data poisoning during training, confidentiality attacks, or exploitable model weaknesses. This ensures the system's resilience to external threats and maintains its security throughout its use.

The relevance to digital democracy is profound, as disinformation can threaten the integrity of elections and undermine public trust in democratic institutions. With strict and transparent regulations through the EU AI Act, AI usage is expected to strengthen democratic processes, provide accurate and useful information to the public, and encourage more active public participation. This regulation aligns with the European Union's commitment to building a safe and transparent digital space. By ensuring that AI systems operate in compliance with ethical and legal standards, society will be better protected from potential manipulation and the spread of disinformation. In this context, the EU AI Act can be seen as a proactive step in creating an information ecosystem that supports democracy, emphasizing the importance of access to truthful and accurate information for informed public decision-making.

Furthermore, Article 50(4) of the EU AI Act states that deployers of AI systems capable of generating or manipulating images, audio, or video to create deepfakes are required to disclose that the content is artificially created or altered. This requirement does not apply if the content is used lawfully for detecting, preventing, investigating, or prosecuting criminal offenses. For content that is evidently artistic, creative, satirical, fictional, or similar in nature, the transparency obligation is limited to appropriately disclosing the presence of such generated or manipulated content without hindering the enjoyment or presentation of the work. Additionally, deployers of AI systems that generate or manipulate text intended to inform the public on matters of public interest must disclose the artificial nature of the content. However, this requirement does not apply if the content is used lawfully for detecting, preventing, investigating, or prosecuting criminal offenses, or if the AI-generated text has been subjected to human review or editorial oversight by an individual or organization with editorial responsibility for its publication.

The Digital Services Act ('DSA') issued by the European Union in 2020 is also a significant step in creating a stronger legal framework for digital platforms to face the challenge of disinformation.[35] The DSA aims to ensure that digital platforms take responsibility for the content they provide, especially unlawful content, including disinformation.[36] Through various articles in the DSA, it is expected that there will be increased transparency and accountability for digital service providers.

One important aspect of the DSA is its systemic risk assessment and mitigation framework for very large online platforms and very large online search engines. Article 34 requires providers of such services to identify, analyse, and assess systemic risks arising from the design and

[35] Luca Nannini et al., "Beyond Phase-in: Assessing Impacts on Disinformation of the EU Digital Services Act," *AI and Ethics*, 2024, 1–29, https://doi.org/10.1007/s43681-024-00467-w.

[36] Aina Turillazzi et al., "The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications," *Law, Innovation and Technology* 15, no. 1 (2023): 83–106, https://doi.org/10.1080/17579961.2023.2184136.

functioning of their services, including risks related to the dissemination and amplification of misleading or deceptive content, including disinformation. Article 35 further requires these providers to implement reasonable, proportionate, and effective mitigation measures addressing the identified systemic risks. The framework is particularly relevant to AI-generated disinformation because the DSA expressly requires attention to the role of algorithmic systems, including recommender and advertising systems, in amplifying such content. This approach places responsibility not simply on individual users who produce or disseminate information, but also on the design and operation of large-scale digital platforms through which information is distributed.

In the context of AI, the DSA also addresses the role of algorithmic systems in the dissemination and amplification of information. Providers of very large online platforms and very large online search engines are required to consider how the design and functioning of recommender systems, advertising systems, and other relevant algorithmic systems contribute to identified systemic risks. The DSA also establishes transparency requirements concerning recommender systems, thereby strengthening accountability for the way information is prioritised and presented to users.[37]

The link between DSA and democratic values is also very relevant. By providing a clear legal framework for addressing disinformation, the DSA can play a role in protecting the integrity of the democratic process. Accurate and reliable information is the foundation for people to make informed decisions, both in the context of elections and in everyday life. The DSA is expected to help reduce the spread of disinformation that has the potential to undermine public trust in democratic institutions and electoral processes.

The European Union's Code of Practice on Disinformation 2022 outlines strategic measures to tackle disinformation in greater depth through an approach that includes transparency, media literacy and demonetisation of misleading content.[38] One of the key points is the commitment to demonetise disinformation (Commitment 1), which requires digital service providers to not only monitor advertising, but also eliminate revenue from content that contains disinformation. This means that platforms must set strict policies to prevent false content from benefiting financially. By reducing economic incentives, the code effectively suppresses the impetus for bad actors to spread misleading content for financial gain, which has been one of the main drivers of disinformation on digital platforms.

In addition to demonetisation, the code also focuses on policing advertisements that contain disinformation (Commitment 2). Signatories that play a role in advertising are required to ensure that their ad systems are not misused to spread disinformation through paid messages or content. This is manifested through stricter verification and labelling policies, where platforms and advertising agencies are required to identify and block ads that do not meet credibility standards. This commitment is critical as disinformation often leverages legitimate-looking ads to reach a wide audience more quickly and effectively. Through this mechanism, the Code of Practice ensures that only adverts that meet the requirements of truthful information can appear on platforms, limiting the space for disinformation actors to operate freely.

In terms of education, the Code of Practice strengthens media literacy by including comprehensive educational measures (Commitment 17). These measures provide tools for the public to more critically assess the information they receive and distinguish between legitimate information and disinformation. Through public education and awareness campaigns, the EU seeks to create a strong bulwark of protection at the individual level to reduce the impact of disinformation on society at large.

[37] Steven M. Williamson and Victor Prybutok, “The Era of Artificial Intelligence Deception: Unraveling the Complexities of False Realities and Emerging Threats of Misinformation,” *Information* 15, no. 6 (2024): 6, https://doi.org/10.3390/info15060299.

[38] European Commission, “The 2022 Code of Practice on Disinformation,” 2024, https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

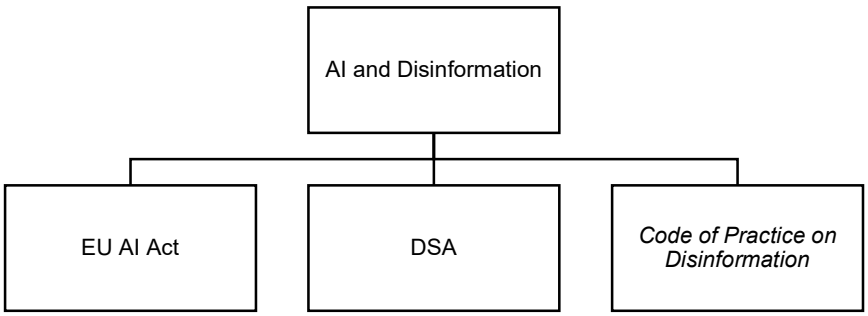


Figure 2. EU Regulation on AI and Disinformation
Source: Authors' Analysis

3.2.2. The United States (US)

The United States, as a global centre of innovation, faces major challenges related to the spread of artificial intelligence (AI)-enabled disinformation, especially in terms of its impact on democracy and public trust. While technological innovation has provided many benefits, the potential for AI to produce and spread false information raises serious concerns. To address this issue, the United States adopts a decentralised and sectoral regulatory approach, with various legal initiatives tailored to sector-specific needs at both the federal and state levels.

The National Artificial Intelligence Initiative Act of 2020 marks a significant milestone by establishing the Office of National AI Initiatives under the White House Office of Science and Technology Policy ("OSTP") responsible for overseeing and implementing the national AI strategy.[39] Under this regulation, the Office is also tasked with ensuring that AI development in the United States is aligned with ethical values and provides broad benefits to society. The Act also allocates substantial funding for AI research programmes, with $4.8 billion to the National Science Foundation for the 2025 budget.[40]

In 2024, the National Defense Authorization Act ('NDAA') further strengthens the role of AI as a tool for national security and defence by mandating the establishment of the Chief Digital and Artificial Intelligence Officer ('CDAO') Governing Council in Section 1521 of the NDAA.[41] The council is tasked with providing strategic guidance and oversight of the Department of Defence's digital and AI initiatives, and in section 350 of the NDAA, the US Navy is also ordered to develop and implement strategies related to the use of AI and automation across shipyards. The 2024 NDAA also includes important provisions related to the American Security Drone Act of 2023 (Sections 1821-1833), which prohibits the federal government and executive agencies from purchasing uncrewed aircraft systems (UAS) manufactured or assembled by a country listed as a 'covered foreign entity' under the definition in those sections, with limited exceptions. Federal agencies are also prohibited from using such UAS in their operations, including through contracted services. These restrictions apply to the use of federal grant funds, which are also subject to the same exceptions. The Act also requires the Office of Management and Budget, the U.S. Department of Homeland Security, the U.S. Department of Justice, and the National Institute of Standards and Technology, to work together to formulate a governmentwide procurement policy regarding the procurement of UAS, This provision will take effect two years after its

[39] American Institute of Physics, "National Artificial Intelligence Initiative Act of 2020," AIP, April 26, 2023, https://ww2.aip.org/fyi/federal-science-bill-tracker/116th/national-artificial-intelligence-initiative-act.

