

RESEARCH PAPER

Improving Southeast Asia's Resilience to Foreign Information Manipulation and Interference (FIMI) Facilitated by Generative Artificial Intelligence

PANEL 3

Regional Responses to Foreign Information Manipulation
and Interference



Farhan Julianto

Farhan Julianto is a Master of Public and International Law candidate at the Melbourne Law School. He holds a Bachelor of Social Science in International Relations from the University of Indonesia. Farhan has engaged in academic and policy research involving Indonesian foreign policy and security, both in traditional and non-traditional sense, through his work at the Indonesian Institute of Advanced International Studies (INADIS) and Centre for Strategic and International Studies (CSIS). As a scholar of both international law and relations, Farhan focuses on the interactions between states and international instruments in addressing existing and emerging challenges.

This paper is circulated for discussion and feedback. The views expressed are solely those of the author(s) and do not represent an official position of SAIL, CSIS, Google, CfDS, Faculty of Social and Political Sciences UGM or any other organization. The author(s) welcome comments on this version and invite you to contact them directly with any feedback or questions.



Improving Southeast Asia's Resilience to Foreign Information Manipulation and Interference (FIMI) Facilitated by Generative Artificial Intelligence

Farhan Julianto

This article examines the escalating threat of Foreign Information Manipulation and Interference (FIMI) facilitated by Generative Artificial Intelligence (GenAI) in Southeast Asia. GenAI's capacity to produce realistic multimodal outputs has amplified the risk of misinformation and disinformation, making it challenging for the unaware public to discern authenticity. This phenomenon could risk domestic stability in a region characterized by diverse characteristics and threats. Moreover, the current legal frameworks, especially public international law, Intellectual Property (IP), and privacy laws, are inadequate to effectively address this phenomenon. To enhance resilience against FIMI in this region, I proposed several reforms. First, retooling IP frameworks to balance data protection with innovation, including limiting AI's use of copyrighted materials and regulating data scraping. Second, labelling AI-generated and deepfakes content to help distinguish various content across platforms. Third, educating the public on the 'gravity' of consent, including its implications and avenues for withdrawal. Fourth, considering extraterritorial enforcement for AI companies. Fifth, cautiously apply foreign interference laws, with acknowledgment of the potential abuse of power. Such adaptation will be crucial to protect national sovereignty and institutions, while allowing people to productively incorporate AI in their activities.



Introduction

The Race of Artificial Intelligence (AI) has begun, and states are increasing their efforts to reap the benefits. Generative AI (GenAI), particularly, is evolving rapidly and is being adopted widely, with at least 400 million weekly active users.¹ GenAI can utilize big data to generate multimodal outputs like texts, images, audio, and video.² The adoption of GenAI brought positive and negative impacts. While GenAI might increase task efficiency,³ it has also amplified misinformation and disinformation in the digital landscape.

For instance, there is a 26% chance that GenAI will agree with misconceptions due to its inability to differentiate actual truth from popular truth.⁴ Moreover, when a GenAI creates 'realistic' yet fabricated content, either audio, text, or video, people tend to find it difficult to distinguish it from the 'real' ones. This is apparent in several case studies. One case study is in Indonesia, where fabricated content involving political figures was hard to distinguish by at least 30 percent of the population.⁵

GenAI also increased the risk of Foreign Information Manipulation and Interference (FIMI). FIMI is a popular term in European policy and academic discourse.⁶ It is significant due to its effect in creating domestic instability. GenAI increases the risk of FIMI due to its ability to create a realistic depiction that could fool society.⁷ The discussion is particularly relevant in Southeast Asia, where states were divided between authoritarian and democratic systems and faced domestic pressures from coups, disputes, or regressing democracies.⁸

¹ Rishi Kant, "OpenAI's weekly active users surpass 400 million," *Reuters*, 21 February 2025, [https://www.reuters.com/technology/artificial-intelligence/openais-weekly-active-users-surpass-400-million-2025-02-20/#:~:text=Feb%20%20\(Reuters\)%20%2D%20ChatGPT,adoption%20of%20artificial%20intelligence%20to%20ols](https://www.reuters.com/technology/artificial-intelligence/openais-weekly-active-users-surpass-400-million-2025-02-20/#:~:text=Feb%20%20(Reuters)%20%2D%20ChatGPT,adoption%20of%20artificial%20intelligence%20to%20ols).

² Pamela Baker, *Generative AI for Dummies*, (John Wiley & Sons, Inc., 2025), chap. 1.

