TECH FOR GOOD INSTITUTE

Report — March 2026

Evolution of Tech Governance in Southeast Asia-6

Table of Contents

Table of Contents

About This Study

The Evolution of Tech Governance in Southeast Asia-6 (SEA-6) is an annual series produced by Tech for Good Institute (TFGI). The series aims to examine how governance approaches to the digital economy and society are evolving across Southeast Asia, document regulatory developments and explore regional trends.

The first edition[1] focused on identifying "who" the key regulators are in the digital economy as of 2023. The second edition[2] built on this 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. This third edition continues the longitudinal approach focusing on progression of governance approaches in SEA-6 in 2025.

Across the three editions, the analytical scope has intentionally expanded, from tech regulators to tech policy, to tech governance. In this series, governance refers to the broader context that encompasses policy while also covering the structures, systems, and decision-making processes that shape the digital economy. This involves mechanisms beyond formal legislation, including guidelines, co-regulation, voluntary codes of conduct, technical standards, sandbox arrangement, and multi-stakeholder platforms. By adopting this wider perspective, the series examines not just what rules are introduced, but how authority is exercised, by whom, and through which instruments.

The third edition highlights how governments are progressively moving from agenda-setting towards more established regulatory frameworks, implementation mechanisms, and institutional arrangements in the digital economy and digital society. By tracking developments over time, it offers a comparative perspective on how tech governance across Southeast Asia is evolving in practice.

This report continues to spotlight 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 both the opportunities and challenges presented by emerging technologies.

With contributing partners from each country, this report provides in-depth insights into the national developments while situating them within a broader regional context. Given the rapid pace of technological advancement and the unique trajectories of each country, the regulatory landscape of the digital economy will remain dynamic and continue to evolve. As a review of 2025 developments, this report aims to serve as a practical resource for policymakers, researchers and industry practitioners seeking to understand the region's evolving governance 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 reference point on policy and governance developments, this paper seeks to foster dialogue and collaboration in shaping effective and forward-looking regulatory frameworks. With the substantial conclusion of the Digital Economy Framework Agreement (DEFA) negotiations in October 2025, this report also identifies common areas of convergence where tangible cooperation on regional interoperability can be advanced.

Acknowledgements

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
- 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 National Institute for Economics and Finance, Vietnam
- Pierre Tito Galla Democracy.Net.PH, 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 (TFGI) is a non-profit policy research institute working to advance the promise of technology and the digital economy for inclusive, equitable and sustainable growth in Southeast Asia (SEA).

With a population twice the size of the US and having strong demographics, SEA'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. TFGI serves as a platform for research, conversations and collaborations focused on SEA, 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.

TFGI works in partnership with the Mastercard Center for Inclusive Growth and Grab, to advance the vision of a thriving and innovative SEA 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

In 2025, digital governance within the SEA-6 entered a phase of consolidation. Governments moved from policy formulation to implementation and enforcement. Cybersecurity, artificial intelligence (AI), and digital platform governance are increasingly recognised as core pillars of economic resilience, public trust, and national security. Regulatory frameworks have progressed to operationalisation, oversight responsibilities have expanded, and enforcement measures have become more visible. The transition occurred amid intensifying global competition in AI and changing geopolitical and geoeconomic dynamics, placing greater demands on Southeast Asian nations to strengthen digital sovereignty while maintaining competitiveness and fostering regional interoperability. The defining feature of 2025 was not simply the passage of new laws, but the integration of strategic intent into institutional practice.

This report explores recent developments through two interrelated dimensions: first, the policy priorities shaping governance across the SEA-6; and second, the broader evolution of governance architectures, including emerging models of digital sovereignty, structural reforms within state institutions, and enhanced regional coordination. Through this dual perspective, three interconnected shifts distinguish 2025 from previous years. These shifts are not merely continuations of existing trends; rather, they represent significant transformations in how governments operationalise regulatory power within the digital economy.

From framework to function

In 2025, the SEA-6 experienced a notable shift from regulatory design to practical execution. Legislative developments in AI governance, online safety, cybersecurity and digital platforms were accompanied by strengthened enforcement agencies, defined compliance timelines, and clearer penalties for non-compliance.

Vietnam implemented its AI Law and the Law on the Digital Technology Industry, formalising state oversight of emerging technologies. Malaysia's Online Safety Act has introduced mandatory licensing for large platforms. Thailand enacted 24-hour takedown obligations and mechanisms for shared financial liability in technology-related offences. Singapore's Protection from Scams Act empowered authorities to impose immediate banking restrictions to prevent fraud. Collectively, these actions indicate a regional transition towards active enforcement as opposed to declaratory policy signalling.

This shift fundamentally alters the relationship between governments and the technology industry. States are building durable institutional capabilities by creating new agencies, inter-ministerial committees, and supervisory units, rather than relying on ad hoc measures. Implementation has become a central metric of governance performance.

Balancing innovation and sovereignty

AI governance across the region has undergone a significant reframing. While earlier years emphasised ethical principles and voluntary guidance, 2025 saw governments move toward more binding regulation and increasingly treat AI as strategic national infrastructure, comparable in significance to energy systems or defence capabilities. In the SEA-6, AI policy approaches have evolved, now combining risk management with infrastructure investment and capacity-building.

Vietnam initiated construction of a national AI supercomputing centre and a centralised National Data Centre. Indonesia's National AI Roadmap prioritises sovereign Graphics Processing Units (GPUs), Tensor Processing Units (TPUs), and national cloud infrastructure. Malaysia committed to establishing a National Sovereign AI Cloud by 2026. Thailand allocated substantial public funding for AI advancement. Whereas Singapore strengthened practical AI safety testing frameworks and enterprise-level compute support.

At the same time, regulatory sandboxes became institutionalised within sectoral governance regimes. Vietnam embedded sandbox mechanisms directly within its AI Law and the Digital Transformation Law, signalling a shift away from blanket prohibition towards controlled experimentation in fintech, telecommunications and digital services. Singapore evolved its "innovation with guardrails" models by pairing experimentation with structured test protocols and assurance artefacts in health technology and AI-enabled medical devices. Indonesia continued to pilot its digital rupiah within a supervised sandbox environment.

This layered approach, combining infrastructure investment, binding regulation and supervised experimentation, signals a structural evolution. Governments are positioning themselves not merely as regulators, but also as investors, coordinators and market shapers.

National differentiation within regional convergence

While regulatory approaches remain diverse, 2025 marked a transition from aspirational coordination toward negotiated interoperability. The ASEAN Digital Economy Framework Agreement (DEFA) reached substantive conclusion in October 2025, with a formal signing anticipated in 2026. Malaysia and the Philippines prioritised DEFA as a strategic economic deliverable. The formal establishment of the ASEAN AI Safety Network and the operationalisation of the "Hanoi Convention" on cybercrime further strengthened regional coordination in AI safety and cross-border enforcement.

Regional alignment is increasingly embedded in structured commitments rather than informal dialogue. Instruments like DEFA and ASEAN's data initiatives are gradually shaping digital trade, regulatory compliance, and cross-border data governance. The adoption of the Hanoi Digital Declaration in January 2026 further reinforces this trajectory, signalling commitment to enhance digital cooperation and expedite regional digital transformation.

However, this growing regional integration is unfolding alongside strengthened sovereignty strategies. Vietnam's enhanced data control measures, Indonesia's infrastructure and payment sovereignty initiatives, and Singapore's assurance-based regulatory perimeter approach illustrate distinct domestic pathways that might hinder seamless integration. The primary governance tension for the SEA-6 lies in balancing sovereign control with interoperable regional systems. The management of this balance will shape whether the region evolves into a cohesive digital market or remains characterised by regulatory fragmentation.

As frameworks enter enforcement phases, 2026, will determine the durability of this consolidation. Expanded enforcement needs to translate into quantifiable public benefits instead of merely increasing compliance burdens. Sovereign AI infrastructure ambitions necessitate a careful balance between the openness to investments with strategic control. DEFA's formal signing and implementation will test whether interoperability commitments can move from negotiation to operational reality. These developments will define whether the governance consolidation of 2025 evolves into a stable and coherent institutional framework.

The implications are profound. For governments, the priority shifts from announcing reforms to ensuring institutional coherence and effective execution. Strengthening technical capacity, aligning mandates across agencies, and preventing regulatory overlap will be critical to sustaining governance performance. For industry, regulatory diversity across the SEA-6's increases compliance complexity, particularly for cross-border operators. At the same time, participation in sandbox and assurance regimes offers structured pathways to markets access and regulatory clarity. For research institutions and associations, the transition to implementation creates an expanded role in facilitating multi-stakeholder dialogue, translating complex regulation into operational guidance, and generating evidence to support policy improvement.

Ultimately, the next stage of SEA's digital governance will depend on whether interoperability and sovereignty can be balanced through coordinated institutional strengthening. Governments should consider investments in regional compatibility mechanisms, structured public-private collaboration, and cross-agency coherence as enforcement becomes more stringent and infrastructure strategies become more comprehensive. Without deliberate alignment, regulatory consolidation risks entrenching fragmentation beneath the surface of convergence. With effective implementation, the region can translate its aspirations into digital governance that is resilient, interoperable, and globally competitive.

1. Introduction

2025 marks a pivot from digital strategy to regulatory execution. SEA-6 governments are moving beyond high-level digital roadmaps toward implementation and enforcement, signalling a more proactive and institutionalised phase of tech governance.

Growth is strong but governance capacity is uneven. While SEA's digital economy continues to expand rapidly, differences in digital readiness and institutional maturity shape how effectively countries can translate policy ambition into regulatory outcomes.

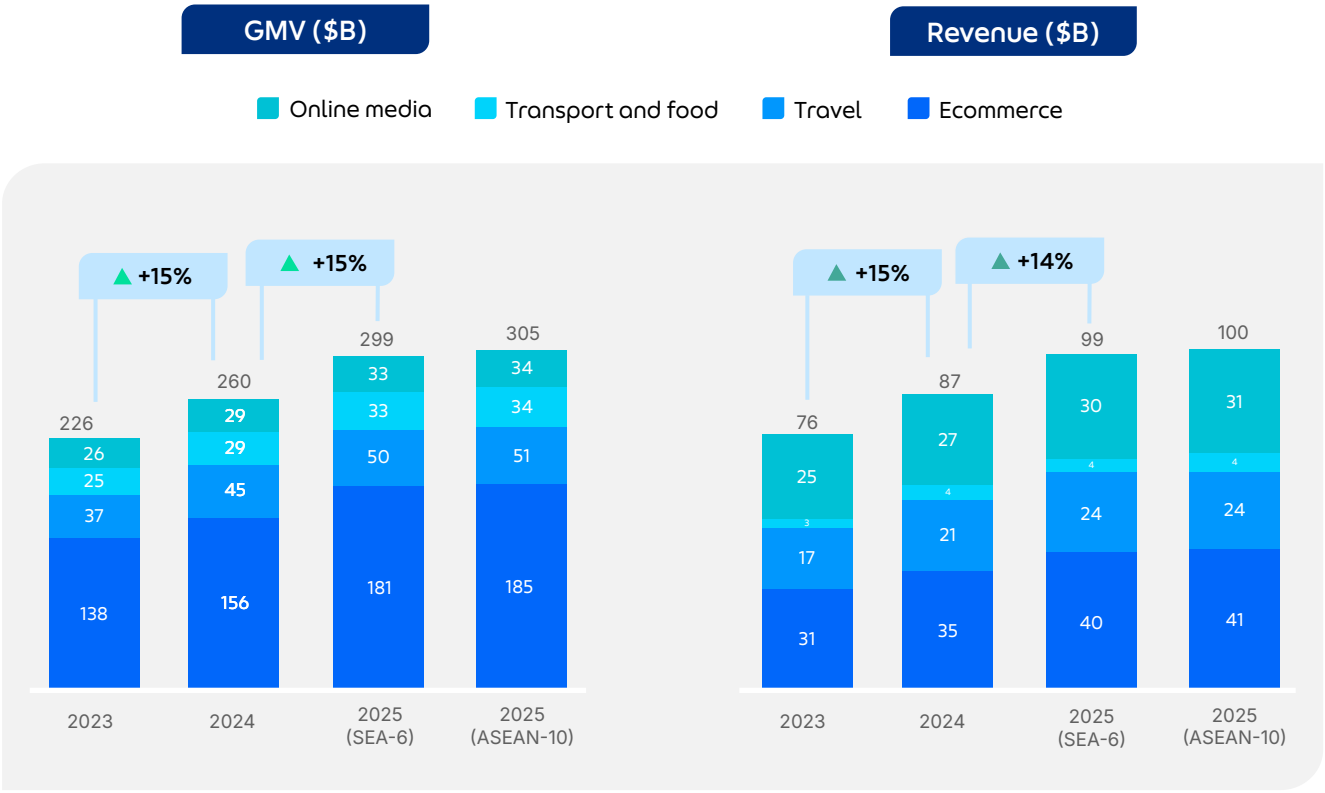
National differentiation is unfolding alongside cautious regional convergence. Countries increasingly align on common priorities, AI, cybersecurity, and platform regulation, yet pursue distinct regulatory pathways, even as regional coordination advances under emerging ASEAN frameworks.

2025 marked a more pronounced transition from policy design to implementation and enforcement across the SEA-6. Governments moved beyond outlining high-level strategies and frameworks toward operationalising them in practice. While policy priorities continued to converge around areas such as AI, cybersecurity and data protection, and platform regulation, implementation approaches remained differentiated. At the same time, regional coordination advanced through efforts to align governance frameworks, enhance interoperability and facilitate cross-border cooperation. The emerging trend in 2025 points to national differentiation alongside regional convergence. Whether this regulatory consolidation translates into sustained institutional maturity remains to be seen, underscoring the importance of tracking governance evolution over time.

As digital technologies are increasingly treated as critical strategic assets amid intensifying global competition, the regulatory decisions of SEA-6 governments (Indonesia, Malaysia, the Philippines, Singapore, Thailand, and Vietnam) have taken on heightened economic and geopolitical significance. These economies sit at the intersection of global supply chains, rapid digital-consumer growth, and intensifying competition for data, cloud infrastructure, and artificial intelligence (AI)-related investment. Regulatory choices extend beyond simple administrative adjustments; they shape market structure, capital allocation and investment flows, cross-border interoperability, and the distribution of economic and societal risks. They also determine whether the region's fast-growing digital economy is underpinned by an inclusive, trusted digital society or reinforces existing divides and vulnerabilities. Tracking the evolution of technology governance in the SEA-6 is therefore essential to understanding how these countries are adjusting their development frameworks amid expanding opportunity and tightening geopolitical and regulatory constraints.

The scale of the region's digital economy underscores the stakes of these governance decisions. By the end of 2025, the region's digital gross merchandise value (GMV) is forecasted to exceed USD 300 billion[3], which is 1.5 times the initial 10-year projection. Revenue is also anticipated to reach USD 135 billion[4], as profitability advances across sectors such as e-commerce, food delivery, online travel, and digital financial services. At the same time, private funding in the region has experienced a 15% increase year-on-year[5], reaching an estimated USD 8 billion[6] by the end of 2025. Resources are increasingly directed toward software and services, as well as AI and deep technology.

Figure 1. Digital Economy Growth in GMV and Revenue



Source: *e-Conomy SEA 2025 report: From digital decade to AI reality: Accelerating the future in ASEAN*

However, this expansion is accompanied by uneven levels of national digital readiness and institutional maturity. Singapore[7] leads the region with a score of 88 out of 100, establishing itself as the benchmark for digital maturity in the region. Malaysia, Thailand, and the Philippines[8] follow with a score above 60, reflecting relatively advanced digital capabilities. Vietnam[9] has demonstrated significant progress, transitioning from emerging to leading digital nations with a score approaching 50. Indonesia[10] positions itself within the emerging nations category with scores below 50. These differences are consequential. Variations in readiness influence regulatory maturity, enforcement capability, and the government ability to translate policy ambition into effective implementation. As a result, while countries across SEA-6 may articulate similar strategic priorities, their implementation pathway and regulatory outcomes continue to diverge.

Across the region, governments face the common challenges: to sustain digital economic growth while safeguarding social stability, national interests and public trust. Promoting the digital economy requires fostering innovation, attracting investment and strengthening industrial competitiveness. At the same time, protecting the digital society entails managing data governance, cybersecurity risks, platform accountability and emerging AI-related concerns. By 2025, this balancing act increasingly emerged around digital sovereignty. Concerns regarding infrastructure resilience, data governance, control over digital economic activity have become more explicitly integrated in binding legal instruments, enforcement practices and institutional mandates.

These developments have taken place amid intensifying global competition in AI, shifting geoeconomic dynamics, and heightened trade and tariff challenges impacting digital supply chains. As digital infrastructure and data governance become more closely intertwined with industrial strategy and national security, governments in SEA faced growing pressure to translate strategic objectives into actionable authority. In light of these circumstances, governance consolidation has shifted from a matter of policy aspiration to a practical necessity for economic positioning and resilience.

This report examines how these dynamics unfolded over the course of 2025. The report adopts a longitudinal approach to document the progression of digital governance across the SEA-6 on an annual basis. This approach allows us to identify institutional shifts, emerging patterns of consolidation or fragmentation in digital governance over time. Its analytical scope has progressively expanded from examining tech regulators, to reviewing broader tech policy and governance. In this report, governance is understood not merely as the existence of rules, but as the architecture through which authority is exercised and digital transformation is steered. It encompasses policy frameworks alongside institutional structures, coordination mechanisms and enforcement processes. By adopting this approach, the report examines not only what rules are introduced, but also who exercises authority and how implementation unfolds in practice.

Applying this longitudinal lens, the remainder of the report is organised as follows. Chapter 2 discusses common policy priorities of SEA-6 countries in 2025, highlighting key challenges in the digital economy, including AI governance, cybersecurity and data protection, and digital platform regulation. Chapter 3 explores the evolving institutional landscape, looking at how regulators are adapting to rapid technological change, how sovereignty considerations are operationalised, and how coordination mechanisms are structured domestically and regionally. Chapter 4 looks ahead to 2026, outlining what recent developments may signal for governments, industry and research institutions/think tanks/associations. Chapter 5, contributed 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. Together, these chapters support a clear understanding of whether ongoing regulatory consolidation can underpin inclusive, trusted, and sustainable digital growth across the region.

