TECH FOR GOOD INSTITUTE

Report

The Evolution of Tech Governance in Southeast Asia-6

March 2025

Table of Contents

About this Study

The Evolution of Tech Governance in Southeast Asia-6 is the second edition in Tech for Good Institute's series to shape the tech ecosystem of Southeast Asia. While the 2023 edition focused on identifying "who" the key regulators are in the digital economy, this edition builds on that foundation by exploring "who" the key players are, "how" governments are approaching tech governance and "what" policy areas gained prominence in 2024, offering insights into the region's evolving regulatory landscape.

A key contribution of this report is its expanded scope, reflected in its title. While regulations pertain to specific policies and legislation, governance encompasses the structures, processes and administrative considerations involved in the exercise of government authority. By moving beyond understanding who latest regulators and what their regulations are to a more holistic understanding of governance, we hope to offer insights into the broader direction of the region's approach to the digital ecosystem.

This report spotlights the six major digital economies of the region—Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam (collectively referred to as the SEA-6). As the region undergoes rapid digital transformation, governments are adopting diverse policies and frameworks to effectively address the opportunities and challenges presented by emerging technologies.

With contributing partners from each country, this report provides in-depth insights into the dynamic landscape of tech governance across SEA-6. Acknowledging the rapid pace of technological advancement and the unique trajectories of each country, we recognise that the regulatory landscape of the digital economy will remain dynamic and continue to evolve. As a summary of 2024 developments, however, we hope that this report will serve as a useful resource for policymakers, researchers and industry practitioners seeking to understand the region's evolving regulatory frameworks.

The goal of this paper is to serve as a starting point for meaningful conversations. Southeast Asia presents valuable opportunities for learning from each other's experience in technology governance. By offering a shared resource that highlights key governance advancements across the region, this paper seeks to foster dialogue and collaboration in shaping effective and forward-looking regulatory frameworks. With the anticipated conclusion of the Digital Economy Framework Agreement (DEFA) negotiations later this year, this report also aims to identify common areas of convergence where tangible cooperation on regional interoperability can be advanced.

Acknowledgments

The Tech for Good Institute would like to thank our partners for their invaluable inputs and feedback on this paper:

- **Anont Tanaset**, Office of National Higher Education Science Research and Innovation Policy Council, Thailand
- **Ariane Yasmin**, TIA Editors, Malaysia
- **Farlina Said**, Institute of Strategic and International Studies, Malaysia
- **Hafiz Noer**, Center for Digital Society, Indonesia
- **Irfan Dwi Putra**, Center for Digital Society, Indonesia
- **Lim How Khang**, Singapore Management University, Singapore
- **Nguyen Minh Thao**, Central Institute for Economic Management, Vietnam
- **Oliver Reyes**, University of the Philippines Law Center, Philippines

The Tech for Good Institute is also grateful to Grab for supporting TFGI's mission of leveraging the promise of technology and the digital economy for inclusive, equitable and sustainable growth in Southeast Asia. Funders do not determine research findings nor the insights and recommendations of research.

Disclaimer

The information in this paper is provided on an “as is” basis. This paper is not to be considered as a recommendation for investments in any industry. This document is produced by the Tech for Good Institute and has been prepared solely for information purposes over a limited time period to provide a perspective on the region. The Institute and any of its affiliates, or any third party involved make no representation or warranty, either expressed or implied, as to the accuracy or completeness of the information in the paper, and no responsibility or liability whatsoever is accepted by any person of the Institute, its affiliates and its respective officers, employees or agents.

About the Tech for Good Institute

The Tech for Good Institute is a non-profit organisation working to advance the promise of technology and the digital economy for inclusive, equitable and sustainable growth in Southeast Asia. With a population twice the size of the US and strong demographics, Southeast Asia's digital economy is evolving rapidly. At the same time, the region's trajectory is unique, shaped by its diverse cultural, social, political and economic contexts. The Tech for Good Institute serves as a platform for research, conversations and collaborations focused on Southeast Asia, while staying connected to the rest of the world. Our work is centred on issues at the intersection of technology, society and the economy, and is intrinsically linked to the region's development. We seek to understand and inform policy with rigour, balance and perspective by using research, effective outreach and evidence-based recommendations.

The Institute was founded by Grab to advance the vision of a thriving and innovative Southeast Asia for all. We welcome opportunities for partnership and support, financial or in-kind, from organisations and individuals committed to fostering responsible innovation and digital progress for sustainable growth in the region.

More information about the Institute can be accessed at www.techforgoodinstitute.org.

Executive Summary

As Southeast Asia's digital economy continues to drive economic progress, policy and governance trends are shifting from rapid expansion to responsible development. In 2024, governments in the region focused on sustainable growth and trust in the digital ecosystem amid the rapid innovation and adoption of artificial intelligence (AI) models, algorithms and products.

In the early stages of Southeast Asia's digital economy journey, the prevailing "move fast and break things" mindset prioritised speed and innovation. The pandemic further accelerated rapid scale and adoption. However, as digital technologies become more embedded in society, the risks have become more apparent. Governments are now adopting a more measured approach to mitigate unintended consequences, including misinformation, cyber threats and workforce disruptions. Moreover, regulatory clarity and interoperability are vital to attracting investment and reducing operational costs as companies mature.

Digital ecosystem governance is therefore expected to remain a central policy priority for governments in the region. In Southeast Asia, this unfolds in two key ways: balancing the **promotion** of the digital economy to enable emerging technologies, while simultaneously **advancing and safeguarding** digital society. Governments of Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam (collectively called the SEA-6) are implementing a range of governance mechanisms to achieve these dual objectives. Promoting the digital economy and fostering innovation maximises economic benefits of digital technologies as a horizontal force across all industry sectors. Meanwhile, protecting the digital society emphasises inclusion, trust and sustainability, ensuring that digital progress aligns with national priorities while mitigating risks and unintended harms.

The promotion of the digital economy and the protection of the digital society can reinforce one another. Building trust in the digital ecosystem, implementing robust data governance and developing digital public goods, for example, create a strong foundation for innovation and long-term digital progress in Southeast Asia.

Across the region, this balancing act can be observed in shared policy areas (*what*) of AI governance, cybersecurity and data protection, and promotion of safety and trust. Governments across the region have introduced new policies or updated their existing regulations to address opportunities and potential disruptions posed by AI, the evolving cyber threat landscape, and the deepening integration of e-commerce, fintech and digital platforms. Cyber resilience strategies were updated to protect critical infrastructure, and combating online harms and scams remains a key focus.

Beyond policy priorities, this balancing act is also evident at the structural level (*who*) and its approach (*how*). At the structural level, 2024 saw the emergence of new agencies tasked with governing the digital ecosystem holistically, from fostering digital economy growth to safeguarding citizens in the digital space and advancing digital public infrastructure. Specialised bodies in areas such as AI, e-commerce and cybercrime were established to build deep knowledge and implementation. As noted in TFGI's 2023 report *Evolution of Tech*

Regulation in the Digital Economy,[1] tech policy coordination is more important than ever, with whole-of-government approaches advancing cross-sectoral efforts for policy coherence. This is needed in the national and sub-national levels of government agencies, across various industry verticals, and between key stakeholders to promote skills and capability development within society. Additionally, for digital economy companies, greater clarity from improved policy coordination will ease regulatory transitions, particularly as new and specialised agencies continue to be established.

Governments are expanding their tech governance toolbox beyond traditional regulation as they recognise the need to foster innovation and maintain relevance. In addition to hard laws, policy innovations such as soft guidelines, frameworks and sandboxes were implemented in the region, especially for emerging technologies. This approach allows governments to understand technologies and business models and understand the increased attention on mitigating unintended consequences before new products and services reach the market. By leveraging policy innovation initiatives, regulators were able to monitor technological advancements in real time while fostering public-private collaboration to safeguard the public interest.

A regional view on tech governance developments across SEA-6 reveals that while countries share common policy priorities, they often diverge in structure and approach. Shaped by their legal traditions, governance frameworks and cultural norms, regulatory strategies vary significantly across markets. In AI governance, for instance, some countries like Indonesia favour legally binding regulations, while others lean toward more flexible, principle-based guidelines to encourage innovation while managing risks. Despite these differences, the broad alignment on key priorities such as AI governance, cybersecurity and data protection, and online safety and trust presents valuable opportunities for regional cooperation.

At a regional level, the ASEAN Digital Economy Framework Agreement (DEFA) is set for conclusion in 2025. DEFA aims to harmonise digital trade rules, facilitate cross-border data flows and establish governance frameworks for emerging technologies. However, for regional alignment to be more achievable, domestic governance mechanisms must first be clearly defined. Regulatory clarity at the national level ensures that governments can engage in meaningful discussions on interoperability with pathways for implementation.

Given the region's diverse levels of development, legal traditions and national priorities, sharing outcomes and focusing on priorities is the starting point for bridging differences in governance approaches and policy implementation. This enables governments to learn from one another while fostering cross-border regulatory coherence. While the ASEAN DEFA provides a broad framework for cooperation, the shared priorities identified in this report, such as AI governance, cybersecurity and data protection, and promoting safety and trust, offer tangible areas for immediate collaboration. Prioritising these common interests enables incremental progress, building trust and practical alignment before tackling more complex areas of integration. Ultimately, a collective commitment to an open, interconnected and interoperable regional digital economy is essential for sustaining Southeast Asia's digital growth and resilience.

1. Introduction

Southeast Asia continued to witness sustained growth in its digital economy in 2024. The region's gross merchandise value (GMV) in 2024 reached approximately US$263 billion, with companies and investors stressing profitability alongside growth.[2] At the same time, governments were increasingly focused on safeguarding the welfare of current and future digital users. This commitment was evident in key governance developments that continuously shape Southeast Asia's digital landscape.

Governments also carefully balanced the promotion of the digital economy and the protection of the digital society. Digital economy promotion focuses on fostering industry growth and innovation, attracting investments, and maximising the economic benefits of digitalisation whereas digital society protection safeguards consumer interests, aligns digital development with national goals, and mitigates unintended consequences.

This balancing act is reflected in the policy decisions and governance approaches, shaping the region's digital landscape. Chapter 2 of this report examines common government priorities in 2024, highlighting key challenges in the digital economy, including AI governance, cybersecurity and data protection, and promoting safety and trust. Chapter 3 explores the regulators responsible for overseeing the digital ecosystem and how they are adapting to its rapid evolution. It dives into institutional changes, oversight mechanisms and regulatory tools, all shaped by each country's unique government structures, legal traditions and cultural norms. Chapter 4, written by local experts, presents country overviews in a deeper and more nuanced perspective, offering insights into how different nations navigate the complexities of tech governance. Finally, in Chapter 5, we emphasise that promotion and protection are not separate objectives but rather interconnected aspects of tech governance. This balance is essential to ensuring that digital economy growth remains inclusive and sustainable.

National developments unfolded alongside the region's efforts to foster meaningful cooperation, as ASEAN member states (AMS) continued negotiations on the ASEAN Digital Economy Framework Agreement (DEFA), anticipated to conclude by 2025. Therefore, the evolution of tech governance impacts the future of domestic tech governance and the broader trajectory of regional integration. While divergence in governance models may persist across Southeast Asia, a shared commitment to address critical issues will be essential in establishing a cohesive, resilient and interconnected digital ecosystem.

2. Key Policy Trends

In 2024, shared priorities across the SEA-6 economies were:

- **Artificial Intelligence (AI) Governance**. Recognising the potential and pace of innovation in the AI sphere, governments responded to the evolving nature of AI, including generative AI, guide responsible AI design, development and deployment.

- **Cybersecurity and Data Protection**. Recognising the increasing threats in the digital space, policies were updated to strengthen cyber resilience and ensure robust data protection practices.

- **Promoting Safety and Trust in the Digital Economy**. With the growing adoption of digital services and the evolution of business models, governments enhanced regulatory oversight to promote confidence in the digital society and maintain trust in the digital economy.

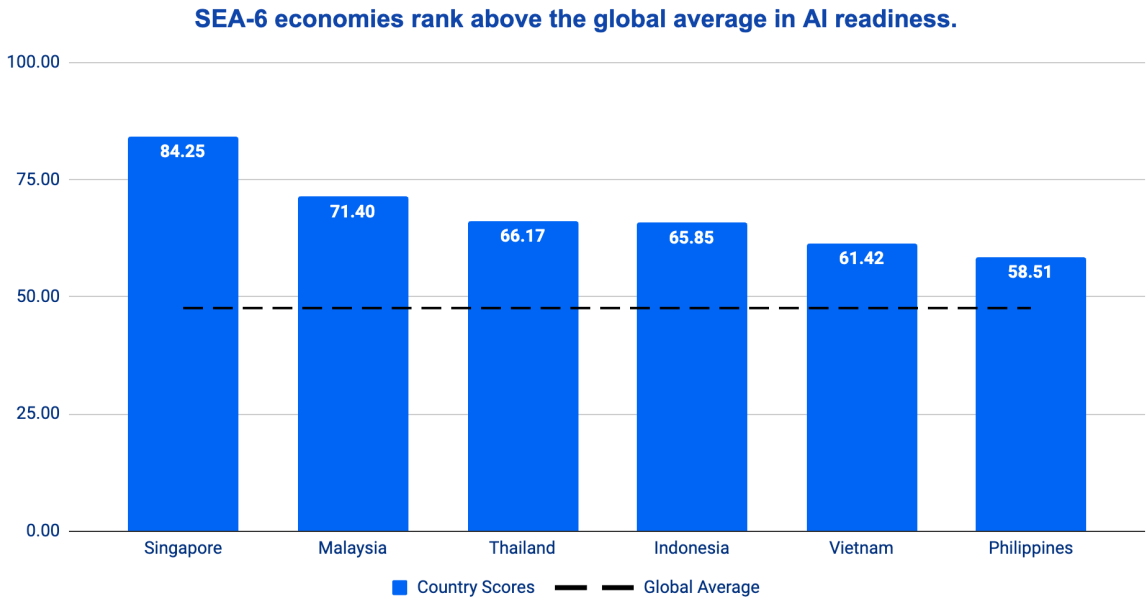
The rest of this section outlines key trends across the shared priorities of Southeast Asian governments.

2.1. AI Governance

AI emerged as the region's most transformative emerging technology, with countries responding quickly to mitigate "*misuse*" while seeking to avoid the "*missed uses*" of AI, and to lay the groundwork for innovation and investment.[3] Southeast Asia saw a surge in AI-related investments, with more than US$30 billion poured into AI infrastructure in the first half of 2024 alone.[4] Additionally, the need for data centres across ASEAN is projected to grow by up to 20% annually through 2028.[5] Microsoft and Google have significant investments in Malaysia,[6] while Singapore is planning to increase its data centre capacity by over one-third.[7] This surge in investment and the announcement of planned projects highlight the region's potential as a hub for AI-driven growth. Estimates suggest that AI could contribute between 10% to 18% of the region's GDP, potentially adding up to US$1 trillion by 2030.[8]

Although investments are starting to grow, AI adoption and readiness across the region remains in its early stages. A 2024 study by Kearney found that 30% of businesses were still in the initial phases of developing AI strategies, while 50% were piloting AI applications. Only 15% of companies—mainly in service-based industries such as finance, telecommunications and e-commerce—have implemented AI on a larger operational scale.[9] There are also varying levels of readiness across countries. According to the 2024 Government AI Readiness Index by Oxford Insights, Singapore leads the region with a readiness score of 82.25, ranking second globally, just behind the United States. Malaysia followed with a score of 71.40, while Thailand (66.17) and Indonesia (65.85) made significant investments to enhance their AI readiness. Meanwhile, Vietnam (61.42) and the Philippines (58.51) continue to make steady progress in developing their AI capabilities. Notably, all SEA-6 economies scored above the global average, reflecting the region's commitment to maximising opportunities of the AI age and positioning itself as a competitive player in the global AI landscape.[10]

Figure 1. SEA-6 Government AI Readiness Index, 2024



Source: Oxford Insights, 2024

Recognising AI as a key driver of productivity and economic growth drove governments across the region to update previously released AI roadmaps and frameworks.[11] 2024 saw expanded coverage to address generative AI and introduced additional guidelines in response to the rapidly evolving nature of the technology. Below are the key AI governance developments across SEA-6 in 2024.

Updating AI roadmaps and guidelines was especially important given its widespread adoption across the region. 90% of students and 72% of employees have used generative AI in some capacity across Indonesia, Malaysia, the Philippines, Thailand and Vietnam.[12] However, only half of employees surveyed believe their managers are aware of their AI usage, highlighting a gap in organisational oversight and AI governance.

Updates to AI governance frameworks tend to incorporate specific provisions to address AI risks, generative AI and ethical considerations. In Thailand, the Ministry of Digital Economy and Society and the Electronic Transactions Development Agency (ETDA), through the AI Governance Center (AIGC), jointly introduced the AI Governance Guideline for Executives and the Generative AI Governance Guideline for Organizations.[13] These guidelines emphasise responsible AI governance to balance generative AI adoption with risk management. Similarly, Singapore released its Model AI Governance Framework for Generative AI in 2024, building upon its original AI Governance Framework from 2019 and the National AI Strategy 2.0, which was released in 2023.[14] The updated Model AI Governance Framework for Generative AI provides clear guidelines on transparency, accountability and risk mitigation for such applications. In Malaysia, the National Guidelines on AI Governance and Ethics includes specific provisions on disclosure, data protection and legal liabilities associated with generative AI.[15]

Table 1. Key AI Governance Developments in SEA-6, 2024

Country	Governance and Policies	Focus Areas
Indonesia	● Draft AI Regulation (released 2024, currently under review)	● AI regulation beyond voluntary ethics ● Mandatory risk classification and compliance for AI firms ● AI liability frameworks and high-risk AI oversight
Malaysia	● National Guidelines on AI Governance and Ethics (NAIGE)	● Promoting AI adoption in a safe, trustworthy and ethical manner
Philippines	● National AI Strategy Roadmap 2.0	● AI talent, ethics, innovation and research
Singapore	● Model AI Governance Framework for Generative AI (MGF-Gen AI)	● Focus on Generative AI regulation and positioning Singapore as a global AI hub
Thailand	● AI Governance Guidelines for Executives & Organizations	● Generative AI guidelines and AI in public services ● AI fairness, bias detection and accountability
Vietnam	● Official dispatch No.83/CD-TTg of 2024 ● Decision No.699/QD-BTTTT of 2024	● Training high-quality human resources in the fields of Semiconductor Microchips, Artificial Intelligence and Cloud Computing ● Strategy for Developing Artificial Intelligence Applications to 2030 (Application AI Strategy)

Source: Tech for Good Institute, 2025

Moreover, the SEA-6 countries emphasised AI research, development and skills training. In the Philippines, the government updated its AI strategy roadmap, originally released in 2021, by launching the National Artificial Intelligence Strategy Roadmap 2.0 and established the Center for AI Research.[16] These initiatives were designed to enhance AI research and development to position the country as a competitive hub for AI innovation. Vietnam's Ministry of Science and Technology (MoST) issued Decision No. 1290/QD-BKHCN (2024), which sets out principles for the responsible research and development of AI systems,[17] a framework for ethical AI governance and reinforces the country's commitment to responsible AI innovation. Recognising the need for skilled talents to support AI adoption, governments are placing greater emphasis on AI skilling initiatives. Thailand's Ministry of Higher Education, Science, Research and Innovation (MHESI) introduced the "MHESI for AI" initiative, which prioritises AI talent development.[18] As part of this effort, the "AI University" programme aims for 90% of its graduates to acquire foundational AI knowledge, with a goal of training 30,000 AI professionals within three years. Initiatives in Malaysia such as the National Digital Literacy Programme and AI for Rakyat aim to close the skills gap and equip the workforce with capabilities needed for high-value jobs.[19]

While Southeast Asian countries share common priorities in AI governance, they diverge in approach. Currently, ASEAN and most countries favour soft laws and non-binding regulations, such as the ASEAN Guide on AI Governance and Ethics (2024). While none of the SEA-6 economies have legally binding AI regulations currently, this may change in 2025. Indonesia, in particular, is thinking about moving towards a stricter AI governance framework. The Ministry of Communication and Digital Affairs is currently developing more robust AI regulations, aligning with international frameworks such as UNESCO's Readiness Assessment Methodology (RAM).[20] This regulation is expected to be formalised through a Ministerial or Presidential decree, introducing legally binding compliance measures in 2025.[21]

2.2. Cybersecurity and Data Protection

Another shared priority in 2024 was cybersecurity and data protection. Despite cybersecurity investments growing at an annual rate of 14% since 2021, with projections reaching US$6.1 billion by 2026, the region continues to face escalating cyber risks with cyberattacks, data breaches and ransomware.[22] In 2023, for example, businesses in Southeast Asia reportedly faced 36,000 attacks on a daily basis.[23] Notably, the Philippines saw a 243% increase in web threats from 2022 to 2023, Singapore recorded an 86% rise while Thailand experienced a 24% increase over the same period.[24]

Table 2. Key Cybersecurity and Data Governance Developments in SEA-6, 2024

Country	Key Cybersecurity and Data Protection Laws	Focus Areas
Indonesia	● Updates to the Electronic Information and Transactions (EI)T Law ● Personal Data Protection (PDP) Law ● National Cyber and Crypto Agency (BSSN) Regulations	● Enhanced provisions against cyber-enabled crimes ● Enforcing data privacy compliance ● Coordinating cyber incident response
Malaysia	● Cybersecurity Act of 2024 ● Amendments to the Communication and Multimedia Act ● Personal Data Protection Act (PDPA) Amendments (2024)	● Protecting Critical Information Infrastructure (CII) ● Enhancing provisions for online safety ● Strengthening cybersecurity compliance for businesses
Philippines	● National Cybersecurity Plan 2025-2028	● Strengthening cyber resilience in critical infrastructure ● Enhancing cross-border cooperation on cyber threats.
Singapore	● Cybersecurity (Amendment) Bill No. 15/2024 ● Personal Data Protection Act (PDPA) Advisory Guidelines	● Securing cloud computing and supply chain vulnerabilities ● Updates to responsible data processing for organisations whose products or services are accessed by children.
Thailand	● Cloud Security Standard 2024	● Enhancing secure cloud adoption in government and industries
Vietnam	● National Data Strategy to 2030 ● Decision No. 1437/QD-TTg	● Ensuring information security, cybersecurity and personal data protection ● Framework to draft the Personal Data Protection Law and the Data Law

Source: Tech for Good Institute, 2025

Therefore, governments across the region updated its cybersecurity laws, prioritised critical infrastructure protection, enhanced enforcement mechanisms and strengthened data protection regulations. The table below provides an overview of key policy developments aimed at improving the security of essential infrastructure and sectors across each country.