[40] Tony Samp et al., "Landmark artificial intelligence legislation advances toward becoming law," DLA Piper, 2020, https://www.dlapiper.com/es-pr/insights/publications/2020/12/landmark-artificial-intelligence-legislation-advances-toward-becoming-law.

[41] Dave McCarthy, "Highlights From the 2024 National Defense Authorization Act (NDAA) and What It Means for the Security Industry," Security Industry Association, January 30, 2024, https://www.securityindustry.org/2024/01/30/highlights-from-the-2024-national-defense-authorization-act-ndaa-and-what-it-means-for-the-security-industry/.

enactment, in December 2025. This effort aims to ensure that artificial intelligence technologies are used safely and in accordance with national defence and strategic objectives.[42]

In addition to federal policies, legislation at the state level also plays a significant role. The Colorado AI Act, signed by Colorado governor Jared Polis on 17 May 2024, emphasises consumer protection through the management of high-risk AI systems.[43] Under this law, AI service providers are required to implement appropriate risk mitigation measures to protect consumer data from misuse. This law will take effect on 1 February 2026.[44]

The New York Artificial Intelligence Bill of Rights (Assembly Bill A8129) was introduced on 13 October 2023, and is currently under consideration by The New York Assembly Science and Technology Committee. It is a bill created with the aim of establishing rights and protections for citizens regarding the use of AI-powered automated systems that affect their lives, ensuring these systems operate lawfully and with oversight. It covers a range of rights, including the right to be informed when automated systems are used, the right to understand how and why decisions are made by such systems, and the right not to be subjected to algorithmic discrimination as set out in §405. In addition, Senate Bill S8209 introduced on 12 January 2024, which is the Senate version of A8129, reflects the same provisions and aims to provide similar protections to New York residents.[45]

The decentralised and sectoral approach in the United States, which is generally more flexible than the risk-based regulatory framework adopted by the European Union. The Blueprint for an AI Bill of Rights published by the White House provides a non-binding national value framework, which aims to guide federal and state-level legislation in ensuring ethical and fair use of AI. The draft aims to protect the rights of individuals in the context of the use of automated systems, and provide guidance for legislation at the federal and state levels. The draft emphasises 5 key principles, namely:[46]

1. Safe and Effective Systems: Protection from unsafe or ineffective systems.
2. Protection against Algorithmic Discrimination: There should be no discrimination by algorithms; the system should be designed fairly.
3. Data Privacy: Protection from harmful data practices, with control over the use of personal data.
4. Notice and Explanation: Consumers should be informed when automated systems are used and understand how decisions are made.
5. Alternative Options: Consumers should be able to opt out of automated systems and have access to an operator to resolve any issues that arise.

Simultaneously, the National Institute of Standards and Technology (NIST) published the AI Risk Management Framework ("AI RMF") on 26 January 2023. The framework is designed to help organisations manage the risks associated with AI technology throughout its lifecycle. The framework consists of four main pillars: governance, risk mapping, risk measurement, and risk management.[47] NIST developed the AI RMF in response to the increasing use of AI technologies in various sectors, including healthcare, finance, transport, and security. As AI systems become more complex, it is important for organisations to have a systematic approach to managing the

[42] Jordan McDonald, "Congress Prioritizes AI, Modernization in Defense Funding Bill," GovCIO Media & Research, September 25, 2024, https://govciomedia.com/congress-prioritizes-ai-modernization-in-defense-funding-bill/.

[43] Arsen Kourinian, et al., "Colorado Governor Signs Comprehensive AI Bill," Mayer Brown, 2024, https://www.mayerbrown.com/en/insights/publications/2024/06/colorado-governor-signs-comprehensive-ai-bill.

[44] Stuart D. Levi et al., "Colorado's Landmark AI Act: What Companies Need To Know," Skadden, 2024, https://www.skadden.com/insights/publications/2024/06/colorados-landmark-ai-act.

[45] Digital Policy Alert, "United States of America: Introduced New York Artificial Intelligence Bill of Rights (S8209) Including User Rights to the State Senate," 2024, https://digitalpolicyalert.org.

[46] The White House, "FACT SHEET: Biden-Harris Administration Announces Key Actions to Advance Tech Accountability and Protect the Rights of the American Public | OSTP," 2022, https://business.cch.com/BFLD/BidenHarrisAdministration.pdf.

[47] Legit Security, "NIST AI Risk Management Framework Explained," 2024, https://www.legitsecurity.com/blog/nist-ai-risk-management-framework.

risks that may arise. Furthermore, in the United States, there is an approach through the Algorithmic Accountability Act that requires companies to disclose how their algorithms work and impact users so as to ensure fairness and prevent bias, including the potential spread of disinformation.

However, while regulation continues to evolve, major challenges remain, especially in addressing the potential misuse of AI to spread disinformation. Technologies such as deepfakes enable massive manipulation of content, which can alter public perception. For example, during the 2016 US Presidential Election, social media algorithms amplified conspiracy theories such as Pizzagate, which had a huge impact on public opinion.[48] In addition, specific policies such as Section 230 of the Communications Decency Act provide legal protection to digital platforms for content uploaded by users. This section states that "*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*." These protections, while designed to promote free speech, indirectly complicate efforts to address AI-based disinformation.[49]

The absence of a national risk-based framework in the United States has led to inconsistencies between states and weak enforcement. Existing policies focus more on the technical and economic aspects of AI, while social impacts such as disinformation have not received adequate attention. Therefore, strategic steps need to be taken immediately, including the adoption of elements of the EU approach such as risk classification of AI systems, periodic audits for high-risk systems, and strengthening the capacity of supervisory institutions to ensure transparency and fairness in the use of AI.

In addition, improving people's digital literacy through national education programmes is crucial to building social resilience. Tech companies should also be required to disclose how their algorithms work to regulators and the public to ensure transparency and accountability. In the face of these complex challenges, AI regulation in the United States requires a more integrated approach to determine the US government's perspective on AI entities, which will form the basis for the formulation of further policies or sectoral policies. Therefore, the establishment of integrated regulations at the federal level is crucial to ensure alignment between the central government and sectoral agencies in formulating more detailed and effective AI regulations. By strengthening the regulatory framework, improving enforcement, and integrating a risk-based approach, the United States can mitigate AI's negative impact on democracy while ensuring the technology is used ethically and responsibly.

3.2.3. China

The increasing use of AI around the world for propaganda and censorship purposes raises deep concerns regarding human rights and individual freedom. Concerns are characterised by the misuse of AI for disinformation that alarms both democratic and authoritarian regimes.[50] The expansion of AI algorithms in providing recommendations to users allows for the risk of misinformation due to the automation of work, as well as the lack of emotional and contextual awareness of AI models.[51] Concerns about the risk of misinformation are amplified by the growth of social media, which increases the acceleration of information dissemination. The acceleration

[48] BBC News, The Saga of "Pizzagate": The Fake Story That Shows How Conspiracy Theories Spread, BBC Trending, 2016, https://www.bbc.com/news/blogs-trending-38156985.

[49] Ambika Kumar and Tom Wyrwich, "The Test of Time: Section 230 of the Communications Decency Act Turns 20," Davis Wright Tremaine, 2016, https://www.dwt.com/blogs/media-law-monitor/2016/08/the-test-of-time-section-230-of-the-communications.

[50] Bilge Azgin and Sevki Kiralp, "Surveillance, Disinformation, and Legislative Measures in the 21st Century: AI, Social Media, and the Future of Democracies," *Social Sciences* 13, no. 10 (2024): 10, https://doi.org/10.3390/socsci13100510.