2.
Policy Priorities across SEA-6 in 2025

- **From strategy to enforcement.** In 2025, SEA-6 governments moved beyond digital roadmaps toward operational regulation across AI, cybersecurity, and digital platforms.
- **Shared priorities, different models.** Countries converge on core issues like AI risk, infrastructure resilience, online safety, fraud, taxation, and gig worker protection, but diverge in regulatory style, ranging from binding regimes to voluntary or hybrid approaches.
- **Sovereignty is shaping governance choices.** Investments in national AI infrastructure, data controls, and local presence requirements reflect growing emphasis on resilience and control over digital economic activity.
- **The gatekeeper role is expanding.** Digital platforms, banks, and telecom operators are increasingly playing a role for fraud prevention, identity verification, tax compliance, and content moderation.
- **Fiscal and labour reforms outpace competition policy.** Digital taxation and worker protections are advancing more concretely than competition frameworks addressing platform market power.

2.1. AI Governance

The AI landscape in Southeast Asia advanced significantly in 2025, driven by strong investment momentum and an acceleration of policy initiatives. The regional AI market expanded from approximately USD 4 billion in 2024[11] to USD 8.22 billion in 2025.[12] During the first half of the year alone, private investment reached USD 2.3 billion,[13] across more than 680 AI start-ups,[14] accounting for around 30% of the total private funding[15] in the region. This growth reflects a combination of factors, including rapid digital adoption among a young tech-savvy population, and increased government emphasis on embedding AI within national strategies.

In this context, SEA-6 governments implemented AI-related policy measures focussing on three interconnected areas in 2025: the establishment of governance and regulatory frameworks, investment in essential AI infrastructure, and enhancement of talent and innovation capacity-building. All six countries acknowledge the need to balance AI competitiveness with systemic risk management; however, their governance approaches and implementation frameworks continue to differ considerably.

2.1.1. Governance and Policy Frameworks

A key feature of AI governance in the SEA-6 is the divergence in regulatory approaches. Rather than converging on a uniform method, countries have adopted three broad strategies: legally binding frameworks, principles-based regimes relying on voluntary and industry-led mechanisms, and hybrid approaches that combine advisory guidance with preparatory measures for future regulation.

Vietnam has emerged as the most comprehensive and formalised regulator in the region. Through two enforceable legal instruments: the Law on Digital Technology Industry[16] and the AI Law,[17] the country has introduced a structured governance framework requiring registration, impact assessments, and conformity evaluations for high-risk AI systems. The nation applies a four-tier risk classification system and embeds AI oversight within established compliance structures, reflecting a strong preference for regulatory clarity and state-led supervision. The Philippines is moving in a similar direction through its proposed AI Regulation Act,[18] which, if enacted, would impose legally binding obligations on AI development and deployment, while fostering ethical innovation.

In contrast, Singapore continues to favor principles-based and voluntary approaches. In 2025, it strengthened its Global AI Assurance ecosystem through initiatives such as the Global AI Assurance Pilot,[19] and the Starter Kit for Safety Testing of LLM-Based Applications.[20] These efforts focus on developing testing protocols, assurance methodologies, and evaluative tools, without introducing mandatory compliance requirements, reinforcing Singapore's preference and industry collaboration.

Malaysia and Indonesia have adopted hybrid approaches characterised by a gradual shift towards binding frameworks. Malaysia released a draft National AI Action Plan 2026–2030,[21] positioning itself as an "AI Nation" under the 13th Malaysia Plan[22] and signalling its intentions to introduce binding AI legislation[23] by the end of 2026. Meanwhile, Indonesia issued AI Ethics Guidelines,[24] inspired by the risk-based approach of the EU AI Act.[25] The country also advanced a National AI Roadmap[26] identifying priority sectors, including food security and health. It is also developing draft AI legislation,[27] that would introduce mandatory risk classification and liability frameworks for high-risk systems. In both scenarios, advisory instruments are being used alongside efforts to build institutional capacity and prepare for enforceable regulations.

Beyond national frameworks, sector-specific governance has advanced, most clearly in financial services. Singapore is formulating draft AI risk management guidelines for financial institutions,[28] requiring model validation, explainability, and human oversight. Thailand has implemented AI Security Guidelines[29] establishing baseline security standards, while concurrently developing risk management guidelines for the financial sector.[30] Sectoral initiatives have also emerged in agriculture and transport. Malaysia's Digital AgTech[31] initiative integrates AI into the aquaculture and livestock production while the Philippines has approved an AI-driven city planning pilot in Naga City,[32] focused on transport and land-use monitoring, pending implementation. These developments suggest that jurisdictions favouring voluntary national frameworks are willing to adopt more binding controls in high-risk sectors or applications.

Table 1. Key AI Governance developments in SEA-6, 2025

Draft/Proposal | *In force/ Implementing* | *Passed/Approved - Pending Implementation*

Country / Approach	Indonesia	Malaysia	Philippines	Singapore	Thailand	Vietnam
Guiding Principles for New Technologies	National AI Roadmap, which identifies priority sectors such as food security and health	National AI Action Plan for 2026–2030 positions the nation as an 'AI Nation' in accordance with the 13th Malaysia Plan		The Global AI Assurance Pilot, targeted at end-to-end application reliability		
	AI Ethics Guidelines that draw inspiration from the EU AI Act's risk classifications			Starter Kit for Safety Testing of LLM-Based Applications		
Legally Binding Regulations	Draft legislation on AI that would include obligatory risk classification and liability frameworks for high-risk systems	AI law, which is anticipated to be completed by late 2026, under the guidance of an inter-agency task force	Artificial Intelligence Regulation Act (AIRA) regulates the development/ use of AI systems, promotes ethical innovation			AI Law that implements a four-tier risk classification system, requiring mandatory registration, impact assessments, and conformance evaluations for high-risk AI systems
						Law on the Digital Technology Industry outlines the core principles for AI governance
Sectoral and Implementation-level Governance		Digital AgTech initiative, which integrates AI into the aquaculture and livestock sub-sectors	AI-driven city planning system - a pilot project launched in Naga City focusing on transport and land-use monitoring	AI risk management specifically for financial institutions	Guidelines on AI risk management that mandate model validation, explicability, and human oversight for the financial sector	
					AI Security Guideline that establishes baseline security standards for AI systems	

2.1.2. Investments for Foundational AI Infrastucture

In 2025, SEA-6 governments allocated substantial public resources to foundational AI infrastructure, signalling a shift towards capacity-building as a core pillar of AI strategy. There is a growing recognition across the region that compute capacity, data infrastructure, and connectivity are prerequisites for effective AI deployment and governance. These investments reflect an effort to strengthen domestic capabilities while improving control over data, computational resources, and system resilience.

Two broad infrastructure strategies stand out. Firstly, several countries are pursuing nationally anchored or sovereign AI infrastructure. Vietnam is establishing a national AI supercomputing centre[33] and a National Data Centre,[34] positioning AI as a part of the country's core intellectual infrastructure and supporting long-term competitiveness and technological self-reliance. Indonesia's National AI Roadmap[35] emphasises sovereign data centres, access to GPU (Graphics Processing Unit) and TPU (Tensor Processing Unit) resources, and the development of a national cloud infrastructure to support domestic innovation and secure data governance. Thailand approved a budget of USD 798.11 million (THB 25 billion) for AI development in 2025,[36] including USD 63.87 million (THB 2 billion) for a National Data Centre to support sovereign AI capabilities. Malaysia has earmarked approximately USD 460 million (MYR 2 billion) for a National Sovereign AI Cloud,[37] scheduled for launch in 2026, with the aim of positioning the country as a regional cloud and digital hub by the year 2030, in alignment with the MyDigital Blueprint.[38]

Secondly, other countries have adopted infrastructure strategies shaped by different national priorities. Singapore continues to position itself as a regional AI hub, promoting green data centres and facilitating cross-border data flows, including through the launch of the APEC Cross-Border Privacy Rules (CBPR) system.[39] The Philippines has prioritisied foundational digital connectivity through the *Konektadong Pinoy Act*,[40] which focuses on nationwide broadband infrastructure as a prerequisite AI adoption, reflecting the view that strong connectivity must precede more specialised AI infrastructure.

2.1.3. Talent and Innovation Capacity

Recognising that AI strategies cannot succeed without skilled human capital and innovation ecosystems, governments have expanded initiatives focused on workforce development, research capacity, and innovation support. These efforts reflect a growing consensus that sustained AI advancement depends on coordinated investment across education systems, research institutions, and entrepreneurial environments.

Countries have increasingly integrated AI into their education and national upskilling programmes. Indonesia introduced coding and AI as elective subjects[41] in primary and secondary schools, facilitating early exposure to computational thinking and essential AI concepts. Malaysia established *MyMahir National AI Council for Industry* (MyMahir–NAICI)[42] to coordinate AI talent development and upskilling across sectors. Thailand launched the THAI Academy[43] through a public–private partnership with Microsoft to support comprehensive AI upskilling for the domestic workforce.

Alongside education, governments have strengthened research and applied innovation capacity. The Philippines established the Education Centre for AI Research (E-CAIR)[44] to link AI research with practical educational applications. Malaysia signalled its focus on frontier technologies through the creation of the Quantum Intelligence Centre,[45] aimed at advancing applied research in emerging computational paradigms relevant to advanced AI applications.

In addition to education and research, governments have also introduced targeted initiatives to promote AI adoption and innovation ecosystems. Singapore's Enterprise Compute Initiative[46] offers cloud credits and advisory support to help firms, especially small and medium-sized enterprises (SMEs), experiment with and deploy AI solutions. Vietnam has embedded regulatory sandboxes within its AI Law and Digital Transformation Law, allowing controlled testing of AI applications while enabling regulators to evaluate risks and refine governance approaches prior to wider implementation.

2.2. Cybersecurity and Data Protection

Cybersecurity remains a defining issue shaping the evolution of Southeast Asia's digital economy. As digital adoption deepens across government, industry, and society, cyber risks have grown in both scale and complexity. Emerging technologies, including AI-enabled systems, agentic technologies, and quantum computing, are introducing new vulnerabilities that existing governance models are not yet fully equipped to manage. As a result, cybersecurity is increasingly framed not merely as a technical issue, but as a foundational pillar of economic resilience, public trust, and national security.

Across the SEA-6, governments have responded by strengthening legal frameworks, enhancing institutional coordination, and shifting towards more preventive and operationally grounded approaches. Rather than relying solely on post-incident responses, policymakers are embedding cybersecurity considerations upstream, aligning infrastructure protection, consumer protection, and emerging technology governance within broader digital strategies. These developments signal a gradual transition from fragmented oversight to more integrated, whole-of-nation cybersecurity governance.

Table 2. Key Cybersecurity and Data Protection developments in SEA-6 by the end of 2025

Draft/Proposal | *In force/ Implementing* | *Passed/Approved - Pending Implementation*

Country / Policy area	Indonesia	Malaysia	Philippines	Singapore	Thailand	Vietnam
Frontier technologies		Cryptology Technology and Management Centre focuses on quantum-resilient encryption		Cyber Trust and Cyber Essentials marks now include AI, cloud, and operational technologies, linking assurance to innovation		Personal Data Protection Law embeds security requirements for AI-enabled data processing
				Quantum-Safe Handbook, the Quantum Readiness Index to prepare organisations for cryptographic risks and increasingly autonomous system behaviour		
Protection of critical infrastucture	Roadmap for the Protection of Vital Information Infrastructure in the Government Administration Sector to deepen protection for Vital Information Infrastructure (VII)	Malaysia Cyber Security Strategy 2025–2030, aims to advance cryptographic capabilities	Mandates ISO Cybersecurity Standards for Telecom Firms	Provisions in the Cybersecurity (Amendment) require Critical Information Infrastructure (CII) reporting and operational resilience		Draft Cybersecurity Law for consultation, merging the 2018 Cybersecurity Law and the 2015 Law on Cyberinformation Security
		New cybercrime bill to replace the Computer Crimes Act 1997		Public consultation on Amendments To Public Sector (Governance)		Network security responsibilities were also centralised under the Ministry of Public Security
		National Cyber Crisis Management Plan for incidents involving National Critical Information Infrastructure				Personal Data Protection Law and the Law on Electronic Transactions
		Cyber Security Exemption Order selected cloud operators to remain subject to Malaysian law and national security obligations				
Scams and fraud			The Anti-Financial Account Scamming Act requires Banks, e-wallet providers, and other financial institutions to enhance fraud detection, allows for regulated inquiries into scam-linked accounts, and implements real-time tracking and the temporary holding of disputed funds	Protection from Scams Act, empowers authorities to issue Restriction Orders that temporarily freeze banking facilities when scams are suspected	Royal Decree on Technology Crimes, introducing joint liability and real-time interventions across banks, telecoms, and platforms	

2.2.1. Frontier Technologies

Southeast Asian governments are increasingly looking beyond traditional infrastructure security to future-proof their cybersecurity frameworks against emerging technological risks. This reflects a broader shift towards anticipatory governance, aimed at safeguarding long-term technological competitiveness while managing systemic risk.

Vietnam's Personal Data Protection Law[47] requires organisations to integrate security, authentication, and access control measures when processing data through AI and cloud services. A draft Cybersecurity Law,[48] currently under development, seek to consolidate existing legislation while addressing AI-related risks, embedding emerging technology governance within a more unified legal structure.

Singapore expanded its Cyber Essentials and Cyber Trust certification schemes[49] to include AI systems, cloud services, and operational technology, raising the security baseline for organisations managing sensitive systems. The government also released for consultation, a Quantum-Safe Handbook, a Quantum Readiness Index,[50] and a guidance on securing agentic AI systems. Together these initiatives aim to prepare organisations for cryptographic risks and increasingly autonomous system behaviour.

Malaysia has begun preparing for quantum migration in recognition of the potential for future large-scale quantum computers to undermine secure communications and financial systems. The establishment of the Malaysian Cryptology Technology and Management Centre,[51] through a collaboration between Universiti Putra Malaysia and the National Cyber Security Agency, seeks to strengthen national encryption capabilities. This reflects growing awareness of the implications of quantum technologies for critical sectors such as banking, telecommunications, and data services.

2.2.2. Protection of Critical Infrastructure

Protection of Critical Information Infrastructure (CII) has become a central pillar of national security and digital economy development across SEA-6, Governments are moving from reactive incident response towards preventive, system-wide approaches that emphasise resilience, institutional clarity, and operational readiness, critical for public services.

Indonesia advanced a more structured approach through Regulation No. 5 of 2025 issued by the National Cyber and Encryption Agency, establishing a roadmap for protecting Vital Information Infrastructure[52] across government administration. The roadmap provides strategic direction for strengthening safeguards in essential public services and reflects a growing focus on systemic risk management.

Malaysia continued strengthening its institutional architecture. The National Cybersecurity Committee priorities finalising the Malaysia Cyber Security Strategy 2025–2030,[53] advancing cryptographic capabilities, and introducing a new cybercrime bill[54] to replace the Computer Crimes Act 1997. The updated strategy builds on the Cybersecurity Act passed in 2024 and focuses on refining the National Cyber Crisis Management Plan[55] for incidents involving National Critical Information Infrastructure. Although a Cyber Security Exemption Order[56] for selected cloud operators raised concerns about uneven enforcement, those operators remain subject to Malaysian law and national security obligations.

The Philippines adopted a standards-based approach by requiring telecommunications companies to obtain certification under the ISO or IEC 27000 series.[57] Aligning national practices with internationally

recognised information security benchmarks strengthens resilience among critical service providers.

Vietnam moved towards legal consolidation by releasing a draft Cybersecurity Law,[58] that merges the 2018 Cybersecurity Law and the 2015 Law on Cyberinformation Security. Network security responsibilities have also been centralised under the Ministry of Public Security.[59] Alongside the Personal Data Protection Law[60] and the Law on Electronic Transactions,[61] these reforms point towards a more unified framework for information and data security.

Singapore continued to enhance operational resilience. Owners of Critical Information Infrastructure[62] will be required to report suspected advanced persistent threat attacks, strengthening early detection and coordinated response. Amendments under consultation to the Public Sector Governance[63] Act also aim to enable carefully governed data sharing with trusted external partners, balancing resilience with collaboration.

2.2.3. Scams and Fraud

Governments across Southeast Asia have broadened their conception of cybersecurity to include consumer protection and trust in digital services, responding to the rapid growth of online scams and fraud. Rather than treating fraud solely as a criminal enforcement issue, policymakers are increasingly adopting cross-sector accountability models that impose shared responsibility on financial institutions, telecom operators, and digital platforms.

Thailand introduced a more interventionist enforcement framework through the Royal Decree on Measures for the Prevention and Suppression of Technology Crimes (No. 2).[64] The decree establishes shared liability for fraud losses linked to negligence and requires coordinated action across banks, telecom operators, and digital platforms. Measures include the deactivation of scam-linked SIM cards, freezing of suspicious accounts, and removal of fraudulent online profiles, all coordinated through the Cybercrime Operations Centre to enable real-time intervention.

Singapore strengthened its consumer protection through the Protection from Scams Act,[65] which took effect on 1 July 2025. The Act empowers authorities to issue Restriction Orders temporarily freezing banking facilities when scams are suspected. It reinforces earlier shared-responsibility measures and provides clearer enforcement powers and redress mechanisms.

In the Philippines, the *Bangko Sentral ng Pilipinas* issued implementing rules for the Anti-Financial Account Scamming Act.[66] Financial institutions must now enhance fraud detection systems, allow regulated inquiries into scam-linked accounts, and implement real-time tracking and temporary holding of disputed funds. The law also criminalises social engineering, money muling, and technology-enabled fraud, marking a significant expansion of consumer protection in the digital financial ecosystem.