In 2024, SEA-6 governments examined the security of critical information infrastructure (CII) and updated its existing guidelines. The Philippines updated its comprehensive roadmap for strengthening infrastructure resilience and mitigating vulnerabilities in key sectors through the National Cybersecurity Plan 2025-2028.[25] Thailand introduced the Cloud Security Standard 2024, which established security protocols for government and industry cloud adoption to ensure compliance with international cybersecurity norms.[26] Singapore, reinforcing its position as a global cybersecurity leader, enacted the Cybersecurity (Amendment) Act 2024, mandating stricter security measures for cloud service providers and to address supply chain vulnerabilities.[27]

With data breaches and online fraud on the rise, Southeast Asian countries also tightened data protection laws and shifted toward stricter enforcement mechanisms. Indonesia's Personal Data Protection (PDP) Law came into full effect on 17 October 2024, requiring businesses to comply with data security mandates.[28] Malaysia made amendments to the Personal Data Protection Act (PDPA) in 2024 to expand its regulatory oversight, particularly for commercial data processing, mandating that businesses adhere to stricter data management practices and ensure compliance with accountability standards. The amendments also introduced data breach notification requirements, though other specific enforcement details are still under development.[29] Vietnam's Decision No. 142/QD-TTg approved the National Data Strategy to 2030 to establish key provisions for information security, cybersecurity and personal data protection.[30]

At a regional level, the region came together to improve capabilities and skills to respond to cyber incidents. At the 9th ASEAN Ministerial Conference on Cybersecurity in October 2024, ASEAN announced the operational launch of the ASEAN Regional Computer Emergency Response Team (CERT) facility,[31] co-located at the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), which aims to enhance the collective cybersecurity efforts across the region.

2.3. Safety and Trust

Ensuring user safety and trust became a top priority for many SEA-6 governments in 2024. While the rapid growth of e-commerce, digital banking and fintech services created new opportunities, it also introduced significant risks, including fraud, misleading advertisements, counterfeit goods and financial scams. Beyond cyber threats targeting businesses and organisations, there was a notable rise in scams and fraud targeting direct consumers.[32]

While cybersecurity and data protection are important components of user protection, preventing data breaches alone is not sufficient. Beyond unauthorised intrusions, consumers faced risks from self-authorised breaches caused by manipulation and social engineering tactics. Financial fraud, including scams that result in significant monetary losses and deceptive e-commerce practices, such as the sale of counterfeit goods and misleading advertising, threaten consumer trust. The Global Anti-Scam Alliance (GASA) reported that scam losses in Asia amounted to an estimated US$688.42 billion in 2024, accounting for more than half of global scam losses.[33] In Singapore, for example, victims lost approximately US$481.4 million in 2023[34], while losses from fraud and scams accounted for nearly 3.6% of Vietnam's gross domestic product (GDP) in the same year.[35]

This growing challenge is shaping conversations around safety and trust in the digital economy. As technology adoption continues to rise, the focus shifts to beyond merely protecting systems and data to ensure overall digital safety. Technical cybersecurity protections alone are no longer sufficient as human-centred concerns such as online harms, scams and fraud are equally critical. This shift is reflected in recent regulatory responses across the region, including Singapore's Online Criminal Harms Act, Malaysia's upcoming Online Safety Bill and Indonesia's revision of the Electronic Information and Transactions (EIT) Law. These measures acknowledge that digital safety must extend beyond system integrity to actively protect users' well-being in the online space. While security serves as the foundation, safety expands the scope by prioritising user welfare. Ultimately, a digital ecosystem that is not only secure and safe but also transparent and accountable fosters public trust, empowering users to engage online with confidence.

In 2024, all SEA-6 governments implemented new regulatory measures to protect consumers, enhance platform accountability and ensure safer digital transactions. Table 3 summarises notable developments to improve consumer welfare and public trust in the digital ecosystem.

Table 3. Key Safety and Trust Policies in SEA-6, 2024

Country	Key Safety and Trust Policies	Key Focus Areas
Indonesia	● Draft Amendments to the Consumer Protection Law (under review) ● OJK Regulation No. 3 of 2024 (Financial Sector Technology Innovations)	● Strengthen e-commerce dispute resolution mechanisms ● Impose registration requirements for fintech providers ● Mandate sandbox testing for fintech innovations before deployment
Malaysia	● Online Safety Act ● Amendment to the Communications and Multimedia Act (CMA)	● Require platforms to implement measures against online fraud and harmful content ● Expand MCMC's authority to enforce penalties on fraudulent digital ads ● Mandate platform accountability for misleading and harmful content ● Strengthen consumer privacy rights in digital transactions
Philippines	● Implementing Rules and Regulations of the Internet Transactions Act ● Anti-Financial Scamming Act (AFASA)	● Establish an E-Commerce Bureau under the Department of Trade and Industry (DTI) ● Require digital platforms to ensure transparency and fair pricing. ● Expand consumer protections against phishing, banking fraud and online scams
Singapore	● Shared Responsibility Framework for Digital Transactions	● Implement liability-sharing between banks, digital platforms and consumers to resolve fraud cases
Thailand	● Digital Platform Services (DPS) Law ● Guidelines for Managing Advertisements on Digital Platform Services ● Cybercrime Case Division	● Require digital platforms to register with ETDA for consumer protection compliance ● Regulate advertising transparency and consumer rights protection ● Created a specialised court division handling cyber fraud, financial scams and e-commerce disputes
Vietnam	● National Data Strategy to 2030 (Decision No. 142/QD-TTg)	● Strengthen consumer data protection and privacy in e-commerce transactions.

Source: Tech for Good Institute, 2025

In particular, oversight of online marketplaces and digital platforms to combat fraud and deceptive practices were strengthened. In the Philippines, the Internet Transactions Act finalised its implementing rules and regulations in 2024, mandating stricter regulation of online selling, requiring platform operators to verify merchant legitimacy and ensure product authenticity.[36] Thailand's Digital Platform Services (DPS) Law and the new advertising transparency guidelines from the Electronic Transactions Development Agency (ETDA) aimed to eliminate deceptive marketing tactics and enhance consumer awareness in digital transactions.[37] Malaysia's recent updates to the Online Safety Act classified financial fraud as priority harmful content, requiring platforms to enhance its efforts to detect and remove it.[38] Indonesia is also considering stricter oversight of online transactions, with the anticipated 2025

Consumer Protection Law (currently under review) set to introduce stronger e-commerce dispute resolution mechanisms to ensure fair business practices in digital marketplaces.[39]

Additionally, Singapore introduced greater accountability along the fraud value chain with the Shared Responsibility Framework, establishing liability-sharing mechanisms between banks, digital platforms and consumers.[40] This initiative was aimed at enhancing consumer confidence by clearly defining the responsibilities of financial institutions and digital platforms in fraud prevention. Similarly, the Philippines' Anti-Financial Scamming Act (2024) strengthened legal protections for victims of online scams, requiring fintech platforms to implement fraud detection and prevention measures.[41] These measures signalled a push to enhance security in digital financial transactions, ensuring that regulators, financial service providers and platforms work together to prevent fraud and protect consumers from financial harm.

Addressing digital fraud and cyber-related offences requires deep expertise and extensive interagency coordination. In Thailand, the government invested in specialised expertise with a new Cybercrime Case Division within the Thai Criminal Court. This dedicated division is responsible for handling cases related to cyber fraud, data breaches and intellectual property infringements.[42] The Philippines also took proactive measures through the Anti-Financial Scamming Act to foster whole-of-government coordination, empowering the central bank Bangko Sentral ng Pilipinas to investigate financial fraud cases, apply for cybercrime warrants and issue enforcement orders, as well as facilitating collaboration between the central bank, the National Bureau of Investigation (NBI) and the Philippine National Police (PNP) to enhance investigative efforts and improve the efficiency of prosecuting financial cybercrimes.[43]

3. Key Governance Trends

Governments are continuously evolving, adapting their structures and approaches to meet emerging policy priorities. In 2024, several significant developments took place, including:

- **Reorganisation.** Governments rebranded and restructured agencies to enhance governance effectiveness to promote holistic digital development. Specialised agencies were created to address specific challenges.

- **Greater Policy Coordination.** As technology impacts all sectors, tech governance requires increasing coordination across government agencies, including sectoral agencies such as education, transportation and sub-national agencies.

- **Increasing Policy Innovation.** The rapid advancement of AI and emerging technologies highlight the need for governments to promote innovation while maintaining government as a relevant key stakeholder. In response, the tech governance toolbox expanded beyond traditional regulation to include frameworks, soft-law guidelines and regulatory sandboxes. These approaches allow governments to observe innovation in real-time and create space for public-private cooperation to safeguard public interest.

This chapter outlines key governance trends in the region.

3.1. Structural Changes in the Regulatory Landscape

2024 saw structural changes in key agencies charged with tech governance, which included renaming existing regulators, establishing new agencies and creating specialised bodies.[44] Table 1 outlines the most recent developments in SEA-6's regulatory landscape.

Table 1. The Evolving Regulatory Landscape in SEA-6, 2024

Country	Key Regulatory and Governance Developments
Indonesia	● Renamed the Ministry of Communication and Informatics (Kominfo) to the Ministry of Communication and Digital Affairs (Komdigi) ● Split the Ministry of Education, Culture, Research & Technology into three: Ministry of Higher Education, Science & Technology, Ministry of Primary and Secondary Education, and Ministry of Culture
Malaysia	● The Ministry of Communications and Digital separated into two ministries: Ministry of Communications and a new Ministry of Digital ● National AI Office (NAIO) launched under MyDIGITAL to coordinate AI policy, R&D, and security
Philippines	● The E-Commerce Bureau was formed under the Department of Trade & Industry (DTI) as mandated by the Internet Transactions Act
Singapore	● Renamed the Ministry of Communications and Information (MCI) to the Ministry of Digital Development and Information (MDDI). MDDI is the parent ministry of IMDA
Thailand	● Established the Cybercrime Case Division of the Thai Criminal Court, effective on April 1st, 2024 ● Established the Special Committee for the Study of Approaches to Regulating and Promoting the Use of Artificial Intelligence (AI) by the Thai Parliament in January 2024
Vietnam	● Planned restructuring of government ministries: 8 ministries to be maintained, while 14 are reorganised or merged in 2025 (e.g., possible merger of Ministry of Planning & Investment with Ministry of Finance; Ministry of Information & Communications (MIC) with Ministry of Science & Technology (MoST))

Source: Compiled by the Tech for Good Institute, 2025

Renaming key ministries signalled a broader focus beyond digital economy growth. Communication and telecommunications ministries, traditionally responsible for overseeing technology development and information infrastructure, took on broader responsibilities to reflect the digital ecosystem's impact across society and the economy. For example, Indonesia's Ministry of Communication and Informatics (Kominfo) became the Ministry of Communication and Digital Affairs (Komdigi), reflecting an expanded mandate that goes beyond basic information and communications services to include the wider digital affairs.[45] A similar evolution can be seen in Singapore's renaming of the Ministry of Communications and Information (MCI) to the Ministry of Digital Development and Information (MDDI).[46] This change emphasises the shift from communications infrastructure but also a broader ambition for digital development across government, the economy and society.[47] The name change follows the

October 2023 restructuring, when the Smart Nation and Digital Government Group (SNDGG) merged with the digital development functions of the Ministry of Communications and Information (MCI) to form an expanded Smart Nation group.[48]

Alongside these structural realignments, countries in the region are either establishing or empowering specialised bodies to address priority policy areas highlighted in the previous chapter. This trend reflects the growing complexity of the digital economy, where a targeted approach with dedicated resources is essential to enhance precision and effectiveness in governance and regulation. For instance, in the field of AI, Malaysia's National AI Office (NAIO), incubated under MyDIGITAL Corporation, was established in 2024 to drive AI investments, promote innovation, and support governance and security goals.[49] Singapore has also recently designated the Infocomm Media Development Authority (IMDA) and NTU's Digital Trust Centre as the country's AI Safety Institute.[50] This aligns with similar initiatives both within the region and globally, where national AI safety institutes have been established to address emerging risks and ensure responsible AI development. Countries such as the United States, Canada and Japan have also launched their own AI safety organisations.[51]

Beyond **AI-focused organisations, new specialised agencies have been established to address broader digital economy issues, including e-commerce and cybersecurity.** In the Philippines, the E-Commerce Bureau was formed under the Department of Trade & Industry (DTI) as mandated by the Internet Transactions Act of 2023. The bureau is tasked with formulating policies, plans and programmes to develop the e-commerce industry while ensuring compliance and enforcement within the sector.[52] In Thailand, the Thai Criminal Court established the Cybercrime Case Division, which became effective on April 1, 2024.[53] This dedicated division is responsible for handling cybercrime cases related to cyber fraud, data breaches and intellectual property, and is expected to enhance the Criminal Court's efficiency, ensuring a faster and more specialised legal proceedings.[54]

Implementation strategies vary across different countries, particularly in how ministries are structured to oversee digital governance. One notable example is the separation of regulatory and promotional functions within government agencies. Thailand's Ministry of Digital Economy and Society (MDES) now oversees both the Electronic Transactions Development Agency (ETDA), which acts as a regulator, and the Digital Economy Promotion Agency (DEPA), which focuses on industry development. This structural distinction provides a clear distinction between regulatory functions and industry support. In contrast, Singapore's IMDA operates as both a regulator and a promotion agency, adopting an integrated governance model that combines regulatory oversight with sectoral development. Meanwhile, some countries are expanding their governance frameworks by creating more specialised ministries, whereas Vietnam is currently reviewing its governance structure with plans to merge and streamline key agencies. These variations highlight the diverse governance models across Southeast Asia, reflecting the different strategies governments are employing to navigate tech governance.

New and reorganised ministries will take time to have steady operations. While many of these changes began in 2024, the transition will extend into 2025 and beyond. In the near term, both regulators and the private sector will go through a learning process as they navigate the evolving regulatory landscape. Businesses, in particular, will need to adapt to new oversight

structures, compliance requirements and engagement channels with newly established agencies. Additionally, government-to-government collaboration involving these newly formed ministries may need to be redefined and strengthened to maintain regulatory clarity and coordination.

3.2. Greater Policy Coordination

The creation of new ministries and agencies, along with the increasingly cross-sectoral nature of governance challenges, demonstrates the need for coordination between agencies. In 2024, agencies that were not traditionally seen as "tech regulators", such as education, transportation and national enforcement, have collaborated to support priority policies and initiatives. As digital technologies continue to shape both the economy and society, a whole-of-government approach will be essential to ensure effective tech governance.

For example, governments across Southeast Asia have accelerated efforts to prepare and upskill the current and future workforce, especially given the increasing pace of innovation. The Indonesian government established the Ministry of Higher Education, Science and Technology and the Ministry of Primary and Secondary Education, which are responsible for developing digital skills, STEM education and data science capabilities to support national goals in renewable energy and food technology.[55] Singapore focused on ensuring continued employability with a new programme for mid-career Singaporeans aged 40 years and above[56], and drive breakthroughs in research by promoting AI methodologies and tools that can be applied across various scientific disciplines.[57] Thailand's Ministry of Higher Education, Science, Research and Innovation (MHESI) launched the "MHESI for AI" Initiative. The programme aims to have 90% of its graduates to possess foundational AI knowledge by 2027, with a target of training 30,000 AI professionals within three years to strengthen the country's digital workforce.[58] Vietnam's Ministry of Education and Training (MoET) was tasked with launching a comprehensive digital literacy and AI education programme, aligning with Vietnam's ambition to become a regional hub for semiconductor and AI talent.[59]

Other sectors also played an active role in governing the digital economy. In the Philippines, the Land Transportation Franchising and Regulatory Board (LTFRB), a regulator under the Department of Transportation, updated its policies to integrate electric vehicles (EVs) into taxi services[60], while extending vehicle age limits for the Transport Network Vehicle Services.[61] The Philippines also took proactive measures through the Anti-Financial Scamming Act to foster whole-of-government coordination, empowering the central bank Bangko Sentral ng Pilipinas to investigate financial fraud cases, apply for cybercrime warrants, and facilitate and issue enforcement orders. The Anti-Financial Scamming Act also supported collaboration between the central bank, the National Bureau of Investigation (NBI) and the Philippine National Police (PNP) to enhance investigative efforts and improve the efficiency of prosecuting financial cybercrimes.[62] To advance and boost confidence in the digital society, Thailand's Department of Provincial Administration (DOPA), under the Ministry of Interior, has implemented digital ID and facial verification systems to offer safe and privacy-focused identity verification solutions.[63]

These examples highlight how more agencies are now essential players in technology governance. Workforce development, combating cybercrimes and digital identity implementation are no longer niche initiatives but fundamental aspects of national digital strategies. Moving forward, the need for whole-of-government coordination will only grow, with governments needing to foster cross-sector coordination and policy coherence to effectively govern the digital economy.

3.3. Continued Policy Innovation

To foster innovation while ensuring effective governance, governments in 2024 have increasingly adopted flexible regulatory tools such as frameworks, soft-law guidelines and regulatory sandboxes. Hard laws are no longer the sole mechanism for regulating the digital economy, as legislation often takes time to develop and even longer to amend. Given the rapid pace of technological advancements, these alternative governance approaches allow governments to observe innovation in real-time, create space for public-private collaboration and safeguard public interest without stifling progress.

Innovative policy approaches are designed to be flexible and responsive to emerging technologies and market dynamics. An example of this is how outcome-based or principle-based regulation shifts away from rigid and prescriptive rules toward broader, high-level objectives that industries must meet.[64] For instance, Australia's autonomous vehicle trial framework adopts performance-based guidelines rather than detailed mandates. Moreover, co-regulation involving shared responsibility between government and industry, is where industries develop codes of practice in consultation with regulators. Singapore's Buy Now, Pay Later (BNPL) Code of Conduct exemplifies this model, with industry-imposed sanctions ensuring compliance.[65] Meanwhile, dynamic regulation leverages real-time data and analytics to continuously monitor and adjust policies. A recent example was the rapidly evolving COVID-19 regulations, where safe distancing measures were frequently updated based on emerging data. These adaptive regulatory models enable governments to strike a balance between innovation, oversight and public interest.

Among these innovative approaches, regulatory sandboxes remain a key trend in the region. This allows regulators to foster innovation in a safe and responsible manner, while providing a structured environment for closer dialogue between regulators and businesses across various industries. It also offers opportunities for deeper regulatory learning and enables regulators to adopt a more adaptive and forward-looking approach to regulation. In addition to existing sandboxes,[66] 2024 saw the following developments:

Table 6. Key Sandbox Developments in SEA-6, 2024

Country	Sandbox Developments
Indonesia	● Updated the framework of the Financial Sector Technology Innovation sandbox under OJK Regulation No. 3 of 2024, superseding the 2018 regulation
Malaysia	● Released policy document on Financial Technology Regulatory Sandbox Framework, updating the 2015 regulation
Philippines	● Established the Strategic Sandbox for the financial sector through a memorandum circular
Singapore	● Expanded the Privacy Enhancing Tech (PET) Sandbox to cover innovations supported by generative AI
Thailand	● Established the Digital Assets Regulatory Sandbox under the SEC ● Updated the framework for testing Fintech Innovations under the BOT
Vietnam	● Updated the draft law on Fintech Regulatory Sandbox under the SBV

Source: Compiled by Tech for Good Institute, 2025

It is worth noting that most regulatory sandboxes in 2024 still focus on the financial sector. This aligns with findings from the Tech for Good Institute, which reported that over 40% of sandboxes in the region were dedicated to financial services between 2016 to 2023.[67] Fintech remains a critical driver of financial inclusion in Southeast Asia, where large segments of the population remain unbanked or underbanked.

It's notable to note that emerging technologies supporting priority policy areas proved to be good candidates for sandboxing. Singapore's Privacy Enhancing Technology (PET) Sandbox expanded in 2024 to support generative AI applications, aligning with global trends in AI governance and data privacy.[68] Thailand's Digital Asset Regulatory Sandbox was designed to facilitate the adoption and integration of digital assets into mainstream financial services.[69] Singapore's Generative AI Sandbox for SMEs sought to bridge the gap between governance at the theoretical and practical levels, providing small and medium-sized enterprises to gain hands-on experience with adopting AI solutions responsibly.