³ Yukun Liu et al, "Research: Gen AI Makes People More Productive – and Less Motivated," *Harvard Business Review*, 13 May 2025, <https://hbr.org/2025/05/research-gen-ai-makes-people-more-productive-and-less-motivated>

⁴ Aisha Katun and Daniel G. Brown, "Reliability Check: An Analysis of GPT-3's Response to Sensitive Topics and Prompt Wording," *arXiv preprint arXiv:2306.06199*.

⁵ Arya Fernandes, Beltsazar Krisetya, and Ega Yurnia Yazid, *Mis/Disinformation Map in Indonesia: Trust Levels and its Impact on Democracy* (Safer Internet Lab, 4 February 2025), p.25, https://saferinternetlab.org/wp-content/uploads/2025/02/EN_Rilis-Survei-Publik-CSIS_SAIL_.pdf

⁶ European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the architecture of FIMI operations* (EEAS, March 2025), 9-13, <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3rd-ThreatReport-March-2025-05-Digital-HD.pdf>

⁷ European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats*, 24.

⁸ Joshua Kurlantzick, "The State of Democracy in Southeast Asia Is Bad and Getting Worse," *World Politics Review*, published 9 August 2023, <https://www.worldpoliticsreview.com/southeast-asia-economy-democracy-thailand-philippines-myanmar/>

Unfortunately, most states, including those in Southeast Asia, lacked an adequate national and regional framework to respond to FIMI facilitated by GenAI. At the global level, states' responsibilities in the digital landscape are not customary. This left states with wide avenues to manage FIMI-related content. Due to the absence of relevant regulation at the global level, the scope of policy and regulatory responsibility to observe trends of FIMI tend to fall into what exists at the national level, complemented by corresponding regional norms. In Southeast Asia, the closest to such national level regulation governing information manipulation are regulations on privacy and intellectual property. In this article, I will address the question about the role of Intellectual Property (IP) and privacy laws in addressing FIMI facilitated by GenAI, in the absence of coherent global, regional, and national laws more specific to addressing the FIMI facilitated by GenAI.

I argue that in the case of Southeast Asia, although IP and privacy laws are mostly private laws, the role of public authorities is significant in drawing the limitations of the law. I further argue that the current legal frameworks need to be updated to properly address FIMI facilitated by GenAI. The article is delivered in the following logic. First, I will define FIMI and put it into context in the Southeast Asia region. Second, I will discuss the established IP and privacy laws to assess issues concerning GenAI. Third, I will provide national and regional recommendations to realistically address the issue.

FIMI in Southeast Asia: An Evolving Phenomenon

FIMI is defined as coordinated operations in the digital landscape by state and non-state actors to disrupt existing political values and procedures. The concept originated in Europe after Russia's military operations in Ukraine.⁹ The discourse, or the use of the concept more precisely, is dominated by Western countries like the U.S.,¹⁰ Canada,¹¹ France,¹² the EU,¹³ and

⁹ European External Action Service, 3rd EEAS Report on Foreign Information Manipulation and Interference Threats, 4.

¹⁰ "The Framework to Counter Foreign State Information Manipulation," U.S. Department of State, published 18 January 2024, <https://2021-2025.state.gov/the-framework-to-counter-foreign-state-information-manipulation/>

¹¹ "Joint Statement by Canada, United States, and United Kingdom on Foreign Information Manipulation," Global Affairs Canada, published 16 February 2024, <https://www.canada.ca/en/global-affairs/news/2024/02/joint-statement-by-canada-united-states-and-united-kingdom-on-foreign-information-manipulation.html>

¹² "Statement by the Ministers for European Affairs of France, Germany, Poland, Austria, Bulgaria, Croatia, Czechia, Denmark, Greece, Italy, Latvia, Luxembourg, Portugal, Romania, Slovenia, Spain," German Federal Foreign Office, published 21 May 2024, <https://www.auswaertiges-amt.de/en/newsroom/news/2657768-2657768>

¹³ European External Action Service, 3rd EEAS Report on Foreign Information Manipulation and Interference Threats.

the U.K.¹⁴ Those countries also cited the Rapid Alert System (RAS) by the EU and the G7 to manage FIMI.¹⁵

FIMI can also be seen as an umbrella concept for malinformation, disinformation, and misinformation.¹⁶ These actions can be amplified by GenAI, assuming the threat actor can ‘poison’ the datasets or simply by inaccurate content. Sadly, these behaviors are not just possibilities, but actions that have happened. For example, Russia, through its “Pravda Network”, has allegedly poisoned the internet with pro-Russian content to be ingested by the GenAI, which can be considered a coordinated disinformation campaign.¹⁷ GenAI has also become a platform for FIMI by creating inaccurate content. This has happened multiple times recently. Several examples include a deepfake of President Biden during the election to urge Americans not to vote¹⁸, and an audio deepfake of a Presidential Candidate, Anies Baswedan, being reprimanded by Surya Paloh, his biggest supporter in the election, all of which can have significant impact that could have influence election results.¹⁹