2.3. Digital Platform Regulation

Digital platforms are now deeply embedded in SEA's digital economies, functioning as essential infrastructure for commerce, payments, logistics, social interaction, and content distribution. Over the past decade, over 200 million new users[67] have come online across the region. Three in five individuals[68] now engage in online shopping regularly, with over 60% of transactions[69] conducted digitally. Digital platforms support the livelihoods of more than 7 million platform-based gig workers in Indonesia and around 1.2 million[70] in Malaysia. Additionally, one in five micro,[71] small, and medium enterprises (MSMEs) throughout SEA-6 rely on e-commerce platforms for market access.

As a result, digital platforms are no longer viewed solely as private market actors. They are increasingly recognised as systemically important infrastructure shaping market competition, consumer access, and cross-border flows of data, payments, and labour. This recognition, combined with the substantial conclusion[72] of the ASEAN Digital Economy Framework Agreement (DEFA)[73] in late 2025 and its anticipated signing in 2026,[74] has intensified efforts to strengthen national and regulatory frameworks.

Against this backdrop, SEA-6 governments are accelerating updates to existing rules and introducing platform-specific measures. While there is convergence around key challenges, including content moderation, transaction integrity, market competition, and worker protections, regulatory approaches differ significantly. Developments in 2025 can be grouped into three interconnected areas: i) content governance; ii) commerce, transactions and payment security; and iii) competition, taxation and labour governance.

Table 3. Key Digital Platforms Regulations developments in SEA-6 by the end of 2025

Draft/Proposal | *In force/ Implementing* | *Passed/Approved - Pending Implementation*

Country / Policy area	Indonesia	Malaysia	Philippines	Singapore	Thailand	Vietnam
Content governance	Government Regulation No. 17/2025 (PP Tunas) on Child Protection in Digital Space, adopted risk-based approach, requires all electronic system providers to enforce minimum age requirements for users	Online Safety Act introduced mandatory licensing for social media and internet messaging platforms, requiring content moderation, age verification		Code of Practice for Online Safety requires designated app stores to implement pushed child-safety and harmful-content controls upstream, including age-assurance expectations	Notification of the Electronic Transactions Commission on Measures to Prevent Technological Crimes for Social Media Service Providers establishes 24-hour takedown obligations	
		Deeming provision; content moderation		Online Safety (Relief and Accountability) Bill introduced models for victim redress and platform accountability		
Commerce, transactions & payment security	Revision of Consumer Protection Law to revise and update regulations in response to the rapid evolution of the current digital landscape		The enactment of the Internet Transactions Act, which regulates e-commerce to ensure the security of online transactions, encompasses both business-to-business *(B2B) and business-to-consumer (B2C) transactions*	Protection from Scams Act (Restriction Orders) authorises the Police to issue restriction orders to banks, thereby limiting an individual's banking and credit facilities when there is a reasonable suspicion that the individual intends to transfer, withdraw, or access funds for the benefit of a scammer	Emergency Decree on Measures for the Prevention and Suppression of Technological Crimes established shared liability structure that mandates banks, telecom operators, and digital platforms to incorporate fraud detection and provide compensation to victims if negligence results in harm	E-commerce Law established comprehensive framework, requires national electronic identification (VNeID) for seller traceability and foreign platforms' compliance via local presence
			Launch of E-Commerce Philippine Trustmark, a mandatory certification designed to enhance consumer confidence in digital transactions	Financial Services and Markets Act mandates that Singapore-based digital token service providers must obtain a licence or cease operations in providing services to overseas clients	Notification of the Electronic Transactions Committee Re: Other Actions for Digital Platform Service Operators requires platforms to conduct identity verification business users and implement measures to enhance transparency and compliance	
Competitive market and Operating environment	Ministry of Finance Regulation No. 37/2025 (PMK 37/2025) appoints digital marketplace platforms to withhold 0.5% of gross turnover from domestic sellers	Gig Workers Bill introduced comprehensive legal framework and safeguard the rights of gig workers	The implementation of Republic Act No. 12023 mandates that digital services consumed domestically shall be subject to a 12% Value-Added Tax (VAT)	Platform Workers Act redefines the responsibilities of platform entities and the rights of their workers, formally incorporates gig workers into Singapore's social protection system *(In force)*	Trade Competition Commission of Thailand (TCCT) is developing a draft guideline addressing anti-competitive behaviour in multi-sided platforms	Corporate Income Tax Law classifies e-commerce and digital platform businesses as permanent establishments and outline applicable taxing mechanisms
				Enhanced Technical Reference 76 on Guidelines for electronic commerce (TR 76) provides updated guidelines to enhance consumer trust and promote market competitiveness		E-commerce Law classifies platforms to accommodate various business models and considers KOLs and KOCs as sellers subject to similar responsibilities, necessitating platforms to monitor livestreams in real time and to remove or terminate sessions displaying violations

2.3.1. Content governance

SEA-6 countries have accelerated the shift towards mandatory platform accountability for online safety, particularly in content moderation and child protection. Digital platforms are recognised as key gateways for information access, prompting regulators to prioritise upstream controls. Rather than relying heavily on reactive enforcement, governments are embedding responsibility and accountability within platform design, governance processes, and operational safeguards.

Malaysia and Indonesia both adopted prevention-oriented approaches. Malaysia's Online Safety Act[75] introduces mandatory licensing for major social media and messaging platforms with at least 8 million users, requiring content moderation systems and age verification measures. Meanwhile, Indonesia's Government Regulation No. 17/2025 (*PP Tunas*)[76] mandates minimum age requirements and stronger child-protection obligations for electronic system providers. Both reflect a preventive strategy focused on reducing harms before it occurs.

Singapore's approach remains more targeted and outcomes-oriented. Under the Code of Practice for Online Safety,[77] designated App Distribution Services must implement age assurance and mitigate children's exposure to harmful content. By expanding regulatory scope to include App Distribution Services under the Broadcasting Act, Singapore broadened oversight while maintaining a calibrated, performance-based regulatory model.

On the other hand, Thailand prioritised rapid risk mitigation through 24-hour takedown obligations for social media service providers.[78] This reflects a regulatory preference for prompt responsiveness to harmful content.

2.3.2. Commerce, Transactions and Payment Security

Governments have enacted significant reforms addressing digital commerce, payment security, and online fraud. These measures reflect a shift from reactive consumer protection towards proactive, ecosystem-wide accountability. Financial institutions, telecommunications operators, and digital platforms, are increasingly positioned as gatekeepers responsible for fraud prevention, identity verification, and transactional integrity.

Singapore's Protection from Scams Act[79] exemplifies an early-intervention model. The Act authorises law enforcement to issue Restriction Orders to banks, temporarily suspending banking and credit services of individuals identified as potential scam victims. This preventive intervention addresses a persistent enforcement challenge: victims continue transferring funds despite warnings.

Thailand adopted a shared-liability framework that redistributes responsibility for technology-enabled fraud.[80] digital platforms, telecommunications operators, and banks are required to establish fraud detection systems and may be liable for compensation where negligence leads to harm. Complementing this, a Notification by the Electronic Transactions Committee[81] designated platforms to perform identity verification of business users before allowing them to operate.

Vietnam has also prioritised traceability and local accountability. Its E-commerce Law[82] requires sellers to use national electronic identification (VNeID) and obliges foreign platforms to establish a local presence, thereby reinforcing local laws and enforcement mechanisms.

In contrast, the Philippines has pursued a mixed regulatory strategy. The Internet Transactions Act[83] governs both business-to-business (B2B) and business-to-consumer (B2C) transactions, while the E-Commerce Philippine Trustmark,[84] initially voluntary but now mandatory, seeks to enhance consumer trust through certification.

Similarly, Indonesia has proposed revision to its Consumer Protection Law[85] to enhance regulatory safeguards for digital commerce. The ongoing review of the proposals necessitates further clarification regarding the scope and enforcement implications for digital platforms.

2.3.3. Competition, Taxation and Labour Governance

Platform governance in 2025 expanded beyond mere transaction integrity to encompass digital taxation, competition policy, and labour protections. These measures introduce mandatory social protections for gig and platform workers, selective competition tools targeting platform conduct, and tax withholding mechanisms. They reflect an effort to address market fairness, revenue capture, and social protection within platform-mediated economies.

Digital taxation represents the most prominent area of convergence. Indonesia's PMK 37/2025[86] designates digital marketplace platforms as withholding agents, requiring them to collect 0.5% of gross turnover from domestic sellers. Similarly, the Philippines expanded a 12% value-added tax[87] to digital services, thereby extending its fiscal reach to cross-border digital commerce. Vietnam amended its Corporate Income Tax Law,[88] to extend permanent establishment rules to platform-based activities and introduced platform-mediated tax withholding requirements effective from 2026.[89] Collectively, these measures leverage platform payment systems to improve tax compliance and auditability among fragmented digital sellers.

Competition regulation, however, remains comparatively nascent. Thailand's Trade Competition Commission has developed draft guidelines to address anti-competitive behaviour in multi-sided digital platforms,[90] signalling growing awareness of platform market power, although enforcement is in its infancy. Singapore has taken a softer approach by updating Technical Reference 76 (TR 76),[91] which provides voluntary guidance on consumer trust, fair dealing, and marketplace integrity. Developed through a multi-stakeholder process led by Enterprise Singapore, TR 76 reflects an industry-led standard-setting approach rather than prescriptive competition regulation.

In parallel, labour protections have seen more decisive progress. Malaysia's Gig Workers Bill,[92] pending implementation, recognises gig workers as a distinct category entitled to statutory safeguards. including contractual transparency and protection against unjust termination. Singapore's Platform Workers Act,[93] now in effect, formally incorporates platform workers into the social protection system through mandatory contributions and work injury coverage. Taken together, these developments indicate that while fiscal and labour measures are advancing concretely, competition policy remains the least developed aspect of platform regulation across the SEA-6.

In 2025, AI governance, cybersecurity, and platform regulation surfaced as common policy priorities; however, the sequencing and intensity of regulatory actions differed markedly. Some governments advanced comprehensive statutory frameworks with enforceable obligations, whereas others continued to rely on voluntary guidance or hybrid models. This divergence indicates that convergence in policy themes does not necessarily translate into uniform regulatory outcomes, especially when countries are at varying stages of institutional capacity and legal development. Consequently, asymmetries in compliance expectations and supervisory readiness may continue to exist throughout the region.

3. Evolution of Tech Governance across SEA-6 in 2025

- **Digital sovereignty has become operational.** Across the SEA-6, sovereignty is increasingly expressed through infrastructure control, data governance, fiscal tools, and regulatory perimeter enforcement, reflecting efforts to manage geopolitical risk while preserving economic openness.

- **Institutional architectures are being redesigned for complexity.** Governments are establishing specialised AI and data agencies, expanding coordination mechanisms, and restructuring ministries to better manage cross-cutting digital risks and technologies.

- **Sovereignty models differ by national context.** Vietnam and Thailand prioritise infrastructure and data control; Indonesia advances economic and payment-system sovereignty; Malaysia and the Philippines consolidate jurisdiction through licensing and local compliance requirements; while Singapore focuses on regulatory assurance and supervisory oversight.

- **Regional coordination is advancing through interoperability rather than harmonisation.** Initiatives such as DEFA, ASEAN AI SAFE, UBIN, and cross-border payment systems prioritise system compatibility and cooperation while respecting domestic regulatory diversity.

- **Implementation capacity will determine impact.** Many 2025 milestones remain in framework or declaration stages. The durability of regional integration and sovereignty strategies will depend on ratification, legal alignment, and operational follow-through in 2026 and beyond.

3.1. Models of Digital Sovereignty

Digital sovereignty has become a central governance theme across SEA-6 in 2025, shaped by intensifying geopolitical and geoeconomic competition. Trade tensions between the United States and China have evolved into broader contests over "technology sovereignty", particularly in AI, semiconductors, and critical minerals. Both powers are now using export controls, supply chain restrictions, and infrastructure partnerships as strategic instruments.

For Southeast Asia, this environment poses a notable challenge. Overreliance on any single external power carries economic and security risks. Yet full technological self-sufficiency is economically impractical for most countries in the region. At the same time, regional developments, including the completion of the ASEAN Digital Masterplan (ADM 2025)[94] and the substantial conclusion of negotiations for the Digital Economy Framework Agreement (DEFA),[95] have provided coordination platforms which member states can pursue digital sovereignty strategies within a regional integration framework.

In response to these pressures, SEA-6 countries accelerated their digital sovereignty strategies with concrete progress in 2025. These developments can be summarised into three interrelated dimensions: infrastructure control, data governance, economic policy, and operational oversight.

3.1.1. Infrastructure Sovereignty

Digital infrastructure, which includes cloud services, data centres, and connectivity networks, is increasingly treated as an essential national backbone infrastructure requiring domestic oversight or strategic control. Thailand expanded its designated Critical Information Infrastructure (CII) organisations under the Cybersecurity Act B.E. 2562 (2019),[96] explicitly recognising cloud providers and data centres as the nation's "essential digital backbone." These services are subject to enhanced regulatory supervision and security obligations, reflecting a state-centric approach to infrastructure sovereignty.

The Philippines has adopted a different approach that combines openness to attract long-term investment with jurisdictional control. The *Konektadong Pinoy Act*[97] establishes an "open-access" framework for data transmission infrastructure to promote equitable competition and effective spectrum utilisation. The Investors' Lease Act[98] allows foreign entities to obtain long-term land leases, aiming to attract large-scale ICT investments while preserving domestic legal jurisdiction.

These approaches illustrate varying strategies of sovereignty: Thailand emphasises regulatory oversight of essential existing infrastructure, whereas the Philippines balances infrastructure openness with mechanisms to retain legal and policy authority.

3.1.2. Data Sovereignty

Data governance has become a core pillar of digital sovereignty, with governments strengthening localisation, classification, and regulatory oversight mechanisms for foreign platform operations. Vietnam established one of the region's most comprehensive data sovereignty frameworks. The creation of a National Data Centre[99] centralises storage, analysis, and coordination of government data under unified management. Decision No. 20/2025/QĐ-TTg[100] introduces classifications of "critical data" and "core data", subjecting them to heightened protection regimes, thereby preventing risks of exploitation and attacks on national data. Additionally, the Law on E-Commerce[101] requires foreign platform operators to set up legal entities in Vietnam, facilitating direct regulatory oversight within the country.

Malaysia has taken a licensing and compliance-based approach. Through deeming provisions, overseas-based platforms are governed under Malaysian law, ensuring better compliance with national regulations. A National Cloud Computing Policy, delineating clear data sovereignty and residency principles for designated data categories. This policy requires technological safeguards, such as encryption and access controls, for data stored outside national borders.

These frameworks demonstrate a shared understanding that data is a strategic national asset. Sovereignty in this domain increasingly involves not only localisation requirements, but enforceable regulatory visibility and compliance mechanisms.

3.1.3. Economic, Financial, and Operational Sovereignty

The remaining two SEA-6 countries, Indonesia and Singapore, pursue distinct approaches to digital sovereignty, beyond infrastructure and data localisation.

Indonesia emphasises economic and financial sovereignty. Through Project Garuda, the country is developing a digital rupiah central bank digital currency (CBDC) to reduce reliance on external payment rails dominated by international card networks and foreign payment platforms. Simultaneously, Indonesia expanded its cross-border QRIS payment system to nine countries, demonstrating that sovereignty can also be pursued through regional network integration rather than purely national systems. New Value-added Tax (VAT) collection mechanisms on cross-border digital transactions further enable Indonesia to assert fiscal authority over foreign platforms serving domestic users.

Singapore pursues what might be described as "sovereignty-by-assurance," Rather than relying solely on infrastructure ownership or data localisation, Singapore emphasises measurable resilience, auditability and regulatory perimeter control. Upstream governance obligations are placed on gatekeepers such as app distribution services, while downstream real-time operational controls such as scam intervention mechanisms, strengthen systemic integrity. Regulatory hardening is evident in requirements that digital token services serving overseas clients must "license or cease" operations. This illustrates Singapore's strategy of ensuring that systemically significant digital services remain within Singapore's regulatory perimeter, regardless of where they are technically operated.

Across the SEA-6, digital sovereignty is not expressed through a single model. Instead, it manifests through different combinations of infrastructure oversight, data governance, economic control, and operational enforcement. Although the underlying motivation centers around resilience and strategic autonomy, implementation reflects national capacity, economic structure, and geopolitical positioning.

3.2. Structural Changes

In 2025, SEA-6 countries undertook significant structural adjustment to their digital governance architectures. These reforms build on trends emerging in 2024 and reflect the increasing complexity of AI development, cybersecurity risks, and frontier technologies. Governments are responding by establishing specialised agencies, strengthening coordination mechanisms, and in some cases, fundamentally restructuring existing institutions.

Broadly, two governance trajectories are visible. Some countries are consolidating and streamlining institutional architectures to improve efficiency and coherence. Others are expanding their governance architecture through specialised entities and inter-agency coordination bodies.

3.2.1. Establishment of Specialised Agencies

Most countries have set up dedicated entities to operationalise AI strategies, strengthen research capacity, and institutionalise digital governance. For instance, Indonesia established a Directorate of AI and New Technology Ecosystem[102] within the Ministry of Communication and Digital Affairs to oversee AI adoption. A separate Directorate General for Government Digital Technology[103] was also created to standardise digital services and strengthen security oversight.

Malaysia enhanced its applied research capacity through the establishment of the Quantum Intelligence Centre[104] and announced plans for an AI Trust Institute[105] to strengthen governance and assurance mechanisms for AI deployment. Vietnam reinforced its data-centric governance model by establishing two major data infrastructure hubs: the National Data Centre,[106] under the Ministry of Public Security to synchronise state data, and the National Science and Technology Data Centre,[107] under the Ministry of Science and Technology to support research and innovation. These institutions underscore Vietnam's focus on data infrastructure as the foundation of digital governance.

Thailand partnered with UNESCO to create the AI Governance Practice Centre,[108] positioning the country as a regional training and capacity-building hub. Meanwhile, the Philippines relocated the Education Centre for AI Research (E-CAIR)[109] from the Department of Trade and Industry to the Department of Education, signalling deeper integration of AI research within the education system.

Together, these developments reflect a shift from policy articulation toward institutionalisation of digital governance functions.

3.2.2. Adopting Coordination Mechanisms

The proliferation of task forces and inter-agency committees underscores persistent coordination challenges across multiple ministries and agencies. At the same time, it reflects governments' efforts to ensure policy coherence and stakeholder engagement.