Governments are actively reviewing and updating their sandbox frameworks to ensure they remain fit for purpose. For example, Indonesia revised its POJK 3/2024 2018 framework by introducing stricter eligibility criteria, mandatory test plans and clearer exit procedures to reflect a more structured oversight.[70] Malaysia's 2024 policy document on Financial Technology Regulatory Sandbox Framework replaced its 2016 version, highlighting the central bank's commitment to adapting regulatory approaches in response to evolving fintech developments.[71] Similarly, Thailand updated its sandbox framework in June 2024, enhancing flexibility while safeguarding financial stability and consumer protection.[72] Vietnam's regulatory sandbox remains in the draft stage but the latest version has narrowed its scope to within the banking industry, reducing the covered areas from seven sectors to three: credit scoring, Open Application Programming Interfaces (Open API), and peer-to-peer lending (P2P lending).[73]

4. Country Overviews

Country overviews provide an in-depth analysis of the SEA-6, namely Malaysia, Indonesia, the Philippines, Singapore, Thailand and Vietnam. Experts from each country have contributed deep dives that highlight significant advancements in governance structures and policy frameworks. This section details how each country navigates the evolving digital landscape while identifying strategic priorities to shape its national tech governance.

Shaping the Digital Future: Regulatory Updates from Indonesia

Hafiz Noer, Head of Research at Center for Digital Society (CfDS)
M. Irfan Dwi Putra, Research Assistant at Center for Digital Society (CfDS)

Indonesia's digital ecosystem is experiencing a major transition under the newly inaugurated President Prabowo Subianto. Under the new administration, Indonesia has introduced a new governance structure, reallocated regulatory oversight duties and updated national policies aimed at enhancing government coordination while addressing risks associated with digital technology.

The new government has outlined an ambitious vision for digital transformation across all sectors, as emphasised in the National Development Plan 2025-2045.[74] This initiative positions digital transformation as a cornerstone for achieving the administration's bold target of 8%economic growth,[75] reflecting its commitment to leveraging technology to drive innovation, efficiency and sustainable development.

Interestingly, the government's approach towards digital technology has become more stringent, highlighting regulatory refinement compared to the previous administration, which were often criticised for their lack of clarity and inadequate law enforcement in an evolving digital technology landscape.[76]

Key Trends in Indonesia's Tech Policy

Indonesia made strides toward legal maturity in 2024 by addressing emerging digital technologies. Regulatory measures were introduced and amended to adapt with the dynamic technological advancement and its associated challenges, focusing on three key areas: advancing AI development, strengthening cybersecurity, cyber resilience and data protection frameworks, and enhancing consumer protection and competition laws.

1. AI Governance

To ensure trustworthy and responsible AI governance in Indonesia, the Ministry of Communication and Digital Affairs is currently developing stricter AI regulation.[77] Aligned with international frameworks like UNESCO's Readiness Assessment Methodology (RAM), this measure is expected to take a more legally binding Ministerial or Presidential Regulation[78] by adopting a dual approach: a horizontal approach by harmonising existing regulations and guidelines such as the Electronic Information and Transactions Law (EIT Law), the Personal Data Protection Law (PDP Law) and the AI Ethics Circular Letter; and a vertical approach that addresses sector-specific applications in areas such as health and finance. To this date, AI governance in Indonesia has been primarily guided by the AI Ethics Circular Letter,[79] which is not legally binding and has relied on the voluntary compliance of tech firms. However, if the current draft of AI regulation is enacted, Indonesia will establish a robust, legally binding regulatory framework for AI governance, potentially introducing sanctions for non-compliance.

2. Cybersecurity and Data Protection

Beyond AI, the government also strengthened regulatory frameworks for cybersecurity, cyber resilience and data protection. Reflected in the Second Amendment of the EIT Law,[80] it enhances provisions against cyber-enabled crimes, introduces safeguards for child online safety and strengthens the government's role in creating a secure digital ecosystem. In 2024, the National Cyber and Crypto Agency (BSSN)—Indonesia's primary authority on cybersecurity, issued a series of regulations to bolster cybersecurity and cyber resilience. These include guidelines on cyber incident[81] and cyber crisis management,[82] information security self-assessments for MSMEs,[83] the National Action Plan for Cybersecurity,[84] the implementation of the conformity assessment of Indonesia Common Criteria for IT Security Evaluation[85] and the implementation of Indonesian cryptographic algorithms.[86]

As of October 17, 2024, the grace period for data protection compliance with PDP Law has officially ended. This means that businesses are now required to fully comply with PDP Law, with potential administrative and criminal sanctions for any violations. The implementing regulation for the PDP Law is currently undergoing harmonisation[87] and is expected to be enacted in 2025. Furthermore, the government is currently drafting a Presidential Regulation to establish a Personal Data Protection Authority, which will serve as the oversight body for PDP Law implementation.

3. Consumer Protection and Competition

The last focus area is consumer protection and competition laws. In 2024, the Draft Law on Consumer Protection[88] was prioritised in the nation's legislation programme, with plans for re-entry in 2025. This bill will address the evolving landscape of digital technology by introducing provisions for consumer protection in online transactions. Furthermore, the bill will introduce strict liability for businesses, holding them accountable for harm caused to consumers by their goods or services, regardless of fault. The Financial Services Authority (OJK) is also strengthening consumer protection in the financial sector through new regulations on fintech innovations to ensure safety and reliability before products reach consumers.

Additionally, the government is currently assessing the implementation of anti-monopoly regulation within the digital ecosystem.[89] This new regulation is expected to draw inspiration from the European Union's Digital Market Act (DMA) and Digital Services Act (DSA), though its precise form remains undecided. Concurrently, the Indonesia Competition Commission (KPPU) is intensifying its oversight of the digital economy, closely monitoring major tech firms such as Shopee,[90] TikTok[91] and Starlink,[92] after previous cases involving alleged competition violations by Google.[93]

Key Trends in Indonesia's Tech Governance

1. Renaming of Relevant Digital Ministries

There are two major governance shifts that reflect President Prabowo's digital technology direction. First is the renaming of the Ministry of Communication and Informatics ("Kominfo") to the Ministry of Communication and Digital Affairs ("Komdigi"). The ministry is led by Meutya Hafid, a seasoned politician of the Golongan Karya Party, previously holding a position as the Head of Commission I of the Indonesian House of Representatives (DPR RI) which focuses on ICT, foreign affairs, defense and intelligence. Meutya was appointed due to her lengthy experience in parliament for 15 years, navigating ICT issues. She is aided by two vice ministers: Vice Minister Nezar Patria and Angga Raka Prabowo. Both vice ministers have stayed in their post in the previous administration with Nezar being appointed since former President Joko Widodo's second term (2019-2024), whereas Angga, who is a Gerindra cadre, was appointed later in August 2024.

Renaming this ministry accentuates Prabowo's ambition to accelerate digital transformation. Prabowo's administration views digital technology as a catalyst for efficient public service delivery, economic growth, job creation and innovation, all in pursuit of the ambitious goal of achieving 8%economic growth. Regardless of the ambitious move, the Komdigi is encountering administrative adjustments due to the renaming of the ministry. Through Presidential Regulation No. 174 of 2024,[94] Komdigi restructured its internal organisation by defining 'digital' both as a device and as a system. Below is the comparison between the Kominfo and the Komdigi structure:

Ministry of Communication and Informatics 2019 - 2024	Ministry of Communication and Digital Affairs 2024 - 2029
● Directorate General of Resources and Postal and Informatics Equipment	● Directorate General of Digital Infrastructure
● Directorate General of Postal and Informatics Services	● Directorate General of Government Digital Technology
● Directorate General of Informatics Applications	● Directorate General of Digital Ecosystem
● Directorate General of Public Information and Communication	● Directorate General of Digital Space Surveillance
● Agency for Human Resources Research and Development	● Directorate General of Public Communication and Media
● General Secretariat	● General Secretariat
	● Human Resources Development Agency for Communication and Digital

This reorganisation and renaming highlights the shifting objectives in the ministry's role. The previous administration focused on traditional communication and informatics, such as providing postal and informatics services. Although these strategies provided foundational roles in the ICT infrastructure and addressed legacy systems, it was less equipped with handling digital technology issues. Current arrangements within the ministry indicate a stronger focus on building a robust digital infrastructure, developing a comprehensive digital ecosystem and addressing digital technologies risks. This shift reflects a proactive government approach, recognising digital technology both as a device and as a system that can foster economic growth. Furthermore, this restructuring represents a significant step toward more targeted and effective digital technology regulation.

2. Restructuring of Key Agencies to be Responsive to the Digital Age

Furthermore, Prabowo's administration restructured the Ministry of Education, Culture, Research, and Technology to the newly arranged Ministry of Higher Education, Science and Technology, Ministry of Primary and Secondary Education, and the Ministry of Culture. As part of his vision, President Prabowo aims to introduce STEM subjects from early elementary school.[95] While STEM subjects have been introduced at this level, he believes that the current curriculum is inadequate to generate students who excel in STEM fields. This is reflected through Indonesia's PISA low results in mathematics, reading comprehension and science as compared to the previous years.[96] To address this, Prabowo asked the Minister of Primary and Secondary Education, Abdul Mu'ti, to review the existing mathematics curricula, as it is believed to be a foundational competence in science and technology.[97] Moreover, STEM subjects will be prioritised for candidates who pursue master's and doctoral studies through Indonesia's Endowment Fund for Education Agency (LPDP). This initiative seeks to strengthen the link between education, research and industry, with the ultimate goal of supporting the President's policy priorities in food, energy, water management and downstreaming.[98] However, the specific mechanisms for integrating LPDP scholars into these national visions remain unclear.

3. Sector-Specific Approaches to Digital Governance

Within the digital economy landscape, the financial sector remains at the forefront of regulatory development, particularly under the Financial Services Authority (OJK). In 2024, OJK prioritised regulations that target financial sector technology innovations under the OJK Regulation No. 3 of 2024[99], which covers digital banks, fintech lending and digital assets. To support its implementation, OJK has issued several regulations, including requirements for registering fintech providers,[100] implementing a sandboxing mechanism,[101] reporting obligations related to innovative deployments in the financial sector[102] and establishing an association of fintech providers.[103]

Additionally, OJK currently holds regulatory authority over digital financial assets, including crypto assets. Indonesia has regulated crypto assets since 2018 under the Minister of Trade Regulation No. 99 of 2018.[104] It classifies crypto assets as commodity futures under the oversight of the Commodity Futures Trading Supervisory Agency (Bappebti). However, due to the rapid development and growing use of crypto assets as an investment instrument, it has become increasingly difficult for Bappebti to maintain effective supervision. As a result, in 2023, the Law on Financial Sector Development and Strengthening (UU P2SK) transferred the authority to oversee crypto assets to OJK. The OJK's oversight of crypto assets took place in January 2025. Ahead of this shift, OJK issued a regulation on crypto assets trading on December 10, 2024, where regulation took effect on January 10, 2024.[105] It will impose more stringent requirements on crypto assets trading in Indonesia, encompassing compliance with anti-money laundering and counterterrorism financing measures, robust consumer protection and a more stringent cybersecurity standard.

Moving forward

Indonesia's digital landscape in 2024 witnessed a complete overhaul in terms of governance structure and tech regulation. President Prabowo's vision on digital technology is clear as he addressed his ambitions in renewable energy, food, data science and water management, with the ultimate objective of building industry downstreaming across sectors. Digital technology is positioned as a tool to achieve these sectoral goals. STEM subjects at schools and higher education are prioritised to generate skillful human resources that can fit in those sectors.

However, new governance structures may halt these objectives. Ministries with new internal structures like the Komdigi and the Ministry of Higher Education, Science and Technology must align with the new working procedures and organisational structures (SOTK)—a vital component in a newly-organised government agency that addresses the division of labour, streamlining and well-structuring of the organisation.

Additionally, the vision to prioritise STEM subjects is not yet matched by adequate job opportunities in the market, posing a systemic challenge as Indonesia is trapped in a 'premature'[106] deindustrialisation phase, due to the decline of the manufacturing industry's contribution to the national gross domestic product (GDP) since 2009. While downstreaming is important, the government must identify and prioritise key sectors in its industrial policy roadmap. This roadmap should extend beyond downstreaming to address the entire value chain of the industry.

2024 marks a shift toward legal maturity in technology regulation, characterised by more stringent regulations on emerging technologies. Previously, Indonesia was exploring how to effectively regulate certain technologies, which resulted in issuing non-binding guidelines. However, the current regulatory approach is more structured and enforceable, aimed at managing the complexities of new digital advancement. While stricter regulations enhance consumer and user protection, they also introduce new challenges for businesses as business owners may face increased regulatory requirements to maintain compliance in the evolving digital landscape.

4.2. Malaysia

Malaysia's New Governance Landscape Amid Regulation Updates

Farlina Said, Institute of Strategic and International Studies
Ariane Yasmin, TIA Editors

Malaysia's governance and regulatory landscape in 2024 can be captured by four laws, one social media licensing regime, one new ministry and one new AI office. The four laws are the Communications and Multimedia Act (CMA) amendment, Personal Data Protection Act (PDPA) amendment, and the Cybersecurity Act and Online Safety Act. The Social Media Licensing Framework encompasses internet messaging and social media service providers. The Ministry of Communications and Digital was split into two, while the new AI office was launched as the National AI Office (NAIO).

Key Trends in Malaysia's Tech Policy

Malaysia's tech policy developments in 2024 covers digitalisation goals, security and safety-related objectives.

1. Development of artificial intelligence

The year 2024 saw various initiatives on AI. These include the launch of an AI Office at the end of 2024 and the introduction of policy documents such as the National Guidelines on AI Governance and Ethics (NAIGE) to provide ethical guidance for developers and users.[107] The AI Office was formed to help drive AI investments, promote innovation, and support governance

and security goals.[108] Strengthening economic growth, improving public services and supporting Sustainable Development Goals are key focus areas. The Office has seven deliverables for 2025, including adoption of regulatory framework, a code of ethics, a technology action plan and creating datasets related to AI technology.

2. Online safety

Malaysia's policy areas for 2024 were targeted in online safety, specifically for protecting children and preventing financial fraud. Malaysia has seen a rise in cyberbullying cases, where in 2023, cases logged fared around 10 cases per day; in 2024 this reached 27 cases daily.[109] The RM100 fine imposed on a cyberbully whose actions contributed to the suicide of TikTok influencer A Rajeswary raised concerns on legal gaps - it did not penalise and place proportional responsibilities in such circumstances.[110] Additionally, child sexual abuse material (CSAM) increased by approximately 55% between 2023 and 2024. Against this backdrop, the Online Safety Act and amended CMA specifically highlights offences involving children.

In the Online Safety Act, CSAM is categorised as priority harmful content, requiring platforms to immediately remove such material. Furthermore, Section 18 (3) of the act mandates safety and design measures to protect children, such as limiting users identified as adults to communicate with users identified as a child and controlling personalised recommendation systems for child users. Meanwhile, amendments to CMA Section 233 clearly define obscene, indecent, false, menacing and grossly offensive content, especially where it is communicated to children.[111]

On the other hand, more than 95,800 online scams were reported from 2021 until April 2024, worth about RM3.18 billion.[112] In 2023, Bukit Aman Commercial Crime Investigation Department reported that e-commerce fraud cases rose by 37% from January to November 2023 with total losses amounting to RM1.13 billion.[113] Due to the sheer losses from scams and fraud, the Online Safety Act now categorises content on financial fraud as priority harmful content, thus requiring the utmost diligence for its removal from platforms. CMA's Section 233 also specifically mentions fraud, and a new provision under Section 233A includes prohibitions on unsolicited commercial electronic messages, including spam. Penalties for Section 233(2) has an increased penalty up to RM500,000 and/or imprisonment for up to two years.

Moreover, the penal code and criminal procedure code were updated for bullying and financial losses. The Penal Code (Amendment) (No 2) expanded its definition of harm to include harm to a person's body, mind, reputation or property, including psychological harm.[114] Criminal Procedure Code Amendment (No.2) Act 2024 articulates the punishments for offences such as harassment, provocation to cause harm and the publication of identity information for the purpose of causing harm.[115] The Penal Code (Amendment) Act 2024 highlights new sections on online financial fraud such as unlawful possession or control of payment instruments or the unlawful transfer of an account controls to another person for unlawful purposes.[116] The punishments of these are articulated in the Criminal Procedure Code (Amendment) Act 2024.[117]

3. Competition and consumer protection

While 2024 did not introduce specific policies to safeguard competition, efforts were made to reduce monopolistic behaviour through data sharing and data portability laws. Newly-inserted Section 43A in the PDPA amendment, for instance, states the right to data portability where a data subject can request for a data controller to transmit the personal data to another data controller if there is technical feasibility and compatibility of the data format.[118] Additionally, the Malaysia Competition Commission will conduct a market review on the digital economy ecosystem under the Competition Act in order to prevent market concentration among a few online marketplace platform operations. It is also expected to table amendments on a merger control regime from the Competition Act 2010 and the Competition Commission Act 2010.

The Online Safety Act features specific obligations for consumer protection, including duties to mitigate risk exposure and issuing guidelines. Sections 15, 16 and 17 aim to empower users by obligating platforms to make available mechanisms that would: (i) allow users to manage online safety, (ii) report harmful content, and (iii) allow users to seek assistance or raise concerns.[119] Furthermore, the Online Safety Committee would require licensed platforms to demonstrate methods to reduce risk and exposure to harmful content to satisfy the Committee. Lastly, while the Cybersecurity Act and PDPA amendment does not state explicitly steps for the protection of consumers; the Act's purpose is to monitor national cybersecurity incidents and mandate data breach notifications, which in turn will shape future cybersecurity policies that allows Malaysia to develop improved preventive and resilient measures.

Key Trends in Malaysia's Tech Governance

1. Specialised mandates

The separation of the Ministry of Communications and Ministry of Digital[120] has resulted in certain agencies shifted to the latter. This includes MyDIGITAL, Malaysia Digital Economy Corporation (MDEC), Personal Data Protection Department, Cybersecurity Malaysia, MYNIC Berhad and the government's ICT modernisation vehicle, MAMPU.[121] Furthermore, in December 2024, the National AI Office launched and was incubated under MyDIGITAL Corporation under the Ministry of Digital.[122] The Ministry of Communications maintains its hold on the Malaysia National News Agency (Bernama) as well as creative industry growth vehicles My Creative Ventures and National Film Development Corporation. The enforcement powerhouse, the Malaysian Communications and Multimedia Commission (MCMC), also remains under the Ministry of Communications.

2. Legal updates and implications on governance

2.1. Expansion of powers

Malaysia's patchwork of laws has specific jurisdictions. The Cybersecurity Act is specifically for national critical information infrastructure (NCII) operators, while the PDPA is applicable to data controllers and processors involved in commercial transactions. The CMA is applicable to communication and multimedia industry players where the CMA's licensing regime obligates

compliance. The Social Media Licensing framework brings application service providers with eight million Malaysian users (or more) into CMA's mandate. Furthermore, the Online Safety Act builds on the Social Media Licensing framework and the CMA for compliance and penalties.

2.1.1. Cyber Security Act

The Cyber Security Act aims to govern the cybersecurity environment in Malaysia.[123] It establishes the National Cyber Security Committee, outlining the duties and powers of the Chief Executive of NACSA, and the functions and duties of the NCII sector leads and entities. In protecting consumers and supply chains, the act also addresses the management of cybersecurity threats and incidents related to NCII.

2.1.2. CMA amendment

The amended Communication and Multimedia Act expands the power of MCMC, allowing it to issue directions and mandatory standards on players in the industry. The Commission can carry out audits and create industry and technical standards, and consumer forums. The Minister's powers have also expanded to include all matters regarding unsolicited commercial electronic messages, as well as the ability to formally designate class licenses to industry players. The Communications and Multimedia Act amendments come with raised penalties reaching no higher than RM1 million in fines, 10 years in imprisonment and RM100,000 every day the offence continues after conviction.

2.1.3. PDPA amendment

The amended PDPA mandates data controllers and data processors to appoint data protection officers.[124] Any business or establishment in Malaysia managing data for commercial transactions would be required to conform to data management practices and be accountable for compliance. Additionally, the amendment sets requirements for data breach notifications. Details of the obligations are still being developed with Futurise and is set to be released in early 2025.[125]

2.2. New and wider scope on content controls

Wider scopes were identified with 2024 legislations, namely the Social Media Licensing Framework, Online Safety Act and the amended CMA 1998. The Social Media Licensing Framework operationalises the CMA through a licensing requirement for internet messaging and social media service providers under the Applications Service Provider Class (ASP (C)) License. Although the class license existed before the framework's introduction in August 2024, its expansion to include internet messaging and social media service providers was a key update that year. The platforms would need to have at least eight million users in Malaysia, therefore it is currently applicable to platforms such as Facebook, Instagram, TikTok, WhatsApp, Telegram, WeChat, X and YouTube, and such platforms must apply for the class license lest they risk fines or imprisonment, or both.[126] The Online Safety Act also identifies duties for providers of applications, content application and network services that are related to the

establishment of mechanisms that addresses the availability of content labelled as priority harmful content and harmful content on the platform. Furthermore, the CMA update gave six explanations of content equating to the misuse of networks. These range from obscene to false and confusing.

2.3. Policymaking committees for security and safety

The Cybersecurity Act and Online Safety Act both introduced multi-stakeholder committees to craft national cybersecurity policies. The National Cyber Security Committee (NCSC) is chaired by the Prime Minister and has 12 other representatives, including the Ministers of Finance, Defence, Home Affairs, Communications and Digital. Meanwhile, the Online Safety Committee will be led by the MCMC Chairman with representatives from the Ministries of Women, Family and Community Development and Education, as well as representatives from the disabled community, licensed applications, content and network service providers.[127] It will determine categories of harmful content and priority harmful content, and introduce methods to analyse measures to mitigate the risk of users being exposed to harmful content.