Table 1. Distinguishing between key terms covered by the definitions of FIMI

Misinformation	Inaccurate output
Malinformation	Misuse of truthful information for malicious purposes
Disinformation	Intentional act to distribute inaccurate information

(Source: processed by the author from Bjurling, Thore, and Riad, 2024)

This article defines FIMI as an umbrella concept for externally coordinated behavior to influence the political and societal stability of a country using the digital landscape. FIMI can be observed in Southeast Asia, mainly through the concept of Hostile Information Campaigns (HICs). HICs are conducted through information manipulation and the creation of public sentiments of support or rejection through fake accounts and bots on social media.

¹⁴ “Joint Statement by Canada, United States, and United Kingdom on Foreign Information Manipulation,” Global Affairs Canada.

¹⁵ “Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI),” European Union External Action, updated 14 March 2025, https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

¹⁶ Bjorn Bjurling, Andreas Thore, and Stella Riad, *Foreign Information Manipulation & Interference: A Large Language Model Perspective* (RISE Report, 2024), p.7.

¹⁷ Craig Timberg and Joseph Menn, “Russia is Trying to Poison AI Chatbots with Disinformation,” *The Washington Post*, April 17 2025, <https://www.washingtonpost.com/technology/2025/04/17/llm-poisoning-grooming-chatbots-russia/>.

¹⁸ Ali Swenson and Will Weissert, “New Hampshire Investigating Fake Biden Robocall Meant to Discourage Voters Ahead of Primary,” *Associated Press*, January 23 2024, <https://apnews.com/article/new-hampshire-primary-biden-ai-deepfake-robocall-f3469ceb6dd613079092287994663db5>

¹⁹ Burhanuddin Muhtadi and Maria Monica Wihardja, *Deepfakes and Selective Belief: How Partisanship Affects Voters’ Exposure and Susceptibility to Deepfake Content* (ISEAS Yusof Ishak Institute PERSPECTIVE, 26 July 2024), p.6, https://www.iseas.edu.sg/wp-content/uploads/2024/06/ISEAS_Perspective_2024_58.pdf

For example, in one of the more high tension episode of maritime dispute between Malaysia and Singapore back in 2018, there was a spike of artificial social media comments produced by bots, specifically targeting the Singaporean government.²⁰ Indeed, information operations are hard to tackle or mitigate since they might be difficult to distinguish from innocent online interactions.²¹

Another common tactic is cyber threats against claimant countries of the South China Sea, primarily the Philippines. There has been an increase in 35% misinformation campaigns in the Philippines, mainly from China, to create favorable conditions for them in the South China Sea. These threats could contribute to domestic instabilities. For instance, an audio deepfake of President Marcos initiating a military action in the South China Sea sparked nationwide reaction in the Philippines, which might support a favorable condition to China in the dispute.²² Other tactics may also include covert funding to non-state actors which have crucial role in domestic policy formulation.²³ This has resulted in litigation in Singapore, where a citizen was charged with foreign interference.²⁴ Considering the detrimental effect of FIMI, states have to react to protect their national interest and integrity. To do that, states might choose several avenues. One of them is to utilize legal measures.

Legal Avenues

Countering FIMI facilitated by GenAI effectively would require the adoption and adaptation of legal avenues, especially for response and regulation. While technical, societal, or even cultural measures remain essential, legal frameworks provide enforceable standards for accountability, liability, and protection. This section will analyze how different levels of law, from public international norms, IP, and privacy laws react to the development of AI-facilitated FIMI. I will close this section with suggestions of realistic improvement, especially on the regulatory gaps.

²⁰ Muhammad Faizal Bin Abdul Rahman et al, *Cases of Foreign Interference in Asia* (RSIS Policy Report, 2020), p.17

²¹ Muhammad Faizal Bin Abdul Rahman et al, *Cases of Foreign Interference in Asia* (RSIS Policy Report, 2020), p.17-19.

²² Abhishek Sharma and Ishanya Sharma, "China's cyber aggression and the South China Sea dispute," Observer Research Foundation, published 25 March 2025, <https://www.orfonline.org/expert-speak/china-s-cyber-aggression-and-the-south-china-sea-dispute>

²³ Muhammad Faizal Bin Abdul Rahman et al, *Cases of Foreign Interference in Asia*, p.12-15.