Indonesia stands out as a notable example. The government has formed a 443-member National AI

Roadmap Taskforce[110] to draft national AI policy with broad stakeholder participation. It also created a National Taskforce for Digital and AI Talent Development,[111] and a Committee for the Acceleration of Government Digital Transformation[112] under Presidential Regulation.

Similarly, Malaysia formed the MyMahir National AI Council[113] to coordinate talent development and announce both an Online Safety Committee[114] and a Gig Workers Consultative Council.[115] Thailand established a National AI Committee[116] addressing sectoral priorities, and a National Committee on the Prevention and Suppression of Technology Crime,[117] coordinating 15 agencies.

Vietnam created of a Central Steering Committee[118] on science and technology under the Politburo and a National Steering Committee on Data,[119] functioning as a coordinating body across various sectors. In contrast, Singapore adopted a more targeted approach, establishing a dedicated Online Safety Commission[120] focused on victim redress and platforms accountability.

3.2.3. Fundamental Restructuring

Some countries pursued deeper structural consolidation. Vietnam performed a significant administrative restructuring,[121] reducing the number of ministries, merging provinces, and eliminating the district governance level. This restructure represents a systematic effort to streamline operations and enhance efficiency. The Philippines reorganised the National Economic Development Authority (NEDA) into the Department of Economy, Planning, and Development (DEPDev).[122] This reorganisation transformed the Department into a fully-fledged executive department, strengthening its institutional authority.

Malaysia adopted a distributed model, requiring every ministry to establish Digital Transformation Units,[123] embedding digital responsibility across government rather than centralising it. Singapore integrated consumer protection functions into the Competition and Consumer Commission of Singapore (CCCS).[124] This integration aims to consolidate consumer protection, legal metrology, and competition oversight under a single agency to improve operational synergy.

3.2.4. Regulatory Experimentation and Sandbox

Alongside institution expansion and restructuring, 2025 witnessed continued use of regulatory sandboxes for adaptive governance across the SEA-6. Vietnam formalised sandbox mechanisms within its AI Law and Digital Transformation Law, enabling controlled experimentation in domains including fintech, open API data sharing, and low-earth-orbit telecommunications services. Singapore refined its “innovation with guardrails” model by linking sandbox participation with structured testing protocols and assurance requirements specifically in the areas of health technology, AI-enabled medical devices, and cybersecurity. In contrast, Indonesia has progressed with targeted pilots, such as the digital rupiah sandbox.

These developments indicate a transition to adaptive supervisory tools that manage technological uncertainty while shaping market evolution. Nonetheless, differences in sandbox scope, evaluation criteria, and cross-border recognition may introduce interoperability challenges as these mechanisms become embedded within formal governance systems.

3.3. Regional Coordination

In accordance with the national policy developments outlined above, SEA-6 countries intensified regional coordination efforts in 2025, with increasing emphasis on interoperability mechanisms. Regional collaboration is progressing in three main areas: digital economy integration through the ASEAN Digital Economy Framework Agreement (DEFA), AI safety coordination through network-based mechanisms, and cybersecurity cooperation under the Hanoi Convention.

This evolving model reflects ASEAN's dual reality: member states pursue differentiated domestic policies in areas such as AI governance, platform regulation and cybersecurity, yet recognise the need for interoperable systems across borders. While 2025 marked important milestones, most initiatives are still in the framework or declaration stages. Their operational effectiveness will depend on implementation progress in 2026 and subsequent years.

3.3.1. ASEAN DEFA and Digital Economy Coordination

The ASEAN DEFA[125] represents a landmark initiative to establish comprehensive regional digital economy governance. DEFA reached substantial conclusion in October 2025[126] after fourteen rounds of negotiations at the 26th ASEAN Economic Community Council in Kuala Lumpur. It is set to be signed and implemented in 2026 under the Philippine ASEAN Chairmanship.

The agreement comprises nine core pillars covering digital trade facilitation, cross-border data flows, cybersecurity, digital payments, and emerging technologies. Its overarching objective is to foster a more integrated digital economy within ASEAN by facilitating the interoperability across data systems, payments infrastructures, cybersecurity frameworks, paperless trade mechanisms, and digital identity models. DEFA is projected to support ASEAN's digital economy growth from USD 1 trillion to USD 2 trillion by 2030.[127]

Political commitment has been evident. Malaysia prioritised DEFA's substantive conclusion as its flagship economic deliverable during its 2025 ASEAN Chairmanship.[128] The Philippines has designated DEFA signing as a priority deliverable for its 2026 ASEAN Chairmanship.[129] Member states have begun aligning domestic legislation in anticipation of implementation. For instance, Indonesia announced plans to revise its Consumer Protection Law to better address digital economy challenges.

Operational interoperability is also advancing. Indonesia expanded its QRIS cross-border payment system to nine Asian countries,[130] facilitating low-cost, real-time retail payments. This demonstrates how regional integration can proceed through functional payment connectivity even before full DEFA implementation.

Another initiative aligns with DEFA's is the Unique Business Identification Numbers (UBIN).[131] It seeks to tackle ongoing challenges to cross-border trade by establishing a standardised business identification system. In 2025, UBIN entered the implementation phase with the formal adoption of an Implementation Roadmap[132] for a regionally comparable and recognised identifier. Upon full implementation, UBIN has the potential to unlock up to USD 2 trillion[133] in additional digital value by 2030. By facilitating business verification and trust, UBIN support digital trade integration and complement DEFA's broader objectives.

Despite these advances, translating DEFA's into practice will require sustained effort. Member states need to finalise detailed provisions and conduct legal harmonisation reviews and align domestic frameworks with regional commitments. Implementation capacity will ultimately determine DEFA's impact.

3.3.2. AI Governance and Safety Coordination

Regional AI coordination continues to operate through network-based, non-binding mechanisms. It reflects ASEAN's preference for flexibility and respect for national sovereignty, while seeking to reduce governance gaps through shared capacity-building, practical guidance, and peer learning.

A major significant development in 2025 was the formal adoption of the ASEAN AI Safety Network (ASEAN AI SAFE)[134] at the 47th ASEAN Summit in Kuala Lumpur. This voluntary mechanism serves as ASEAN's first dedicated platform for AI safety coordination. It focuses on capacity building, regulatory preparedness, and the exchange of best practices, while explicitly respecting national regulatory autonomy. The network adopts a multistakeholder model, that specifically includes governments, industry, academia, and civil society, academia, aiming to ensure diverse perspectives inform safety standards and governance practices.

Thailand establishment of the AI Governance Practice Centre[135] in partnership with UNESCO further support regional training and algorithmic accountability. The centre functions as a regional hub for capacity building allowing peer-learning among countries at different stages of AI development.

These initiatives illustrate that ASEAN's AI governance framework emphasises assurance, knowledge exchange, capability development, and collaborative practices. This approach accommodates the regulatory diversity, ranging from Vietnam's mandatory legislation to Singapore's voluntary frameworks, and hybrid models in other regions, while seeking to reduce safety gaps through shared learning.

3.3.3. International and Regional Cybersecurity Frameworks

Cybersecurity cooperation gained momentum at the global and regional l levels in 2025. At the international level, the opening of the United Nations Convention against Cybercrime,[136] known as the Hanoi Convention, represents a landmark achievement. The convention establishes a global framework for evidence-sharing and mutual legal assistance in combating transnational cybercrime and online child exploitation. It provides legal architecture for cross-border enforcement cooperation while affirming the importance of protecting fundamental rights.

At the regional level, cybersecurity features as one of DEFA's nine core pillars,[137] recognised as essential for building the trust required for cross-border digital trade and data flows. DEFA's cybersecurity provisions aim to create common baseline standards and coordination mechanisms that complement the enforcement cooperation architecture established by the Hanoi Convention.

However, both frameworks remain in early implementation stages. The Hanoi Convention is open for signature until the end of 2026 and requires ratification by 40 states to enter into force. DEFA, while substantially concluded, needs to undergo signing, domestic ratification, and phased implementation. The legal architecture is emerging, but operational cros-border enforcement effectiveness remains to be tested. It will depend on countries' capacity to ratify agreements, develop operational procedures, and allocate resources for coordinated enforcement activities.

3.3.4. Cross-Border Governance Initiatives

Beyond format intergovernmental agreements, cross-border governance is also advancing through hybrid and industry-driven initiatives aimed at addressing transnational challenges within the region. These initiatives indicate that regional coordination is increasingly multi-layered, combining formal agreements, network-based mechanisms, and sector-driven collaboration.

In 2025, the Global Anti-Scam Alliance (GASA), a non-profit organisation dedicated to safeguarding consumers against scams, established two new chapters in Southeast Asia: Indonesia[138] and the Philippines.[139] Both country chapters are led by prominent telecom providers. This industry-driven model combines central coordination with local operational leadership to address transnational online scams.

The Nexus Global Payments (NGP)[140] initiative represents a state-led approach. Founded on March 26, 2025, by the central banks and instant payment system operators of India, Malaysia, the Philippines, Singapore, and Thailand, NGP aims to enable cross-border public digital payment infrastructure. It reflects a pragmatic approach to interoperability grounded in financial connectivity.

4. Looking Ahead to 2026

2026 will test implementation capacity. Governments must translate digital frameworks into effective enforcement. Public institutions need stronger technical capacity; industry should prepare for closer oversight; research institutions and think tanks can support implementation through evidence generation, capacity-building, and multi-stakeholder dialogue.

Regulatory diversity will shape market conditions. Compliance obligations and enforcement approaches will continue to differ across SEA-6. Cross-border operators must strengthen regional compliance strategies, while domestic firms may benefit from targeted national support.

Regional coordination needs to move from commitment to delivery. DEFA and regional AI and cybersecurity initiatives are entering implementation phases. Policymakers must align domestic reforms with regional commitments, and industry should prepare for evolving interoperability standards.

SEA-6 governments are entering a decisive phase in their digital governance trajectory. The policy architecture developed in recent years across AI governance, cybersecurity, and digital platform governance is now moving into implementation and enforcement, and recognised as core pillars of economic growth, public trust, and national security.

The 2025 developments reveal three defining patterns:

- A shift from agenda-setting to operational implementation as laws and regulations move from passage to enforcement;
- Calibrated efforts to balance innovation and competitiveness with systemic risk management and public trust safeguards; and
- National differentiation within regional convergence, as countries pursue distinct regulatory pathways while strategically aligning governance frameworks to enable regional interoperability and cross-border cooperation.

As multiple initiatives enter critical implementation stages in 2026, the central challenge will be translating policy commitments into operational reality and enforceable systems.

4.1. What this means for Governments

The transition from framework development to functional enforcement creates substantial demands on institutional capacity. Effective implementation of binding platform regulation, AI governance, and cybersecurity frameworks will require technical expertise, particularly in areas such as AI risk assessments, cybersecurity resilience, and supervisory oversight. This necessitates sustained investment in the regulatory capacity. That includes not only skill development for government officials but also adequate resourcing and digital infrastructure to support monitoring and enforcement.

Moreover, the majority of binding regulations across the SEA-6 remain in the proposal or early enactment stages. Key operational details, such as enforcement procedures and supervisory protocols, are still being defined. With multiple frameworks scheduled to take effect in 2026, governments face a challenging timeframe to build the institutional capacity required for implementation.

In response, structural reorganisation trends observed since 2024 and continuing into 2025 signal deliberate efforts to prepare for this transition. Specialised agencies task forces have been established to manage emerging governance areas, and coordination mechanisms have been adopted to facilitate cross ministerial alignment and stakeholder engagement. Whether these coordination mechanisms, consolidation, distributed responsibility, or specialised entities prove most effective in managing complex digital governance challenges will become clear as implementation unfolds in 2026.

4.2. What this means for Industry

Platform operators, AI developers, and digital service providers operating across SEA-6 are likely to encounter increasing compliance complexity. Businesses must navigate diverse governance frameworks, including AI risk classifications and conformity requirements, platform obligations spanning content moderation to worker protections, and cybersecurity and data protection requirements that differ substantially in scope and enforcement. This regulatory diversity requires significant investment in regional compliance expertise, jurisdiction-specific legal counsel, and potentially differentiated product or operational strategies tailored to national requirements.

The compliance challenge is particularly challenging for cross-border operators. Licensing regimes, liability structures, worker classification models, and reporting obligations differ not only in substance but also in timelines and enforcement among jurisdictions. Without greater regulatory interoperability, compliance costs are likely to rise. Thus, it potentially affects smaller operators disproportionately since they lack the resources to maintain specialised regional compliance functions.

However, regulatory diversity also creates opportunities for proactive engagement. Investment in domestic infrastructure and innovation ecosystems open pathways for public-private partnership in areas such as training, research centres, and regulatory sandboxes. Coordination mechanisms that engage multiple stakeholders create opportunities for businesses to contribute to implementation guidelines and operational clarity. Regional coordination mechanisms, including DEFA's provisions on cross-border data flows and digital payments, offer pathways to mitigate fragmentation while preserving national regulatory sovereignty over substantive policy choices.

For domestic firms and SMEs, government investments in talent development and innovation infrastructure may reduce barriers to digital adoption. Curriculum integration, upskilling programmes, and research centres and subsidised experimentation environments can strengthen domestic innovation ecosystems and enable broader participation in evolving digital value chains.

4.3. What this means for Research Institutions/Think Tanks/ Associations

Research institutions, think tanks, and associations are positioned to play an important bridging role during this transition from policy design to implementation across diverse regulatory contexts. These organisations can convene multi-stakeholder dialogues during implementation phases, translate complex regulatory requirements into accessible guidance, and facilitate knowledge sharing between regulators and regulated entities. They can also generate evidence through research to inform iterative policy refinement such as assessing the effectiveness of institutional restructuring models or analysing regulatory impact on SMEs, larger firms, and consumers. Importantly, they are well placed to amplify under-represented voices, particularly SMEs and civil society organisations that may lack direct access to the policy processes.

4.4. Conclusion

2026 represents a pivotal year for the SEA-6 as the region moves from policy formulation toward effective implementation. The coming year will test how governments balance between innovation and risk management, all while safeguarding public trust.

Successful implementation will depend on strengthened technical expertise, institutional coordination and constructive engagement from industry. Regional mechanisms will play an important role in translating framework commitments into operational cooperation. How effectively these governance arrangements are operationalised in 2026 will shape the region's ability to adapt as emerging technologies continue to evolve rapidly.

5.
Country Overviews

Across the SEA-6, governments are moving beyond policy formulation toward institutionalised enforcement, infrastructure investment, and capacity-building, while balancing domestic sovereignty priorities with regional interoperability commitments that will shape the region's digital integration trajectory.

Indonesia: Transitioning from digital adoption to integrated digital state governance. Governance focus shifted toward institutionalising AI policy, strengthening digital government integration, and aligning financial, payment, and data frameworks, signalling a move toward a more coordinated, state-led digital transformation.

Malaysia: Consolidating digital trust through legislation, talent, and infrastructure. The country advanced implementation of its cybersecurity, online safety, and cloud governance frameworks, while anchoring long-term competitiveness through its AI nation strategy, talent pipeline reforms, and strengthened digital identity and data systems.

Philippines: Prioritising investment-led infrastructure and foundational digital reforms.
The nation focused on enabling ICT investment, accelerating e-government rollout, and strengthening institutional leadership, though overall progress remained gradual and uneven amid political and implementation constraints.

Singapore: Operationalising governance through enforceable assurance and system-level intervention.
Singapore moved decisively from frameworks to practice, embedding audit-ready standards, real-time scam prevention powers, and AI assurance mechanisms, reinforcing its model of sovereignty-by-assurance in a highly connected economy.

Thailand: Shifting toward risk-based enforcement and national digital security consolidation.
The country strengthened cybersecurity coordination, platform accountability, and AI risk governance, reflecting a transition from policy design to active enforcement aimed at restoring trust amid rising cyber threats.

Vietnam: Advancing the region's most comprehensive legal-institutional digital governance architecture.
Vietnam accelerated governance consolidation through new technology laws, national data infrastructure, regulatory sandboxes, and major institutional restructuring, signalling a state-driven approach to digital sovereignty and implementation.

5.1. Indonesia

By Hafiz Noer, Center for Digital Society, Indonesia. Irfan Dwi Putra, Center for digital Society, Indonesia

Indonesia enters a relatively robust and consolidated technology governance and policy landscape in 2025. The new administration perceived the 'digital' as a tool for enhancing public service delivery, accelerating economic growth, and achieving national priorities; hence, several rearrangements can be highlighted under two domains: tech governance and tech policy. One key tech policy trend is on artificial intelligence (AI). The government of Indonesia has moved forward to a clearer position following the non-legally binding document of ethical principles published in 2023. The Indonesian government is preparing two presidential regulations on National AI Roadmap and AI Ethics Guidelines to strengthen its adoption and development. In terms of tech governance, the government is transitioning the existing electronic government (e-government) framework into digital government that streamlined digital services both at the national and the regional-level institutions, building upon the earlier efforts to consolidate government applications.

In what follows, the next section provides a brief overview on Indonesia's 2025 technology development, incorporating key developments on both tech governance and tech policy trends, including a short analysis on ASEAN Digital Economy Framework Agreement (DEFA) on Indonesia's digital economy landscape.

5.1.1. Policy Priorities for Indonesia in 2025

5.1.1.1. Preparing AI-ready ecosystem and human capital

Indonesia released several regulations and draft policies on AI in 2025, targeting both the development of the AI ecosystem and the human capital that support it. The Taskforce coordinated by Komdigi produced two policy drafts: the National AI Roadmap and the Concept on AI Ethics Guidelines.[141] The National AI Roadmap outlines policy directions, strategies, and programmes for developing the national AI ecosystem, as well as the designation of priority sectors for AI use-case innovation aligned with national priorities such as food security, health, and the financial economy. Meanwhile, the Concept on AI Ethics Guidelines builds upon the existing Circular Letter on AI Ethics[142] by adding elements such as practical safeguards corresponding to each ethical principle, delineation of roles and responsibilities, AI risk classification (adopting the EU AI Act), and mechanisms for monitoring and evaluation. Both remain in draft form and are currently under submission to the Ministry of State Secretariat[143] for enactment as presidential regulations.