[51] Jeannette Paschen, "Investigating the Emotional Appeal of Fake News Using Artificial Intelligence and Human Contributions," *Journal of Product & Brand Management* 29, no. 2 (2019): 223–33, world, https://doi.org/10.1108/JPBM-12-2018-2179.

of information dissemination on social media allows unintended consequences to arise, especially due to the difficulty of recognising the veracity of information.[52]

One of China's efforts to address AI-generated disinformation was marked by the Draft Measures for Labelling Artificial Intelligence Generated Synthetic Content ("AI Labelling Draft") on 14 September 2024.[53] Based on Article 1 of the AI Labelling Draft, the regulation of AI content labelling aims to promote the healthy development of AI through the standardisation of labelling of synthetic content produced by AI to protect the rights and interests of citizens, legal entities, certain organisations, and safeguard the public interest of society.[54] The scope stipulated in the AI Labelling Draft includes the labelling of AI-generated synthetic content by online information service providers that meet the requirements on the management of algorithmic recommendations in internet information services, the provisions on the administration of deep synthesis internet information services, and the administration of generative AI services. However, the provisions of the AI Labelling Draft do not apply to the research and development or application of AI technologies whose services are not provided to the domestic public (Article 2 Draft Labelling AI).

The AI Labelling Draft classifies the labelling of synthetic content generated by AI into 2 (two) types, namely explicit labelling and implicit labelling. Explicit labelling is the labelling of generated synthetic content or interactive scenario interfaces that appear in the form of text, sound, or images, and can be clearly seen by the user. Meanwhile, implicit labelling is the labelling of the generated synthetic content data files using technical measures that are not easily perceived or known by the user (Article 3 Draft Labelling AI). The requirements for adding explicit labels on synthetic content, as stated in Article 4 of the Draft Labelling AI, state:

> *"Where the generative or synthesis services provided by service providers fall within the situations of the first paragraph of Article 17 of the Provisions on the Administration of Deep Synthesis Internet Information Services, explicit labels shall be added to the generated synthetic content in accordance with the following requirements.*
> *(1) Add labels such as text notifications, or notifications using common symbols, at appropriate positions in the beginning, end, or middle of text, or add conspicuous notification labels in interactive scenario interfaces or beside text;*
> *(2) Add labels such as voice notifications or audio and rhythmic notifications at appropriate positions in the beginning, end, or middle of audio, or add conspicuous notification labels in interactive scenario interfaces;*
> *(3) Add conspicuous notification labels in appropriate places in images;*
> *(4) Add conspicuous notification labels to video starting screens at appropriate positions around the video playback area; conspicuous notification labels may be added to the end and middle of the video at appropriate locations;*
> *(5) When presenting virtual scenes, conspicuous notification labels shall be added in appropriate positions on the starting screen, and conspicuous notification labels can be added in appropriate positions during the ongoing virtual scene services;*
> *(6) Explicit labels that are effective in giving conspicuous notice shall be added in other generation and synthesis service scenarios based on the characteristics of the applications.*
> *When service providers provide means such as for downloading, reproducing, or exporting generated synthetic content, they shall ensure that the files contain explicit labels that satisfy these requirements."*

[52] Rafharum Fatimah et al., "AI-Generated Misinformation: A Literature Review," *Indonesian Journal of Artificial Intelligence and Data Mining* 7, no. 2 (2024): 2, https://doi.org/10.24014/ijaidm.v7i2.26455.

[53] CMS Law-Now, "China Proposes New Regulations on AI-Generated Content Labelling," 2024, https://cms-lawnow.com/en/ealerts/2024/09/china-proposes-new-regulations-on-ai-generated-content-labelling.

[54] China Law Translate, Measures for Labeling of AI-Generated Synthetic Content (Draft for Solicitation of Comments), 2024, https://www.chinalawtranslate.com/ai-content-labels/.

The requirements relate to the conditions stipulated in Article 17 of the Provisions on the Administration of Deep Synthesis Internet Information Services, namely that providers of deep synthesis services that are likely to cause confusion or mislead the public must place a prominent label in a reasonable position on the edited or generated information content.[55] In addition to the inclusion of the content label, providers are also obliged to add a label to the file metadata that provides information on the synthetic content attributes, service provider name or code, and content reference number.

The regulatory plan in the draft labelling AI is also strengthened by the provision of sanctions against synthetic content that is not labelled, especially against content that causes serious consequences. The provision of sanctions against synthesis providers is stipulated in Article 22 of the Provisions on the Administration of Deep Synthesis Internet Information Services, which states that:

> *"Where Deep synthesis service providers and technical supporters violate these provisions, they are to be punished in accordance with relevant laws and administrative regulations; and where serious consequences were caused, heavier penalties are to be imposed in accordance with law.*
>
> *Where violations of public security are constituted, the public security organs are to give public security administrative sanctions in accordance with law; where a crime is constituted, criminal responsibility is pursued in accordance with law."*

The explanation of sanctions is regulated in a separate regulation as stated in Article 21 of the Measures for the Management of Generative Artificial Intelligence Services. In addition to regulating sanctions in accordance with laws and regulations, Article 21 also gives the relevant departments the authority to impose certain sanctions or warnings for violations that have not been regulated. If analysed further, service providers that spread disinformation can also be sanctioned. For further explanation of sanctions against synthetic content, as listed in the following table:

Table 1.
Sanctions against Service Providers

Regulation	Article	Analysis
Cybersecurity Law of the People's Republic of China (2017)	***Article 69*** *"Network operators who violate the provisions of this Law by engaging in any of the following conduct shall be ordered to take corrective action by the relevant competent authority; if the network operator refuses to take correct action or in serious circumstances, a fine of RMB50,000 to RMB500,000 shall be levied, and the directly responsible supervisor and other directly responsible personnel shall be subject to a fine of RMB10,000 to RMB100,000:*	Article 69 stipulates obligations for network operators as well as sanctions for violations. This provision aims to maintain cybersecurity, public order, and national security. Violations may incur fines of RMB 50,000 to RMB 500,000 for network operators. In addition, directly responsible supervisors and other responsible personnel may also be subject to personal fines of RMB 10,000 to RMB 100,000.
	i) Failure to comply with the requirements of relevant departments to take measures to stop the transmission of or delete information of which the publication or dissemination is prohibited by laws and administrative regulations;	This article identifies three main forms of offences. Firstly, failure of network operators to comply with orders of relevant authorities to stop transmission or delete information that is prohibited to be published or disseminated in accordance with laws

[55] China Law Translate, Provisions on the Administration of Deep Synthesis Internet Information Services, 2022, https://www.chinalawtranslate.com/deep-synthesis/.

Regulation	Article	Analysis
	i) Refusing or obstructing the supervisions and inspections carried out by authorities in accordance with law; *i) Refusal to provide technical support and assistance to public security authorities and State security authorities."*	and administrative regulations. Second, refusing or obstructing supervision and inspection conducted by the authority in accordance with the law. Third, refusing to provide technical support and assistance to public security authorities or state security authorities. This article demonstrates the Chinese government's approach to ensuring network operators' compliance with strict regulations, while strengthening control over information circulating in the digital space. By sanctioning not only entities but also responsible individuals, this provision emphasises the importance of personal responsibility in network management.
Order of the President of the People's Republic of China No. 84 about The Data Security Law of the People's Republic of China (2021)	***Article 44*** *"Where relevant regulatory departments performing data security oversight and management duties discover that data handling activities have larger security risks, they may give the relevant organizations and individuals a talking to in accordance with the authority and procedures provided, and require the relevant organizations or individuals to employ measures to correct or eliminate the risks."*	Article 44 gives regulatory authorities the power to take preventive action against data management activities that have high security risks. Authorities can summon relevant organisations or individuals for discussions and request that they take corrective measures to eliminate or mitigate such risks. This approach reflects the Chinese government's focus on preventing potential threats before risks develop into larger incidents.
	Article 51 *"Where the theft or other illegal acquisition of data or carrying out of data handling activities eliminates or restricts competition, or harms the lawful rights and interests of individuals or organizations, punishment is to be given in accordance with laws and administrative regulations."*	Article 51 provides for sanctions against illegal acts such as data theft or data management activities that harm competition or the rights of individuals and organisations. Such offences are subject to penalties in accordance with laws and administrative regulations. This article emphasises the importance of maintaining fairness in business competition and protecting the rights of individuals and organisations from data misuse.
	Article 52 *"Where violations of the provisions of this law cause harm to others, civil liability is to be borne in accordance with law.* *Where provisions of this Law are violated, constituting a violation of public security management, public security administrative sanctions are given in accordance with law; where a crime is*	Article 52 establishes legal responsibility for offences that cause harm to others. The perpetrator is required to bear civil liabilities in accordance with applicable legal provisions. In addition, if the offence involves disturbance of public order, public security administrative sanctions may be imposed. If the offence meets criminal elements, the perpetrator will be held criminally