²⁴ Xinghui Kok and Ryan Woo, "Singapore invokes foreign interference law against naturalised citizen," *Reuters*, 5 February 2024, <https://www.reuters.com/world/asia-pacific/singapore-invokes-foreign-interference-law-against-naturalised-citizen-2024-02-05/>

Public International Law Obligations

The general duties and responsibilities of states in the digital landscape remain vague. In the general sense, the principles of sovereignty and non-intervention²⁵ can be invoked to handle FIMI. However, there are questions about whether those principles also regulate the digital landscape. Generally, states have due diligence obligations to prevent harmful acts against another state.²⁶ This is unclear whether that duty covers the digital landscape where 'physical' damage is not apparent. According to the Tallinn Manual²⁷, a soft law, this duty does exist.²⁸ However, the adopted UN General Assembly Resolution did not establish due diligence obligations.²⁹

Another issue is attribution. Assuming FIMI is an 'internationally wrongful act' that injures a state, the extent of the injury, and the perpetrators must be explicitly named.³⁰ Although the Western world mostly attributed China and Russia,³¹ lawful attribution is difficult to establish under international law, considering most FIMI acts trace back to private entities or cyber groups.³² Moreover, the Tallinn Manual also established that the origin of a cyber operation is not sufficient for attribution under international law.³³ Lastly, FIMI is also hard to distinguish compared to cyberthreats like ransomware and DDoS. Since international obligations are mostly absent, states will most likely refer to their domestic law.

²⁵ As stated in the: Charter of the United Nations, (adopted 26 June 1945, entered into force 24 October 1945), 1 UNTS XVI, art 2 para.1 & 4.

²⁶ International Court of Justice, *Corfu Channel (United Kingdom v. Albania)*, Merits, Judgment, ICJ Reports 1949, 4.

²⁷ Tallinn Manual is a scholarly study, developed by NATO, that outlines applicability of international law in the cyber space.

²⁸ *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, ed. Michael N. Schmitt (Cambridge: Cambridge University Press, 2017), p.29-33

²⁹ The operative word in the Resolution is "states should..." which indicates that it is not an obligation *per se*, but it is persuasive for states to adopt it. Moreover, the Resolution is not a legally binding document under international law. Further details: United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/RES/70/174 (22 July 2015), Art. 13 para (c).

³⁰ International Law Commission, *Responsibility of States for Internationally Wrongful Acts* (United Nations, 2001), Article 2&4.

³¹ European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats*.

³² European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats*.

³³ Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights," *Georgetown Journal of International Law* 48, No. 735 (March 2017): 750-752.

IP Law

A universal IP law is absent. However, efforts to harmonize IP laws exist among states through the Berne Convention and the TRIPS Agreement. The Convention deals with minimum Copyright protection and is managed by the World Intellectual Property Organization (WIPO).³⁴ Meanwhile, the Agreement deals with aspects of the Convention with an expanded focus that includes trademarks, patents, and trade secrets. The Agreement is governed by the World Trade Organization (WTO).³⁵ Most Southeast Asian states are already parties to the Convention, with Myanmar the only exception.

For this article, Copyright law is the most relevant IP law with few references to trade secrets. Copyright law gives the rights-holders exclusive rights to control the use of their work.³⁶ I argue this is the most relevant pillar of the IP law since GenAI needs information to operate, and that information might be copyrighted works. However, Copyright may be exempted by states as long as they apply the three-step test. It means that the exceptions must be used for 'certain special cases', must not interfere with exploitation efforts, and must not prejudice the legitimate interest of rights-holders.³⁷ These exceptions are adopted in national laws, mostly referred to as the fair use doctrine.

This doctrine became the justification for AI companies to use copyrighted material to train their model. This is apparent in several ongoing case laws of copyright infringements between copyright holders and AI companies.³⁸ While most of these case laws have not been decided, the judicial decision will be influential in analyzing the interaction between IP law and AI. Another contributing factor that complicates the situation is the state's policy. A state, in pursuit of economic growth, may regulate lightly in terms of copyright infringement.


³⁴ "Berne Convention for the Protection of Literary and Artistic Works," WIPO, <https://www.wipo.int/treaties/en/ip/berne/> x

³⁵ "Agreement on Trade-Related Aspects of Intellectual Property Rights (unamended)," World Trade Organization, https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm

³⁶ *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)*, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, art. 11.

³⁷ *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)*, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, art. 13.