In relation to human capital development, the Ministry of Primary and Secondary Education issued Ministerial Regulation No. 13/2025,[144] integrating coding and AI into the primary and secondary education curriculum as elective subjects. Additionally, through Ministerial Regulation No. 12/2025,[145] the Ministry incorporated digital technology (including foundational concepts and AI ethics) into the content standards for primary and secondary education. These developments illustrate the efforts of the country in preparing young Indonesians to be ready for a digital driven economy.

5.1.1.2. Strengthening digital transformation through e-government and interoperability

Digital transformation in the public sector is increasingly reinforced through regulations on e-government and data interoperability. Through Presidential Regulation No. 83 of 2025,[146] the President established the Committee for the Acceleration of Government Digital Transformation, mandated to coordinate, synchronize, and provide recommendations for accelerating and aligning the integration of priority agendas in government digital service transformation. Strengthening efforts are also carried out on the technical front by Komdigi through Ministerial Regulation No. 6 of 2025,[147] which governs technical standards and procedures for the development of e-government applications, aiming to create a standardised, interoperable, and sustainable e-government application ecosystem for public service delivery.

Further reinforcement of digital transformation in the public sector is undertaken from a security perspective. The National Cyber and Crypto Agency (BSSN) issued the Roadmap for the Protection of Vital Information Infrastructure in the Government Administration Sector,[148] which sets forth policy directions, work plans, and achievement targets through 2029. In the context of data interoperability, the Ministry of Tourism and the Ministry of Creative Economy[150] issued regulations on integrated data governance applicable to their respective sectors, aligned with the principles of One Data Indonesia.

5.1.1.3. Complementary digital economy regulations

Several regulations were also issued in response to the rapid growth of the digital economy, particularly in its cross-border dimensions.

- Presidential Regulation No. 68 of 2025[151] establishes a mechanism for collecting value-added tax (VAT) on cross-border digital transactions. A state-owned enterprise subsidiary, Jalin Pembayaran Nusantara,[152] is designated as the implementing entity. In carrying out its mandate, Jalin Pembayaran Nusantara may appoint prospective foreign partners that meet the necessary requirements regarding adequate infrastructure capacity and supporting systems. Additional digital taxation regulations were issued by the Minister of Finance,[153] imposing VAT and income tax on crypto-asset trading transactions. These regulations intend to improve tax fairness and reinforce the compliance of digital business players, and subsequently boosting public revenue from the digital sector.

- In the payment system sector, Bank Indonesia, through Regulation No. 4 of 2025,[154] incorporated the digital rupiah into the national payment system governance framework. The digital rupiah, developed under Project Garuda,[155] is currently in the sandboxing phase.[156] As of August 2025, Bank Indonesia has also advanced the expansion of cross-border QRIS payment[157] systems to nine countries in Asia, supporting interoperability and facilitating cross-border payment efficiency.

- In the financial technology sector, the Financial Services Authority (OJK) issued Regulation No. 16 of 2025,[158] stipulating fit-and-proper assessments for digital-financial-asset providers prior to commencing business activities. OJK also issued Circular Letter No. 16/SEOJK.07/2025,[159] regulating the implementation of anti-money laundering, counter-terrorism financing, and counter-proliferation financing programs for digital-asset traders, to ensure that the digital asset trading ecosystem is not misused for criminal activities.

5.1.2. Evolution of Tech Governance in Indonesia in 2025

5.1.2.1. Establishing working groups on AI ecosystem development

The government of Indonesia strengthens its stance towards AI. Following the Circular Letter on AI Ethics in 2023, the government reinforced the need to have robust AI policy response through the formation of National AI Roadmap Taskforce which consists of 443 members[160] from the government, academia, industry, civil society organisations, and the media; coordinated by the Ministry of Communication and Digital Affairs (Komdigi). In August 2025, the Taskforce released the National AI Roadmap White Paper and Concept on AI Ethics Guidelines. Further, the Coordinating Ministry of Human Development and Cultural Affairs (Kemenko PMK) established the National Taskforce for Digital and AI Talent Development.[161] This Taskforce bears several responsibilities, including streamlining digital and AI literacy initiatives across ministries under the coordination of Kemenko PMK.

5.1.2.2. Transitioning e-government into digital government framework

In terms of public service delivery, the Ministry of State Apparatus Utilisation and Bureaucratic Reform (PAN-RB) will transform the existing electronic-based government system (*Sistem Pemerintahan Berbasis Elektronik* or SPBE) to "Digital Government" (*Pemerintah Digital*).[162] The year 2025 marks a transition from the SPBE framework, which primarily focused on consolidating diverse government digital applications and integrating digital infrastructure across national and local governments, to a broader Digital Government approach that emphasises integration citizen-centric, integrated digital services. Digital Government will act as both an information portal and service centre for citizens.

To actualise Digital Government, the initiative will be anchored under a new presidential regulation that consolidates and replaces several existing SPBE-related regulations—such the regulation on SPBE architecture—into a single Digital Government regulation. Several changes that will be covered within the new regulation include alignment between digital-based services with national development goals, optimisation of human resources, collaboration between government and non-government actors, institutional reconstruction and coordination mechanisms, consolidated planning and budgeting, and outcome-based evaluation to evaluate Digital Government practices.

5.1.2.3. Institutional reforms of ministries in response to digital transformation

Several ministries under the new administration have reorganised their internal management to respond to digital technologies. This includes the internal restructuring of Komdigi with the new formation of Directorate of AI and New Technology Ecosystem.[163] The new Directorate is set to address the adoption and development of AI, preparing regulations on advanced technology, and designing digital innovation ecosystems. Komdigi has also formed a new Directorate General for Government Digital Technology.[164] One of its functions is to develop policy and strategic planning for the development, utilisation, supervision, and monitoring of digital government technology and security standards.

Other ministries have responded to digital transformation similar to Komdigi. For example, PAN-RB initiates the Deputy for Government Digital Transformation[165] that is responsible for consolidating digital services among government ministries and offices to be integrated and interoperable. The Coordinating Ministry for Economic Affairs formed the Deputy for Coordination of Commerce and Digital Economy.[166] This restructuring shifts the digital portfolio, which was previously under the Deputy for Coordination of Digital Economy, Employment, and Micro, Small, and Medium Enterprises (MSMEs), into its own dedicated deputy. The institutional reform reflects the Indonesian government's recognition that digital strategy is not a sectoral agenda, but rather a cross-cutting governance planning. By repositioning digital portfolios into dedicated government units, the government signals for strengthening digital governance and reducing silos.

5.1.3. Regional Cooperation

Indonesia has been engaged in the ASEAN Digital Economy Framework Agreement (DEFA) negotiation since its first launch in 2023. As of October 2025, DEFA has reached its substantive conclusion,[167] with finalisation targeted for 2026 under the Philippine ASEAN Chairmanship. Although the draft agreement has not yet been published, several implications for Indonesia's technology policy direction can be identified through the negotiated pillars.[168]

- Under the Digital Trade pillar, Indonesia has enacted several consumer protection regulations in the financial sector[169] and is currently revising the Consumer Protection Law[170] to incorporate digital trade dynamics. Tax regulation on cross-border digital transactions[171] also issued in 2025.
- Under the Cross-border E-Commerce pillar, the 2024 amendment to the Electronic Information and Transactions Law (EIT Law)[172] introduced provisions on international electronic contracts, establishing applicable law standards for cross-border transactions.
- Under the Payments and E-Invoicing pillar, the expansion of QRIS across ASEAN countries[173] and the development of the digital rupiah[174] demonstrate Indonesia's efforts to strengthen interoperability in payment systems.
- Under the Digital ID and Authentication pillar, relevant provisions are included in the 2024 amendment to the EIT Law[175] concerning electronic certification, including digital identity and mutual recognition arrangements.
- Under the Cross-border Data Flows and Data Protection pillar, Indonesia has enacted the Personal Data Protection Law (2022)[176] and is currently preparing its implementing regulations.
- Under the Online Safety and Cybersecurity pillar, regulatory provisions are accommodated in the 2024 amendment to the EIT Law and Government Regulation No. 17 of 2025 (PP Tunas)[177] on child protection in the digital environment, alongside additional regulations issued by the National Cyber and Crypto Agency (BSSN).[178]
- Under the Competition Policy pillar, although Indonesia's competition regime continues to rely on Law No. 5 of 1999, revisions are planned to incorporate digital business practices.[179]
- Under the Cooperation on Emerging Technologies pillar, Indonesia is intensively developing regulations on the national AI ecosystem under Komdigi.
- Under the Talent Mobility and Cooperation pillar, digital skills development is being advanced throught curriculum integragion[180] and digital and AI literacy initiatives.[181]

These policies collectively reflect Indonesia's efforts to align with DEFA and contribute to ASEAN's digital economy. Nevertheless, Indonesia must continue addressing gaps in several pillars, particularly personal data protection—which requires more detailed regulation—and the completion of AI-related regulations.

5.1.4. Moving Forward

The year 2025 reflects Indonesia's efforts to advance the maturity of its digital ecosystem, both within the public sector and the broader digital economy. In 2026, the transition from e-government to a digital government framework is expected to reshape the landscape of public-sector digital transformation, enabling public services that are more streamlined, user-oriented, and collaborative between government and non-government actors. On the other hand, the planned enactment of presidential regulations on the AI Roadmap and AI Ethics Guidelines in 2026 will also clarify policy directions for AI adoption and development in Indonesia, including the delineation of actors responsible for each policy and program.

Although governance reform on digital technology policy sets the tone for a more consolidated strategy, coordination and policy alignment across institutions both at the national and the local level remains crucial. The division of responsibilities among ministries has to be agreed upon to mitigate the risk of policy disintegration and low enforcement.

The final agreement of the DEFA negotiations next year will likewise have significant implications for Indonesia's existing technology policies. Although Indonesia has issued numerous regulations aligned with DEFA's pillars, acceleration and adjustment of ongoing initiatives will be required to ensure coherence with the agreement, particularly in areas concerning consumer protection and competition in digital trade, as well as the development of digital talent.

5.2. Malaysia

By Farlina Said, Institute of Strategic and International Studies, Malaysia.

Malaysia's 13th Malaysia Plan [182] (MP) was announced mid-year 2025, setting Malaysia's national development compass from 2026 to 2030 on transitions towards digitalisation and advanced technologies. This indicates anchoring growth of the economy on technology, be it economic complexity value chain or cultivating an inclusive society and a strong social system amidst digital transitions. The 13th MP holds specific goals for the digital economy such as increasing the digital economy's contribution to GDP to 30% by 2030 where it was 23.5% in 2023. [183] It also builds on the 12th Malaysia Plan [184] formed in the years pandemic recovery, specifically through completed policies that acknowledges Malaysia's ageing society, such as the National Ageing Blueprint 2025-2045,[185] and writing technical and vocational education and training programmes to be in line with high growth high value industries such as AI while enhancing public services with the GovTech ecosystem.

The 13th Malaysia Plan also touts the goal of building Malaysia as an AI nation which the document articulates as building an inclusive and sustainable AI nation, developing Malaysia as a regional hub for digital technology production and raising capacity for 'Made in Malaysia' products. Realising such goals would mean Malaysia has to address data infrastructure, build a talent pipeline relevant for the future and provide support to scale up local digital services and manufacturing players. For the latter, it was reported that investments have been channelled to local start-ups, where until 30 June 2025, the Ministry of Science, Technology and Innovation's Cradle Fund had supported 329 companies[186] under the 12th MP where 118 were in advanced intelligence and data analytics and 12 companies are in sustainable and clean energy.

The Ministry of Finance's domestic investment drive, GEAR-uP[187] have also mobilised approximately USD 4 billion (RM 16 billion)[188] by the third quarter of 2025 into sectors such as semiconductor and energy transition. Among the investments are on AI-based optical inspection for semiconductors, integrated circuit (IC) semiconductor design and digital platforms. Further efforts for data infrastructure and talent pipeline will be explored below. Essentially, the 13th MP aimed to raise Malaysia' competitiveness in developing economic landscapes while raising the well-being and livelihoods of Malaysians. The Plan arrived in the midst of mid-term reviews of digital economy policies such as the Digital Economy Blueprint and the Malaysia Fourth Industrial Revolution Roadmap, which warranted streamlining exercises for current policies.

5.2.1. Policy Priorities for Malaysia in 2025

5.2.1.1. Centralising cybersecurity leadership

Malaysia passed hefty laws in 2024, which were the Cybersecurity Act and the Online Safety Act while amending the Communications and Multimedia Act and the Personal Data Protection Act. Further guidelines and executive orders for the Cybersecurity Act were issued in 2025 such as the NACSA Chief Executive Directive No 6[189] on the extension of grace period to obtain a cybersecurity service provider license, NACSA Chief Executive Directive No 7[190] on the development of a code of practice by national critical information infrastructure leads, NACSA Chief Executive Directive No 8[191] on cybersecurity related audits for national critical information infrastructure entities and NACSA Chief Executive Directive No 9[192] on the development of data and information migration for post-quantum cryptography by national critical information infrastructure entities.

Currently awaiting further updates is the Cyber Crime Act, which is delayed for improvements to Section 116D on empowering police officers to seize bank accounts, inclusive of mule accounts. A Cyber Crime Plan of Action is also being developed by the Ministry of Home Affairs to address cyber dependent crime. While laws in 2024 see phases of implementation, Malaysia passed the Gig Workers Bill, announced an incoming AI regulation and a National Identity Security Act in the making. Furthermore, policies such as the National Cyber Security Strategy 2025-2030 have been completed while a Digital Trust and Data Security Strategy is in the works. Malaysia has also introduced the Education Development Plan 2026-2030, which charts Malaysia's education modules for the digital era and the National Cloud Computing Policy for commitments to the safe deployment and adoption of cloud. The following marks three major developments in tech policy for Malaysia.

5.2.1.2. Strengthening digital trust in the platform economy

The Gig Workers Bill[193] was passed in Dewan Rakyat in August 2025 and the Dewan Negara in September 2025. The Bill has been in development since 2021[194] where the Employment Act 1955 was amended to clearly define employers and employees to take into account gig workers. Malaysia's legislation environment has gaps for the protection of workers, especially in the p-hailing sector, which the Gig Workers Act is expected to address. The Act states the rights of a gig worker which includes responsibilities to respond for dispute resolutions, the right to enter into any agreement with parties other than the contracting entity and that there could be no termination without just cause

or excuse. Furthermore, platform-based workers have the right for transparency and human review for automated monitoring and decision-making systems through electronic means. A tripartite Gig Workers Consultative Council[195] is also established to monitor developments such as wages, minimum standards and appropriate working hours.

5.2.1.3. Institutionalising AI governance

The National AI Action Plan 2026 to 2030[196] is slotted for completion by end 2025. As reported in parliament, it focuses on (i) building global talents (ii) acceptance of AI across strategic sectors (iii) to strengthen the data and data processing infrastructure (iv) ensure responsible management of AI and (v) attracting investment and financing. The first stop of the action plan is to create more AI jobs, thus the Plan is expected to create 300,000 to 500,000 jobs, raising productivity of the public sector by 30% and placing Malaysia in top 10 of global rankings for AI ecosystem. Realising jobs are partnerships with KESUMA and TalentCorp who will build AI sectoral clusters in transportation, health, agriculture, entrepreneurship and public sector adaptation. Clarity on responsible AI which protects innovation is also expected on the AI Action Plan. While an AI regulation[197] is being discussed in an inter-agency task force, an AI Trust Institute[198] would also be established to strengthen governance capabilities in this space.

Additionally, the National Cloud Computing Policy[199] was developed to encapsulate the significance of cloud computing and ideate possibilities for Malaysia's adoption of cloud. The Cloud Computing Policy also outlines regulatory frameworks and data sovereignty principles which includes data sovereignty, data residency for specific categories, technological safeguards for non-resident data and classification as well as recommended security measures. A consumer protection process is also encouraged in the adoption of cloud, especially for consumers to be aware of trustworthiness of Could Service Providers (CSPs) while CSPs should practice transparency and offer compensation and remedies for incidents.

5.2.1.4. Building an AI-ready talent

Among Malaysia's greatest challenges to realise the AI nation is talent development and a number of programmes have rolled out through the years to reskill, upskill or enhance digital literacy. Among these are the eUsahawan and Global Online Workforce (GIOW), a digital literacy and upskilling programme for rural areas, and Rakyat Digital, a platform that offers introduction sessions on AI, generative AI, Cybersafe, Blockchain and Cloud. In 2025, the Ministry of Education unveiled the Education Development Plan 2026 to 2030[200] which aims to ensure that schools are equipped with high-speed internet, students achieve high digital competency scores (at least at the level of intermediate and above) and that all Ministry of Education institutions have the Lestari icon which would mark commitment for sustainable development goals awareness programmes. Malaysia's school curriculum would also be revised to meet the digital future with the School Curriculum 2027[201] placing digital literacy as a core component of the syllabus where digital aptitude is one of seven core competencies to be mastered by students. Being digitally literate means, they are able to manage information and data, solve problems through a computational mindset and write ethical digital content. The digital literacy will be captured in a class titled Technology and Digital, which will be taught for students in standard three of primary schools all the way to high school. Classes include learning about AI, data analysis and computer science. A specific 'learn with AI and learn about AI' classes are also tested in a phased approach which began with 27 pioneer schools in 2025. The programme is expected to expand to 260 schools in 2026 and should reach all 10,245 schools by 2030.

5.2.2. Evolution of Tech Governance in Malaysia in 2025

5.2.2.1. Strengthening platform accountability and online safety

Malaysia's 2025 also featured digital incidents which prompted response. Rising cases of bullying and fatalities[202] in the ages of 6 to 16 were reportedly linked to social media use and strengthened the call for responsible digital platforms. As child users emerge as specifically vulnerable in digital spaces, Malaysia passed an anti-bullying legislation[203] and is exploring a social media ban for people under 16[204] while strengthening governance tools such as the Online Safety Act late 2024. The Online Safety Act awaits enforcement details as guidelines[205] are finalised, though the Deeming Provision was invoked on December 15, 2025, for enforcement on January 1, 2025. The Deeming Provision[206] is a legal clause bringing major overseas-based online platforms under Malaysia's jurisdiction. Effectiveness of the Online Safety Act would be dependent on compliance, especially as all internet messaging and social media service providers with eight million or more users would be automatically granted an application service provider license by January 1, 2025. An Online Safety Committee[207] would be formed to advise and make recommendations, as per section 10 of the act.