Regulation	Article	Analysis
	constituted, criminal responsibility is pursued in accordance with law."	liable. This provision demonstrates a comprehensive approach to law enforcement, covering civil, administrative and criminal aspects. The overall provisions of this law reflect the Chinese government's holistic efforts to proactively manage data security. By combining preventive measures and strict sanctions, the regulation aims to protect data security, individual rights, and fair competition in the digital age.
Personal Information Protection Law of the People's Republic of China (2021)	***Article 66*** *"Where personal information is handled in violation of this Law, or where the obligations for the protection of personal information provided for in this Law are not performed in handling personal information, the departments performing duties on personal information protection are to order corrections, give warnings, and confiscate unlawful gains; applications that illegally handle personal information are to be ordered to have their provision of services suspended or stopped, and a fine of up to 1,000,000 RMB is to be given; the directly responsible managers and other directly responsible personnel are to be given a fine of between 10,000 and 100,000 RMB.*	Article 66 provides for sanctions against violations in the management of personal information. When personal information is managed in violation of the law or data protection obligations are not fulfilled, the authority in charge of personal information protection may order rectification, issue warnings, and confiscate ill-gotten gains. In addition, an app that illegally manages personal information may be ordered to discontinue or suspend its services, accompanied by a fine of up to 1,000,000 RMB. Directly responsible individuals, including relevant managers and staff, may be subject to fines of between 10,000 and 100,000 RMB.
	Where the circumstances of the illegal activities provided for in the preceding paragraph are serious, the provincial level or higher departments performing personal information protection duties are to order corrections, confiscate unlawful gains, and give a concurrent fine of up to 50,000,000 RMB or up to 5% of the preceding year's business income, and may order that operation be suspended, suspend operations for rectification, or report to relevant regulatory departments for the cancellation of business permits or licenses; and a fine of between 100,000 and 1,000,000 RMB is to be given to the directly responsible managers and other directly responsible personnel, and a decision may be made to prohibit their serving as the board member, supervisor, senior management, or person in charge of personal information protection for an enterprise during a set period of time."	If the offence is serious, more severe sanctions apply. Provincial or higher-level authorities may order rectification, confiscate illegal profits, and impose fines of up to 50,000,000 RMB or 5% of the company's annual revenue in the previous year. In addition, business operations may be temporarily suspended for rectification, or business licences may be cancelled through reporting to relevant regulators. Directly responsible individuals may be subject to a fine of between 100,000 to 1,000,000 RMB. Furthermore, the individual may be prohibited from serving as a board member, supervisor, senior management, or person in charge of personal information protection for a period of time.

Regulation	Article	Analysis
	Article 71 *"Where provisions of this Law are violated, constituting a violation of the administration of public security, public security administrative sanctions are given in accordance with law; where a crime is constituted, criminal responsibility is pursued in accordance with law."*	Article 71 clarifies that violations of this law that also violate public security administration will be subject to administrative sanctions under applicable law. Where the offence meets criminal elements, criminal liability will be imposed.

3.2.4. Spatial Ontology and Post-Territorial Paradigms in AI Regulation

Based on the comparative analysis of the legal frameworks of the European Union, the United States, and China, it is evident that each jurisdiction seeks to formulate regulatory mechanisms to address AI-driven disinformation. The EU takes a risk-based, rights-oriented approach, placing strict obligations on high-risk systems through the AI Act and the Digital Services Act. The US relies on a decentralized, sectoral model that weighs consumer protection against constitutional speech guarantees. China takes a state-centric, security-oriented approach built on labelling requirements, censorship, and administrative sanction.

The divergence of these approaches is shaped by distinct cultural and social contexts, which in turn influence differing perspectives and responses to the issue of AI disinformation. Despite these variations and the potential for legal transplants or cross-border regulatory influence each jurisdiction remains fundamentally tied to territorially bounded legal paradigms.

That territorial limit of jurisdiction in addressing disinformation become particularly urgent in relation to the question of AI sovereignty, which reflects states' efforts to enforce digital sovereignty as a means of controlling infrastructure, data, and information flows within their territories.[56] However, the ability of AI to generate disinformation through decentralized, cross-border digital infrastructures significantly undermines the effectiveness of such sovereignty claims in shaping the development, distribution, and use of AI. Algorithms and databases that operate across multiple jurisdictions render national laws incapable of addressing the non-spatial nature of AI applications. This situation produces an ontological mismatch: a fundamental misalignment between the posthuman, networked operational logic of AI and the modern legal assumption of bordered sovereignty. AI no longer functions solely through human actors or specific institutions, but through mechanisms of self-learning and global data distribution that transcend territorial boundaries. In contrast, modern legal systems continue to presume territorial sovereignty as the primary parameter of regulatory effectiveness. As a result, AI sovereignty often remains at the level of a normative ideal, difficult to realize when confronted with the deterritorialized nature of AI technologies.

From the perspective of spatial ontology, this ontological mismatch requires jurisdiction to be reconceptualized beyond geographical territory alone. Spatial ontology understands digital space as constituted by dynamic networks, data flows, and algorithmic interactions rather than fixed physical locations.[57] Consequently, jurisdiction in AI governance should not be determined exclusively by where an AI model is developed, where a server is physically located, or where a platform is incorporated. Instead, a post-territorial paradigm emphasizes the functional relationships created by AI systems, including where AI-generated content is disseminated, where legal harm materializes, which users are targeted, and how algorithmic systems operate across multiple jurisdictions. As Dan Svantesson argues, the increasing deterritorialization of digital technologies necessitates a reconceptualization of jurisdiction based on substantial

[56] Huw Roberts, "Digital Sovereignty and Artificial Intelligence: A Normative Approach," *Ethics and Information Technology* 26, no. 4 (December 2024): 70, https://doi.org/10.1007/s10676-024-09810-5.

[57] Dan Svantesson, "A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft," *AJIL Unbound* 109 (January 2017): 69–74, https://doi.org/10.1017/S2398772300001197.

connections and the location of legally relevant effects rather than rigid territorial boundaries.[58] Similarly, Julie Cohen observes that information technologies fundamentally disrupt conventional territorial assumptions by creating regulatory spaces that transcend national borders and require new jurisdictional logics to govern networked environments.[59]

This post-territorial understanding does not eliminate state sovereignty but redefines how sovereignty is exercised within transnational digital ecosystems. Rather than relying solely on territorial control, states increasingly regulate AI through the locus of harmful effects, obligations imposed on digital intermediaries, extraterritorial regulatory mechanisms, and international cooperation. The European Union's Digital Services Act, for example, applies certain obligations to online platforms regardless of where they are established when their services are directed toward users within the Union. Such regulatory developments demonstrate an emerging shift from territorially bounded jurisdiction toward governance based on functional regulatory connections.

The practical significance of this paradigm is evident in AI-generated disinformation affecting Indonesia. Consider a scenario in which disinformation intended to manipulate public opinion during an Indonesian general election is generated using a foundation model developed in the United States, fine-tuned by developers in another jurisdiction, hosted on cloud infrastructure in Singapore, and disseminated through a global social media platform to Indonesian users. Although the legal harm, such as electoral manipulation, public disorder, or democratic interference, occurs primarily within Indonesia, the actors responsible for developing, deploying, and distributing the AI-generated content are dispersed across multiple jurisdictions governed by different legal regimes. Under a conventional territorial approach, Indonesian authorities may exercise jurisdiction only over actors or infrastructure located within Indonesian territory, creating regulatory gaps where foreign developers, AI providers, or digital platforms remain beyond effective domestic enforcement. A post-territorial approach instead recognizes that jurisdiction should be informed by the location of the legal effects, the intended target audience, the transnational circulation of data, and coordinated mechanisms of international regulatory cooperation. Accordingly, jurisdiction becomes a multidimensional legal framework that allocates regulatory responsibility across interconnected actors rather than a purely territorial exercise of sovereign authority. This operationalization of spatial ontology demonstrates that AI-generated disinformation cannot be effectively regulated through territorially bounded legal frameworks alone. Instead, the cross-border architecture of AI systems requires jurisdictional models capable of responding to distributed technological infrastructures, transnational data ecosystems, and multi-layered regulatory responsibilities. A post-territorial paradigm therefore provides a more appropriate conceptual foundation for AI governance by aligning legal authority with the networked spatiality through which AI systems generate and disseminate disinformation across borders.