³⁸ In *New York Times v. OpenAI*, OpenAI argues that its use of New York Times material is justified under the fair use doctrine. However, on February 11th 2025, the U.S. District Court of Delaware, a lower court, decided the case between *Thomson Reuter v. Ross Intelligence* where the fair use justification was rejected. The doctrine was rejected because it deprives the right holders' rights. However, it must be noted that the Delaware case did not involve GenAI. For further details: Audrey Hope, "NYT v. OpenAI: The Times's About-Face," *Harvard Law Review*, 10 April 2024, <https://harvardlawreview.org/blog/2024/04/nyt-v-openai-the-timess-about-face/>; "An Early Win for Copyright Owners in AI Cases as Court Rejects Fair Use Defense," *Debevoise and Plimpton LLP*, 14 February 2025, <https://www.debevoise.com/insights/publications/2025/02/an-early-win-for-copyright-owners-in-ai-cases-as->



For example, Singapore introduced an immunity against infringement as long as the data was used for computational data analysis.³⁹ The fair use doctrine is also being cited in debating the existence of deepfakes. Deepfakes might use copyrighted materials, but they may not qualify as infringement due to the transformative nature of the end product.⁴⁰ In sum, states became paralyzed due to the fair use doctrine. On one side, they must grant the doctrine as part of compliance with international obligations. On the other side, the fair use doctrine has been interpreted widely and allows practical immunities for AI companies and GenAI content.

Another issue with regard to IP law is surrounding transparency of the AI companies following data mining. Currently, AI platforms are not required to disclose their training data, including how and when they use personal information collected from users and data scraping from several online sites.⁴¹ AI companies justify their actions by treating the training data as a trade secret, which is protected under IP law. This is problematic considering the data might not even be theirs to begin with.

In terms of FIMI facilitated by GenAI, several challenges presented themselves. First, a loose IP law means platforms and users have access to authoritative sources that might be key to producing believable misinformation or disinformation. Moreover, the lack of transparency on training data means an individual might not even consent to the data collection by AI companies. This is problematic since threat actors in FIMI might use that personal data in manufacturing personalized content to target a specific part of society, which can disrupt political stability.

Privacy Law

Similar to IP law, there is no singular international privacy law. Moreover, there is also no singular global standard in terms of defining privacy and its limits. This meant that privacy is regulated on a state-by-state basis even when the whole operation in the digital landscape is transnational. These different standards lead to global regulatory competition, especially

³⁹ computational data analysis defined as extraction of information and using the work to improve the functioning of a computer program in relation to the data. This means that it covers data mining for training GenAI model. Further information: *Copyright Act 2021* (Singapore), s.243.

⁴⁰ There has not been known copyright infringement cases involving deepfakes. However, the ‘transformative nature’ can be inductively drawn from the cases involving *Authors Guild v. Google* in the U.S. For further information: *Authors Guild, Inc. v. Google Inc.*, 804 F.3d 202 (2d Cir.2015).

⁴¹ Claudio Novelli et al, “Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity,” *Computer Law & Security Review* 55, (Jan 2024).

with the emergence of AI in daily activities.⁴² The gold standard of privacy regulation is the EU's General Data Protection Regulation (GDPR),⁴³ even when the regional body has released its Artificial Intelligence Act (AIA).⁴⁴ Privacy law is involved in data collection, data processing, and data output processes. In Southeast Asia, specifically, privacy regimes also differ from one another, which poses a challenge in harmonizing regulation and forming a cohesive regional mechanism.⁴⁵

In the data collection process, privacy laws govern how AI companies can collect data directly or indirectly. AI companies collect data directly through user performance.⁴⁶ The biggest issue in direct data collection is consent, where it is often provided without proper knowledge of the implications and limitations.⁴⁷ Meanwhile, in indirect data collection, AI companies often collect data through scraping social media and websites.⁴⁸ This action may conflict with the consent of the data subject and the terms of the platform itself.⁴⁹ Even if the scrapings were conducted through open-access data, privacy laws still apply.⁵⁰

Privacy laws also interact with the data processing and output processes. In data processing, platforms are mostly required to remove personal information.⁵¹ However, anonymization is not secure enough since the data can be deanonymized.⁵² Meanwhile, in data outputs, the biggest concern is malicious content created through deepfakes. Deepfakes are also widely used in fraudulent actions across the Southeast Asia region, with origins from Cambodia, Myanmar, and the Lao PDR.⁵³

To examine the success rate of the law in addressing those issues, there are several mechanisms to be addressed. First, governing law. Governing law is important since it will

⁴² Michal Czerniawski, "Towards the Effective Extraterritorial Enforcement of the AI Act," in Hoepman, J.H. et al, *Privacy Symposium 2024 – Data Protection Law International Convergence and Compliance with Innovative Technology (DPLICIT)* (Springer, 2025), p.8.

⁴³ The GDPR is a gold standard in cyber regulation due to its detailed design and extraterritorial jurisdiction.