3. Enhancing investigations and digital evidence collection

The amended CMA, Online Safety Act and Cyber Security Act aim to close gaps for information collection and gathering. Notably, the amended CMA contains the most provisions affecting investigations. The altered Section 248, for instance, empowers an authorised officer to enter premises without a warrant, which opens the possibility of MCMC officers to conduct investigations, thus further strengthening the Commission's enforcement powers. Additionally, the amended CMA includes pre-emptive measures such as Section 252 (b) which states the possibility of an authorised officer to enter any premise and install a device for the interception and retention of a specified description, and to remove and retain such device. The authority to preserve and retain data can also be found in the Online Safety Act Sections 60 and 61 and Cybersecurity Act Sections 38 to 52.

Moving into 2025

2024 was a year of restructuring agencies and approaches for a chip-to-code economy, but Malaysia's primary technology regulation impact is in identifying areas in need of strengthened regulations and/or protection, such as social media regulation and online scams. Malaysia's Budget 2025 indicates such allocation of activities for the year, including improving capacity to address scams, building a larger national cybersecurity agency and implementing MyDIGITAL ID. Government digitalisation will be 2025's goal, especially with Malaysia's National Digital Department and NAIO focusing on government AI transformations.

Jobs and talent remain a key conversation piece for Malaysia's digital future. A new incentive framework is in the works, targeting execution in the third quarter of 2025, which would include preparations for high-earning jobs in AI and emerging technology. Additionally, tax exemptions will be given to private institutes for higher learning and training centres to introduce new

courses, such as digital technology, AI, robotics, IoT, data science, fintech and sustainable technology.

Meanwhile, a few regulatory updates are still awaiting development. Among them is the Gig Workers Act that aims to provide social protections and means for gig workers. Additionally, a new Cybercrime Bill might be in the works, especially to meet international obligations. The maturity of policies such as the National Cyber Security Strategy 2020-2024 and the ASEAN Cyber Security Cooperation Strategy 2021-2025 could result in updates of national and regional cybersecurity goals. As Malaysia continues to shape the nation's digital future, policies for security and digitalisation in government sectors are to be expected.

4.3. Philippines

Balancing Growth and Governance: How the Philippines is Reshaping its Digital Economy

Oliver Xavier Reyes, University of the Philippines Law Centre

Consistent with trends over the last few years, the Philippine digital economy continued to surge in 2024. The value of the overall digital economy grew to US$31 billion in 2024, up by 20% from the previous year.[128] Statistics released in April 2024 by the Philippine Statistics Authority indicate that the digital economy in 2023 totalled PhP 2.05 trillion, a 7.7% growth from the previous year, where the digital economy contributed 8.4% to the Gross Domestic Product of the country.[129]

According to the PSA statistics, the gross value added by e-commerce in 2023, reached PhP 286.67 billion, accounting for 14% of the total digital economy. This figure is expected to rise. The Department of Trade and Industry (DTI) further noted[130] that the 2024 UNCTAD Digital Economy Report identified the Philippines as "one of the leaders in e-commerce sales growth among 43 economies".[131] The PSA statistic also indicated that e-commerce contributed to 87.3% employment out of 9.68 million employed persons in the digital economy.

While these statistics reinforce the narrative of the continued growth of the Philippine digital economy, the year 2024 may be even more notable as the beginning of a more robust regulatory infrastructure overseeing the digital sector. A law was enacted to ensure that digital services offered in the Philippines were subject to value-added taxes (VAT), explicitly requiring non-resident digital services providers deriving significant income from the Philippines to register with Philippine tax authorities. Another landmark law, signed in 2023, established a new regulatory framework for internet-based transactions with the promulgation of fully

implementing rules set to take effect in 2025. Meanwhile, providers of digital payments and online financial accounts were subjected to more stringent regulations through the enactment of law designed to protect users from fraudulent acts. Even as the surge in the digital economy continues to be driven by the private sector, the regulatory developments in 2024 reflect the state's ongoing recalibrations of its governance framework in response to the economic landscape increasingly shaped by technology.

Key Trends in Philippines' Tech Policy and Governance

1. Taxation and the digital economy

- *Value-added taxation of digital services*

The Republic Act No. 12023 was enacted in 2024,[132] amending the National Internal Revenue Code to ensure that digital services provided by both Philippine resident and non-resident enterprises are subjected to VAT, as long as digital services are consumed in the Philippines. While the tax is ultimately borne by the final consumers, digital service providers are obligated under the VAT system to withhold and remit the tax to the Bureau of Internal Revenue. The tax rate is set to 12% of the gross sales derived from the sale or exchange of digital services. Previously, the Code had been silent as to whether digital services were indeed subject to VAT, and whether such taxes were applied to services provided by non-resident service providers - entities with no physical presence in the Philippines.

Digital services are defined under the law as any service supplied over the internet or other electronic network using information technology, where the supply of the service is essentially automated. The law provides a non-exclusive list of digital services, including online search engines, online marketplaces, cloud services, online media and advertising, online platforms and digital goods.

The new law further requires service providers, whose taxable gross sales in the previous 12 months or whose projected taxable gross sales in the next 12 months reach PhP 3,000,000.00, to register for VAT with the Bureau of Internal Revenue. Failure to register will not affect the service provider's liability for VAT but will affect their ability to benefit from the input tax credits that service providers are able to claim under the Philippine VAT system. The law requires the Bureau to establish a simplified automated registration system for non-resident digital service providers. Additionally, if a digital service provider fails to register for VAT, the Commissioner of Internal Revenue may authorise the Department of Information and Communications Technology to block such digital services rendered in the Philippines.

The Philippine National Internal Revenue Code was adopted prior to the rise of the digital economy and the increasing ability of non-resident service providers to generate sales income in the Philippines. By imposing VAT on digital services and requiring non-resident digital service providers to register their business, the Philippines has aligned itself with other SEA economies such as Singapore, Malaysia, Indonesia and Thailand. While it could be argued that the broad language of the existing Tax Code makes no distinction between digital and non-digital

services, it enabled the Philippine tax authorities to require such sales to be covered by VAT and, the new law provides greater clarity on revenue collection. It enforces compliance by imposing a registration requirement on higher income non-resident providers and to withhold and remit VAT from payments made by the final consumers. Additionally, blocking websites of non-compliant digital service providers, similar to the mechanism adopted by the 2023 Internet Transactions Act illustrates a regulatory approach by the Philippine government that may increasingly be found in future regulatory enactments affecting non-resident online businesses.

The new law is limited to the revision of the VAT framework and does not modify the applicable rules for income taxation, even on non-resident service providers. However, the increased registration of non-resident digital service providers to the Philippine tax authorities, following Republic Act No. 12023, could eventually facilitate income tax collection from such providers on revenue derived in the Philippines. Nonetheless, there are complexities surrounding cross-border income tax involving the digital economy (such as the prospect of double taxation). It is anticipated that it would be the Philippine Congress itself, rather than the tax authorities under their rule-making powers, that would enact the appropriate solutions.

Other significant new tax enactments

Other tax enactments in 2024 are expected to bear impact on investment decisions by all enterprises.

- **Republic Act No. 12066,[133] otherwise known as the CREATE MORE Act,** further lowered corporate income tax rates by 20% for registered businesses entitled to the Tax Code's enhanced deductions regime.

- **Administrative Order No. 23,[134]** signed by President Marcos to implement the Customs Modernization and Tariff Act, established a single electronic invoicing system on importing goods into the Philippines, which enables a verified and registered foreign exporter to create an export invoice on a single electronic platform controlled by the Philippine government. The Administrative Order also directs the Bureau of Customs to implement a technical verification system that verifies the declared specifications of commodities prior to exporting to the Philippines.

2. **Enhanced Consumer Protections**

Updates on implementation of the Internet Transactions Act

The **Implementing Rules to the Internet Transactions Act** ("ITA"),[135] were promulgated in May 2024. Enacted five months earlier, the ITA introduced a new regulatory framework for consumer online transactions by creating an E-commerce Bureau within the Department of Trade and Industry (DTI) and imposed minimum obligations on parties engaged in internet transactions, such as e-marketplaces, digital platforms, online merchants, e-retailers and consumers. The law also established instances where platforms and e-marketplaces may be held liable for failed internet transactions.

Notably, while the ITA provides an 18-month transition period from its effectiveness date for online merchants, e-retailers, e-marketplaces and digital platforms to comply with the law, the Implementing Rules clarified that other existing laws or rules remain enforceable during this period. These include the 1993 Consumer Act and the 2022 Guidelines for Online Business, which reiterate applicable laws and regulations for online businesses and consumers.

Unlike the 1993 Consumer Act, the ITA applies to both business-to-business and business-to-consumer transactions, if at least one party is based in the Philippines, or the digital platform, e-retailer or online merchant targets the Philippine market and has sufficient commercial presence. The law exempts consumer-to-consumer transactions, defined as transactions between end-users done for personal, family or household purposes and not for an ordinary course of business. Nonetheless, the Implementing Rules presume certain transactions as business-to-consumer transactions, such as when a person sells or offers to sell a product through an organised business entity, or as a continuous business activity to generate income. Factors such as transaction value, frequency and sales volume may be considered in determining ITA coverage.

The DTI under the ITA is expected to continue exercising its rule-making powers in the coming months with the Implementing Rules anticipating creating additional rules for compliance, takedown and blacklist orders by the DTI Secretary. This establishes the online business database of digital platforms, e-marketplaces, e-retailers and online merchants engaged in e-commerce in the Philippines. It also includes developing and implementing the E-commerce Philippine Trustmark, managed by an industry-led private sector governance body and the rules governing the new online dispute resolution system to facilitate alternative dispute resolution of disputes arising from internet transactions. Following the Implementing Rules' release, the DTI has initiated consultations on these forthcoming regulations

The Anti-Financial Account Scamming Act

Republic Act No. 12010,[136] also known as the **Anti-Financial Scamming Act (AFASA), was enacted in July 2024**to protect the public from cybercriminals and syndicates who target financial accounts or manipulate account owners into enabling fraudulent activities. The new law covers various financial accounts, including credit card and transaction accounts with banks, non-banks or financial institutions, e-wallets, and other accounts used for financial products and services. It also defines newly prohibited acts, such as committing social engineering schemes to gain access to a customer’s financial accounts and using financial accounts for money muling activities associated with crimes, offenses and social engineering schemes.

Notably, the law introduced a mechanism that authorises financial institutions to temporarily hold funds involved in a disputed transaction if there is reasonable ground to believe that the transaction is unusual, lacks a clear economic purpose, originates from an unknown or illegal source, involves any unlawful activity, or facilitated through social engineering schemes. If an institution fails to temporarily hold such funds, it may be held liable for any resulting loss or damage. Furthermore, such institutions are required to implement robust risk management

systems and controls and exercise the highest degree of diligence and take proactive measures to prevent financial fraud and customer losses.

The AFASA complements the 2022 Financial Products and Services Consumer Protection Act ("FPSCPA"),[137] which enhanced the regulatory powers of financial authorities over financial products and services in the Philippines. However, unlike the FPSCPA, which applies to services regulated by the Securities and Exchange Commission and the Insurance Commission, the AFASA's regulatory scope only covers BSP-regulated financial services.

Launch of the Digital National ID System

Amid the backlog in printing physical ID cards for the PhilSys National ID system, the Philippine government launched the digital version of the national ID in June 2024.[138] In line with the 2018 Philippine Identification System Act, the digital national ID serves as a valid proof of identification for any government or private transactions, further enhancing security in commercial transactions.

3. Improved Internet Infrastructure and Cybersecurity

National Cybersecurity Plan (NCSP) 2028

April 2024 saw the promulgation of Executive Order No. 28,[139] adopting the National Cybersecurity Plan 2023-2028 prepared by the Department of Information and Communications Technology (DICT).[140] DICT Secretary Ivan John Uy cited the widespread adoption of e-commerce, e-banking and cashless transactions, along with the rising threat of cybercrime as key drivers for this second iteration of the NCSP.

The plan highlights the potential enactment and expected draft of an Executive Order of a Critical Information Infrastructure (CII) Protection law. Companies that are identified as CII would be subjected to regular monitoring by the DICT to ensure compliance with cybersecurity risk reduction regulations.

E-Governance Bill

As of this writing, the proposed E-Governance Act is pending second reading in the Senate.[141] The House of Representatives had already passed its own counterpart bill in 2023.[142] In addition to establishing a framework for electronic government service processes under the DICT, the Act also initially identifies several sectors as CII, including public finance, banking, business process outsourcing, telecommunications, media, energy, water, health and government transportation.

Konektadong Pinoy Bill

As of this writing, the proposed Konektadong Pinoy Act is pending second reading with the Senate.[143] The House of Representatives had earlier passed its own counterpart bill (titled Open Access in Data Transmission Act) in 2022.[144]

The proposed law seeks to remove the requirement for data transmission industry participants, including value-added service providers, to secure a legislative franchise or a certificate of public convenience and necessity, and requiring them to register with the National Telecommunications Commission as industry participants in order to construct, operate, lease or own networks or facilities in the Philippines.

Other notable policy developments

The Securities and Exchange Commission in April 2024 issued a Memorandum Circular, establishing a regulatory sandbox for innovative products, services or business models. The Commission may grant waivers and modifications to applicable regulatory rules, depending on the level of risk of the activity, the security measures in place, and the benefits of the new product and service to the public.[145] The Philippine e-wallet service GCash was reported to have submitted a sandbox application for its GStocks Global offering.[146]

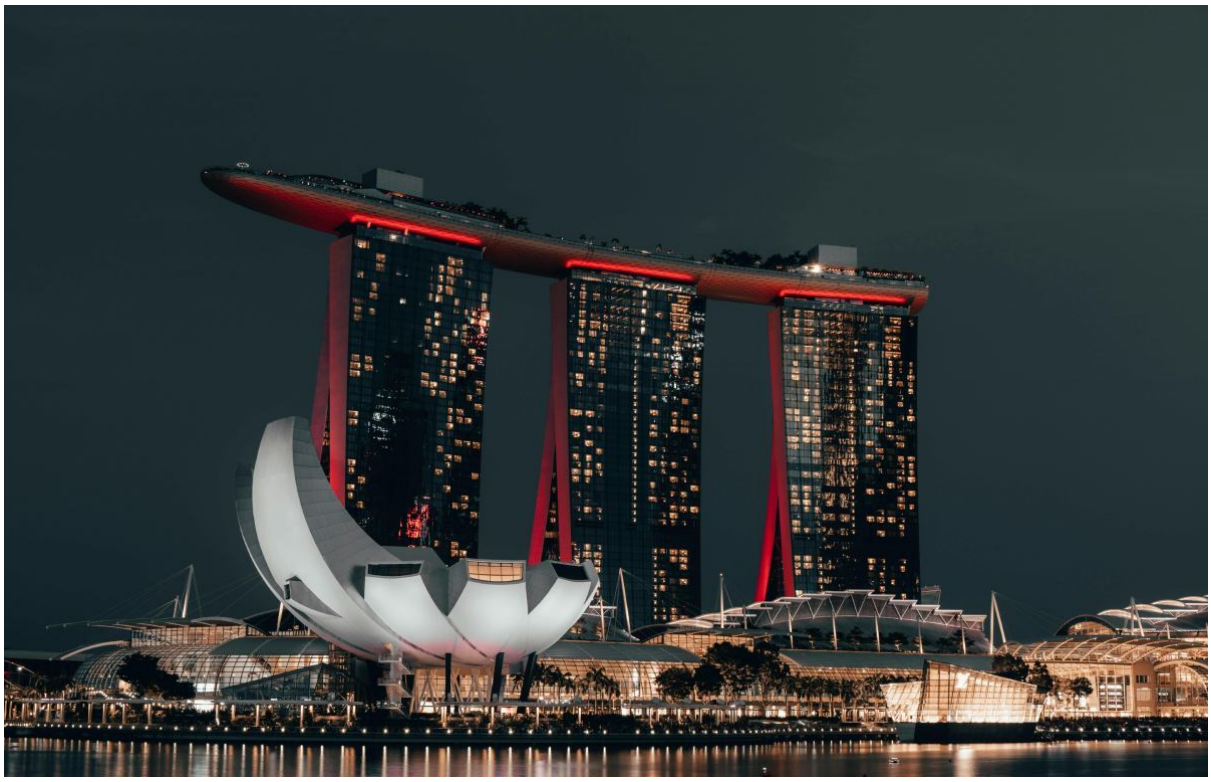
The Land Transportation Franchising and Regulatory Board (LTFRB), established in November 2024, updated guidelines for issuing certificates of public convenience to the operators of public utility vehicles, as they are currently limited to internal combustion engine vehicles due to the 2022 Public Service Act.[147] Additional guidelines were issued by the LTFRB for public convenience certificates to operate taxi services using electric vehicles.[148] Moreover, in May 2024, the LTFRB allowed an additional two years to the maximum age limit of Transport Network Vehicle Service vehicles, which applies to sedans, AUVs, SUVs and vans from 2016 to 2019.[149] Meanwhile, the Land Transportation Office in October 2024 temporarily suspended its current registration requirements of light electric vehicles[150] (such as electric scooters and electric bicycles), and licensing requirements for its users. This suspension will remain in effect until the Implementing Rules of the 2022 Electric Vehicle Industry Act are amended.[151]

The Implementing Rules of Republic Act No. 11981, also known as the “Tatak Pinoy (Proudly Filipino) Act”, were promulgated in May 2024.[152] Both the law and its rules establish a ten-year period during which Philippine products and services will be given preference and priority in government procurement. The specific sectors and economic activities eligible for this preference will be identified by a multi-agency council. Digital goods and services are included in the definition of Philippine products and services as promoted under the law.

4.4. Singapore

Singapore's Strategic Approach to the Future of the Digital Economy

Lim How Khang, Singapore Management University



Singapore's technology governance landscape in 2024 was marked by significant developments that built upon and enhanced the nation's approach to managing digital transformation. The launch of Smart Nation 2.0 established three key pillars: Growth, Community and Trust - providing a framework for various governance initiatives throughout the year.[153]

From AI governance frameworks to consumer protection measures, Singapore continued to develop comprehensive approaches to emerging technological challenges. The year saw several landmark developments, including the establishment of new institutions like the Agency for Online Safety and Assurance (AOSA),[154] the implementation of the Model AI Governance Framework for Generative AI[155] and innovative approaches to digital security through the Shared Responsibility Framework.[156]

These initiatives demonstrate Singapore's systematic approach to fostering technological innovation while ensuring appropriate safeguards and benefits for its citizens. As Southeast Asia's digital transformation accelerates, Singapore's experience in developing effective governance frameworks while maintaining innovation offers valuable insights for the region, particularly in balancing technological progress with social protection.

This analysis examines key trends in Singapore's technology governance and policy landscape through 2024, highlighting significant developments and its implications for the future of digital transformation in the region.

Key Trends in Singapore's Tech Policy

1. Digital security and trust

Singapore prioritised comprehensive approaches to digital security and building trust in 2024, addressing both immediate security needs and future challenges.

Quantum security emerged as a key focus area, with the Cyber Security Agency announcing plans to help organisations prepare for the quantum computing era.[157] This initiative prioritises essential service providers while providing tailored guidance for different organisational needs, including Singapore's 310,000 SMEs.

The banking sector saw significant security enhancements, including the integration of Singpass Face Verification and the phasing out of OTP authentication for digital token users.[158] The Monetary Authority of Singapore collaborated with banks and technology partners, including a $100 million enhancement to the FSTI 3.0 scheme for quantum and AI capabilities, further strengthening the financial sector's security preparedness.[159]

Looking ahead, the planned Digital Infrastructure Act, announced as part of Smart Nation 2.0, signals a broader approach to infrastructure resilience. The Act will extend beyond cybersecurity concerns to address physical hazards like fires and cooling system failures, reflecting a comprehensive understanding of digital infrastructure protection needs.[160]

2. Digital economy and consumer protection

Consumer protection and online safety received significant policy attention in 2024, with multiple initiatives addressing various aspects of digital risk and harm. The government's approach combined institutional development with practical protection measures.

The Shared Responsibility Framework introduced a structured approach to protecting consumers in digital transactions.[161] The framework's "waterfall" approach to liability creates clear accountability, while providing practical pathways for consumer redress. Complementing this framework is the Enhanced E-payments User Protection Guidelines, where it introduced additional requirements, such as restrictions on clickable links and enhanced transaction monitoring.

The Platform Workers Act provided protections for workers in the digital economy while maintaining operational flexibility.[162] By carefully balancing workers' rights with business innovation, the Act serves as a model for regulating emerging forms of digital employment.

3. Innovation and social impact

Singapore remained committed to fostering innovation while ensuring technology serves broader societal goals and promotes inclusion.

The launch of Smart Nation 2.0 represented a major strategic refresh of Singapore's digital transformation roadmap, emphasising the importance of community and trust alongside growth.[163] This was complemented by the release of the first AI Playbook for Small States, which demonstrates Singapore's commitment to inclusive technological development.[164]

Moreover, Singapore's commitment to practical innovation was shown through the expansion of IMDA's Privacy Enhancing Technology (PET) Sandbox.[165] As the country's first sandbox initiative, it provides businesses with a safe space to trial privacy-preserving technologies across multiple use cases. The programme's scope was further enhanced in 2024 to support generative AI applications, with IMDA providing technology, financial and regulatory support to showcase the government's commitment to fostering innovation while maintaining privacy protections.

Recognising the need for strong social safeguards in an increasingly digital world, Singapore also established the Agency for Online Safety and Assurance (AOSA), an agency dedicated to protecting citizens from online harms.[166] The agency's work is supported by new legislation, enabling victims to seek civil remedies and ongoing public education efforts.