3.3. Strategic Steps to Regulate the Dissemination of Disinformation by AI

The comparative analysis of the regulatory frameworks adopted by the European Union, the United States, and China demonstrates that no single jurisdiction has yet developed a comprehensive legal model capable of effectively addressing AI-generated disinformation. While each framework reflects different regulatory priorities, they collectively reveal common challenges concerning jurisdiction, accountability, transparency, and enforcement. These findings provide an important foundation for developing a regulatory framework that is responsive to Indonesia's constitutional values, institutional capacity, and digital governance landscape.

The rapid development of generative artificial intelligence has fundamentally transformed the production and dissemination of information. AI systems are capable of autonomously generating and amplifying content at an unprecedented scale, allowing disinformation to spread rapidly across digital platforms without direct human intervention. As a result, conventional regulatory approaches that primarily attribute legal responsibility to natural or legal persons are

[58] Dan Jerker B. Svantesson and Dan Jerker B. Svantesson, Solving the Internet Jurisdiction Puzzle (Oxford, New York: Oxford University Press, 2017).

[59] Julie Cohen, “Cyberspace As/And Space,” *Georgetown Law Faculty Publications and Other Works*, January 1, 2007, https://scholarship.law.georgetown.edu/facpub/807.

increasingly inadequate when AI systems operate through complex interactions involving developers, deployers, platform providers, and end users.[60] Therefore, an adaptive regulatory approach is needed, both to address immediate needs in the short term and to build a strong regulatory foundation in the long term.

3.3.1. Short-term Solution: Establishment of Presidential Regulation on AI

Given the rapid advancement of artificial intelligence technologies and the absence of a dedicated legal framework governing AI in Indonesia, the immediate regulatory priority should be the issuance of a Presidential Regulation (*Peraturan Presiden or Perpres*) on Artificial Intelligence. The choice to enact a Perpres, rather than other regulations, is based on several practical and legal reasons. Based on P3 Law, a Presidential Regulation has a faster and simpler formation process compared to a law or government regulation.[61] This allows the government to respond swiftly to urgent needs and new challenges in the digital space, especially as the urgency of AI regulation is growing amidst the increasing spread of disinformation through digital media.

A Presidential Regulation constitutes the most feasible short-term legal instrument because it can be enacted more expeditiously than a statute while providing an immediate regulatory basis for AI governance within the existing legislative hierarchy. Pursuant to Law Number 12 of 2011 on the Formation of Laws and Regulations, as amended by Law Number 13 of 2022, a Presidential Regulation may be issued to implement existing legislation and to facilitate the exercise of executive authority. Consequently, a Perpres may operationalise the general obligations contained in the Electronic Information and Transactions Law and Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE) by introducing AI-specific regulatory standards.

The proposed Presidential Regulation should establish minimum governance requirements applicable to providers and deployers of generative AI systems operating within Indonesia.[62] At a minimum, the regulation should contain four principal obligations. First, AI-generated content that is reasonably capable of influencing public opinion or democratic processes should be clearly identified through mandatory labelling requirements to enhance transparency and enable users to distinguish synthetic content from human-generated information. Second, providers of high-risk AI systems should be required to conduct periodic risk assessments identifying the potential dissemination of disinformation and the mitigation measures implemented to reduce such risks. Third, Electronic System Providers (*Penyelenggara Sistem Elektronik* or PSEs) integrating generative AI should adopt reasonable and proportionate measures to detect, report, and mitigate AI-generated disinformation distributed through their platforms. Finally, providers should submit periodic transparency reports to the Ministry of Communication and Digital Affairs (*Kementerian Komunikasi dan Digital* or Komdigi), detailing the deployment of AI systems, the volume of AI-generated content identified, and the measures taken to address harmful outputs.

To ensure effective implementation, the Presidential Regulation should clearly allocate institutional responsibilities. Komdigi should function as the lead regulatory authority responsible for supervising compliance, issuing technical standards, and imposing administrative sanctions for non-compliance. Sector-specific regulators should retain complementary responsibilities within their respective jurisdictions. For instance, the General Elections Commission (*Komisi Pemilihan Umum* or KPU) and the Election Supervisory Agency (*Badan Pengawas Pemilihan Umum* or Bawaslu) should oversee the use of AI-generated content during electoral campaigns,

---

[60] Bérénice Boutin, "State responsibility in relation to military applications of artificial intelligence," *Leiden Journal of International Law* 36, no. 1 (2023): 133–50, https://doi.org/10.1017/S0922156522000607.

[61] Rahayu Prasetianingsih, "Menakar Kekuasaan Presiden dalam Pembentukan Peraturan Perundang-undangan Menurut Undang-Undang Dasar 1945," *Padjajaran Jurnal Ilmu Hukum* 4, no. 2 (2017): 263–80; Chandra Yusuf, "Dampak Pemisahan Kewenangan antara Mahkamah Konstitusi dan Mahkamah Agung dalam Menginterpretasikan Undang-undang dan Peraturan Dibawahnya," *Jurnal Hukum Unissula* 37, no. 2 (2021): 85–100, https://doi.org/10.26532/jh.v37i2.17377.

[62] Angga Prastyo, "Limitation of Meaningful Participation Requirements in the Indonesian Law-Making Process," *Jurnal Hukum dan Peradilan* 11, no. 3 (2022): 3, https://doi.org/10.25216/jhp.11.3.2022.405-436.

while the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara* or BSSN) should develop technical standards concerning cybersecurity and AI system integrity. Such a coordinated allocation of authority would reduce institutional fragmentation and improve regulatory consistency across sectors.

In addition to the reporting mechanism, the Presidential Regulation could also stipulate periodic audits and risk evaluation. For example, the government could require digital platforms and AI providers to conduct an evaluation of the potential spread of disinformation that may be generated by their algorithms. This will provide temporary protection and serve as a mitigative measure against the adverse impact of disinformation by AI.

From a practical perspective, the adoption of a Presidential Regulation is legally and administratively feasible because it does not require the establishment of a new regulatory institution or substantial legislative reform. Instead, it builds upon the existing institutional framework governing digital platforms under PP PSTE. Nevertheless, implementation may encounter resistance from digital platforms due to increased compliance costs associated with transparency obligations, AI risk assessments, and mandatory content labelling. To address these concerns, the regulation should adopt a phased implementation strategy by initially applying enhanced obligations only to high-risk AI systems and large digital platforms whose services have significant societal impact. Such an approach would balance regulatory effectiveness with innovation while allowing both regulators and industry sufficient time to develop the necessary technical and institutional capacity.

3.3.2. Long-term Solution: Comprehensive AI-Specific Regulation

While the proposed Presidential Regulation and amendments to PP PSTE provide immediate and medium-term responses to AI-generated disinformation, these instruments remain limited in their capacity to address the broader governance challenges posed by artificial intelligence. They primarily regulate AI through the existing framework governing electronic systems and digital platforms rather than recognising AI as a distinct regulatory subject requiring comprehensive governance. Accordingly, Indonesia's long-term regulatory strategy should culminate in the enactment of a dedicated Artificial Intelligence Act that establishes a coherent legal framework governing the development, deployment, and use of AI across both the public and private sectors.

As reflected in the legal adage *inde datae leges ne fortior omnia posset* (laws must be made, otherwise, important or powerful people have unlimited power)[63]; in light of this, the law must be able to adapt, especially to the rapid development of technology. This principle is particularly relevant in the context of artificial intelligence, where the rapid development of generative AI has fundamentally transformed the production and dissemination of information. As AI systems increasingly generate and amplify content with limited human intervention, the absence of a comprehensive legal framework creates regulatory gaps that may be exploited, thereby undermining transparency, accountability, democratic integrity, and public trust. A dedicated AI Act is therefore necessary to ensure that technological innovation develops within a legal framework capable of protecting both individual rights and the public interest.