5.2.2.2. Advancing cybersecurity and frontier technology governance

Concerns over threats posed by quantum computers have instigated policies for post-quantum cryptography such a national post-quantum cryptography readiness roadmap[208] and established the Malaysian Cryptology Technology and Management Centre.[209] Approaches to address risks are led by the National Cyber Security Agency and spearheaded by existing efforts from Cybersecurity Malaysia[210] and universities such as University Putra Malaysia. Malaysia's interest for quantum computing is also associated with the technology's convergence in AI for quantum intelligence. To explore this further, Malaysia's R&D centre under the Ministry of Science, Technology and Innovation, MIMOS, have launched a Quantum Intelligence Centre[211] for applied quantum R&D.

5.2.2.3. Consolidating digital state infrastructure and data governance reform

Meanwhile, closing the digital gap is a great concern in Malaysia, whether this may be to monitor digitalisation efforts across states from Kedah to Sabah or to conduct digital skills classes that ensures no one gets left behind in the process of digital transformation. Sectors such as agriculture receive support from MDEC's Digital AgTech initiative,[212] which in 2025 also featured AI to be implemented in aquaculture and livestock sub-sectors for Sabah. Meanwhile, the Ministry of Human Resources conducts training programmes for Persons with Disabilities, which also held training in graphic design and digital printing, among other programmes. As of October 2025, the Ministry's efforts have trained 785 trainers[213] in the community. TalentCorp and MyDigital also launched a MyMahir National AI Council[214] in May to coordinate AI talent development across sectors.

At the same time, Malaysia's tech governance trends continue the process for e-government transformation and adoption, data safety as well as talent development. On government transformation,

each ministry is required to establish a Digital Transformation Unit[215] who could oversee the establishment of the MyGov Malaysia portal or MyDigital ID adoption. This is an extension to ongoing digitalisation processes such as system migrations or the development of a single digital portal for internal or external use. The Malaysian government regularly reports the efficacy of digital adoption, where in Sabah, the Sabah Economy, Development and Investment Agency shortened the collection and analysis of data for programmes[216] such as the Population Income Initiative Programme and Elimination of Hardcore Poverty from 10 weeks to 1 week while the Ministry of Transport's Maritime Single Window reduced ship clearance[217] from 36 hours to 45 minutes. The advantage of increasing digitisation is the ease of developing a database which can be used for data analytics which could improve government delivery of services. Already in 2024, was the launch of the Central Database Hub (PADU) and the passing of the Data Sharing Act. This was preceded by the introduction of the MyDigital ID, which aims to provide an identity verification system across government services. Introduced in 2023, the adoption of MyDigital ID have been voluntary thus far, but from 2026, the ID is required to access government services while prepaid SIM registrations must embed MyDigital ID in processes. The identity verification system will be the cornerstone of the government's GovTech[218] ambitions thus would require greater data protection for the population.

It is perhaps for these ends that idea of a data commission floated in 2024 were raised in Dewan Rakyat,[219] with further discussions on the need for a review body or an independent body amidst Malaysia's data centre hub and AI ambitions elaborated. A Digital Trust and Data Security strategy 2026-2030 is also in the works, a regulatory body responsible over data-related issues could address gaps of regulation and governance which are concentrated on personal data. At the same time, the Ministry of Digital established an inter-agency task force to draft a legislation on AI expected to be tabled at the end of 2026.[220]

5.2.3. Regional Cooperation

Malaysia's approach to technology governance have always been linked to regional and international efforts for security or economic purposes. The Framework of Responsible State Behaviour adopted by the UN General Assembly resolution 70/237 in 2015 anchored Malaysia's foreign policy and cybersecurity nexus. Thus, Malaysia championed its commitments through the development of the ASEAN Checklist[221] for the Implementation of the Norms of Responsible State Behaviour in Cyberspace and the Regional Action Plan on the norms. As cyber presents transboundary and asymmetrical governance challenges due to the heavy presence of the private sector, Malaysia has also pursued the Kuala Lumpur Declaration on Safe and Responsible Use of Social Media Platforms[222] and the development of regional guidelines to strengthen harmonisation across the bloc but also to present a united ASEAN front[223] for a trusted media and information ecosystem. Malaysia's 2025 ASEAN chairmanship also saw the Declaration on the Establishment of an ASEAN AI Safety Network[224] at the 47th ASEAN Leaders Summit in Kuala Lumpur which would further strengthen ASEAN as a harmonised market in a developing sector, thus contributing to the goal of developing ASEAN as the fourth-largest economy by 2045 – an aim of the ASEAN Community Vision 2045.

To this, the *substantial conclusion*[225] of the Digital Economy Framework Agreement is welcomed. Negotiations for rules have largely finished, with these covering cross-border data flows, digital payment, data privacy and ASEAN Unique Business Identification Number. While clarity in Malaysia's policies on

cybersecurity and data management would anchor negotiations, newer areas of policy development such as on digital identities or AI could mean that these may not be covered holistically should the agreement be signed in 2026. Malaysia is currently exploring a framework of understanding to possibly support the usage of digital identity in crossboundary services that resembles the Roadmap for Instant Payment Connectivity.

5.2.4. Moving Forward

The year 2026 could see details to policies such as the National Cyber Security Strategy 2026-2030 and the AI Action Plan while goals for Digital Economy Blueprint and the Malaysia Fourth Industrial Revolution Roadmap could be further specified, especially latter policies meet its halfway assessments. Further efforts to strengthen the AI ecosystem is expected, primarily due to the Digital Trust and Data Security Strategy,[226] incoming Data Commission and an AI legislation in the works. There would be further impetus for government digital transformations to continue a display of efficacy and efficiency, especially as the Madani government also hits a halfway point since elections in November 2022.

5.3. The Philippines

By Pierre Tito Galla, *Democracy.Net.PH, Philippines*

The Philippines is a lower middle income economy,[227] with a GDP of USD 461.62 billion in 2024.[228] The backbone of the Philippine economy is the micro, small, and medium enterprises (MSME) sector which latest Department of Trade and Industry (DTI) statistics say[229] accounts for 99.63% establishments collectively generating 66.57% of jobs.

The country[230] has a healthy labor force participation rate of 65.7% which translates to 52.4 million individuals. The unemployment rate is 3.7%, translating to 1.9 million unemployed individuals, while underemployment is at 11.4%, or 5.8 million underemployed. The services sector (under which the ICT sector is classified) accounts for the largest share of employment at 61.4%, followed by agriculture at 20.9% and industry at 17.7%.

The market size of the information and communications technology (ICT) sector in the Philippines is estimated at USD 28.13 billion,[231] contributing about 8.5% to the country's GDP,[232] and creating an estimated 11.3 million jobs.[233]

Recognizing that ICT is a significant driver of the Philippine economy, investment in ICT was declared to be one of priorities of the administration of President Ferdinand "Bongbong" Marcos jr. from its beginning[234] in 2022 and continues to be so in the middle of his term[235] in 2025. However, with 2025 being a midterm election year, initiatives towards improving the state of ICT policy, regulation, investment, and growth were seen to be not as aggressive as previous years. Also of note is an increase in political noise which is also seen to contribute to slow progress by the government in terms of policy.

5.3.1. Policy Priorities for the Philippines in 2025

The top three ICT policy trends in the Philippines can be grouped into: enabling long-term investment, transforming public governance, and developing trust in the digital marketplace. While policy development and implementation has not been rapid, the progress by the Philippines in this area is not insignificant.

5.3.1.1. Strengthening ICT infrastructure policy to enable long-term investment

Nonetheless, the Philippines has achieved a significant ICT policy milestone – the enactment of Republic Act No. 12234,[236] or the "Konektadong Pinoy (Connected Filipino) Act." An initiative originally filed in the Philippine House of Representatives in 2017 as the "Open Access in Data Transmission Act (OADTA)," the Konektadong Pinoy Act mandates the adoption of an open access model for the data transmission industry, which promotes the following:[237]

The enactment of the Konektadong Pinoy Act is expected to encourage investment[238] in the Philippine ICT sector, benefiting incumbent telecommunications service providers as well as emerging digital transmission and internet service providers.

Other initiatives that are also expected to encourage investment in the Philippine ICT sector that were recently enacted are the Investors' Lease Act,[239] the E-Governance Act,[240] and the ARROW Act.[241]

The Investors' Lease Act increases the number of years a foreign entity may lease land in the Philippines from 25 to 99 years. This increase in the maximum lease period for foreign entities allows for longer investment horizons, especially for large ICT infrastructure investments.

The ARROW Act relaxes rules relevant to eminent domain and right-of-way issues between owners of privately held land and government entities and private sector companies. The acquisition of right-of-way sites for private infrastructure projects designed for public use, including ICT infrastructure projects, particularly involving wired technologies, is expected to be less cumbersome.

Also intended to promote infrastructure and investment, the National Telecommunications Commission (NTC) released NTC Memorandum Circular No. 003-09-2025, "Decommissioning of Third Generation (3G) and Second Generation (2G) Mobile Network Services." The circular, effective mid-September 2025, mandates that all public telecommunications entities (PTEs) offering 3G services shall ensure nationwide phase-out of 3G services by December 31, 2026. The presumed clawback of spectrum used for 2G and 3G services is intended to spur savings among telecommunications companies' spending on Spectrum User Fees (SUFs) and Supervisory and Regulatory Fees (SRFs), providing opportunities for investment elsewhere.

5.3.1.2. Accelerating the digital transformation of public governance

The E-Governance Act is designed to facilitate the transition of government services to digital platforms, with the goal of making such services more accessible and efficient for citizens. Implementation of the E-Governance Act is expected to put pressure on the ICT services sector to expand reach, improve network speeds, and improve reliability across the Philippines. Similar pressure is expected to be provided by the issuance of the Department of Information and Communications Technology (DICT) of Department Circular No. HRA-001, "Adoption of a Standards-Based Approach to Information Systems Strategic Plan (ISSP) Compliance," wherein standards are imposed on government agencies in their acquisition and procurement of ICT goods and services.

On the other hand, the DEFA (see above) puts pressure on the Philippine government to fast-track the implementation of existing laws, such as the Internet Transactions Act (Republic Act. No. 11967), and push for more digital enablement reforms. One such reform, the proposed CADENA Act (Senate Bill No. 1506),[242] intends that government agencies would be required to post transaction documents — such as contracts and bills of materials — on a blockchain-backed digital platform within seven days, refined to integrate advanced digital infrastructure for transparency.

Independently, there are local government units that have independently of the national government pursued the potential use of digital transformation tools and technologies for improved governance. For example, the city of Naga, Camarines Sur, recently received approval from the DEPDev[243] for a PHP 6.793 million (USD 115 thousand) grant to build what is expected to be the country's first AI-empowered city planning, transport, and land-use monitoring system.

5.3.1.3. Fostering trust and security in the evolving digital marketplace

On the other hand, the implementation of the National Cybersecurity Plan (NCSP) 2023-2028[244] has been slow. Only two (2) cybersecurity-related policies have been released in 2025: National

Telecommunications Commission (NTC) Memorandum Circular (MC) No. 001-01-2025, "Guidelines on the Management of Internet Traffic and Reporting Mechanism of Internet Service Providers" and the DICT Department Circular No. HRA-003, "Prescribing International Organization for Standardization (ISO) Standards on Information Security for Entities Engaged in the Telecommunications Business."

NTC MC No. 001-01-2025[245] is intended to enhance the resiliency and security of the Philippine internet infrastructure by improving network protection, reduce the likelihood of harmful traffic within networks, mitigate the risk of data breaches, protect users from cyber-attacks, and manage internet security posture. The NTC is prescribing the use of a protective domain name service (DNS) for all internet service providers (ISPs), with ISPs choosing between using the protective DNS managed by the DICT or their own.

The DICT DC No. HRA-003 was published in compliance with the following provisions of law:

- Section 26 of Republic Act No. 11659, or "An Act Amending Commonwealth Act No. 146, Otherwise known as the Public Service Act, As Amended" and Section 47 of its IRR mandates entities engaged in the telecommunications business to obtain and maintain certifications from an accredited certification body attesting to compliance with relevant ISO standards on information security as prescribed by the DICT.

- Section 6 of Republic Act No. 11934, or the Subscriber Identity Module (SIM) Registration Act, requires public telecommunications entities (PTEs) to comply with the minimum information security standards prescribed by the DICT consistent with internationally accepted cybersecurity standards and relevant laws, rules, and regulations.

Covered entities are to refer to the Philippine National Standards (PNS) ISO/IEC 27000 - Information Security Management family of standards as provided by the DC. While the Konektadong Pinoy Act (see below) was enacted later, the provisions of this DC are consistent with provisions of Section 9 of the Konektadong Pinoy Act, with the law allowing for adoption of other information security and cybersecurity standards other than ISO standards as long as they are approved by the DICT.

In parallel fashion, the Department of Trade and Industry published Department Administrative Order No. 25-07 series of 2025, "Implementing Rules and Regulations on the E-Commerce Philippine Trustmark,"[246] implementing a voluntary trust mark in a bid to encourage trust of the public regarding e-commerce transactions.

As mentioned above, the United Nations Convention Against Cybercrime was recently signed by the Philippines. The convention creates a global framework and platform for collaboration to combat cybercrime while safeguarding human rights and making sure that global digital spaces are protected, inclusive and adaptable to emerging threats. The convention prioritizes inclusivity and equity, offering vital capacity-building support to countries with limited resources. The treaty will enter into force after forty countries have formally become State Parties. The Philippines, having signed the treaty, may choose to ratify the treaty through an amendment of the Cybercrime Prevention Act (Republic Act No. 10173) or the enactment of a new statute.

Overall, in 2025, the Philippine government focused on ICT policy initiatives encouraging investment in the Philippine ICT sector, with some initiatives in cybersecurity and e-commerce.

5.3.2. The Evolution of Tech Governance in the Philippines in 2025

5.3.2.1. Reorganising institutions to strengthen ICT leadership

ICT governance trends in the Philippines have been leaning towards the implementation of previously enacted policies and the strengthening of existing institutions, with an eye on opportunities to explore further reforms that could be characterized as low hanging fruits.

A significant governance milestone is the reorganization of the National Economic Development Authority (NEDA) to the Department of Economy, Planning, and Development (DEPDev).[247] DEPDev's charter was legislated by Republic Act No. 12145 which was signed into law by President Ferdinand "Bongbong" Marcos, jr on April 10, 2025. DEPDev is a prime mover of ICT reform initiatives such as the Konektadong Pinoy law.

5.3.2.2. Digitalising government services through the e-Gov SuperApp

Further evidence of the Philippine government's priorities regarding ICT are the continuous rollouts of the e-Gov SuperApp.[248] Launched in June 2023,[249] the government through the Department of Information and Communications Technology (DICT) is continuing efforts to encourage the use of the app while simultaneously onboarding more government services into the app.[250] Similarly, the government in June 2025, began implementation of the Internet Transactions Act (Republic Act No. 11967, enacted December 2023) and the value added tax (VAT) for digital services[251] (Republic Act No. 12023, enacted in October 2024).

5.3.3. Regional cooperation

Of recent significance are two international cooperation initiatives' milestones reached, namely the ASEAN Digital Economy Framework Agreement (DEFA)[252] and the United Nations Convention Against Cybercrime.[253] The DEFA aims to accelerate ASEAN's transformation into a leading digital economy that fosters greater digital cooperation and paves the way for regional digital integration and inclusive growth and development. Meanwhile, the United Nations Convention Against Cybercrime acknowledges that cybersecurity is not just a technical issue but a human rights imperative, ensuring protections for marginalized communities and safeguarding fundamental freedoms in the digital age.

5.3.4. Moving Forward

The Philippines continues to look for opportunities to improve its ICT policies. Some initiatives are akin to small actions of moving building blocks around, such as the movement of the Education Center for AI Research (E-CAIR)[254] system from the Department of Trade and Industry (DTI) to the Department of Education (DepEd), intended to be fully implemented in June 2025.

The government still continues to engage stakeholders in public consultations, such as for[255] policies on National Protective Domain Name System (PDNS) Framework and Accreditation of Cybersecurity Assessment Providers (ACAP). The PDNS Framework mandates telecommunications companies, internet service providers (ISPs), and various government sectors (NGAs, GOCCs, LGUs, public education, and DICT-assisted projects) to adopt proactive cybersecurity measures with the goal of reducing malware, phishing, unregistered financial platforms, and other malicious cyber activities. Meanwhile, the ACAP policy institutionalizes a formal accreditation process for Vulnerability Assessment and Penetration Testing (VAPT) and Information Security Management System (ISMS) service provider as part of the plan to ensure the security of Critical Information Infrastructure (CII), covering government, individual, and business information assets. Non-government organizations have significant roles to play in moving policy conversations forward.

Other initiatives, such as those recently presented by the National ICT Planning, Policy, and Standards Bureau (NIPPSB) of the DICT, include proposals for the enactment of a Cybersecurity Act and the establishment of a Cybersecurity Bureau,[256] a National Telecommunications Commission (NTC) Revitalization Act intended to bring regulatory governance in line with digital communications, a Spectrum Management Act intended to update the 1930s-era governance of the Radio Control Law (Act No. 3846) towards readiness for 21st century realities, among others.

As of this writing, the evolution of ICT governance and policymaking in the Philippines is characterized by fits and starts that does include reforms with potentially significant impact. There is still much opportunity to improve policymaking coherence, of which the Philippines has the talent and time to leverage.

5.4. Singapore

By Lim How Khang, Singapore Management University, Singapore

Singapore's approach to technology governance shifted in 2025 from framework-building to implementation. Safeguards moved upstream to gatekeepers (notably app distribution services) and downstream into operational controls (including real-time intervention tools to reduce scam losses). In parallel, regulators published more audit-ready expectations for cloud services, data centres and cybersecurity.