Efforts to expand digital inclusion programmes and skills training initiatives further demonstrates Singapore's continued commitment to ensuring that technology's benefits reach all segments of society. These efforts recognise that successful digital transformation requires broad-based participation and capability development.

The PET Sandbox's success in fostering innovation while maintaining privacy protections demonstrates how policy can support technological advancement while addressing societal concerns.[167] Additionally, notable collaborations with major technology companies and financial institutions have addressed challenges ranging from customer engagement to financial fraud prevention.

These comprehensive digital strategies reflect Singapore's understanding that successful technological development requires attention to security, economic development and social impact. The interconnected nature of these policies creates a framework for sustainable and inclusive digital transformation, providing valuable lessons for other countries.

Key Trends in Singapore's Tech Governance

Singapore's technology governance landscape in 2024 demonstrated three major trends: leadership in AI governance and international cooperation, enhanced institutional and regulatory frameworks, and multi-stakeholder engagement approaches. These developments reflect Singapore's systematic approach to managing technological change while ensuring its benefits reach all segments of society.

1. AI governance and international leadership

Singapore reinforced its position as a global leader in AI governance through both domestic frameworks and international partnerships. Building on its pioneering work in AI governance principles, the nation made significant strides in addressing the challenges of generative AI while fostering international collaboration.

A key milestone was finalising the Model AI Governance Framework for Generative AI (MGF-Gen AI) in May 2024.[168] Initially proposed by AI Verify Foundation and IMDA, this framework received strong endorsement from over 70 stakeholders, including major technology companies, leading corporations, audit firms and government agencies. The framework's nine comprehensive dimensions established guidelines for all key stakeholders, creating a robust ecosystem for responsible AI development and deployment.

Singapore's international leadership in AI governance extended beyond national borders through initiatives such as the Digital Forum of Small States (Digital FOSS).[169] The introduction of the world's first AI Playbook for Small States, announced at the United Nations Summit of the Future Action Day, represented a groundbreaking effort to shape inclusive global discourse on AI adoption and governance. The playbook, developed in collaboration with Rwanda's Ministry of ICT and Innovation, addresses crucial challenges faced by small states in AI implementation, including resource constraints, limited access to data and AI talent, and difficulties in developing governance policies.

International partnerships further strengthened this leadership position. Agreements established with the United Kingdom and the European Union facilitated collaboration on AI safety research, testing and standards development. The Cyber Security Agency's Guidelines on Securing AI Systems further demonstrated Singapore's comprehensive approach to AI governance, advocating for 'secure by design' and 'secure by default' principles.

2. Enhanced institutional and regulatory frameworks

Singapore established new institutions and regulatory frameworks in 2024 to address emerging digital challenges while maintaining flexibility for innovation. These developments demonstrated a coordinated approach to governance enhancement.

The establishment of AOSA in October 2024 positioned Singapore among the first countries globally to create a dedicated agency for addressing online harms.[170] The agency's mandate includes providing swift assistance to victims, directing perpetrators to cease harmful activities and promoting responsible online behaviour.

The Online Criminal Harms Act (OCHA),[171] which came into full effect in February 2024, complemented AOSA's work by establishing a comprehensive framework for addressing criminal activities in the digital space. The Act grants authorities the ability to issue various types of directions while maintaining due process through a robust appeals mechanism.

Singapore's commitment to regulatory innovation was further demonstrated by the passage of the Platform Workers Act,[172] passed in September 2024. This groundbreaking legislation creates a distinct category for platform workers, introducing key protections while maintaining operational flexibility through market-driven solutions.

The creation of the Global Finance & Technology Network (GFTN) marked Singapore's transition from fintech experimentation to scaled growth and global connectivity.[173] Under the chairmanship of Mr. Ravi Menon, GFTN focuses on advancing industry and policy dialogues in payments, asset tokenisation and AI/quantum applications.

3. Multi-stakeholder engagement and innovation

Singapore's governance approach emphasised collaboration between government, industry and civil society, particularly in developing and testing new technologies and frameworks.

The Privacy Enhancing Technology (PET) Sandbox exemplifies this collaborative approach, providing businesses with a safe space to trial privacy-preserving technologies.[174] The programme's expansion to support generative AI applications in 2024 demonstrates Singapore's commitment to fostering innovation while maintaining privacy protections.

The Shared Responsibility Framework,[175] implemented in December 2024, showcases effective multi-stakeholder collaboration in addressing digital risks. This framework establishes clear accountability measures for financial institutions and telecommunication companies in protecting consumers from phishing scams to showcase how different sectors can work together effectively.

Recognising the importance of supporting small businesses in digital transformation, Singapore introduced the Small and Medium-Sized Enterprises Pro-Enterprise Office (SME PEO).[176] This initiative, scheduled to launch in Q1 2025, will serve as a one-stop entity to assist SMEs with regulatory feedback, particularly for nascent or cross-cutting issues.

Moving Forward

As Singapore enters 2025, the nation's technology governance and policy landscape will likely evolve in response to accelerating technological change and shifting societal needs. Several key developments are poised to shape this evolution.

The maturation of AI technologies, particularly generative AI, will test the resilience and adaptability of Singapore's governance frameworks. While the nation has established comprehensive guidelines for AI governance, the rapid evolution of these technologies will require continuous refinement of regulatory approaches. The interaction between AI systems and critical infrastructure, financial services and public services will demand particular attention as integration deepens.

Digital infrastructure development will likely extend beyond traditional cybersecurity to encompass broader resilience considerations. As digital systems become more deeply embedded in daily life, the focus will increasingly shift toward ensuring these systems can withstand both technological and physical challenges. This reflects a growing recognition that digital infrastructure represents a fundamental pillar of national resilience.

Safety and trust in the digital economy will remain paramount as online interactions become more complex and sophisticated. Singapore's pioneering approach to online safety regulation through the Agency for Online Safety and Assurance will face new challenges as digital threats evolve and emerging technologies create novel forms of online harm. The success of collaborative approaches to digital security, as demonstrated by the Shared Responsibility Framework, will likely influence future regulatory developments.

Technology governance will also increasingly intersect with social equity and inclusion. As digital transformation accelerates, preventing digital divides and ensuring that technology serves broader societal goals will become increasingly critical. Singapore's experience in balancing innovation with social protection will be particularly relevant for other nations navigating similar challenges.

At the regional level, cross-border collaboration and standardisation will take on greater significance. Singapore's role in initiatives like the Digital Forum of Small States positions it to help shape inclusive approaches to technology adoption and governance across the region. As regional economies work to harness digital opportunities while mitigating risks, Singapore’s experience in crafting comprehensive yet flexible regulatory frameworks will offer valuable insights.

These ongoing developments suggest that Singapore's approach to technology governance will continue evolving toward more integrated and adaptive strategies that balance innovation with societal needs. The nation's experience in developing these comprehensive frameworks may provide valuable insights for the ongoing challenge to ensure that technology serves as a force for inclusive progress in an increasingly digital world.

4.5. Thailand

Thailand's Digital Leap: AI, Cybersecurity and the Future of Tech Governance

Anont Tanaset, Office of National Higher Education Science Research and Innovation Policy Council

Thailand made significant progress in 2024 to strengthen its digital economy through strategic policies and infrastructure development. These efforts have enhanced the country's digital competitiveness and created an environment that supports innovation while addressing emerging challenges.

Thailand's rise in the International Institute for Management Development's (IMD) World Digital Competitiveness Ranking is notable, climbing five spots to 35th globally.[177] This improvement reflects the effectiveness of its digital policy framework, especially in areas like technology infrastructure and high-tech manufacturing. The telecommunications sector continues to be a strong asset, maintaining its global fifth-place ranking. This connectivity has been a key enabler of Thailand's broader digital transformation across industries.

Additionally, Thailand ranks 11th globally in high-tech exports, highlighting its strengths in advanced manufacturing and innovation.[178] AI adoption is another significant achievement. The AI Readiness Measurement 2024 report by the Electronic Transactions Development Agency (ETDA) and the National Science and Technology Development Agency (NSTDA) shows a 73.3% AI adoption rate among Thai organisations, highlighting the country's proactive digital transformation.[179]

However, the rapid growth of the digital economy is not without its challenges. Rising online scams, misinformation and cybersecurity threats underscore the need for a balanced approach to innovation and regulation. Addressing these risks is critical to ensuring that digital technologies benefit society while mitigating its negative impacts.

Key Trends in Thailand's Tech Policy

1. AI development and ethics: A pivotal year for AI in Thailand

2024 was a landmark year for AI in Thailand, marked by significant policy developments and strategic initiatives aimed at positioning the country as a leader in AI innovation and ethics. The Ignite Thailand campaign, announced by the Prime Minister in early 2024, focused on establishing Thailand as a digital economy hub by fostering high-tech industries such as semiconductor manufacturing, cloud computing and AI research. This campaign included financial incentives like matching funds, regulatory sandboxes to ease business operations and partnerships with global tech firms to attract deep-tech companies to Thailand.

At the ministerial level, the Ministry of Higher Education, Science, Research and Innovation (MHESI) launched the "MHESI for AI" initiative, which emphasises talent development through programmes like "AI University."[180] This initiative aims to ensure that 90% of graduates possess foundational AI knowledge, with a goal of producing 30,000 AI professionals within three years. By integrating AI education into higher education institutions nationwide, Thailand is cultivating a skilled workforce to drive its AI ambitions.

A significant highlight of Thailand's AI policy landscape was announcing that the country will host the first Asia-Pacific UNESCO Global Forum on the Ethics of AI in 2025. This announcement was made on December 4, 2024, and the event is scheduled to take place in Bangkok from June 24-27, 2025.[181] Organised in collaboration with the Ministry of Digital Economy and Society (DE), MHESI, the Ministry of Education (MOE) and UNESCO, the forum will attract over 800 participants from UNESCO's 194 member countries. It will provide a platform for global leaders and experts to discuss and shape ethical governance frameworks for AI, further reinforcing Thailand's commitment to responsible AI development.

2. Cloud First Policy: Fortifying Thailand's digital defenses

As Thailand continues to expand its digital economy, securing the nation's digital infrastructure remains a critical priority. Central to the country's cybersecurity strategy is the Cloud First Policy, which emphasises the adoption of centralised and secure cloud infrastructure for government operations. This policy encourages government agencies to prioritise cloud-based solutions, ensuring that both efficiency and security are enhanced through the use of advanced and secure cloud technologies. The transition to the cloud will improve government services and lay the foundation for broader adoption of secure cloud solutions across other sectors in Thailand.

Aligned with this policy, the current Cloud Security Standard 2024 ensures that cloud environments across government agencies, regulated industries and critical infrastructure providers are secure. This standard includes rigorous security controls such as data encryption, access management and incident response protocols to ensure Thailand's resilience in digital systems. It complements the Cloud First Policy by providing specific technical standards for secure cloud adoption, reinforcing the nation's commitment to building a secure digital ecosystem.

Additionally, partnerships between the Ministry of Digital Economy and Society (DE) and private sector entities like Huawei have played a pivotal role in strengthening Thailand's cybersecurity capabilities. These collaborations have led to establishing specialised training centres focused on developing AI and cloud technologies expertise. These centres aim to certify 10,000 professionals annually, addressing critical skill gaps and ensuring a robust workforce capable of supporting Thailand's digital transformation.

3. E-commerce and consumer protection: Ensuring a trustworthy digital marketplace

Thailand's digital platform economy has advanced significantly with the implementation of the Digital Platform Services (DPS) law, effective August 21, 2023.[182] This regulation seeks to protect digital platform users, which includes buyers, sellers and intermediaries, while fostering fairness and transparency in the ecosystem. It requires digital platform operators to register their information with ETDA. Additionally, the DPS law addresses key issues such as compensation systems, fraudulent practices and data security, contributing to a safer and more equitable digital marketplace.

As e-commerce continues to grow rapidly in Thailand, the government has implemented several key policies aimed at ensuring consumer protection and promoting fair market practices. These include the Guidelines for Managing Advertisements on Digital Platform Services, the Guideline on the Management of Standardized Product Sales on Digital Platforms and the establishment of the Cybercrime Case Division within the Thai Criminal Court.

These policies are designed to regulate digital advertising practices, improve product sales transparency, and address digital fraud and data breaches. By setting standards for online transactions and enforcing legal measures, Thailand is continuously working to create a secure and trustworthy digital marketplace. The Cybercrime Case Division, specifically, plays a crucial role in ensuring that violations related to digital fraud and intellectual property are swiftly handled to maintain consumer confidence and market integrity.

Overall, these policies contribute to fostering a fair, transparent and accountable e-commerce environment. By regulating digital platforms and addressing legal challenges, Thailand is enhancing consumer protection and supporting the sustainable growth of the digital economy.

Key Trends in Thailand's Tech Governance

1. Soft regulation and multi-stakeholder collaboration

Thailand's tech governance strategy emphasises the use of soft regulation frameworks, supported by collaboration across government, industry and academia. A key example is the AI Governance Center (AIGC), established under ETDA, which has issued several important guidelines, such as the AI Governance Guideline for Executives and the Generative AI Governance Guideline for Organizations.[183] These documents offer structured guidelines for ethical AI adoption, prioritising risk management, data privacy, fairness and transparency - all aiming to create an environment where AI technologies can thrive without compromising societal values or ethical principles.

Another approach besides soft regulation was the formation of the Special Committee for the "Study of Approaches to Regulating and Promoting the Use of Artificial Intelligence to Support Future Changes". Established by the Thai Parliament, this committee includes experts from academia, industry and government, and is tasked with evaluating global best practices while addressing gaps in existing regulations. Its focus spans ethical considerations, societal impacts and strategies to balance innovation with citizen protections. The committee's forthcoming report is expected to influence legislative frameworks that guide the responsible integration of AI into Thailand's socio-economic landscape. This collaborative and flexible approach ensures that Thailand's governance keeps pace with technological advancements, while safeguarding societal values.

2. Ensuring common standards

Thailand's tech governance emphasises the establishment of comprehensive technology standards to ensure consistency, resilience and trust across sectors. For example, the National Cyber Security Committee (NCSC) has spearheaded efforts to strengthen data and system security, while publishing minimum cybersecurity standards for public and private sectors. These include protocols for data protection, access control and incident management, creating a foundation for enhanced national cybersecurity.

The Cloud Security Standard 2024, a mandatory framework that targets critical infrastructure providers, government agencies and regulated industries, is one of the standards that were issued in 2024. This framework enforces security measures to protect sensitive data, with a compliance timeline extending to 2026, allowing organisations to adapt to its requirements.

Similarly, ETDA has also introduced standards for digital legal processes, ensuring that electronic transactions, contracts and legal acts are secure and enforceable. By aligning legal frameworks with digital practices, Thailand has streamlined e-commerce and other digital services, boosting trust and efficiency.

3. Sector-specific guidelines

Thailand's governance model also highlights the use of sector-specific guidelines to address distinct challenges in emerging digital domains. For example, protecting consumers and fostering a safe digital environment have become priorities in Thailand's governance efforts, with a significant focus on regulating digital advertisements and online product sales. To support these efforts, ETDA has introduced key guidelines, including the Guidelines for Managing Advertisements on Digital Platform Services and the Guideline on the Management of Standardized Product Sales on Digital Platforms, aimed at regulating and standardising digital advertisements, ensure product transparency to combat deceptive marketing reduce the sale of substandard products on online platforms and ensure e-commerce platforms provide a fair and trustworthy experience. These initiatives seek to build consumer confidence and ensure fair competition in Thailand's rapidly expanding digital marketplace.

Complementing these efforts is the establishment of the Cybercrime Case Division within the Thai Criminal Court, where it marks a critical step in addressing legal challenges in the digital domain. This specialised division is tasked with handling cases involving cyber fraud, data breaches and intellectual property violations. By equipping the judiciary with dedicated resources and expertise, the division enhances the efficiency and effectiveness of legal proceedings related to digital platform services, reinforcing Thailand's commitment to upholding justice in the digital era.

Lastly, the government has introduced guidelines for utilising digital identification systems, such as the DOPA-Digital ID and the facial verification service (FVS) managed by the Department of Provincial Administration. These systems aim to provide secure and privacy-conscious solutions for identity verification in order to boost trust in digital services while addressing privacy concerns.

Through implementing soft regulation, establishing common standards and developing targeted guidelines, Thailand's governance approach balances innovation with protection, fostering a secure and inclusive digital ecosystem.

Moving forward

As Thailand moves into 2025, the foundation laid in 2024 sets the stage for continued advancements in tech governance and regulation. The country's strategic focus on established technologies like e-commerce, cybersecurity and cloud computing is complemented by its forward-looking approach to emerging fields such as AI. Thailand has demonstrated a balanced approach, prioritising both innovation and protection, ensuring that the digital economy can thrive sustainably.

For established tech domains, detailed regulations and standards are being enacted to enhance security, consumer protection and market fairness. Providing a robust framework supports the ongoing growth of these sectors while safeguarding against potential risks. In the realm of cybersecurity, the Cloud Security Standard 2024 and other guidelines ensure that

Thailand's digital infrastructure remains resilient and secure, fostering a trustworthy environment for both businesses and consumers.

In the case of AI, Thailand laid the groundwork for a comprehensive governance framework that addresses ethical considerations, societal impact and economic opportunities. The establishment of the Special Committee on AI Regulation and the proactive initiatives by the AI Governance Center (AIGC) under ETDA exemplify Thailand's commitment to responsible AI development. The upcoming UNESCO Global Forum on the Ethics of AI 2025 will further solidify Thailand's leadership in ethical AI governance, providing a platform for international collaboration and knowledge sharing.

Thailand's advancements in tech governance and regulation have laid a strong foundation for sustained growth in its digital economy. Looking ahead to 2025, the country's emphasis on detailed regulations and ethical guidelines ensures that established sectors like e-commerce and cybersecurity remain resilient and trustworthy, while emerging technologies like AI are governed responsibly. As part of the regional Southeast Asian tech ecosystem, Thailand is positioned to contribute to the collective progress of the region, supporting a digital transformation that aligns with both societal and economic goals.

4.6. Vietnam

Shaping Vietnam's Digital Future through Governance

Thao Nguyen Minh, Central Institute for Economic Management

Digital technology and digital enterprises are recognised as central to a fast and sustainable growth model, driving the expansion of both the digital economy and digital society. They transform state management, business operations, consumer behaviour, and cultural and social life. Emerging technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), blockchain, cloud computing, virtual reality (VR), augmented reality (AR) and mixed reality (MR) advance rapidly, significantly shaping Vietnam's socio-economic landscape. In response, the government has introduced policies on digital transformation and the development of digital technology enterprises, underscoring technology's crucial role in the country's economic progress.

In his opening speech at Vietnam Innovation Day 2024 on October 1, 2024, the Prime Minister reaffirmed that innovation is an irreversible trend and a key driver of digital and green transformation in the country's development. Vietnam's digital economy indicators showed significant progress in 2024. The country's e-government development ranking improved to 71st, climbing 15 places from its 2022 position.[184] Vietnam rose by two spots to 44th in The Global Innovation Index, with three indicators leading globally.[185] Additionally, Vietnam was among the 46 countries classified in Tier 1 for 2024 in the Global Cybersecurity Index.[186]

Vietnam's startup ecosystem is also expanding, with approximately 4,000 startups, 208 investment funds, 84 incubators, 35 business accelerators and 20 startup centres. The country's Global Startup Ecosystem Index ranking increased by two places to 56th, positioning

it 5th in ASEAN and 12th in the Asia-Pacific region.[187] Hanoi and Ho Chi Minh City are both ranked among the top 200 global cities for startups, and Vietnam holds the 31st position worldwide in terms of the number of startups. Key sectors attracting the most investment include e-commerce, fintech, food technology, enterprise solutions and IT services.

Vietnam consistently prioritises science, technology and innovation as pillars of its economic strategy.[188] The government has identified "vigorous development of science, technology, innovation and digital transformation as the main driver of economic growth" and is committed to "promoting national digital transformation and developing the digital economy based on science, technology, and innovation."

Key Trends in Vietnam's Tech Policy

1. Policy for semiconductor industry development

The semiconductor industry is gradually becoming a key sector with significant influence on socio-economic development. Vietnam is rapidly emerging as a focal point in the global semiconductor market, leveraging numerous advantages and opportunities for cooperation and growth. Consequently, the semiconductor industry is a critical component of digital technology industry development in Vietnam.

In the draft Law on Digital Technology Industry, provisions were introduced regarding principles, classification of activities, mechanisms and special policies with priority given to the semiconductor industry. In addition, related legal frameworks, such as the Law on Corporate Income Tax and the Law on Investment, are expected to be amended to concretise the preferential policies for this industry.

Furthermore, the Ministry of Information and Communications (MIC) is finalising the Semiconductor Industry Development Strategy, - a sector that Vietnam has identified as a key industry and a driving force for the country's development in the new era.

2. Policies of promoting AI development and application

Artificial intelligence has been advancing rapidly, particularly with the rise of Generative AI (GenAI), showcasing its immense potential in driving socio-economic development and addressing societal challenges. Therefore, effective management to mitigate risks while harnessing AI's benefits is essential. Vietnam's Prime Minister issued Decision No. 127/QD-TTg on the National Strategy for Research, Development and Application of Artificial Intelligence by 2030, which emphasises human- and business-centred AI development and application, avoiding the misuse of technology and the infringement of the legitimate rights and interests of organisations and individuals.[189]

In 2024, the draft Law on Digital Technology Industry introduced definitions, principles for AI management and AI development guidelines. Drawing from the EU Artificial Intelligence Act and legal frameworks of AI governance in countries like China, the United States and the OECD,

the draft law proposes AI regulations, including: (i) Definitions of AI and AI systems; (ii) Principles for developing, providing, deploying and using AI; (iii) Risk management for AI systems; (iv) Responsibilities of stakeholders involved in the development, provision, deployment and use of AI systems; and (v) Labelling requirements and procedures for digital products created by AI systems.