The comparative analysis undertaken in this research demonstrates that no single jurisdiction provides a complete regulatory model for AI-generated disinformation. Nevertheless, each jurisdiction offers regulatory approaches that may be adapted to Indonesia's legal system. The European Union demonstrates the effectiveness of a risk-based regulatory framework through the AI Act by imposing differentiated obligations according to the level of risk posed by AI systems. China illustrates the importance of imposing due diligence obligations upon digital platforms together with mandatory transparency requirements for AI-generated content, while developments in the United States increasingly emphasise algorithmic accountability and corporate governance despite the absence of comprehensive federal legislation. Rather than transplanting these models directly, Indonesia should adopt a contextual approach by integrating

[63] Faizal Kurniawan et al., "The Principle of Balance Formulation as the Basis for Cancellation of Agreement in Indonesia," Lex Scientia Law Review 6, no. 1 (June 2022): 1, https://doi.org/10.15294/lesrev.v6i1.55468.

their complementary strengths into a unified legislative framework that reflects Indonesia's constitutional values, administrative structure, and digital governance priorities.

A comprehensive Artificial Intelligence Act should therefore be built upon four principal regulatory pillars. First, the legislation should adopt a risk-based regulatory framework that classifies AI systems according to the level of risk they pose to fundamental rights, public order, democratic processes, and national security. AI systems capable of generating or disseminating disinformation that may influence elections, public health, financial markets, or other matters of significant public interest should be categorized as high-risk AI systems. Providers and deployers of such systems should therefore be required to comply with enhanced obligations, including mandatory transparency, comprehensive risk assessments, human oversight, periodic conformity assessments, and independent compliance audits.

Second, the legislation should establish clear legal responsibilities throughout the AI value chain. Existing Indonesian regulations primarily impose obligations upon Electronic System Providers (PSEs), which is no longer sufficient given the distributed nature of AI development and deployment. Instead, the AI Act should distinguish between AI developers, AI deployers, digital platform operators, and end users, assigning legal obligations proportionate to their respective roles. Developers should ensure that AI systems are designed in accordance with principles of safety, transparency, accountability, and privacy by design. Deployers should conduct context-specific risk assessments before implementing AI systems in high-impact sectors, while digital platform operators should establish effective mechanisms to detect, label, and mitigate AI-generated disinformation distributed through their services. Such differentiation would improve legal certainty by allocating responsibility according to each actor's degree of control over AI systems and their capacity to prevent harm.

Third, the legislation should strengthen institutional governance and regulatory coordination. The Ministry of Communication and Digital Affairs (Komdigi) should function as the central coordinating authority responsible for AI governance, regulatory supervision, and the issuance of technical implementation guidelines. The National Cyber and Crypto Agency (BSSN) should continue developing cybersecurity standards and technical requirements relating to AI systems, while sector-specific regulators should retain supervisory authority within their respective jurisdictions. For example, the General Elections Commission (KPU) and the Election Supervisory Agency (Bawaslu) should regulate the use of AI during electoral processes, whereas financial, health, and other sectoral regulators should oversee AI deployment within their respective sectors. In addition, the establishment of a National Artificial Intelligence Advisory Council comprising representatives from government, academia, industry, and civil society should be considered to provide policy recommendations, ethical guidance, and technical expertise. Rather than functioning as an additional regulatory authority, this body would strengthen evidence-based policymaking and improve coordination among existing institutions.

Fourth, the legislation should introduce a comprehensive enforcement and accountability framework. Administrative sanctions should include written warnings, administrative fines, mandatory corrective measures, temporary suspension of AI-related services, and revocation of operating licenses for serious or repeated violations. Civil liability mechanisms should also be available where AI-generated disinformation causes demonstrable harm to individuals or the public. Such graduated enforcement measures would strengthen legal certainty while encouraging compliance through proportionate regulatory responses.

Given the inherently transnational nature of AI systems, the proposed legislation should further incorporate mechanisms for international regulatory cooperation. AI-generated disinformation frequently involves developers, cloud infrastructure, foundation models, and digital platforms operating across multiple jurisdictions, thereby limiting the effectiveness of purely domestic regulation. Consequently, the AI Act should establish a legal basis for information sharing, mutual administrative assistance, cooperation in regulatory enforcement, and participation in international AI governance initiatives. Such provisions would strengthen Indonesia's ability to address cross-border AI-related harms while promoting regulatory interoperability with foreign jurisdictions.

From a feasibility perspective, the enactment of a comprehensive Artificial Intelligence Act represents the final stage of Indonesia's AI governance roadmap and therefore requires

substantial political commitment, institutional capacity, and stakeholder engagement. Technology companies may oppose increased compliance obligations, including mandatory transparency, algorithmic auditing, and independent conformity assessments, while government agencies may express concerns regarding institutional overlap and implementation capacity. These challenges, however, can be mitigated through meaningful public participation during the legislative process, extensive consultation with industry and civil society, and a phased implementation schedule that allows regulators and AI providers to progressively adapt to new regulatory obligations. Moreover, the institutional experience gained through implementing the Presidential Regulation and the amended PP PSTE will provide an important administrative foundation for comprehensive AI legislation.

Ultimately, the enactment of an Artificial Intelligence Act should be understood not merely as the adoption of another sectoral regulation, but as the culmination of Indonesia's long-term AI governance strategy. By integrating risk-based regulation, differentiated legal responsibilities, coordinated institutional governance, effective enforcement mechanisms, and international regulatory cooperation within a single legislative framework, the proposed AI Act would establish a coherent and adaptive legal system capable of regulating AI-generated disinformation while simultaneously promoting technological innovation, protecting democratic integrity, and safeguarding fundamental rights.

4. Conclusion

Indonesia's current regulatory framework is inadequate to address the escalating threat of AI-generated disinformation. While existing regulations provide a general basis for handling harmful digital content, they fail to specifically target AI-generated material or define distinct responsibilities for AI developers, platforms, and users. Consequently, Indonesia urgently requires a more specific and adaptive regulatory framework to tackle these unique risks.

A comparative analysis reveals three distinct regulatory paradigms. The European Union employs a comprehensive, risk-based, and transparency-oriented framework (e.g., the AI Act and the DSA). China focuses on state control, mandatory content labeling, and strict liability for service providers. In contrast, the United States adopts a decentralized, sector-specific approach that relies heavily on voluntary guidelines and targeted initiatives.

Drawing on these international approaches, this study proposes a phased regulatory model tailored to Indonesia's context. In the short term, a Presidential Regulation should be issued to provide immediate guidance on transparency, risk assessment, and institutional governance. In the medium term, existing regulations must be strengthened to establish clearer accountability for electronic system operators. Ultimately, in the long term, Indonesia should enact comprehensive, risk-based AI legislation that delineates responsibilities and establishes coordinated oversight. This adaptive framework aims to safeguard the integrity of information and democratic processes without stifling technological innovation.

However, this study has certain limitations, primarily due to the rapidly evolving nature of AI technology and the research's focus on a limited number of comparative jurisdictions. Future research should explore practical enforcement mechanisms for this proposed regulatory framework within Indonesia and examine the specific impact of AI-generated disinformation on democratic processes, such as national elections.

Data availability statement

The participants of this study did not provide written consent for their data to be publicly shared. Consequently, due to the sensitive nature of the research, supporting data is not available.

Ethical approval

Not applicable. This study did not involve human participants, animals, or sensitive data requiring ethical clearance.

Consent to participate

Not applicable. No human participants were involved in this study.

Consent to publish

Not applicable. This study does not contain any individual person's data in any form (including individual details, images, or videos).

Funding Statement

None.

Conflict of Interest Statement

No potential conflict of interest was reported by the authors

References

Achmad, Deni, Muhammad Farid, Rasti Putri Januarti, and Alyfia Syavira. "Legal Protection Against Victims of Doxing Crime in Indonesia." *Jurnal Bina Mulia Hukum* 8, no. 1 (2023): 92–105. https://doi.org/10.23920/jbmh.v8i1.1062

Ahdarrijal, Yujitia, and Dian Eka Rahmawati. "The Role of Digital Media in Determining the Direction of Indonesia's Democracy in 2023." *The Journal of Society and Media* 8, no. 1 (2024): 144–64. https://doi.org/10.26740/jsm.v8n1.p144-164.