⁴⁴ Felipe Romero Moreno, "Generative AI and Deepfakes: a Human Rights Approach to Tackling Harmful Content," *International Review of Law, Computers & Technology* 38, (2024), p.297-326.

⁴⁵ Jessica Aurelia and Lewiandy, "The Challenge of Harmonizing Cross-Border Data Transfer Regulations Among ASEAN Member States," *Jurnal Kertha Semaya* 13, No.3 (2025), 287-300.

⁴⁶ Felipe Romero Moreno, "Generative AI and Deepfakes: a Human Rights Approach to Tackling Harmful Content," 301-302.

⁴⁷ Magdalena Eitenberger, Barbara Prainsack, and Maya Sabatello, "Consent at the Ease of a Click? Technosolutionist Fixes Cannot Replace Human Relations and Solidarity," *The American Journal of Bioethics* 25, No.4 (2025), 121-123.

⁴⁸ Daniel J. Solove, "Artificial Intelligence and Privacy," *Florida Law Review* 77, No.1 (2025), 26-32.

⁴⁹ Daniel J. Solove, "Artificial Intelligence and Privacy," 33-35.

⁵⁰ Daniel J. Solove, "Artificial Intelligence and Privacy," 32.

⁵¹ Daniel J. Solove, "Artificial Intelligence and Privacy," 33.

⁵² Hannah Ismael, "Examining Generative Image Models Amidst Privacy Regulations," *Journal of Integrated Global STEM* 1, No.2 (2024): 75-82.

⁵³ Global Initiative Against Transnational Organized Crime, *Criminal Exploitation of Deepfakes in Southeast Asia* (Singapore: World Economic Forum, 2025).

determine the jurisdiction and enforcement. In terms of AI, data collection and processing are naturally determined by the laws where the AI companies are based. For instance, the law of California⁵⁴ applies to OpenAI, which means that they will be required to label AI-generated content, including election-related deepfakes and political advertisements.⁵⁵ This is not the best model since AI companies could, theoretically, base themselves in a state with loose regulatory mechanisms.⁵⁶ The most effective laws in regulating AI are those that have extraterritorial jurisdiction. It means that the law applies even when AI companies are not based in a particular territory. For instance, GDPR and AIA apply to platforms that want to market their products in the EU.⁵⁷ These extraterritorial jurisdictions are important considering that AI players mostly come from China and the U.S.⁵⁸ However, extraterritorial jurisdiction can also be a barrier to entry for a certain platform, and it might also deter platforms from a certain jurisdiction.⁵⁹

In terms of data output, privacy laws tend to govern depending on the content generated by the AI. While some countries may have specific laws regarding foreign interference or deepfakes, most countries rely on existing laws since the issue is still emerging. One of the pivot points is the defamation law. Governing AI through defamation could be problematic since different countries have different thresholds between freedom of expression and criticism.⁶⁰

In Southeast Asia, extraterritorial jurisdiction might be hard to implement regionally due to the absence of a supreme regional organization like the EU and a capacity gap among its states. In an overall sense, those states have stronger control over data outputs because the region was dominated by newcomer countries. Not all Southeast Asian states have regulations to protect personal data or AI.⁶¹ These states tend to rely on defamation laws, which could limit freedom of expression within society. With regards to FIMI, their response

⁵⁴ The U.S. does not have a national/federal law on privacy. If an AI company is located in a state with national-level law, then the national law will apply.

⁵⁵ Hope Anderson, "From California to Kentucky: Tracking the Rise of State AI Laws in 2025," White & Case LLP, 27 May 2025, <https://www.whitecase.com/insight-alert/california-kentucky-tracking-rise-state-ai-laws-2025>

⁵⁶ Referring to shipping policies, where ships adopt a flag which is less-regulated to enable more freedom.

⁵⁷ Michal Czerniawski, "Towards the Effective Extraterritorial Enforcement of the AI Act," p.4-5.

⁵⁸ Will Knight, "The AI Race Has Gotten Crowded-and China is Closing In on the US," *Wired*, 7 April 2025, <https://www.wired.com/story/stanford-study-global-artificial-intelligence-index/>

⁵⁹ Michal Czerniawski, "Towards the Effective Extraterritorial Enforcement of the AI Act," p.5.

⁶⁰ For example, Australia categorizes defamation as civil matter, and emphasizes the harm the act caused towards the person. Meanwhile, Singapore and Indonesia categorizes defamation as a criminal matter with emphasis on reputation rather than harm. Further information: X

⁶¹ Shota Watanabe, Ema Ogura, and Keita Oikawa, *Current Status of ASEAN Data Governance and Its Implications for the Digital Economy Framework Agreement: ERIA Discussion Paper Series No. 539* (Economic Research Institute for ASEAN and East Asia, 2025), 5.

remains weak since most policymakers tend to protect the reputation of the political figure rather than addressing political instabilities.