Additionally, in 2024, Vietnam's Ministry of Science and Technology (MoST) issued Decision No. 1290/QD-BKHCN, the first document to establish and outline general principles for responsible research and development of AI systems.[190] It provides voluntary guidelines for organisations, units and individuals to refer and apply when researching, designing and developing AI systems.

3. Policies on data governance, information security and cybersecurity

Data is a new resource and a key factor for national digital transformation. As such, on February 2, 2024, Vietnam's Prime Minister issued Decision No. 142/QD-TTg, approving the National Data Strategy to 2030, establishing the following principles: (i) Placing citizens and businesses at the centre, with the state playing a leading role in connecting and sharing data; (ii) Gradually establishing and promoting the data market; (iii) Ensuring information security, cybersecurity and personal data protection; and (iv) Developing human resources.

To implement the National Data Strategy, the Government has outlined key tasks for ministries and agencies. As part of this, the MIC was tasked in 2024–2025 with drafting the Law on Digital Technology Industry and developing a Decree on e-transactions within state agencies and information systems supporting such transactions. Therefore, on October 23, 2024, the Government approved Decree No. 137/2024/ND-CP on e-transactions within state agencies and information systems supporting e-transactions.

According to Decision No. 1437/QD-TTg dated November 20, 2024, the Ministry of Public Security (MoPS) was assigned to draft the Personal Data Protection Law and the Data Law for data governance. The Data Law is scheduled for approval in May 2025.[191]

Key Trends in Vietnam's Tech Governance

1. Development and governance of digital technology

With the rapid advancement of new technologies, the digital technology industry has integrated into all economic sectors. It has solidified its role and position itself as a key driver of development and will continue to lead the fast and sustainable growth of various industries, further advancing the digital economy and digital society.

The development and governance of digital technology play a pivotal role in enhancing national competitiveness. The draft Law on Digital Technology Industry was submitted to the National Assembly for discussion at the 8th session in October 2024. The Ministry of Information and Communications (MIC) serves as the advisory and drafting agency for this law.

The drafting of this law stems from the need for a comprehensive legal framework to guide and promote the development of digital technology, digital products and digital technology enterprises. Key provisions include developing the digital technology industry, supporting digital technology enterprises, implementing sandboxes for digital technology products and services, such as with the semiconductor industry, AI, etc.

A notable breakthrough in the draft law is the sandbox for converged digital technology products and services. Inspired by policies in South Korea, Japan and Taiwan, this initiative aims to keep pace with the rapid integration of digital technologies across sectors. It aims to create a legal framework to promote the development of converged digital technology products and services that either lack regulation or differ from current legal provisions. The sandbox will outline procedures and principles for evaluating enterprise applications and will designate authorities responsible for processing and handling on a case-by-case basis based on the scope and field of the test. This approach ensures enhanced decentralisation, timeliness and efficiency, thereby providing favourable conditions for businesses to test digital technology products and services.

The draft law is expected to balance sandbox regulation, development and proper oversight. It will include provisions for exemptions from civil and administrative liability for authorised agencies, individuals and organisations involved in the experimental process, provided they act in good faith and fully comply with legal requirements. Criminal liability exemptions, however, will remain governed by the Penal Code.

Additionally, under Decision No. 1437/QD-TTg dated November 20, 2024, MIC was assigned tasks related to ICT-based digital economy and digital data development.[192] These tasks include: (i) Proposing regulation amendments to develop IT industrial parks; and (ii) Proposing sandboxes for establishing ownership, management, processing and distribution of data.

2. Developing the startup ecosystem

Vietnam's startup ecosystem is widely regarded as highly promising. Over the years, the Government has introduced policies to support investment and capital mobilisation for startups. However, startups in Vietnam still face significant challenges in raising funds. Legal barriers and regulatory bottlenecks hinder the unlocking of capital sources. According to statistics, there are currently around 210 venture capital funds investing in startups in Vietnam, including nearly 40 domestic funds. Therefore, the Vietnamese government assigned the Ministry of Science and Technology (MoST) to draft a decree, Resolution 65/NQ-CP dated May 7, 2024, regulating certain aspects of innovation and startups.[193]

Another key milestone in 2024 was the Prime Minister's announcement designating October 1st as Vietnam Innovation Day to honour, encourage and promote innovation. Additionally, on October 28, 2024, the National Assembly Standing Committee adjusted the legislative agenda to include the Law on Science, Technology and Innovation for 2025[194] This law is being drafted by the MoST.

3. Developing human resources for digital technology

Human resources in digital technology are essential to achieving the national goals of digital transformation. This priority has been consistently emphasised in the government's strategies and directions. For example, the Prime Minister issued Official Dispatch No. 83/CD-TTg on August 23, 2024, focusing on enhancing high-quality workforce training for the semiconductor industry, AI and cloud computing to align with trends in investment and technological advancements.[195] As such, various ministries have been assigned specific tasks to build related policies: (i) The Ministry of Planning and Investment (MPI) was assigned to submit the Proposal on the "Development of Human Resources for Semiconductor Industry by 2030, with a Vision to 2050", which will include content related to AI and cloud computing; (ii) The Ministry of Education and Training (MoET) was assigned to develop a proposal on cultivating high-quality human resources for high-tech industries; and (iii) MIC was tasked to formulate a plan to develop large scale data computation centres to support higher education institutions in training high quality human resources.

Moving Forward: Thoughts on the Direction of Evolution

Semiconductor industry and AI to remain dominant in 2025

The year 2024 saw the rapid convergence and growth of cutting-edge technologies such as AI, IoT, ML, VR, cloud computing and quantum computing. This created a dynamic and robust technological ecosystem, driving demand for innovative technology products and services, as well as advanced security solutions. These technological trends are expected to continue evolving in 2025 and beyond.

Vietnamese technology enterprises also have significant opportunities in the semiconductor industry. With government support, favourable policies, competitive costs and the concerted effort to build a high-quality workforce, Vietnamese companies are well-positioned to expand and integrate into the global semiconductor market. Consequently, the semiconductor industry in Vietnam is poised for significant growth in the coming years.

As such, the development and application of AI, along with advancements in the semiconductor industry are anticipated to remain dominant trends in Vietnam in the years ahead.

Developing and applying Green Tech

Green Tech is set to play a crucial role in technological advancements in Vietnam, referring to technology applications that do not pollute the environment and may even help reduce CO_2 emissions to purify the air. Key technologies such as AI, blockchain, cloud computing, extended reality (ER), robotic process automation (RPA) and others are becoming top priorities for enterprises.

Green Tech is expected to remain a central focus in the coming years as nations and major global companies continue to strive toward fulfilling their environmental commitments. At the

same time, individuals are increasingly encouraged to adopt sustainable technology to minimise their environmental impact.

With climate change becoming more severe, Green Tech will stand out as one of the most critical trends. Businesses and economies that embrace this shift will be better positioned for efficient and sustainable development.

Improving the legal framework

Vietnam's legal framework on digital transformation and technology is gradually being refined, establishing clear regulations that foster a transparent legal environment, innovation and fair competition. This solid foundation enables Vietnamese tech companies to expand and thrive. The government has also outlined key priorities to improve legal frameworks to effectively manage and promote technological development. Key areas of focus include policies to attract financial investment, particularly for research and development in areas such as AI, semiconductors, and green energy. As such, refining the legal framework and policies for technological development will remain a priority in 2025 and beyond.

For emerging policies such as the Digital Technology Industry Law, the Data Law or sandboxes for digital technology development, the government aims to prioritise the following aspects: (i) Ensuring regulations support innovation by adopting a flexible approach to governance; (ii) Developing risk management regulations to address technological risks, cybersecurity concerns, and data protection for businesses and individuals; (iii) Incorporating international best practices in technology governance and policy making, including experiences from ASEAN countries; (iv) Enhancing coordination among various agencies responsible for different policies to ensure consistency and alignment; and (v) Allowing streamlined processes, such as simplified procedures for implementing regulatory sandboxes.

In order to maximise advantages and opportunities in technological development and achieve the government's digital economy objectives, a comprehensive review of existing legal documents is essential. Necessary amendments and supplements should ensure that policies remain aligned, coherent and relevant, particularly in investment attraction policies and technology development incentives, to adapt and evolve to new development trends.

Streamlining government structure and expected changes in 2025

Under Plan No. 141/KH-BCDTKNQ18, the government's organisational structure is set on restructuring and streamlining. While eight ministries will be maintained (including MoPS), fourteen (14) ministries will undergo restructuring, consolidation or mergers. The Steering Committee has proposed merging MPI with the Ministry of Finance (MoF), as well as MIC with MoST.[196] Despite the mergers, the core functions of these ministries will remain intact, though its organisational structures will be adjusted.

Therefore, draft legislation such as the Digital Technology Industry Law, amendments to Decree No. 154/2013/ND-CP, studies on regulatory sandboxes for data ownership, management, processing and distribution, and the Human Resources Development Plan for the

Semiconductor Industry will be spearheaded and submitted by these newly consolidated ministries starting in 2025

Digital transformation is seen as a strategic pathway for Vietnam to achieve prosperous economic development. The role and contributions of digital technology and digital enterprises are widely recognised. Vietnam is considered a safe environment for long-term investments in technology, inspiring investor confidence to develop digital technology, due to its stable political system, consistent macroeconomic policies, steadily improving business environment, favourable geographical location and its potential as an emerging market.

5. Moving Forward

Technology governance in Southeast Asia is evolving rapidly. In 2025, governments across the region will likely continue pursuing inclusive economic growth in the digital economy and digitalising all sectors, while also actively working to safeguard digital society to promote security, trust and sustainability. In particular, the rapid innovation towards general, agentic and embedded AI has catalysed governments to address the protection of systems, livelihoods and its citizens.

Structural changes will require adjustments for all stakeholders, and continued coordination across agencies remains a priority. Without coordinated efforts, policy fragmentation may arise.[197] Vietnam is currently reviewing its governance structure with plans to merge and streamline key agencies. Transition challenges may be compounded by capability and expertise gaps. This is where multi-stakeholder engagement can support governance. Through collaboration with industry, academia and civil society, governments can leverage expertise and enable good regulatory practice. Structured engagement platforms, such as regular innovation ecosystem consultations or policy dialogues, will go a long way in fostering trust among stakeholders, creating a mutual understanding of respective desired outcomes and ensuring smoother policy execution.

As Southeast Asia prepares for the release of the ASEAN Digital Economy Framework Agreement (DEFA) in 2025, domestic regulatory clarity will advance cooperation on foundational issues such as cybersecurity, data governance and data flows. Sharing knowledge and governance approaches on emerging topics supports learning, especially when no one has all the answers, or even all the questions. Establishing sandbox corridors, for instance, enables governments to refine their approaches based on shared experiences and encourage innovation that draws upon the strengths of different countries. Similarly, upskilling and reskilling initiatives can benefit from greater cross-country collaboration. As the digital skills gap remains a pressing challenge, governments can work together on regional AI and cybersecurity training programmes, foster industry-academia partnerships and facilitate knowledge exchanges to build a more competitive and future-ready workforce in the region.

Finally, while the DEFA will establish the foundation for a cooperative framework, the shared priorities identified in this report can serve as a starting point for tangible areas of collaboration. There is value in starting even in small areas. Collaborative programmes to address common interests in AI, cybersecurity and data protection, and promoting safety and trust can begin as information-sharing or capability development initiatives. In addition, while a region-wide approach is ideal, the ASEAN 2+X"[198] or "ASEAN minus X" formulae of flexible participation allow for two or more Member States to pursue bilateral arrangements first, and others are welcomed to join once they are ready. By focusing on incremental steps, shared priorities and cross-border cooperation, Southeast Asia can cultivate a trusted, future-ready and competitive digital ecosystem.

References

[1] Tech for Good Institute. (2024, January). *Spotlight of Southeast Asia: Evolution of tech regulation in the digital economy.* Retrieved January 30, 2025, from https://techforgoodinstitute.org/research/tfgi-reports/spotlight-of-southeast-asia-evolution-of-tech-regulation-in-the-digital-economy/

[2] Google, Temasek, & Bain & Company. (2024). *e-Conomy SEA 2024 Report.* Google. Retrieved January 30, 2025, from https://economysea.withgoogle.com/report/.

[3] United Nations (UN). (2024, September). *Governing AI for humanity: Final report.* Retrieved January 30, 2025, from https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf

[4] Google, Temasek, & Bain & Company. (2024).

[5] Board, J. (2025, January 2). *Awash with billions in Big Tech money, but Southeast Asia's cloud and AI boom faces limits. Channel News Asia.* Retrieved January 30, 2025, from https://www.channelnewsasia.com/asia/focus-southeast-asia-data-centres-ai-hot-market-investments-limits-4816111

[6] AP News. (2024, May 30). *Google to invest $2 billion in Malaysian data center and cloud hub.* AP News. Retrieved January 30, 2025, from https://apnews.com/article/malaysia-google-investment-94764341b721e1c1f3fb2d607604f011

[7] Economic Development Board (EDB). (2024). *Singapore to expand data centre capacity by at least one-third, pushes for green energy use.* Retrieved January 30, 2025 from https://www.edb.gov.sg/en/business-insights/insights/singapore-to-expand-data-centre-capacity-by-at-least-one-third-pushes-for-green-energy-use.html.

[8] Kearney. (2020, October 7). *Racing Towards the Future: Artificial Intelligence in Southeast Asia.* Retrieved January 30, 2025, from Racing toward the future: artificial intelligence in Southeast Asia | Kearney

[9] Ibid.

[10] Nettel, P. F., Hankins, E., Stirling, R., Cirri, G., Grau, G., Rahim, S., & Crampton, E. (2024). *Government AI Readiness Index.* In S. Rahim (Ed.), Oxford Insights. Retrieved January 30, 2025, from https://staging2.oxfordinsights.com/ai-readiness/ai-readiness-index/

[11] Maslej, N., Fattorini, L., Perrault, R., Parli, V., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J. C., Shoham, Y., Wald, R., & Clark, J. (2024). *Artificial*

intelligence index report 2024. Stanford University, Institute for Human-Centered AI. Retrieved January 30, 2025, from https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf

[12] Johnston, S. (2024, May 13). *Generative AI in Asia Pacific: Young employees lead as employers play catch-up.* Deloitte Insights. Retrieved January 30, 2025, from https://www2.deloitte.com/us/en/insights/topics/emerging-technologies/generative-ai-adoption-asia-pacific-region.html

[13] Electronic Transaction Development Agency (ETDA). (2024c, October 30). *DE and ETDA announce new Guideline "Guidelines for applying Generative AI with good governance for organizations."* ETDA. Retrieved January 30, 2025, from https://www.etda.or.th/th/pr-news/AI_Gov_Anual.aspx

[14] Infocomm Media Development Authority (IMDA). (2024a, May 30). *SG launches Gen AI and AI Governance Playbook for Digital FOSS.* Retrieved January 30, 2025, from https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/gen-ai-and-digital-foss-ai-governance-playbook

[15] Foong, K. (2024, October 29). *National Guidelines on Artificial Intelligence Governance and Ethics: Key principles.* Rahmat Lim & Partners. Retrieved January 30, 2025, from https://www.rahmatlim.com/perspectives/articles/29210/mykh-national-guidelines-on-artificial-intelligence-governance-and-ethics-key-principles

[16] Department of Trade and Industry (DTI). (2024, July 2). *DTI launches National AI Strategy Roadmap 2.0 and Center for AI Research, positioning the Philippines as a Center of Excellence in AI R&D.* Retrieved January 30, 2025, from https://www.dti.gov.ph/archives/news-archives/dti-launches-national-ai-strategy-roadmap-2-0-center-ai-research-positioning-philippines-center-excellence-ai-rampd/

[17] Ministry of Science and Technology (MOST). (2024, June 17). *Ministry of Science and Technology guides principles for responsible research and development of artificial intelligence.* Retrieved January 30, 2025, from https://most.gov.vn/vn/tin-tuc/24448/bo-khcn-huong-dan-nguyen-tac-nghien-cuu--phat-trien-tri-tue-nhan-tao-co-trach-nhiem.aspx

[18] Ministry of Higher Education, Science, Research, and Innovation (MHESI). (2024, September 30). *"Supamas" announced the strategy for developing AI skills to move forward with teaching in higher education institutions nationwide through the "AI University" project to "Education 6.0" with the goal of having 90 percent of graduates have basic knowledge of AI.* Retrieved January 30, 2025, from https://www.mhesi.go.th/index.php/news-and-announce-all/news-all/106-minister-supamas/10698-ai-ai-university-education-6-0-90-ai.html

[19] Bigar, F. (2024). *The Importance of Humanising AI in Business: Transforming the Modern Workforce.* Tech for Good Institute. Retrieved January 30, 2025 from

https://techforgoodinstitute.org/blog/articles/the-importance-of-humanising-ai-in-business-transforming-the-modern-workforce/

[20] DataGuidance. (2024, April 26). *Indonesia: Kominfo announces preparation of regulations on governance of AI technology.* Retrieved January 30, 2025, from https://www.dataguidance.com/news/indonesia-kominfo-announces-preparation-regulations

[21] Bestari, N. P. (2024, August 20). *AI Regulations in Indonesia Tightened, Deputy Minister of Communication and Information: More Powerful!* CNBC Indonesia. Retrieved January 30, 2025, from https://www.cnbcindonesia.com/tech/20240820143612-37-564842/aturan-ai-di-indonesia-diperketat-wamenkominfo-lebih-powerful

[22] Mastercard. (2024, October 16). *Mastercard and ASEAN Foundation sign MoU to Launch Cyber Resilience Program to bolster cybersecurity capacity across the region.* Retrieved January 30, 2025, from https://www.mastercard.com/news/ap/en/newsroom/press-releases/en/2024/mastercard-and-asean-foundation-sign-mou-to-launch-cyber-resilience-program-to-bolster-cybersecurity-capacity-across-the-region/

[23] Knowles, C. (2024, May 28). *Cyber threats surge in SEA: Kaspersky detects 13 million attacks.* Retrieved January 30, 2025, from https://itbrief.asia/story/cyber-threats-surge-in-sea-kaspersky-detects-13-million-attacks

[24] Ibid.

[25] Philippine News Agency. (2025, February 14). *DICT fortifies PH cybersafety with National Cybersecurity Plan '23-'28.* Retrieved February 23, 2025, from https://www.pna.gov.ph/articles/1244121#:~:text=DICT%20fortifies%20PH%20cybersafety%20with%20National%20Cybersecurity%20Plan%20%2723%2D%2728,-By%20Philippine%20News&text=MANILA%20%E2%80%93%20President%20Ferdinand%20R.%20Marcos,the%20growing%20threat%20of%20cyberattacks

[26] Digital Policy Alert. (n.d.). *Thailand: Cybersecurity regulation in NCSC Standards for the Maintenance of Cybersecurity in Cloud Computing Systems B.E. 2566 (2023).* Retrieved January 30, 2025, from https://digitalpolicyalert.org/change/11180-cybersecurity-regulations-in-ncsc-standards-for-the-maintenance-of-cybersecurity-in-cloud-computing-systems-be-2566-2023

[27] Government of Singapore. (2024, July 5). *Cybersecurity (Amendment) Act 2024 No.19 of 2024*. Singapore Statutes Online. Retrieved January 30, 2025, from https://sso.agc.gov.sg/Acts-Supp/19-2024/Published/20240704?DocDate=20240704

[28] Walalangi & Partners. (2024, September 20). *W&P Newsletter – Countdown to Compliance: Personal Data Protection ("Pdp") Law Comes into Full Force On 17 October 2024.* Retrieved

January 29, 2025, from https://www.wplaws.com/wp-newsletter-countdown-to-compliance-personal-data-protection-pdp-law-comes-into-full-force-on-17-october-2024/

[29] Personal Data Protection (PDP) Commissioner & Futurise Sdn. Bhd. (2024, November 18). *PDP Commissioner, Futurise on Track to Complete Guidelines and Standard Under the Act 709 by the end of 2024* [Press release]. Retrieved January 30, 2025, from https://www.pdp.gov.my/ppdpv1/en/pdp-commissioner-futurise-on-track-to-complete-guidelines-andstandard-under-the-act-709-by-the-end-of-2024/

[30] Government of Vietnam. (2024). *Approving the National Data Strategy by 2030 (Decision 142/QD-TTg 2024).* LuatVietnam. Retrieved January 30, 2025, from https://english.luatvietnam.vn/thong-tin/decision-142-qd-ttg-2024-approving-the-national-data-strategy-by-2030-295383-d1.html

[31] Cyber Security Agency of Singapore (CSA). (2024, October 16). Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region [Press release]. Retrieved January 30, 2025, from https://www.csa.gov.sg/news-events/press-releases/singapore-and-asean-member-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region

[32] Global Anti-Scam Alliance & Gogolook. (2023). Asia Scam Report 2023. Retrieved January 30, 2025, from https://www.gasa.org/_files/ugd/b63e7d_aaaa062b799344a6897a5819fa96340f.pdf

[33] Ibid.