Aïmeur, Esma, Sabrine Amri, and Gilles Brassard. "Fake News, Disinformation and Misinformation in Social Media: A Review." *Social Network Analysis and Mining* 13, no. 1 (2023): 30. https://doi.org/10.1007/s13278-023-01028-5.

American Institute of Physics. "National Artificial Intelligence Initiative Act of 2020." AIP, April 26, 2023. https://www.congress.gov/bill/116th-congress/house-bill/6216/text

Azanella, Luthfia Ayu, and Bayu Galih. "Penjelasan Soal Foto Kampanye PKI DN Aidit Yang Terdapat Pria Mirip Jokowi." Kompas.com. 2018. https://nasional.kompas.com/read/2018/11/23/15185081/penjelasan-soal-foto-kampanye-pki-dn-aidit-yang-terdapat-pria-mirip-jokowi.

Azgin, Bilge, and Sevki Kiralp. "Surveillance, Disinformation, and Legislative Measures in the 21st Century: AI, Social Media, and the Future of Democracies." *Social Sciences* 13, no. 10 (2024): 10. https://doi.org/10.3390/socsci13100510.

BBC News. The Saga of Pizzagate: The Fake Story That Shows How Conspiracy Theories Spread. BBC Trending. 2016. https://www.bbc.com/news/blogs-trending-38156985.

Bontridder, Noémi, and Yves Poullet. "The Role of Artificial Intelligence in Disinformation." *Data & Policy* 3 (2021): 1–21. https://doi.org/10.1017/dap.2021.20.

Boutin, Bérénice. "State responsibility in relation to military applications of artificial intelligence." *Leiden Journal of International Law* 36, no. 1 (2023): 133–50. https://doi.org/10.1017/S0922156522000607.

Bruns, Axel. It's Not the Technology, Stupid: How the 'Echo Chamber' and 'Filter Bubble' Metaphors Have Failed Us. The Iamcr 2019 Conference In Madrid, Spain, 7-11 July 2019. https://snurb.info/files/2019/It%E2%80%99s%20Not%20the%20Technology,%20Stupid.pdf

Cancela-Outeda, Celso. "The EU's AI Act: A Framework for Collaborative Governance." *Internet of Things* 27 (2024): 1–11. https://doi.org/10.1016/j.iot.2024.101291.

China Law Translate. Measures for Labeling of AI-Generated Synthetic Content (Draft for Solicitation of Comments). 2024. https://www.chinalawtranslate.com/ai-content-labels/.

———. Provisions on the Administration of Deep Synthesis Internet Information Services. 2022. https://www.chinalawtranslate.com/deep-synthesis/.

Chen, Kelly. “China Proposes New Regulations on AI-Generated Content Labelling.” CMA Tax Law Future 2024. https://cms-lawnow.com/en/ealerts/2024/09/china-proposes-new-regulations-on-ai-generated-content-labelling.

Cohen, Julie E. “Cyberspace As/And Space.” Georgetown Law Faculty Publications and Other Works, January 1, 2007. https://scholarship.law.georgetown.edu/facpub/807.

Collins, Botambu, Dinh Tuyen Hoang, Ngoc Thanh Nguyen, and Dosam Hwang. “Trends in Combating Fake News on Social Media – a Survey.” *Journal of Information and Telecommunication* 5, no. 2 (2021): 247–66. https://doi.org/10.1080/24751839.2020.1847379.

Digital Policy Alert. “United States of America: Introduced New York Artificial Intelligence Bill of Rights (S8209) Including User Rights to the State Senate.” 2024. https://digitalpolicyalert.org/event/17580-introduced-data-privacy-regulation-in-new-york-artificial-intelligence-bill-of-rights-a8129s8209.

European Commission. “The Code of Practice on Disinformation.” 2024. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

McPherson, Poppy. "Exclusive: Fake Accounts Drove Praise of Duterte and Now Target Philippine Election." Reuters, April 11, 2025. https://www.reuters.com/world/asia-pacific/fake-accounts-drove-praise-duterte-now-target-philippine-election-2025-04-11/?utm_source=chatgpt.com.

Fachri, Ferinda K. “CEO Hukumonline Soroti Beberapa Peraturan Terkait AI di Indonesia.” Hukumonline.com, 2024. https://www.hukumonline.com/berita/a/ceo-hukumonline-soroti-beberapa-peraturan-terkait-ai-di-indonesia-lt66c4ccd9763ce/.

Fatimah, Rafharum, Auziah Mumtaz, Fauzan Muhammad Fahrezi, and Diky Zakaria. “AI-Generated Misinformation: A Literature Review.” *Indonesian Journal of Artificial Intelligence and Data Mining* 7, no. 2 (2024): 2. https://doi.org/10.24014/ijaidm.v7i2.26455.

Hanum, Cholida. “Analisis Yuridis Kedudukan Surat Edaran Dalam Sistem Hukum Indonesia.” *Humani (Hukum Dan Masyarakat Madani)* 10, no. 2 (2020): 2. https://doi.org/10.26623/humani.v10i2.2401.

Kertysova, Katarina. “Artificial Intelligence and Disinformation : How AI Changes the Way Disinformation Is Produced, Disseminated, and Can Be Countered.” *Security and Human Rights* 29 (2018): 55–81. https://doi.org/10.1163/18750230-02901005.

Khan, Ali, Kathryn Brohman, and Shamel Addas. “The Anatomy of ‘Fake News’: Studying False Messages as Digital Objects.” *Journal of Information Technology* 37, no. 2 (2022): 122–43. https://doi.org/10.1177/02683962211037693.

Kourinian, Arsen, Amber C. Thomson, Vikram Sidhu, and Lauren N. Williams. “Colorado Governor Signs Comprehensive AI Bill.” Mayer Brown, 2024. https://www.mayerbrown.com/en/insights/publications/2024/06/colorado-governor-signs-comprehensive-ai-bill.

Kravets, Daria, Anna Ryzhova, Florian Toepfl, and Arista Beseler. “Different Platforms, Different Plots? The Kremlin-Controlled Search Engine Yandex as a Resource for Russia’s Informational Influence in Belarus during the COVID-19 Pandemic.” Journalism 24, no. 12 (December 2023): 2762–80. https://doi.org/10.1177/14648849231157845.

Kumar, Ambika, and Tom Wyrwich. “The Test of Time: Section 230 of the Communications Decency Act Turns 20.” Davis Wright Tremaine, 2016. https://www.dwt.com/blogs/media-law-monitor/2016/08/the-test-of-time-section-230-of-the-communications.

Kurniawan, Faizal, Xavier Nugraha, Gio Arjuna Putra, Vicko Taniady, and Bart Jansen. "The Principle of Balance Formulation as the Basis for Cancellation of Agreement in Indonesia." *Lex Scientia Law Review* 6, no. 1 (June 2022): 1. https://doi.org/10.15294/lesrev.v6i1.55468.

LeCun, Yann, Yoshua Bengio, and Geoffrey Hinton. "Deep Learning." *Nature* 521, no. 7553 (2015): 436–44. https://doi.org/10.1038/nature14539.

Legit Security. "NIST AI Risk Management Framework Explained." 2024. https://www.legitsecurity.com/blog/nist-ai-risk-management-framework.

Levi, Stuart D., Ken D. Kumayama, William E. Ridgway, and MacKinzie M. Neal. "Colorado's Landmark AI Act: What Companies Need To Know." Skadden, 2024. https://www.skadden.com/insights/publications/2024/06/colorados-landmark-ai-act.

Liadi, Olusegun Fariudeen, Musediq Olufemi Lawal, and Olawale Olufemi Akinrinde. "Fake News and Hate Speech in Nigeria's Development and Security Trajectory: A Qualitative Assessment." *Jurnal Pertahanan: Media Informasi Tentang Kajian Dan Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism Dan Integrity* 10, no. 1 (2024): 1. https://doi.org/10.33172/jp.v10i1.19369.

Lucas, Jason, Adaku Uchendu, Michiharu Yamashita, Jooyoung Lee, Shaurya Rohatgi, and Dongwon Lee. "Fighting Fire with Fire: The Dual Role of LLMs in Crafting and Detecting Elusive Disinformation." In *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing*, edited by Houda Bouamor, Juan Pino, and Kalika Bali, 14279–305. Singapore: Association for Computational Linguistics, 2023. https://doi.org/10.18653/v1/2023.emnlp-main.883.