Regulatory Suggestions⁶²

Considering the limitations of current regulatory frameworks to manage FIMI facilitated by GenAI, a reform needs to be conducted in the short and long term. Therefore, in this part, I will provide some recommendations to tackle and manage FIMI, especially when by GenAI. The recommendations will be structured similarly to the discussions.

In public international law, Southeast Asian states must bear the burden of an ineffective ASEAN. ASEAN has strong norms like non-interference and friendly cooperation.⁶³ However, the Association is always hesitant to name common threats and draw red lines, especially with dialogue partners. As a result, ASEAN cooperation on sensitive areas is often stagnated and has only resulted in statements and guidelines.⁶⁴ Therefore, it is important to consider cooperation among like-minded countries. If we look closer among Southeast Asian states, there is a common interest and concern that could be the basis for cooperation, namely Chinese information campaigns.⁶⁵ This could be the basis of practical cooperation, policy harmonization, and capacity-building to tackle those risks.

Beyond regional cooperation, states should also step up in their domestic regulatory landscape. The first legal reform that states should consider is to retool their IP framework to include the developments of AI. IP should be developed with a balance between basic protection for data subjects and innovation with quality data. Therefore, I suggest a limitation for AI platforms to use data subjects from copyrighted materials. Moreover, a regulatory sandbox⁶⁶ should also be developed to allow firms to innovate using limited copyrighted materials to train their models.

The regulation should have an adequate monitoring system and enforcement mechanisms. In terms of monitoring, states could force organizations to appoint a Data Protection Officer

⁶² Regulatory efforts can take many forms, including Act, technical guidelines, and non-binding guidelines.

⁶³ The ASEAN Charter, Art. 2(a); Treaty of Amity and Cooperation in Southeast Asia, Art 2(a), Art 3.

⁶⁴ For instance: 2023 ASEAN Guideline on Management of Government Information in Combating Fake News and Disinformation in the Media. The point is not to prove that statement is wrong, but to emphasize that statement is not and should not be the end-goal.

⁶⁵ Julia Voo, "Driving Wedges: China's Disinformation Campaigns in the Asia Pacific," in *Asia Pacific Regional Security Assessment 2024: Key developments and trends*, edited by Evan Laksmana (International Institute of Strategic Studies, 2024), 121; Muhammad Faizal Bin Abdul Rahman et al, *Cases of Foreign Interference in Asia*, 11.

⁶⁶ Limited waiver to enable new business models and innovations. Definition adapted from: OECD, *Regulatory sandboxes in artificial intelligence* (OECD, 2023), 8.

(DPO) to ensure compliance.⁶⁷ The rule should also be enforceable, including for companies that are based abroad. States, especially larger states, could consider applying extraterritorial jurisdiction. While there are risks that platforms will move away entirely, the market power of the state should be attractive enough for platforms to comply with the requirements.⁶⁸ This regulation will also be helpful from privacy law perspectives, as it moves states away from regulating data output to inputs.

While some data input processing has been covered in the discussion of IP, a concern remains. One of the biggest concerns is about consent. There has been no singular formula to revamp the consent format, with both the opt-in and opt-out options having their concerns.⁶⁹ Therefore, instead of regulating consent, I argue that it is more important to educate what consent means, to give more meaning to the opt-in choice. States ideally should give more knowledge to their people about what consent means and who can give consent. In my opinion, there should be guidance to clarify consent and the minimum age to give consent.⁷⁰

In terms of data processing, states should explicitly regulate the terms and conditions for scraping through social media and websites. While scraping might be beneficial for many purposes, its conduct must be regulated to ensure that the data being extracted does not contain sensitive personal information or copyrighted materials. Ideally, there should also be a mechanism where individuals, or data subjects, must be informed prior to the scraping. The regulatory sandbox might waive several limitations for scraping, but regulators must ensure that the amount of data is minimized and desensitized appropriately.

Lastly, in terms of data output, there are two avenues that states could implement. The first is to require platforms and creators to label AI-generated content. This could help viewers to

⁶⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 37, General Data Protection Regulation, 2016.