[34] The Business Times. (2024, February 18). *Scams victims in Singapore lost S$651.8 million in 2023, with record high cases*. Retrieved January 30, 2025, from https://www.businesstimes.com.sg/singapore/scam-victims-singapore-lost-s6518-million-2023-record-high-cases

[35] Vietnam Plus. (2024, January 8). *Vietnamese loss 16.23 billion USD to online scams.* Retrieved January 30, 2025, from https://en.vietnamplus.vn/vietnamese-loss-1623-billion-usd-to-online-scams-post276711.vnp

[36] Philippine Congress. (2023b, May 24). *Implementing rules and regulations of the Internet Transactions Act of 2023 (Republic Act No. 11967)*. Retrieved January 30, 2025, from https://www.dti.gov.ph/?sdm_process_download=1&download_id=111608

[37] Suwanmatajarn, P. (2024, June 24). *Thailand's ETDA Unveils Comprehensive Guidelines to Combat Online Advertising Fraud.* The Legal. Retrieved January 30, 2025, from https://thelegal.co.th/2024/06/24/thailands-etda-unveils-comprehensive-guidelines-to-combat-online-advertising-fraud/

[38] Christopher & Lee Ong. (2024, December 27). *An Overview of the Online Safety Bill 2024.* Retrieved January 30, 2025, from https://www.christopherleeong.com/viewpoints/an-overview-of-the-online-safety-bill-2024/

[39] Anggraeni and Partners. (2024, July 14). *Reforming Consumer Protection in Indonesia: Glimpse of the new Draft Bill 2024. Lexology.* Retrieved January 30, 2025, from https://www.lexology.com/library/detail.aspx?g=7860ab20-2e05-4f4b-b63f-2f3774ac3b37

[40] Monetary Authority of Singapore (MAS). (2024b, October 24). *Guidelines on Shared Responsibility Framework.* Retrieved January 30, 2025, from https://www.mas.gov.sg/regulation/guidelines/guidelines-on-shared-responsibility-framework

[41] Bangko Sentral Ng Pilipinas. (2024, July 20). *BSP Welcomes Passage of Anti-Financial Account Scamming Law.* Retrieved January 30, 2025, from https://www.bsp.gov.ph/SitePages/MediaAndResearch/MediaDisp.aspx?ItemId=7179

[42] Ramirez, M., & Vitooraporn, P. (2024, April 11). *Thailand's Criminal Court Establishes Cybercrime Division.* Mondaq. Retrieved January 30, 2025, from https://www.mondaq.com/crime/1449502/thailands-criminal-court-establishes-cybercrime-division

[43] Bangko Sentral Ng Pilipinas. (2024, July 20).

[44] Tech for Good Institute. (2024, January).

[45] Dharmaraj, S. (2024, October 24). *Digital Equity and Security: Indonesia's new Digital Minister's vision.* OpenGov Asia. Retrieved January 30, 2025, from https://opengovasia.com/2024/10/24/digital-equity-and-security-indonesias-new-digital-ministers-vision/

[46] Abdullah, Z. (2024, May 13). *MCI to be renamed Ministry of Digital Development and Information.* The Straits Times. Retrieved January 30, 2025, from https://www.straitstimes.com/singapore/politics/mci-to-be-renamed-ministry-of-digital-development-and-information

[47] Ministry of Digital Development and Information (MDDI). (2024c, August 6). *MDDI's response to PQ on considerations for new ministry name*. Retrieved January 30, 2025, from https://www.mddi.gov.sg/pq-on-considerations-for-new-ministry-name/

[48] The Straits Times. (2024, September 12). *Smart Nation agency and MCI's digital development functions to merge.* The Straits Times. Retrieved January 30, 2025, from https://www.straitstimes.com/singapore/smart-nation-agency-to-merge-with-mci-s-digital-development-functions?_gl=1*uw06fq*_gcl_au*MTg4Mzc5NDMzMC4xNzMzNjE5MzQ1

[49] National AI Office (NAIO). (n.d.). *AI Leadership in Malaysia and Beyond. Malaysia National AI Office (NAIO).* Retrieved January 30, 2025, from https://ai.gov.my/about-naio

[50] Infocomm Media Development Authority (IMDA). (2024, May 24). *Digital Trust Centre designated as Singapore's AI Safety Institute.* Retrieved January 30, 2025 from https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/digital-trust-centre

[51] Meltzer, J. (2024, May 21). *Developing global AI governance for foundational AI.* Retrieved January 30, 2025 from https://www.hinrichfoundation.com/research/article/tech/developing-global-ai-governance-for-foundational-ai/.

[52] Huld, A. (2024, February 15). *Philippines enacts new E-Commerce regulation.* ASEAN Briefing. Retrieved January 30, 2025, from https://www.aseanbriefing.com/news/philippines-enacts-new-e-commerce-regulation/

[53] Ngamkham, W. (2024, March 20). *Special court planned to handle cybercrime.* Bangkok Post. Retrieved January 30, 2025, from https://www.bangkokpost.com/thailand/general/2761478/special-court-planned-to-handle-cybercrime

[54] Ramirez, M., & Vitooraporn, P. (2024, April 11). *Thailand's Criminal Court Establishes Cybercrime Division.* Mondaq. Retrieved January 30, 2025, from https://www.mondaq.com/crime/1449502/thailands-criminal-court-establishes-cybercrime-division

[55] British Council. (2024, November 15). *Indonesia reorganises education ministry to help meet development agenda.* Retrieved January 30, 2025, from https://opportunities-insight.britishcouncil.org/short-articles/news/indonesia-reorganises-education-ministry-help-meet-development-agenda

[56] Ministry of Education (MOE). (2024, March 4). *New SkillsFuture Level-Up Programme to Boost Mid-Career Upskilling and Reskilling.* Retrieved January 30, 2025 from https://www.moe.gov.sg/news/press-releases/20240304-new-skillsfuture-level-up-programme-to-boost-mid-career-upskilling-and-reskilling.

[57] Ministry of Digital Development and Information (MDDI). (2024d, October 1). *Further S$120M investment in "AI for Science".* Retrieved January 30, 2025 from https://www.sgpc.gov.sg/api/file/getfile/5%20Further%20SGD120M%20investment%20in%20AI%20for%20Science%20Factsheet_FINAL.pdf?path=/sgpcmedia/media_releases/mddi-ced/press_release/P-20241001-1/attachment/5%20Further%20SGD120M%20investment%20in%20AI%20for%20Science%20Factsheet_FINAL.pdf

[58] Vietnam Investment Review. (2024b, May 31). *Thailand intensifies AI policy to transform economy. Vietnam Investment Review.* Retrieved January 30, 2025, from https://vir.com.vn/thailand-intensifies-ai-policy-to-transform-economy-111562.html

[59] Socialist Republic of Vietnam. (2024b, August 23). *On enhancement of high-quality human resources training in the fields of semiconductors, artificial intelligence and cloud computing* (No. 83/CD-TTg). Retrieved January 30, 2025, from https://thuvienphapluat.vn/van-ban/So-huu-tri-tue/Cong-dien-83-CD-TTg-2024-dao-tao-nhan-luc-chat-luong-cao-linh-vuc-vi-mach-ban-dan-tri-tue-nhan-tao-622423.aspx

[60] Land Transportation Franchising and Regulatory Board (LTFRB). (2024a, March 25). *Guidelines on the application for the issuance of certificate of public convenience to operate taxi services using electric vehicles* (Memorandum Circular No. 2024-007). Retrieved January 30, 2025, from https://ltfrb.gov.ph/wp-content/uploads/2024/03/MC-2024-007.pdf?appgw_azwaf_jsc=5WaD9_1FKhdzLRVA3xZrkDA9Szi_mqRiGj9-hXJaU9E

[61] Land Transportation Franchising and Regulatory Board (LTFRB). (2024b, May 24). *Board Resolution No. 072, Series of 2024*. Retrieved January 30, 2025, from https://drive.google.com/file/d/1uepxyVHXCtfhmJv7yG7oG5yyv17XS1V2/view

[62] Bangko Sentral Ng Pilipinas. (2024, July 20).

[63] ID Tech. (2024, July 25). *Thailand launches selfie-based digital wallet registration.* Retrieved January 30, 2025, from https://idtechwire.com/thailand-launches-selfie-based-digital-wallet-registration/

[64] Decker, C. (2018). *Regulation: Goals and rules-based approaches*. Retrieved January 30, 2025 from https://assets.publishing.service.gov.uk/media/5b17b32eed915d2cb16267d9/regulation-goals-rules-based-approaches.pdf

[65] Singapore FinTech Association. (2023, May). *Buy Now, Pay Later (BNPL) Code of Conduct*. Retrieved January 30, 2025 from https://singaporefintech.org/wp-content/uploads/2023/05/BNPL-CoC-Final-170822-Code.pdf

[66] Detros, K., & Lim, S. (2024). *Sandbox to Society: Fostering Innovation in Southeast Asia.* Tech For Good Institute. Retrieved January 30, 2025, from https://techforgoodinstitute.org/research/tfgi-reports/sandbox-to-society-fostering-innovation-in-southeast-asia/

[67] Ibid.

[68] Infocomm Media Development Authority (IMDA). (n.d.). *PETs Sandbox Expansion – Use of PETs for generative AI use cases.* Retrieved January 30, 2025, from https://www.imda.gov.sg/-/media/imda/files/programme/pet-sandbox/pets-for-generative-ai.pdf

[69] The Securities and Exchange Commission (SEC). (2024, August 9). *SEC launches Digital Asset Regulatory Sandbox on 9 August 2024.* Retrieved January 30, 2025, from https://www.sec.or.th/EN/Pages/News_Detail.aspx?SECID=11004

[70] Makarim & Taira S. (n.d.). *Refining Digital Financial Innovation: New OJK regulation aims to enhance regulatory sandbox.* Retrieved January 30, 2025, from https://www.makarim.com/news/refining-digital-financial-innovation-new-ojk-regulation-aims-to-enhance-regulatory-sandbox#:~:text=POJK%203%2F2024%20introduces%20a,or%20the%20public%20in%20Indonesia

[71] Skrine - Advocates & Solicitors. (2024, May 8). *Bank Negara issues new Fintech Sandbox Framework.* Retrieved January 30, 2025, from https://www.skrine.com/insights/alerts/march-2024/bank-negara-issues-new-fintech-sandbox-framework

[72] Tilleke & Gibbins. (2024, October 21). *Fintech Insights: The Bank of Thailand's Sandbox Framework for Fintech Innovation*. Retrieved January 30, 2025, from https://www.tilleke.com/insights/fintech-insights-the-bank-of-thailands-sandbox-framework-for-fintech-innovation/

[73] One Asia Lawyers. (2024, September 17). *Vietnam: Regulatory Sandbox for Fintech Companies in Banking Sector.* Retrieved January 30, 2025, from https://oneasia.legal/en/6051

[74] Sekretariat RPJN 2025 - 2045. (n.d.). *Indonesia Emas 2045: Rencana Pembangunan Jangka Panjang Nasional (RPJPN) 2025 - 2045.* Retrieved January 30, 2025, from https://indonesia2045.go.id/

[75] Novarina, A. (Ed.). (2024, November 11). *Investment in digital sector important for 8% growth: govt* (L. Kristianti & Y. Difa, Trans.). ANTARA. Retrieved January 30, 2025, from https://en.antaranews.com/news/333729/investment-in-digital-sector-important-for-8-growth-govt

[76] Purwanto, A. (2021, September 20). Tracing the Potential, Challenges, Regulations, and National Strategy of the Digital Economy in Indonesia. Retrieved January 30, 2025, from https://www.kompas.id/baca/paparan-topik/2021/09/20/merunut-potensi-tantangan-regulasi-dan-strategi-nasional-ekonomi-digital-di-indonesia

[77] DataGuidance. (2024, April 26).

[78] Bestari, N. P. (2024, August 20).

[79] Ministry of Communication and Information (Kominfo). (2023, December 19). *AI ethics No. 9/2023*. Retrieved January 30, 2025, from https://jdih.komdigi.go.id/produk_hukum/view/id/883/t/surat+edaran+menteri+komunikasi+dan+informatika+nomor+9+tahun+2023

[80] Government of Indonesia. (2024, January 2). *Second amendments of Law No. 11/2018 on electronic transaction and information law, Law No. 1/2024*. Retrieved January 30, 2025, from https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024

[81] State Cyber and Signal Agency (BSSN). (2024a, January 10). *Management of cyber incident, State Cyber and Signal Agency Regulation No. 1/2024.* Retrieved January 30, 2025, from https://peraturan.bpk.go.id/Details/291240/peraturan-bssn-no-1-tahun-2024

[82] State Cyber and Signal Agency (BSSN). (2024b, January 10). *Management of cyber crisis, State Cyber and Signal Agency Regulation No. 2/2024.* Retrieved January 30, 2025, from https://peraturan.bpk.go.id/Details/291245/peraturan-bssn-no-2-tahun-2024

[83] State Cyber and Signal Agency (BSSN). (2024c, May 29). *Information security self-assessments for MSMEs, State Cyber and Signal Agency Regulation No. 4/2024.* Retrieved January 30, 2025, from https://peraturan.bpk.go.id/Details/293671/peraturan-bssn-no-4-tahun-2024

[84] State Cyber and Signal Agency (BSSN). (2024d, June 7). *National action plan for cybersecurity, State Cyber and Signal Agency Regulation No. 5/2024.* Retrieved January 30, 2025, from https://peraturan.bpk.go.id/Details/309728/peraturan-bssn-no-5-tahun-2024

[85] State Cyber and Signal Agency (BSSN). (2024e, September 9). *Implementation of the conformity assessment of Indonesia common criteria for IT security evaluation, State Cyber and Signal Agency Regulation No. 7/2024.* Retrieved January 30, 2025, from https://peraturan.go.id/id/peraturan-bssn-no-7-tahun-2024

[86] State Cyber and Signal Agency (BSSN). (2024f, November 19). *Implementation of Indonesian cryptographic algorithms, State Cyber and Signal Agency Regulation No. 11/2024.* Retrieved January 30, 2025, from https://peraturan.bpk.go.id/Details/309832/peraturan-bssn-no-11-tahun-2024

[87] Ministry of Communication and Information (Kominfo). (n.d.). *Draft Government Regulation on Implementing Regulations of Law No.27/2022 on Personal Data Protection.* Retrieved January 30, 2025, from https://pdp.id/rpp-ppdp/1

[88] Government of Indonesia. (2023, February 16). *Regulation on consumer protection draft*. Retrieved January 30, 2025, from https://berkas.dpr.go.id/puuekkukesra/na/file/na-225.pdf

[89] CNN Indonesia. (2024a, June 25). *Prevent Google Monopoly, RI Prepares New Regulations for Digital Economy.* Retrieved January 30, 2025, from https://www.cnnindonesia.com/teknologi/20240622220355-190-1112915/cegah-monopoli-google-ri-siapkan-regulasi-baru-demi-ekonomi-digital

[90] Business Competition Supervisory Commission (KPPU). (2024b, May 28). *KPPU Gelar Sidang Perdana Shopee* [Press release]. Retrieved January 30, 2025, from https://kppu.go.id/wp-content/uploads/2024/05/Siaran-Pers-No.39_KPPU-PR_V_2024.pdf

[91] Business Competition Supervisory Commission (KPPU). (2024a, April 2). *TikTok Temui KPPU, Jelaskan Komitmennya Untuk Persaingan Sehat* [Press release]. Retrieved January 30, 2025, from https://kppu.go.id/wp-content/uploads/2024/04/Siaran-Pers-No.25_KPPU-PR_IV_2024.pdf

[92] Business Competition Supervisory Commission (KPPU). (2024c, May 30). *Dampak Hadirnya Starlink Dalam Perspektif Persaingan Usaha* [Press release]. Retrieved January 30, 2025, from https://kppu.go.id/wp-content/uploads/2024/05/Siaran-Pers-No.-42_KPPU-PR_V_2024.pdf

[93] Business Competition Supervisory Commission (KPPU). (2024d, June 28). *Tok! KPPU Muali Sidangkan Google* [Press release]. Retrieved January 30, 2025, from https://kppu.go.id/wp-content/uploads/2024/06/Siaran-Pers-No.-55_KPPU-PR_VI_2024-17.05.pdf

[94] President of the Republic of Indonesia. (2024, November 5). *Presidential Decree No. 174/2024*. Retrieved January 30, 2025, from https://jdih.komdigi.go.id/produk_hukum/view/id/947/t/peraturan+presiden+nomor+174+tahun+2024

[95] Savitri, D. (2024, October 23). *Ministry of Primary and Secondary Education: Prabowo Concerns About STEM, Considered Teaching It in Elementary School*. Detik. Retrieved January 28, 2025, from https://www.detik.com/edu/sekolah/d-7602435/mendikdasmen-prabowo-concern-stem-dikaji-diajarkan-awal-sd

[96] Natalia, T. (2024, February 1). *Indonesian Students' Math-Reading Scores One of the Lowest in the World*. CNBC Indonesia. Retrieved January 30, 2025, from https://www.cnbcindonesia.com/research/20240131161319-128-510569/skor-matematika-membaca-pelajar-ri-salah-satu-terendah-di-dunia

[97] Savitri, D. (2024, October 23).

[98] CNN Indonesia. (2024b, November 6). *Ministry of Education Says LPDP Recipients Will Be Prioritized for Science and Technology*. Retrieved January 30, 2025, from

https://www.cnnindonesia.com/nasional/20241106153611-20-1163657/mendikti-sebut-penerima-lpdp-akan-diutamakan-untuk-keilmuan-saintek

[99] Financial Services Authority (OJK). (2024, February 19). *Implementation of financial technology innovation 2024, OJK Regulation No. 3/2024*. Retrieved January 30, 2025, from https://www.ojk.go.id/id/regulasi/Documents/Pages/POJK-2-2024-Penyelenggaraan-Inovasi-Teknologi-Sektor-Keuangan/POJK%203%20Tahun%202024%20Penyelenggaraan%20Inovasi%20Teknologi%20Sektor%20Keuangan.pdf

[100] Financial Services Authority (OJK). (2024a, June 3). *Registration of technological innovators in the financial sectors 2024, Number 6/SEOJK.07/2024*. Retrieved January 30, 2025, from https://ojk.go.id/id/regulasi/Documents/Pages/Pendaftaran-Penyelenggara-Inovasi-Teknologi-Sektor-Keuangan/SEOJK%206-SEOJK.07-2024%20Pendaftaran%20Penyelenggara%20Inovasi%20Teknologi%20Sektor%20Keuangan.pdf

[101] Financial Services Authority (OJK). (2024b, June 3). *Implementation of a sandbox mechanism 2024, Number 5/SEOJK.07/2024*. Retrieved January 30, 2025, from https://www.ojk.go.id/id/regulasi/Documents/Pages/Mekanisme-Ruang-Uji-Coba-dan-Pengembangan-Inovasi/SEOJK%205-SEOJK.07-2024%20Mekanisme%20Ruang%20Uji%20Coba%20dan%20Pengembangan%20Inovasi.pdf

[102] Financial Services Authority (OJK). (2024c, August 8). *Reporting obligations related to the deployment of innovations in the financial sector 2024, Number 7/SEOJK.07/2024*. Retrieved January 30, 2025, from https://www.ojk.go.id/id/regulasi/Documents/Pages/Pelaporan-Penyelenggara-Inovasi-Teknologi-Sektor-Keuangan-yang-Terdaftar-di-Otoritas-Jasa-Keuangan/SEOJK%207-SEOJK.07-2024%20Pelaporan%20Penyelenggara%20Inovasi%20Teknologi%20Sektor%20Keuangan%20yang%20Terdaftar%20di%20Otoritas%20Jasa%20Keuangan.pdf

[103] Financial Services Authority (OJK). (2024d, September 11). *Establishment of an association of fintech providers 2024, Number 8/SEOJK.07/2024*. Retrieved January 30, 2025, from https://www.ojk.go.id/id/regulasi/Documents/Pages/Asosiasi-Penyelenggara-Inovasi-Teknologi-Sektor-Keuangan/SEOJK%208-SEOJK.07-2024%20Asosiasi%20Penyelenggara%20Inovasi%20Teknologi%20Sektor%20Keuangan.pdf

[104] Ministry of Trade. (2018, September 20). *Regulation for organizing crypto assets futures trading No. 99/2018*. Retrieved January 30, 2025, from https://peraturan.bpk.go.id/Details/128487/permendag-no-99-tahun-2018

[105] Financial Services Authority (OJK). (2024e, December 10). *Regulation on digital asset trading and crypto No. 27/2024*. Retrieved January 30, 2025, from https://www.hukumonline.com/pusatdata/detail/lt67622c67d5b0d/peraturan-otoritas-jasa-keuangan-nomor-27-tahun-2024/

[106] Agnes Theodora. (2023, August 6). *Early Deindustrialization Not Enough to Be Overcome with Downstreaming.* Kompas.com. Retrieved January 27, 2025, from https://www.kompas.id/baca/english/2023/08/08/deindustrialisasi-dini-tak-cukup-diatasi-dengan-hilirisasi?open_from=Translator_Mark

[107] Ministry of Science, Technology, and Innovation (MOSTI). (2024, September). *The National Guidelines on AI Governance & Ethics.* Retrieved January 30, 2025, from https://mastic.mosti.gov.my/publication/the-national-guidelines-on-ai-governance-ethics/

[108] National AI Office (NAIO). (n.d.).