Makhortykh, Mykola, Maryna Sydorova, Ani Baghumyan, Victoria Vziatysheva, and Elizaveta Kuznetsova. "Stochastic Lies: How LLM-Powered Chatbots Deal with Russian Disinformation about the War in Ukraine." *Harvard Kennedy School Misinformation Review*, ahead of print, August 26, 2024. https://doi.org/10.37016/mr-2020-154.

Mariani, Marcello M., Isa Machado, Vittoria Magrelli, and Yogesh K. Dwivedi. "Artificial Intelligence in Innovation Research: A Systematic Review, Conceptual Framework, and Future Research Directions." *Technovation* 122 (2023): 1–25. https://doi.org/10.1016/j.technovation.2022.102623.

McCarthy, Dave. "Highlights From the 2024 National Defense Authorization Act (NDAA) and What It Means for the Security Industry." Security Industry Association, January 30, 2024. https://www.securityindustry.org/2024/01/30/highlights-from-the-2024-national-defense-authorization-act-ndaa-and-what-it-means-for-the-security-industry/.

McDonald, Jordan. "Congress Prioritizes AI, Modernization in Defense Funding Bill." GovCIO Media & Research, September 25, 2024. https://govciomedia.com/congress-prioritizes-ai-modernization-in-defense-funding-bill/.

Nannini, Luca, Eleonora Bonel, Davide Bassi, and Michele Joshua Maggini. "Beyond Phase-in: Assessing Impacts on Disinformation of the EU Digital Services Act." *AI and Ethics*, 2024, 1–29. https://doi.org/10.1007/s43681-024-00467-w.

Novelli, Claudio, Federico Casolari, Antonino Rotolo, Mariarosaria Taddeo, and Luciano Floridi. "Taking AI Risks Seriously: A New Assessment Model for the AI Act." *AI & Society* 39, no. 5 (2024): 2493–97. https://doi.org/10.1007/s00146-023-01723-z.

OpenAI. "How ChatGPT and Our Foundation Models Are Developed | OpenAI Help Center." 2024. https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-foundation-models-are-developed.

Paschen, Jeannette. "Investigating the Emotional Appeal of Fake News Using Artificial Intelligence and Human Contributions." *Journal of Product & Brand Management* 29, no. 2 (2019): 223–33. World. https://doi.org/10.1108/JPBM-12-2018-2179.

Pattisina, Edna Caroline. “Prabowo Subianto, Pernah Dipecat atau Tidak?” kompas.id, 2024. https://www.kompas.id/baca/polhuk/2024/02/29/prabowo-pernah-dipecat-atau-tidak.

Perdana, Arif. “AI dan disinformasi: bagaimana kecerdasan buatan dapat memperparah penyebaran hoaks jelang Pemilu 2024.” The Conversation, 2023. http://theconversation.com/ai-dan-disinformasi-bagaimana-kecerdasan-buatan-dapat-memperparah-penyebaran-hoaks-jelang-pemilu-2024-212254.

Prasetianingsih, Rahayu. “Menakar Kekuasaan Presiden dalam Pembentukan Peraturan Perundang-undangan Menurut Undang-Undang Dasar 1945.” *Padjajaran Jurnal Ilmu Hukum* 4, no. 2 (2017): 263–80. https://journal.unpad.ac.id/pjih/vol4/iss2/12/

Prastyo, Angga. “Limitation of Meaningful Participation Requirements in the Indonesian Law-Making Process.” *Jurnal Hukum dan Peradilan* 11, no. 3 (2022): 3. https://doi.org/10.25216/jhp.11.3.2022.405-436.

Putra, Gio Arjuna, Vicko Taniady, and I. Made Halmadiningrat. “Tantangan Hukum: Keakuratan Informasi Layanan AI Chatbot Dan Pelindungan Hukum Terhadap Penggunanya.” *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 12, no. 2 (2023): 2. https://doi.org/10.33331/rechtsvinding.v12i2.1258.

Rahman, Rofi Aulia. “Artificial Intelligence Regulation on Labour Market: Comparative Perspectives on the European Union Artificial Intelligence Act in the Indonesian Context.” *Lex Scientia Law Review* 8, no. 1 (2024): 1. https://doi.org/10.15294/lslr.v8i1.3465.

Roberts, Huw. “Digital Sovereignty and Artificial Intelligence: A Normative Approach.” *Ethics and Information Technology* 26, no. 4 (December 2024): 70. https://doi.org/10.1007/s10676-024-09810-5.

Romero Moreno, Felipe. “Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content.” *International Review of Law, Computers & Technology* 38, no. 3 (2024): 297–326. https://doi.org/10.1080/13600869.2024.2324540.

Saharia, Chitwan, William Chan, Saurabh Saxena, Lala Li, Jay Whang, Emily Denton, Seyed Kamyar Seyed Ghasemipour, et al. “Photorealistic Text-to-Image Diffusion Models with Deep Language Understanding.” arXiv:2205.11487. Preprint, arXiv, May 23, 2022. https://doi.org/10.48550/arXiv.2205.11487.

Samp, Tony, Steven R. Phillips, Charles Dent, and Nathaniel Bell. “Landmark artificial intelligence legislation advances toward becoming law.” DLA Piper, 2020. https://www.dlapiper.com/es-pr/insights/publications/2020/12/landmark-artificial-intelligence-legislation-advances-toward-becoming-law.

Santos, Gustavo Ferreira. “Social Media, Disinformation, and Regulation of the Electoral Process: A Study Based on 2018 Brazilian Election Experience.” *Revista de Investigações Constitucionais* 7 (January 2021): 429–49. https://doi.org/10.5380/rinc.v7i2.71057.

Williams, Evan M., and Kathleen M. Carley, "Search Engine Manipulation to Spread Pro-Kremlin Propaganda," HKS Misinformation Review, February 16, 2023, https://misinforeview.hks.harvard.edu/article/search-engine-manipulation-to-spread-pro-kremlin-propaganda/

Svantesson, Dan. “A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft.” *AJIL Unbound* 109 (January 2017): 69–74. https://doi.org/10.1017/S2398772300001197.

Svantesson, Dan Jerker B., Solving the Internet Jurisdiction Puzzle. Oxford, New York: Oxford University Press, 2017, https://doi.org/10.1093/oso/9780198795674.001.0001.

Taniady, Vicko, and Steven Theonald Siahaan. “Artificial Intelligence and the Constitutional Court: A Newpath of Making Independent Decisions?” *Jurnal Kajian Pembaruan Hukum* 3, no. 2 (2023): 2. https://doi.org/10.19184/jkph.v3i2.41726.

The White House. “FACT SHEET: Biden-Harris Administration Announces Key Actions to Advance Tech Accountability and Protect the Rights of the American Public | OSTP.” 2022. https://business.cch.com/BFLD/BidenHarrisAdministration.pdf.

Turillazzi, Aina, Mariarosaria Taddeo, Luciano Floridi, and Federico Casolari. “The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications.” *Law, Innovation and Technology* 15, no. 1 (2023): 83–106. https://doi.org/10.1080/17579961.2023.2184136.

Urman, Aleksandra, and Mykola Makhortykh. “The Silence of the LLMs: Cross-Lingual Analysis of Guardrail-Related Political Bias and False Information Prevalence in ChatGPT, Google Bard (Gemini), and Bing Chat.” *Telematics and Informatics* 96 (January 2025): 102211. https://doi.org/10.1016/j.tele.2024.102211.

Williamson, Steven M., and Victor Prybutok. “The Era of Artificial Intelligence Deception: Unraveling the Complexities of False Realities and Emerging Threats of Misinformation.” *Information* 15, no. 6 (2024): 6. https://doi.org/10.3390/info15060299.

Wulandari, Virani, Gema Rullyana, and Ardiansah Ardiansah. “Pengaruh Algoritma Filter Bubble Dan Echo Chamber Terhadap Perilaku Penggunaan Internet.” *Berkala Ilmu Perpustakaan Dan Informasi* 17, no. 1 (2021): 1. https://doi.org/10.22146/bip.v17i1.423.

Yusuf, Chandra. “Dampak Pemisahan Kewenangan antara Mahkamah Konstitusi dan Mahkamah Agung dalam Menginterpretasikan Undang-undang dan Peraturan Dibawahnya.” *Jurnal Hukum Unissula* 37, no. 2 (2021): 85–100. https://doi.org/10.26532/jh.v37i2.17377.