A unifying theme was sovereignty-by-assurance: maintaining control and continuity in a connected economy by making compliance, resilience and safety measurable. Internationally, Singapore reinforced "trusted connectivity" through new digital economy commitments with European partners, ASEAN's practical governance guides, and renewed focus on regional energy linkages that underpin digital reliability.

Beyond its borders, Singapore pursued "trusted connectivity": high-standard digital economy rules with Europe and EFTA, practical ASEAN guidance for cross-border data governance and generative AI, and regional energy connectivity as a foundation for digital reliability.

This update examines the year's main developments and identifies what to watch as the region's digital transformation accelerates.

5.4.1. Policy Priorities for Singapore in 2025

5.4.1.1. Operationalising Whole-of-System digital secutity and resilience

Singapore's 2025 security agenda moved beyond "cybersecurity" toward whole-system resilience, covering cloud architecture, operational controls, physical hazards, and sector-specific readiness for AI and quantum threats.

IMDA's Advisory Guidelines for Cloud Services and Data Centres[257] set out practical steps on risk assessment, business continuity, and controls for hazards such as fires, leaks, and cooling failures. The guidelines are voluntary, but they signal an "audit-ready" direction: what "good" looks like now, and what may become mandatory later.

CSA raised baseline expectations by expanding its Cyber Essentials and Cyber Trust certification[258] marks to cover cloud, AI, and operational technology. Trust now depends on demonstrable controls in newer risk domains, not just traditional IT environments. That's the point. The baseline has moved.

In the second half of the year, governance hardened at the critical-infrastructure layer. The commencement of provisions under Singapore's Cybersecurity legislative updates[259] tightened expectations for Critical Information Infrastructure (CII) and extended oversight to Systems of Temporary Cybersecurity Concern (STCCs). A forward indicator: public signalling that CII owners will face stronger reporting expectations for suspected Advanced Persistent Threat (APT) incidents.

What changed in 2025: compared with 2024's emphasis on preparing for emerging risks, this year increasingly treated resilience as something that must be operationalised and evidenced through certifications, reporting expectations, and more explicit regulatory coverage.

Energy also became more visibly a digital policy matter. Singapore advanced cross-border electricity arrangements with Vietnam[260] (including exploration of larger-scale low-carbon imports) and Indonesia.[261] AI-era compute growth makes power security and diversification central to digital continuity.

5.4.1.2. Hardening consumer protection and platform accountability across the digital economy

Consumer protection moved from "user education and shared responsibility" to faster system-level interventions and clearer accountability, especially against scams and online harms.

The most consequential change was the Protection from Scams Act 2025.[262] It empowers police to issue Restriction Orders to banks when there is reasonable belief an individual is at risk of transferring money to scammers. The design: time-bound controls to stop losses in real time, then resolution and redress.

Online safety evolved in two directions. First, gatekeeper controls at the app-store layer: IMDA's Code of Practice for Online Safety[263] covering designated app stores pushed child-safety and harmful-content controls upstream, including age-assurance expectations. Second, public benchmarking for major platforms: IMDA published its inaugural Online Safety Assessment Report[264] for designated social media services, shifting attention from policy statements to measured effectiveness.

Enforcement stiffened under existing criminal-harms powers. The Singapore Police Force issued an Implementation Directive to Meta under the Online Criminal Harms Act[265] to address impersonation scams targeting public figures. Non-compliance carries a penalty of up to USD 1 million.

Beyond scams and content harms, 2025 also tightened consumer-market governance. Enterprise Singapore strengthened TR 76 e-commerce guidelines,[266] targeting fake reviews, misleading interfaces, and merchant verification. Product safety and legal metrology functions shifted[267] from EnterpriseSG to CCCS, consolidating synergistic consumer-protection capabilities. The Platform Workers Act 2025[268] came into operation, requiring defined protections (documentation, contributions) for platform workers while preserving operational flexibility.

A second-half development worth noting: authorities announced measures to restrict scam mules' access[268] to financial, telecommunications, and digital facilities. The aim is to disrupt scam operations by limiting access to the infrastructure they depend on, expanding the anti-scam toolkit beyond consumer vigilance and post-incident recovery.

At the perimeter of the digital economy, Singapore clarified expectations around digital-token services[270] operating from Singapore: "license or cease" for certain in-scope providers serving overseas clients.

5.4.1.3. Scaling responsible innovation through assurance and deployment infrastructure

Singapore continued to encourage innovation, but 2025's defining characteristic was that "innovation policy" increasingly came packaged with test protocols, assurance artefacts, and faster pathways to deployment.

In AI governance, the year shifted from frameworks to testable practice. The Global AI Assurance Pilot[271] targeted end-to-end application reliability (not only model evaluation), and IMDA/AI Verify produced a Starter Kit for Safety Testing[272] of LLM-Based Applications. This provides a practical bridge from governance principles to engineering workflows that address risks like prompt injection and data leakage.

Alongside assurance tooling, Singapore deployed capacity-building instruments to help firms adopt AI. The Enterprise Compute Initiative[273] (announced at Budget 2025) set aside significant support via cloud credits/tools and consultancy for Singapore-based companies to build MVPs and implement change management.

Healthtech followed a similar "innovation with guardrails" pattern. The Health Sciences Authority (HSA) consulted on a sandbox-style exemption approach[274] for certain AI software as a medical device (AI-SaMD) developed within selected public healthcare settings. Synapxe launched HealthX Innovation Sandbox 2.0,[275] expanding access to data and multi-cloud infrastructure for experimentation. A new

Health Information Bill[276] was introduced to establish a statutory framework for the National Electronic Health Record ecosystem, expanding health data sharing for care continuity while imposing privacy and cybersecurity obligations and clear use-limitations.

Ethical governance also advanced for biomedical research via the Bioethics Advisory Committee's report[277] on responsible uses of Big Data and AI.

Innovation policy included time-to-market improvements. IPOS launched updated acceleration programmes[278] (SG Patents Fast and SG Trade Marks Fast) to streamline IP processes.

What changed in 2025: where 2024 leaned heavily on sandboxes and frameworks, this year increasingly paired them with assurance methods (tests, benchmarks, certification standards) and delivery infrastructure (compute support, multi-cloud sandboxes, accelerated IP rails) so that innovation is not just permitted, but scaled.

5.4.2. The Evolution of Tech Governance in Singapore in 2025

5.4.2.1. Operationalising AI governance and advancing trusted digital interoperability

Singapore's AI governance leadership evolved toward assurance markets and interoperable proof.

Domestically, the Global AI Assurance Pilot and the LLM safety-testing starter kit signalled a transition from "what responsible AI should look like" to "how teams can demonstrate it." These artefacts matter because they can become portable: testing results and assurance evidence can, in principle, be reused across organisations and jurisdictions, reducing duplication and building trust.

In the financial sector, MAS consulted on AI risk management guidelines[279] for financial institutions, moving from general principles to supervisory expectations around lifecycle controls, oversight, and institutional capability.

Internationally, Singapore pursued "trusted rules" through high-standard agreements and regional guidance. The EU-Singapore Digital Trade Agreement[280] provides clearer rules for digital trade and cross-border data flows. The EFTA-Singapore Digital Economy Agreement[281] reinforces legal certainty and interoperability across digital trade processes. ASEAN released practical guides[282] covering data anonymisation, model contractual clauses mapping, and generative-AI governance adapted for regional context.

A forward-looking signal: ASEAN's Digital Economy Framework Agreement (DEFA)[283] has been publicly framed as a 2026 signing ambition. If achieved, it would turn today's guidance into more standardised regional commitments.

5.4.2.2. Strengthening institutional enforcement and legal infrastructure

Singapore also strengthened the institutional machinery that makes digital governance enforceable and navigable.

On public law infrastructure,[284] the move to make electronic publication more authoritative (via the Electronic Gazette and Legislation Act) 2025 supports legal certainty in a digital-first society.

Institutionally, Singapore continued a "tight perimeter, clear duties" approach. For online harms: the Online Safety (Relief and Accountability) Bill[285] was passed, establishing faster relief mechanisms and a specialised commission model to support victim redress and platform accountability. For scam harms: beyond Restriction Orders under the Protection from Scams Act,[286] enforcement escalated through criminal law amendments commencing at year-end to sharpen penalties for scam-related offences. For digital infrastructure: cybersecurity oversight[287] expanded via CII/STCC coverage and strengthened reporting expectations.

The year also advanced governance for public-sector data use. MDDI progressed consultation and legislative steps to support data-sharing with authorised external partners[288] under clearer legal bases and safeguards. This issue will grow in importance as public services increasingly depend on outsourced and ecosystem delivery models.

Singapore advanced end-to-end digitalisation in legal and administrative processes,[289] including reforms to support fully digital property conveyancing.

5.4.2.3. Sustaining multi-stakeholder governance and ecosystem resilience

Even as enforcement and perimeter-setting became more visible in 2025, Singapore retained a strong multi-stakeholder operating model, using pilots, standards, and partnerships to build capabilities and raise baselines.

Cross-sector scam disruption tools[290] now span law enforcement, financial institutions, and digital identity/telco ecosystems, designed to break scam operations by limiting access to the facilities they depend on. CSA initiatives include the Safe App Portal pilot,[291] collaboration with industry alliances,[292] and plans for a Cyber Resilience Centre [293] to support organisations (especially SMEs) in readiness and recovery. On workforce measurement, global dialogue convened with the ILO[294] aims to improve statistical frameworks for digital platform work.For SME navigability, the SME Pro-Enterprise Office [295] launched as a coordinating unit to help smaller firms handle cross-cutting regulatory issues.

5.4.3. Moving Forward

By year-end, Singapore's 2024 foundations (frameworks, new agencies, shared-responsibility concepts) had evolved into a 2025 model of assurance in action: codes that move controls to chokepoints, reports that benchmark outcomes, and powers that allow faster intervention and clearer accountability.

In 2026, the question shifts from *what Singapore has launched to what those moves change*: the cost of cross-border compliance, the cycle time of intervention, the marginal cost of assurance, and the social licence for AI adoption. PM Wong[296] has already put the last point on the agenda—jobs and livelihoods are not a side issue; they are the constraint on how far and fast AI can be deployed.

Trusted connectivity: does it reduce compliance work?

Do the Europe/EFTA/ASEAN tracks produce operational reuse—fewer duplicate audits, shorter approval timelines, or explicit acceptance of common evidence—rather than parallel "high-standard" commitments?

Anti-scam cycle time: can interventions bend new vectors quickly?

When a scam pattern spikes, how long before losses from that vector fall—weeks or quarters—and do we see displacement into other channels or a net reduction in harm?

Assurance: is it becoming interoperable or additive?

Across privacy, cyber, cloud, and AI schemes: are requirements being mapped so marginal compliance cost declines (shared controls, reused audit artefacts), or does each scheme require new evidence and new processes?

AI and jobs: are transitions keeping pace with adoption?

If AI use accelerates across sectors, do worker transitions keep up—i.e., do reskilling pathways convert into placements at scale, and are productivity gains showing up as better job quality and wages rather than just headcount pressure?

5.5. Thailand

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

Thailand's digital economy continued to expand in 2025, supported by a mature platform ecosystem, widespread digital payments, and the rapid normalisation of artificial intelligence in both everyday life and the workplace. Surveys indicate that 91% of Thai internet users now interact with AI in their daily routines, up from 77% the year before,[297] demonstrating how AI has become embedded in ordinary digital behaviour. Workplace adoption has accelerated just as quickly. Four in ten Thais now use AI at work, almost double the previous year, relying on AI tools for content development, analytics, and customer service. Together, these trends show that AI is no longer experimental but already a part in day-to-day operations across both private and public sectors.

Yet this progress unfolded alongside an escalating wave of digital threats. According to official data from the Cyber Crime Investigation Bureau,[298] there were almost 300,000 recorded online-fraud cases from January to November 2025, amounting to over 27 billion Baht in reported losses, with an average of 900 cases per day and only about one percent of stolen funds successfully recovered. The scale and persistence of these incidents intensified public concern and underscored the vulnerability of citizens and businesses to increasingly sophisticated scam networks.

Throughout the year, the central question became whether Thailand's rules and systems could evolve fast enough to keep pace with technological change and growing security challenges. Therefore, in 2025, the country shifted its focus from creating new rules and institutions to strengthening national digital security in the digital domain, strengthening enforcement, and embedding risk-based governance into the digital ecosystem.

5.5.1. Policy Priorities for Thailand in 2025

5.5.1.1. Advancing dual-track AI policy: Capability building and Risk governance

AI remained a central strategic priority throughout 2025. National initiatives aimed at strengthening AI-capable human capital and foundational digital infrastructure expanded meaningfully. The National AI Committee, established in April 2025,[299] continued to articulate sectoral deployment priorities, while programmes such as THAI Academy,[300] developed by the Ministry of Digital Economy and Society in partnership with Microsoft Thailand, supported widespread upskilling. Thailand also advanced efforts to build domestic capability through investment in AI datasets, local-language models, and applied AI solutions in healthcare, agriculture, logistics, and industry. Regionally, the establishment of the AI Governance Practice Centre, developed with UNESCO, positioned Thailand as a hub for responsible AI training and capacity building.

At the same time, the governance of AI shifted from ethical principles to detailed risk-management requirements. New security standards and regulatory guidelines introduced obligations for organisations deploying AI systems to implement lifecycle controls, validate models, mitigate hallucination risks, and document model behaviour. AI used in financial services became subject to heightened oversight, particularly in areas where automated decisions affect customers.

This combination, supporting adoption while tightening safeguards, shows how Thailand now treats AI as both an economic priority and a technology that requires careful oversight. As AI becomes more deeply integrated into operational processes, the emphasis on safety, accountability, and resilience becomes an essential complement to innovation.

5.5.1.2. Reinforcing digital trust and citizen safety

Digital trust emerged as a defining theme in Thailand's policy landscape in 2025. The rise in online scams, fraudulent transactions, and unsafe digital practices had reached a level that directly affected public confidence in digital services. As a result, digital trust and citizen safety became priorities across multiple policy domains, influencing how the government approached e-commerce, payments, and digital public services.

Several new measures were introduced to strengthen user protection. Requirements for stronger fraud detection, safer transaction environments, and more transparent service practices reflected an effort to reassure citizens that digital engagement would remain safe. Public awareness campaigns and literacy efforts complemented these measures, helping users navigate online risks and improving their ability to identify and report suspicious activities.

Digital trust is now recognised as a precondition for the growth of e-commerce, fintech, and digital public services. Thailand's 2025 policies therefore treat safety not as a constraint on innovation but as a foundational element of a functioning digital economy.

5.5.1.3. Strengthen fairness and more transparent platform markets

Thailand's platform economy also experienced a shift in regulatory attention in 2025. Building on earlier consumer-protection rules, policymakers moved to address broader concerns related to fairness, transparency, and competition in digital markets. The Trade Competition Commission of Thailand issued a draft guideline addressing anti-competitive behaviour in multi-sided platforms.[301] The guideline identifies practices such as discriminatory algorithms, self-preferencing, coercive contractual terms, and preferential access to third-party data as potential sources of market distortion. Its aim is to clarify how competition principles apply to increasingly complex digital business models.

Alongside competition oversight, transparency obligations for online marketplaces became more prominent. New rules requiring clearer seller identification, more accurate product information, and faster takedown of unlawful goods reflected a maturing regulatory environment that prioritises openness and accountability. Sector-specific rules for ride-hailing and logistics-linked platforms similarly sought to bring greater consistency to safety standards and user protections.

Overall, the trend is toward a more complete set of platform rules that focus on making things fair, transparent, and safe across the whole system. Thailand is positioning itself to address the complexities of platform power in a way that aligns with both domestic priorities and emerging global standards.

5.5.2. The Evolution of Tech Governance in Thailand in 2025

5.5.2.1. Centralising cybersecurity as the core of tech governance

Cybersecurity was the top governance issue in 2025. Fragmented regulations are now coming together into a more coherent national security architecture. The country expanded its oversight of critical information infrastructure, reflecting the recognition that cloud providers, data centres, and industrial systems now form part of the country's essential digital backbone. Draft amendments to the Cybersecurity Act[302] introduced clearer definitions, multi-tier incident reporting requirements, and expanded obligations for organisations that hold or process sensitive digital infrastructure. These changes indicate an effort to align regulatory obligations with how digital services operate today.

Regulatory consolidation continued through the National Cyber Security Agency's issuance of two major instruments: a new Website Security Standard[303] and an AI Security Guideline.[304] These standards define baseline security requirements for the development, deployment, and maintenance of websites and AI systems across the public and private sectors. They emphasise secure configuration, encryption, vulnerability management, lifecycle risk controls, and technical alignment with international frameworks. Their introduction reflects the shift from high-level cybersecurity awareness to specific, operational measures that organisations must implement.

Cybercrime, especially scam networks, emerged as a national priority. The government established the National Committee on the Prevention and Suppression of Technology Crime,[305] responsible for coordinating rapid response across enforcement, digital platform oversight, and financial tracking.

A national campaign brought together fifteen agencies to close regulatory loopholes, disrupt financial channels used by criminals, revoke visas of foreign offenders, and cancel mule accounts. A further step was the introduction of the shared-liability regime under the technology-crime decree,[306] which compels banks, telecom operators, and digital platforms to implement fraud detection measures and compensate victims when negligence contributes to harm.

International engagement also intensified. On 25 October 2025, Thailand signed the United Nations Convention against Cybercrime,[307] joining a global effort to align legal frameworks, facilitate evidence-sharing, and combat online child exploitation and cross-border cyber intrusion. This marked an important step in harmonising domestic policy with international norms and underscored the country's intent to strengthen cooperation in addressing transnational digital threats.

Taken together, these efforts demonstrate Thailand's progression toward the security and resilience objectives set out in the National Cybersecurity Policy and Action Plan (2022–2027), which positions cybersecurity as a national development imperative.