⁶⁸ Drawing parallels from Indonesia's tech licensing scheme. Platforms like Facebook and Netflix initially refused the scheme introduced by Indonesian Ministry of Communication, but eventually registered anyway. For more information: Christian Guntur Lebang and Gatra Priyandita, "Indonesia's controversial tech licensing scheme," *Australian Strategic and Policy Institute*, 9 Aug 2022, <https://www.aspistrategist.org.au/indonesias-controversial-tech-licensing-scheme/>

⁶⁹ In opt-in, people often consented without adequate knowledge. In opt-out, trained models can't exclude a data after they was trained. Further information: Magdalena Eitenberger, Barbara Prainsack, and Maya Sabatello, "Consent at the Ease of a Click? Technosolutionist Fixes Cannot Replace Human Relations and Solidarity," p.12; Daniel J. Solove, "Artificial Intelligence and Privacy," 33.

⁷⁰ Similar with Italian DPA's enquire to OpenAI. Further information: Angela Busacca and Melchiorre Alberto Monaca, "Who's Afraid of Big Bad Generative AI? Brief Notes on the IDPA Provision Against OpenAI ChatGPT," in *Generative Artificial Intelligence and Fifth Industrial Revolution*, edited by Domenico Marino and Melchiorre Alberto Monaca (Springer Nature Switzerland, 2025).

distinguish AI-generated content without specifically limiting certain actors.⁷¹ States should also require platforms to remove fake content that uses deepfake technology on social media.⁷² Second, is to adopt a foreign interference law. This has been adopted and implemented in countries like Singapore.⁷³ However, there is a risk if it is implemented in states with ultra-nationalistic leaders, as they might associate negative news with foreign interference.⁷⁴ Therefore, the second avenue is optional and only implemented when appropriate.

Conclusion

Foreign Information Manipulation and Interference (FIMI), particularly when facilitated by Generative AI (GenAI), presents a pressing challenge for Southeast Asia. The region is already situated with contrasting vulnerabilities and governance systems. As demonstrated in this article, three core legal domains—public international law, intellectual property (IP), and privacy law—each reveal significant limitations in their ability to address the FIMI.

International obligations in the digital landscape remain ambiguous. While principles such as sovereignty and non-intervention may be theoretically invoked, their application in the digital realm, especially when physical harm is absent, is contested. Attribution of FIMI to a particular state or actor remains technically and legally difficult. As a result, states often default to their national laws.

In the realm of IP law, the 'fair use' doctrine and the lack of transparency in AI training datasets have inadvertently enabled the creation of realistic, inaccurate content. The protection of training data as trade secrets further obscures accountability, even when such data includes copyrighted or personal content obtained without consent. This legal vacuum allows threat actors to exploit GenAI tools to manufacture highly convincing falsehoods and manipulate public opinion. Privacy law also has its own limitations, especially given the fragmented and inconsistent regulations across Southeast Asia. The absence of harmonized standards for consent, data scraping, and the handling of sensitive personal information leaves individuals


⁷¹ Mimicking Senate Bill 942 of California; Chanley T. Howell and Leighton B.R. Allen, "Decoding California's Recent Flurry of AI Laws," *Foley & Lardner LLP*, 4 October 2024,

<https://www.foley.com/insights/publications/2024/10/decoding-california-recent-ai-laws/>

⁷² Mimicking Assembly Bill 2655 of California; Chanley T. Howell and Leighton B.R. Allen, "Decoding California's Recent Flurry of AI Laws,".

⁷³ Singapore, *Foreign Interference (Countermeasures) Act 2021*, No. 33 of 2021

⁷⁴ Eka Yudha Saputra, "Prabowo Accuses Foreign Powers of Funding NGOs to Sow Discord in Indonesia," *Tempo*, 2 June 2025, <https://en.tempo.co/read/2013249/prabowo-accuses-foreign-powers-of-funding-ngos-to-sow-discord-in-indonesia>



vulnerable to data misuse. In countries where privacy protections are weak or underdeveloped, the risk of targeted manipulation is amplified.

To address these gaps, this article proposed realistic reforms, including moving away from an ASEAN that is obsessed with norms-building, updating IP and privacy laws to reflect the development of GenAI, and stronger domestic enforcement through transparency obligations and content labeling requirements. I refrained from suggesting the adoption of foreign interference laws regionwide since the regressing democratic states may benefit from those regulations and limit freedom of expression. In summary, Southeast Asia must modernize its legal frameworks to reflect the realities of the AI-driven information age. Failure to do so will leave the region increasingly exposed to FIMI campaigns, undermining democratic institutions, social cohesion, and national sovereignty.



INFORMATION RESILIENCE & INTEGRITY SYMPOSIUM

Generative AI and Information Resilience
in the Asia-Pacific: Actions and Adaptations

Faculty of Social and Political Sciences
Universitas Gadjah Mada

21 August 2025