[109] Bernama. (2024, November 19). *MCMC logs 8,399 cyberbullying cases this year, says Fahmi.* News Straits Times. Retrieved January 30, 2025, from https://www.nst.com.my/news/nation/2024/11/1136644/mcmc-logs-8399-cyberbullying-cases-year-says-fahmi

[110] Busst, N., & Chee, S. (2024, July 17). *Fahmi disappointed with RM100 fine for Esha's cyberbully.* Free Malaysia Today. Retrieved January 30, 2025, from https://www.freemalaysiatoday.com/category/nation/2024/07/17/fahmi-disappointed-with-rm100-fine-for-eshas-cyberbully/

[111] Parliament of Malaysia. (2024). *Communications and Multimedia (Amendment) Bill 2024* (D.R.51/2024). Retrieved January 30, 2025, from https://www.parlimen.gov.my/files/billindex/pdf/2024/DR/DR%2051-BI.pdf

[112] Shazrie, A. (2024, December 8). *Online scams totalling RM3.18b reported from 2021 to April 2024: Gobind.* The Sun Malaysia. Retrieved January 29, 2025, from https://thesun.my/business-news/online-scams-totalling-rm318b-reported-from-2021-to-april-2024-gobind-KP12849829

[113] Zuhair, Q. (2024, February 26). *Increasing online fraud cases a worrying trend.* The Sun Malaysia. Retrieved January 30, 2025, from https://thesun.my/malaysia-news/increasing-online-fraud-cases-a-worrying-trend-IB12139375

[114] Parliament of Malaysia. (2024b). *Penal Code (Amendment) (No.2) Bill 2024* (D.R.57/2024). Retrieved January 30, 2025, from https://www.parlimen.gov.my/files/billindex/pdf/2024/DR/DR57-BI.pdf

[115] Parliament of Malaysia. (2024c). *Criminal Procedure Code (Amendment) (No.2) Bill 2024* (D.R.58/2024). Retrieved January 30, 2025, from https://www.parlimen.gov.my/files/billindex/pdf/2024/DN/DR58-BI.pdf

[116] Parliament of Malaysia. (2024b).

[117] Parliament of Malaysia. (2024c).

[118] Parliament of Malaysia. (2024a). *Personal Data Protection (Amendment) Bill 2024* (D.R.21/2024). Retrieved January 30, 2025, from https://www.parlimen.gov.my/files/billindex/pdf/2024/DN/DR%2021%20BI.pdf

[119] Parliament of Malaysia. (2024d). *Online Safety Bill 2024* (D.R.59/2024). Retrieved January 30, 2025, from https://www.parlimen.gov.my/files/billindex/pdf/2024/DN/DR59-%20BI.pdf

[120] Malaysia Ministry of Digital. (n.d.). *Driving Digitalisation of the Nation*. Retrieved January 30, 2025, from https://www.digital.gov.my/en-GB

[121] Paul, M. (2024, December 13). *YBrs. Ts. Dr. Fazidah binti Abu Bakar, Director General, Jabatan Digital Negara (JDN), Malaysia*. Gov Insider Asia. Retrieved January 30, 2025, from https://govinsider.asia/intl-en/article/ybrs-ts-dr-fazidah-binti-abu-bakar-deputy-director-general-information-and-communication-technology-jabatan-digital-negara-jdn-malaysia

[122] Malaysia Ministry of Digital. (2024, October 4). *National AI Office to Shape Future of AI in Malaysia, Key Leadership Roles Open to Qualified Individuals*. Retrieved January 30, 2025, from https://www.digital.gov.my/en-GB/siaran/National-AI-Office-to-Shape-Future-of-AI-in-Malaysia-Key-Leadership-Roles-Open-to-Qualified-Individuals

[123] Federal Legislation. (2024). *Cyber Security Act 2024* (Act 854). Royal Assent on June 18, 2024. Commencement on August 26, 2024 [P.U. (B) 334/2024]. Retrieved January 30, 2025, from https://lom.agc.gov.my/act-detail.php?language=BI&act=854

[124] Parliament of Malaysia. (2024a).

[125] Personal Data Protection (PDP) Commissioner & Futurise Sdn. Bhd. (2024, November 18).

[126] Malaysian Communications and Multimedia Commission (MCMC). (2024, August 1). *Frequently Asked Questions (FAQ) on the Regulatory Framework for Internet Messaging Service and Social Media Service Providers in Malaysia*. Retrieved January 30, 2025, from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/FAQ-for-Regulatory-Framework.pdf

[127] Parliament of Malaysia. (2024d).

[128] Google, Temasek, & Bain & Company. (2024).

[129] Philippine Statistic Authority. (2024, April 25). *Digital Economy contributes 8.4 percent to the Economy in 2023.* Retrieved January 30, 2025, from https://psa.gov.ph/statistics/digital-economy

[130] Philippines Department of Trade and Industry. (2024, November 6). *PH reclaims title as Southeast Asia's fastest-growing internet economy*. Retrieved January 30, 2025, from https://www.dti.gov.ph/archives/news-archives/ph-reclaims-title-as-southeast-asias-fastest-growing-internet-economy/

[131] United Nations Conference on Trade and Development. (2024). *2024 Digital Economy Report: Shaping an environmentally sustainable and inclusive digital future (UNCTAD/DER/2024).* United Nations. Retrieved January 30, 2025, from https://unctad.org/system/files/official-document/der2024_en.pdf

[132] Philippine Congress. (2024f, October 2). *An Act amending sections 105, 108, 109, 110, 113, 115, 128, 236, and 288 and adding new sections 108-A and 108-B of the National Internal Revenue Code of 1997, as amended* (Republic Act No. 12023). 19th Congress. Retrieved January 30, 2025, from https://www.officialgazette.gov.ph/2024/10/02/republic-act-no-12023/

[133] Philippine Congress. (2024g, November 8). *An Act amending sections 27, 28, 32, 34, 57, 106, 108, 109, 112, 135, 237, 237-A, 269, 292, 293, 294, 295, 296, 297, 300, 301, 308, 309, 310, and 311, and adding new sections 135-A, 295-A, 296-A, and 297-A of the National Internal Revenue Code of 1997, as amended, and for other purposes* (Republic Act No. 12066). 19th Congress. Retrieved January 30, 2025, from https://www.officialgazette.gov.ph/2024/11/08/republic-act-no-12066/

[134] President of the Philippines. (2024b, May 13). *Implementing a digital and integrated system for the pre-border technical verification and cross-border electronic invoicing of all import commodities* (Administrative Order No. 23/2024). Retrieved January 30, 2025, from https://www.officialgazette.gov.ph/2024/05/13/administrative-order-no-23-s-2024/

[135] Philippine Congress. (2023b, May 24).

[136] Philippine Congress. (2024c, July 20). *An Act in defining and penalizing financial account scamming and other offenses and providing for the enforcement mechanisms therefor* (Republic Act No. 12010). 19th Congress. Retrieved January 30, 2025, from https://www.officialgazette.gov.ph/2024/07/20/republic-act-no-12010/

[137] Philippine Congress. (2022b, May 6). *An Act affording more protection to consumers of financial products and services* (Republic Act No. 11765). 18th Congress. Retrieved January 30, 2025, from https://www.officialgazette.gov.ph/2022/05/06/republic-act-no-11765/

[138] Gonzales, A. L. (2024, June 10). Gov't launches digital national ID. Philippine News Agency. Retrieved January 30, 2025, from https://www.pna.gov.ph/articles/1226595

[139] President of the Philippines. (2024a, April 4). *Adopting the National Cybersecurity Plan 2023-2028 and directing the implementation thereof* (Executive Order No. 58/2024). Retrieved January 30, 2025, from https://www.officialgazette.gov.ph/2024/04/04/executive-order-no-58-s-2024/

[140] Department of Information and Communications Technology. (2023). *National Cybersecurity Plan 2023-2028*. Retrieved January 30, 2025, from https://cms-cdn.e.gov.ph/DICT/pdf/NCSP-2023-2028-FINAL-DICT.pdf

[141] Philippine Congress. (2024e, August 14). *An Act institutionalizing the transition of the government to e-governance, establishing for the purpose the e-governance academy, and appropriating funds therefor* (Senate S. No. 2781). 19th Congress. Retrieved January 30, 2025, from https://web.senate.gov.ph/lisdata/4461240587!.pdf

[142] Philippine Congress (2023b, March 7). *An Act institutionalizing the transition of the government to e-governance, establishing for the purpose the e-governance academy, and appropriating funds therefor* (House of Representatives H. No. 7327). 19th Congress. Retrieved January 30, 2025, from https://docs.congress.hrep.online/legisdocs/third_19/HBT7327.pdf

[143] Philippine Congress. (2024a, May 22). *An Act establishing a comprehensive and inclusive data transmission and connectivity framework for the Philippines* (Senate S. No. 2699). 19th Congress. Retrieved January 30, 2025, from https://web.senate.gov.ph/lisdata/4436240331!.pdf

[144] Philippine Congress. (2022b). *An Act promoting open access in data transmission and providing additional powers to the National Telecommunications Commission* (House of Representatives H. No. 6). 19th Congress. Retrieved January 30, 2025, from https://docs.congress.hrep.online/legisdocs/third_19/HBT0006.pdf

[145] Securities and Exchange Commission. (2024). *SEC Stratbox (Strategic Sandbox)* (Memorandum Circular No. 9, Series of 2024).

[146] Mercurio, R. (2024, September 6). GStocks ready to go global. *The Philippine Star*. Retrieved January 30, 2025, from https://www.philstar.com/business/2024/09/06/2383134/gstocks-ready-go-global

[147] Land Transportation Franchising and Regulatory Board (LTFRB). (2024c, November 12). *Guidelines on the issuance of certificate of public convenience to implement Republic Act No. 11659 (Public Service Act, as amended) and its implementing rules and regulations* (Memorandum Circular No. 2024-041). Retrieved January 30, 2025, from https://ltfrb.gov.ph/wp-content/uploads/2024/11/MC-2024-041-1.pdf?appgw_azwaf_jsc=ZDUXQoINDLku7UqSYwCqt31UHF0fEfTwnmdFgPXNPvI

[148] Land Transportation Franchising and Regulatory Board (LTFRB). (2024a, March 25).

[149] Land Transportation Franchising and Regulatory Board (LTFRB). (2024b, May 24)

[150] Land Transport Office. (2024, October 2). *Suspension of LTO Administrative Order No. 2021-039 and LTO Administrative Order No. VDM-2024-044 or the guidelines in the classification, registration, and operation of all types of electric vehicles*. Retrieved January 30, 2025, from https://lto.gov.ph/wp-content/uploads/2024/10/Memo-10022024.pdf?appgw_azwaf_jsc=yhj2oUlWAdcepWVMhAWLPxo_FCjE8HW7loQ_RbOBhPk

[151] Philippine Congress. (2022a, April 15). *An act providing for the development of the electric vehicle industry (Republic Act No. 11697)*. Retrieved January 30, 2025, from https://www.officialgazette.gov.ph/2022/04/15/republic-act-no-11697/

[152] Department of Trade and Industry. (2024). *Department Administrative Order No. 24-01, Series of 2024: Implementing rules and regulations of Republic Act No. 11981 or the "Tatak Pinoy (Proudly Filipino) Act"*. Retrieved January 30, 2025, from https://dtiwebfiles.s3.ap-southeast-1.amazonaws.com/Laws+and+Policies/DAO/Department+Administrative+Order+No.+24-01.pdf

[153] Smart Nation Singapore. (n.d.). *Goals of Smart Nation 2.0*. Retrieved January 30, 2025, from https://www.smartnation.gov.sg/goals-of-sn2/

[154] Ministry of Digital Development and Information (MDDI) & Smart Nation Singapore. (2024, October 1). *New agency for online safety and assurance* [Media factsheet]. Retrieved January 30, 2025, from https://www.sgpc.gov.sg/api/file/getfile/4%20New%20Agency%20for%20Online%20Safety%20and%20Assurance%20Factsheet_FINAL.pdf?path=/sgpcmedia/media_releases/mddi-ced/press_release/P-20241001-1/attachment/4%20New%20Agency%20for%20Online%20Safety%20and%20Assurance%20Factsheet_FINAL.pdf

[155] Infocomm Media Development Authority (IMDA). (2024a, May 30).

[156] Ministry of Digital Development and Information (MDDI). (2024a, January 10). *Measures to protect Singaporeans against online scams* [Press release]. Retrieved January 30, 2025, from https://www.mddi.gov.sg/media-centre/press-releases/measures-to-protect-singaporeans-against-online-scams/

[157] Boo, K. (2024, December 7). *Guidelines to help S'pore businesses shield themselves from quantum threats from 2025: CSA*. The Straits Times. Retrieved January 30, 2025, from https://www.straitstimes.com/business/guidelines-to-help-spore-businesses-shield-from-quantum-threats-from-2025-csa

[158] Cheng, I. (2024, September 18). *Banks to roll out Singpass face verification as part of digital token set-up process*. The Straits Times. Retrieved January 30, 2025, from

https://www.straitstimes.com/singapore/banks-to-roll-out-singpass-face-verification-as-part-of-digital-token-setup-process

[159] Monetary Authority of Singapore (MAS). (2024a, July 18). *MAS commits up to S$100 million to support quantum and artificial intelligence capabilities in the financial sector*. Media Release. Retrieved January 30, 2025, from https://www.mas.gov.sg/news/media-releases/2024/mas-commits-up-to-s$100-million-to-support-quantum-and-artificial-intelligence-capabilities#:~:text=The%20Monetary%20Authority%20of%20Singapore,technologies%2C%20as%20well%20as%20enable

[160] Ministry of Digital Development and Information (MDDI). (2024b, March 1). *New Digital Infrastructure Act to enhance resilience & security of digital infrastructure & services*. Press Release. Retrieved January 30, 2025, from https://www.mddi.gov.sg/media-centre/press-releases/new-digital-infrastructure-act/

[161] Monetary Authority of Singapore (MAS). (2024b, October 24).

[162] Republic of Singapore. (2024a, October 11). *Platforms Workers Act 2024 (No. 30 of 2024)*. Acts Supplement. Retrieved January 30, 2025, from https://sso.agc.gov.sg/Acts-Supp/30-2024/Published/20241011?DocDate=20241011

[163] Smart Nation Singapore. (n.d.)

[164] Infocomm Media Development Authority (IMDA). (2024c, September 22). *AI Playbook for Small States* at the Digital Forum of Small States, in collaboration with the Ministry of ICT and Innovation (Rwanda). Retrieved January 30, 2025, from https://www.imda.gov.sg/-/media/imda/files/news-and-events/media-room/media-releases/2024/09/ai-playbook-for-small-states/imda-ai-playbook-for-small-states.pdf

[165] Infocomm Media Development Authority (IMDA). (2024b, September 4). *Privacy enhancing technology sandboxes*. Retrieved January 30, 2025, from https://www.imda.gov.sg/how-we-can-help/data-innovation/privacy-enhancing-technology-sandboxes

[166] Ministry of Digital Development and Information (MDDI) & Smart Nation Singapore. (2024)

[167] Infocomm Media Development Authority (IMDA). (2024b)

[168] AI Verify Foundation & Infocomm Media Development Authority (IMDA). (2024, May 30). *Model AI governance framework for generative AI: Fostering a trusted ecosystem*. Retrieved January 30, 2025, from https://aiverifyfoundation.sg/wp-content/uploads/2024/05/Model-AI-Governance-Framework-for-Generative-AI-May-2024-1-1.pdf

[169] Infocomm Media Development Authority (IMDA). (2024d, September 23). *Digital forum of small states (Digital FOSS)*. Retrieved January 30, 2025, from https://www.imda.gov.sg/about-imda/international-relations/digital-forum-of-small-states

[170] Ministry of Digital Development and Information (MDDI) & Smart Nation Singapore. (2024)

[171] Republic of Singapore. (2023b, August 11). *Online Criminal Harms Act 2023 (No. 24 of 2023).* Retrieved January 30, 2025, from https://sso.agc.gov.sg/Act/OCHA2023

[172] Republic of Singapore. (2024a, October 11)

[173] Monetary Authority of Singapore (MAS). (2024c, October 30). *MAS announces establishment of global finance & technology network for next phase of FinTech growth* [Media release]. Retrieved January 30, 2025, from https://www.mas.gov.sg/news/media-releases/2024/mas-announces-establishment-of-global-finance-and-technology-network

[174] Infocomm Media Development Authority (IMDA). (2024b, September 4).

[175] Monetary Authority of Singapore. (2024a, October 24).

[176] Enterprise Singapore. (n.d.). *SME Pro-Enterprise Office.* Retrieved January 30, 2025, from https://www.enterprisesg.gov.sg/smepeo

[177] Government Public Relations Department. (2024, May 20). *Thailand ranks 35th in World Digital Competitiveness Ranking 2023.* Retrieved January 30, 2025, from https://thailand.prd.go.th/en/content/category/detail/id/2078/iid/288916

[178] Ibid.

[179] Electronic Transactions Development Agency (ETDA). (2024d, December 4). *Thailand to host the first Asia-Pacific "UNESCO Global Forum on the Ethics of AI 2025," showcasing its leadership in AI ethics through a collaboration between DE, MHESI, MOE, and UNESCO.* Retrieved January 30, 2025, from https://www.etda.or.th/th/pr-news/ai_etda_unesco_EN.aspx

[180] Sawatdee, P. (2024, September 30). *"Supamas" announced the strategy for developing AI skills to move forward with teaching and learning in higher education institutions nationwide through the "AI University" project to "Education 6.0" with the goal of having 90 percent of graduates have basic knowledge of AI.* Ministry of Higher Education, Science, Research, and Innovation. Retrieved January 30, 2025, from https://www.mhesi.go.th/index.php/news-and-announce-all/news-all/106-minister-supamas/10698-ai-ai-university-education-6-0-90-ai.html

[181] Electronic Transactions Development Agency. (2024d, December 4).

[182] Electronic Transactions Development Agency (ETDA). (2023a, July 27). *"DPS Law" Who Benefits? Insights that Digital Platform Users Must Read!* Retrieved January 30, 2025, from https://www.etda.or.th/th/Useful-Resource/dps_inside.aspx

[183] Electronic Transactions Development Agency. (2024b, August). *Generative AI governance guideline for organisations (Volume 1).* Retrieved January 30, 2025, from https://www.etda.or.th/th/Useful-Resource/GovernanceGuideline_v1.aspx

[184] United Nations Department of Economic and Social Affairs. (n.d.). *E-Government Development Index (EGDI).* Retrieved January 30, 2025, from https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index

[185] World Intellectual Property Organization (WIPO) (2024). *Global Innovation Index 2024: Unlocking the Promise of Social Entrepreneurship.* Geneva: WIPO. 10.34667/tind.50062

[186] International Telecommunication Union. (2024). *Global Cybersecurity Index 2024 (5th ed.).* International Telecommunication Union. ISBN 978-92-61-38751-8 (Electronic version). Retrieved January 30, 2025, from https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

[187] Startup Blink. (2024, May 30). *Global Startup Ecosystem Index 2024*. Retrieved January 30, 2025, from https://lp.startupblink.com/report/

[188] Government Electronic Newspaper. (2021, February 26). *Full text of the Resolution of the 13th National Congress of the Party*. Retrieved January 30, 2025, from https://baochinhphu.vn/toan-van-nghi-quyet-dai-hoi-dai-bieu-toan-quoc-lan-thu-xiii-cua-dang-102288263.htm

[189] Socialist Republic of Vietnam. (2021, January 26). *Promulgating the national strategy on research, development, and application of artificial intelligence to 2030* (No. 127/QD-TTg). Retrieved January 30, 2025, from https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-127-QD-TTg-2021-Chien-luoc-nghien-cuu-phat-trien-va-ung-dung-Tri-tue-nhan-tao-den-2030-463680.aspx

[190] Ministry of Science and Technology (MOST). (2024, June 17).

[191] Socialist Republic of Vietnam. (2024d, November 20). *Promulgating the national action plan on digital economy development for the 2024 - 2025 period* (No. 1437/QD-TTg). Retrieved January 30, 2025, from https://thuvienphapluat.vn/van-ban/Thuong-mai/Quyet-dinh-1437-QD-TTg-2024-Ke-hoach-hanh-dong-quoc-gia-phat-trien-kinh-te-so-632568.aspx

[192] Socialist Republic of Vietnam. (2024d)

[193] Socialist Republic of Vietnam. (2024a, May 7). *Regular government meeting April 2024* (No. 65/NQ-CP). Retrieved January 30, 2025, from https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Nghi-quyet-65-NQ-CP-2024-Phien-hop-Chinh-phu-thuong-ky-thang-4-609312.aspx

[194] Socialist Republic of Vietnam. (2024c, October 28). *Adjusting the law and ordinance development program* (Resolution No. 55/2024/UBTVQH15). Retrieved January 30, 2025, from https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Nghi-quyet-55-2024-UBTVQH15-dieu-chinh-Chuong-trinh-xay-dung-luat-phap-lenh-629254.aspx

[195] Socialist Republic of Vietnam. (2024b, August 23).

[196] Socialist Republic of Vietnam. (2024e, December 6). *Orientation for structuring and organizing the government apparatus* (No. 141/KH-BCĐTKNQ18). Retrieved January 30, 2025, from https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Ke-hoach-141-KH-BCDTKNQ18-2024-dinh-huong-sap-xep-tinh-gon-to-chuc-bo-may-cua-Chinh-phu-634500.aspx

[197] Tech for Good Institute. (2024, January). For a discussion on policy coordination for tech governance, please see https://techforgoodinstitute.org/research/tfgi-reports/spotlight-of-southeast-asia-evolution-of-tech-regulation-in-the-digital-economy/, produced in cooperation with the Tech Policy Design Institute (TPDI). TPDI has produced a Tech Policy Coordination Model for Australia here https://techpolicy.au/wp-content/uploads/2023/08/Web_TPDC_Cultivating-Coordination_NO.2_Feb-2023.pdf

[198] Association of the Southeast Asian Nations (ASEAN). (2006, December). *Report of the Eminent Persons Group on the ASEAN Charter.* Retrieved January 30, 2025, from https://www.asean.org/wp-content/uploads/images/archive/19247.pdf

Tech For Good Institute

www.techforgoodinstitute.org