5.5.2.2. Institutionalising risk-based enforcement and oversight

A second defining trend was the transition from conceptual frameworks to real enforcement. Regulations introduced between 2022 and 2024, especially those governing online platforms, began to be implemented with greater precision and urgency. Regulators classified major online marketplaces as high-risk,[308] triggering obligations for seller verification, risk assessments, disclosure rules, and mechanisms to remove harmful goods and fraudulent actors.

The enforcement philosophy centres on risk proportionality. Services with higher economic significance or larger user bases face heavier obligations; smaller services, while not exempt, are subject to more targeted oversight. This approach was visible not only in marketplace regulation but also in transportation platforms, which are now required to ensure driver identity verification, operate licensed vehicles, and provide clear safety information to users.[309]

Risk-based enforcement extended to the financial sector. The Bank of Thailand intensified its supervisory expectations, requiring digital financial institutions to demonstrate readiness before launching virtual-banking operations.[310] Institutions must meet cybersecurity, resilience, and risk-governance standards before approval. In addition, the Bank of Thailand finalised its guidelines on AI risk management, which outline requirements for model validation, explainability, data integrity, and human oversight when AI is used in customer-facing or high-impact decision-making.[311]

These developments reflect a broader regulatory stance that compliance now carries practical consequences rather than remaining a formality. Rules issued in previous years are now enforced through audits, reporting obligations, and explicit mechanisms to correct or penalise non-compliance. Regulators are no longer just making rules but are now actively checking that those rules are being followed.

5.5.2.3. Embedding multi-stakeholder coordination in tech governance

The third governance trend involves the institutionalisation of multi-stakeholder cooperation. Thailand's tech governance is increasingly executed not by a single agency but through coordinated networks that integrate public, private, and international actors.

Domestically, the Secure Network Alliance[312] led by Advanced Info Service (AIS) in partnership with key government agencies exemplifies this model. Combating cybercrime now requires continuous information sharing between telecom operators, enforcement agencies, and security bodies. This alliance pools intelligence, coordinates takedowns, and strengthens incident response capacity across both infrastructure and consumer-facing services.

Internationally, Thailand deepened its role in shaping regional norms. The establishment of the AI Governance Practice Centre in cooperation with UNESCO[311] reflects the country's ambition to become a regional hub for responsible AI capacity building. The ASEAN–UNESCO Forum on the Governance of Digital Platforms[314] further positioned Thailand as a convener of regional dialogues on platform safety, algorithmic accountability, and user empowerment. These initiatives highlight Thailand's integration into global governance networks and its commitment to harmonising national rules with evolving international standards.

Together, these initiatives point to a more decentralised approach to governance, where policy objectives are achieved through collaboration and shared responsibility across multiple sectors. This approach helps Thailand manage increasingly complex risks while advancing its broader digital economy objectives.

5.5.3. Regional Cooperation

DEFA has begun to influence Thailand's digital policy direction by reinforcing the need for greater regulatory interoperability, stronger digital-trust mechanisms, and cross-border compatibility. As the agreement aims to create a seamless regional digital market, Thailand must ensure that its emerging rules on data governance, cybersecurity, platform transparency, and AI oversight are consistent with regional expectations. This has accelerated domestic efforts to strengthen identity verification, enhance online consumer protection, and update cybersecurity and critical-infrastructure rules so that they support cross-border digital services. DEFA also underscores the importance of digital-skills development and SME readiness, aligning closely with national initiatives such as THAI Academy, the AI Governance Practice Centre, and sector-specific AI and platform regulations.

At the same time, Thailand's policies have played a meaningful role in shaping DEFA itself. As chair of the negotiation team in 2025, Thailand helped drive policy consensus on outstanding issues and pushed for timely completion of the agreement within the first quarter of 2026.[314] Thailand's progress on platform-governance rules, competition guidelines, and cybersecurity standards offers practical models for the region's interoperability and trust frameworks. Regional initiatives led or hosted by Thailand, such as the ASEAN-UNESCO forum on platform governance and the establishment of the AI Governance Practice Centre, further support DEFA's pillars on trust, safety, and responsible innovation. These developments show that Thailand is both preparing for DEFA and helping define its direction at the regional level.

5.5.4 Moving Forward

As we look toward 2026, we can expect Thailand's tech governance to become more coordinated and more stringent. Implementation of cybersecurity standards and amendments to foundational laws will require organisations to invest in compliance, audit processes, and governance structures. As AI becomes more routine across sectors, additional sector-specific guidance is likely to follow, especially in healthcare, education, and public administration.

DEFA will drive closer alignment of national rules with regional frameworks, prompting greater regulatory interoperability. It may also encourage the unification of overlapping responsibilities across digital, financial, and telecom regulators, reducing administrative friction for firms while creating a more predictable environment.

The broader challenge will be balancing innovation with security. Thailand's progress in 2025 demonstrates a commitment to supporting digital growth while protecting citizens and infrastructure. Maintaining this balance will require better technical capacity, clearer coordination among regulators, and policies that keep pace with technological change.

2025 therefore marks a pivotal year: the country moves decisively from building digital capability to securing the digital foundations on which future growth depends.

5.6. Vietnam

By Nguyen Minh Thao, *National Institute for Economics and Finance, Vietnam*

In 2025, the digital economy continues to serve as one of the key drivers of Vietnam's economic growth; indicators of industry revenue, technology export turnover, the number of digital enterprises, and the level of public participation in the digital space have improved significantly. According to data from the Ministry of Science and Technology's mid-2025 review report,[316] in the first six months of 2025, contribution of the digital technology industry to GDP increased by 21%; turnover of hardware and electronics export reached USD81 billion, up 27% compared to the same period in 2024. The technology enterprise ecosystem also continued to expand, and by the end of September 2025, the country had 78,502 digital enterprises.[317]

Within the digital economy, the e-commerce accounts for two-thirds of the country's total digital economy value,[318] helping place Vietnam among the world's top 10 fastest-growing e-commerce markets. According to the summary report presented by the E-Commerce and Digital Economy Agency (Ministry of Industry and Trade - MoIT), Vietnam's e-commerce sector has maintained an impressive annual growth rate of 18–25%.[319] In the first nine months of 2025, this sector continued to grow strongly, with a growth rate of more than 30%[320] compared to the same period last year.

5.6.1. Policy Priorities for Vietnam in 2025

In 2025, many of Vietnam's policies and laws related to technology, innovation, and digital transformation were reviewed, amended, and supplemented; several regulatory sandboxes and special policies were issued, helping to address institutional bottlenecks in technology governance. Specifically, in the field of technology and digital transformation, the National Assembly has passed more than 20 laws and 5 resolutions containing relevant provisions. At the same time, the Government and the Prime Minister have issued around 30 Decrees and Decisions detailing these contents. Tech and innovation policies in 2025 focus on the following key areas: (i) Collecting, sharing data, and protecting personal data; (ii) Managing and promoting e-commerce; and (iii) Ensuring cybersecurity and strengthening international cooperation on cybersecurity.

Notably, Vietnam successfully organized the Opening for Signature Ceremony and the High-Level Conference of the United Nations Convention on Countering Cybercrime in Hanoi on 25 October 2025 (the Hanoi Convention). This event holds significant importance as Vietnam is promoting digital transformation closely linked with ensuring cybersecurity. The Hanoi Convention also carries special significance for ASEAN, a region that has been at the forefront of establishing responsible behavior standards in cyberspace.

5.6.1.1. Improving data and facilitating data connectivity and sharing

Data is the foundation, and data connectivity and sharing are core elements of digital transformation. Therefore, improving the data governance framework continued to be a priority in 2025. Accordingly, the Government issued the following documents directly regulating this matter:

- Personal Data Protection Law:[321] The Law aims to establish a legal framework for the protection of privacy and the security of personal data.
- Decree No. 194/2025/NĐ-CP,[322] detailing several provisions of the Law on Electronic Transactions regarding national databases, data connectivity and sharing, and open data serving electronic transactions of state agencies.
- Decision No. 20/2025/QĐ-TTg,[323] issuing the List of Critical Data and Core Data. This document guides implementation of the Data Law (2024) by categorizing "critical data" and "core data" to apply special management and protection regimes, preventing risks of exploitation and attacks on national data.
- Decision No. 1751/QĐ-TTg dated 18 August 2025 of the Prime Minister approving the Data Strategy at the National Data Center. The strategy aims to establish and develop the National Integrated Database; focuses on key tasks, including: data infrastructure; data collection; data security and personal data protection.

Currently, the Ministry of Public Security (MoPS), the Ministry of Science and Technology (MoST), and seven technology enterprises[324] have developed 15 platforms and applications related to databases; 18 platforms and utilities implemented under Scheme 06[325] on developing the application of population data, digital identity, and electronic authentication for national digital transformation; and 61 data-based utilities supporting socio-economic development and social governance.

5.6.1.2. Improving regulations of e-commerce

E-commerce is becoming one of the key pillars driving digital economic growth in Vietnam. However, alongside its impressive achievements, the rapid expansion of e-commerce — with the emergence of many new business models, diverse actors, and increasingly complex practices—has also exposed significant gaps in the existing legal framework, posing risks related to counterfeit goods, prohibited items, and intellectual property infringements. According to MoIT,[326] the number of violations in 2024 increased by 266% compared to 2023. In the first six months of 2025, the E-Commerce and Digital Economy Agency instructed e-commerce platforms to remove more than 33,000 violating products and take action against over 11,000 storefronts showing signs of violations.

Previously, e-commerce activities in Vietnam were mainly regulated by Decrees. However, these are sub-law documents and lack sufficient legal authority to govern the cross-sectoral and complex issues arising from modern e-commerce. Therefore, the promulgation of the Law on E-Commerce is essential to establish a strong, coherent, and modern legal framework; protect the rights and interests of all participants; promote fair and healthy competition; and incentivize innovation. This also forms a technology legal framework aligned with global legal trends.

The Law on E-Commerce provides detailed regulations on e-commerce platforms and the responsibilities of various actors involved in e-commerce activities; the responsibilities of companies providing e-commerce support services; and the settlement of disputes, specialized inspections, and handling of violations in e-commerce. Some key points of this law include:

- Requirements for storing and sharing e-commerce data.
- Expanding the responsibilities of social media platforms engaged in e-commerce activities; adding regulations for multi-service integrated platforms; and adding legal responsibilities for platform operators to prevent the abuse of monopoly positions and algorithmic manipulation that may cause harm.
- Requirements for storing and sharing e-commerce data.
- Adding responsibilities for actors involved in livestream selling and affiliate marketing.
- Adding responsibilities for foreign e-commerce platform operators to establish or authorize a legal entity in Vietnam.
- Adding minimum responsibilities for providers of e-commerce support services (technical infrastructure, logistics, payment, electronic contract authentication services, etc.); and introducing a rapid-response mechanism for state agencies.

5.6.1.3. Elevating cybersecurity as a core pillar of national security and digital transformation

Cybersecurity risks

According to the 2024 Cybersecurity Survey Report[327] by the National Cybersecurity Association (NCA), Vietnam is among the countries most heavily affected by cybercrime. On average, among every 220 smartphone users, one becomes a victim of online fraud; 70% of citizens encounter at least one scam call or message each month. The first 6 months of 2025 alone, Vietnam detected nearly 1,500 online fraud incidents;[328] according to the periodic report of Viettel Threat Intelligence,[329] nearly 8.5 million accounts were stolen in Vietnam — accounting for 1.7% of global incidents; more than 4,500 phishing domains and 1,000 fake websites were recorded; over 528,000 DDoS attacks occurred, increasing in both frequency and sophistication. Cybercrimes are becoming increasingly complex, widespread, and sophisticated.

Hanoi Convention

On 25 October 2025, the United Nations Convention on Countering Cybercrime was opened for signature in Hanoi. This is a global legal framework for countering cybercrime, conveying clear messages on: (i) reaffirming the commitment to shaping order and ensuring safety and security in cyberspace based on international law; (ii) emphasizing the spirit of sharing, solidarity, and mutual support in the fight against high-tech crime; (iii) highlighting the protection of personal privacy; and (iv) requiring member states to incorporate the Convention's provisions into their national legal systems. This document not only aims to broaden cooperation but also to strengthen the capacity of law enforcement agencies and narrow the technological gap among countries.

Opportunities for ASEAN cooperation on cybersecurity

Cybercrime is currently one of the most serious security threats in the ASEAN region. The ASEAN Regional Cybersecurity Report[330] recorded a series of large-scale crackdowns related to cybercrime in 2025, highlighting clear gaps between domestic legal systems and the realities of transnational crime. This situation requires ASEAN countries to engage in multilateral cooperation and adopt proactive, long-term policies to respond effectively. In this context, the signing and implementation of the Hanoi Convention holds special significance for ASEAN — a region that has been at the forefront of establishing responsible behavior standards in cyberspace. This is expected to help open up opportunities for ASEAN to build a regional system for international cooperation in addressing cybercrime.

Cybersecurity Law: Incorporating international commitments into domestic law

The Cybersecurity Law was developed by consolidating the 2018 Cybersecurity Law and the 2015 Law on Network Information Security. This law adds and refines provisions to ensure compliance with modern management requirements and the practical needs of the rapidly developing digital economy. Specifically:

- It introduces regulations on the responsibilities of service providers in cyberspace.
- It designates MoPS as the central state agency for cybersecurity.
- It specifies the content of international cooperation in cybersecurity, including collaboration in sharing information on threats, cyberattacks, and preventive measures.
- It stipulates cybersecurity certification requirements for heads of agencies of critical national information systems.
- It raises awareness of cybersecurity, including guidance on implementing security measures.

The Vietnamese government has always considered countering cybercrime a priority in national security policy and actively engages with the international community in this effort. MoPS is assigned to lead and coordinate the national cybersecurity incident response alliance.

5.6.2. The Evolution of Tech Governance in Vietnam in 2025

5.6.2.1. Streamlining the state administrative apparatus and changes in tech governance

In 2025, Vietnam implemented a "revolution" in streamlining the state administrative apparatus.[331] The Government reduced the number of central-level entities from 30 to 22 (cutting 5 ministries and ministry-level agencies). At the same time, provinces also underwent mergers, reducing the number from 63 to 34, and adopted a two-tier local government model (eliminating the district level). These changes have directly affected tech governance as well as tech policy reforms.

After the restructuring, two ministries that play key roles in technology governance are: The Ministry of Public Security (MoPS) and the Ministry of Science and Technology (MoST). MoPS leads policy development and state management over data and cybersecurity, MoST leads policy development and state management over technology and innovation. One of the key tasks for 2025 is improvement of policies, including refining tech policies and enhancing the effectiveness of policy implementation. Notably, new tech governance approaches have been adopted to improve the quality and effectiveness of policy execution. Specifically:

- Establishing Steering Committees[332] for the development of science, technology, innovation from the central to local levels. The Central Steering Committee is under the Politburo and chaired by the General Secretary of Vietnam's Communist Party.

- Establishing the National Steering Committee on Data.[333] This is an inter-sectoral coordination body responsible for research, consultation, recommendations, and supporting the Government and the Prime Minister in directing and coordinating the implementation of strategies, policies, mechanisms, and solutions related to data.

- Establishing the National Data Association[334] that connects agencies, enterprises, and individuals to build the national data ecosystem.

- Establishing the National Data Center[335] (under MoPS) as the focal point for integrating, synchronising, storing, sharing, analysing, exploiting, and coordinating data from State agencies, serving the development of digital government, digital society, and digital economy, while ensuring national data security.

- Establishing the Strategic Human Resources Alliance,[336] with the participation of five leading training and research institutions. The Alliance is considered a strategic initiative aimed at promoting high-quality human resource development.

- Establishing the National Science and Technology Data Center[337] under MoST, responsible for building, managing, and developing the national database and sectoral databases on science and technology; and managing information infrastructure and science and technology statistics.

5.6.2.2. Approving regulatory sandboxes for tech-related activities

The regulatory sandbox is considered an effective solution to remove institutional bottlenecks for tech development and tech-based business models. In Vietnam, the policy of developing sandboxes has been established in several strategic and important national documents, such as Resolution No. 52-NQ/TW[338] on proactively participating in the Fourth Industrial Revolution; the Digital Government Development Strategy;[339] the Digital Economy and Digital Society Development Strategy;[340] Resolution No. 57-NQ/TW on breakthroughs in science, technology, innovation, and national digital transformation; and Resolution No. 68-NQ/TW[341] on private sector development. In 2025, several tech-related sandboxes were issued, including:

- Under Resolution No. 193/2025/QH15[342] on piloting several special policies to create breakthroughs in science, technology, innovation, and national digital transformation, a sandbox is applied to telecommunications services using low-earth-orbit satellite technology.

- Sandbox in the banking sector:[343] Decree No. 94/2025/ND-CP provides for a sandbox in the banking sector. It aims to promote innovation, modernize banking activities, and enhance financial inclusion in a transparent, safe, and efficient manner with low costs. Under the sandbox, three financial technology (Fintech) solutions are eligible for pilot implementation: (i) Credit scoring; (ii) Data sharing through open application programming interfaces (Open API); and (iii) Peer-to-peer (P2P) lending.

- The Law on Science, Technology, and Innovation[344] stipulates that venture-driven activities in scientific research, tech development, and innovation are encouraged through sandboxes.
- The Artificial Intelligence Law[345] provides for a sandbox for AI.
- The Digital Transformation Law[346] provides for a sandbox in digital economy development.

5.6.2.3. Establishing portals to monitor and evaluate the implementation of tech and digital transformation policies

To enhance the effectiveness of tech governance, information systems for monitoring and evaluating the implementation of tasks related to science and tech development, innovation, and digital transformation have been put into operation. Specifically:

- The system for monitoring and evaluating the implementation of Resolution 57-NQ/TW, operated on the Portal[347] of the Communist Party of Vietnam.
- The portal[348] for receiving and publishing scientific and technological products, innovative solutions, and digital transformation solutions.

5.6.3. Regional Cooperation

The ASEAN Digital Economy Framework Agreement (DEFA) is the region's first digital economy agreement. This is a comprehensive agreement covering many areas, including provisions that promote cooperation such as: AI, personal data protection, online consumer protection, electronic payments, e-invoicing, customs and taxation, cooperation on competition policy, and talent development. DEFA also considers several provisions that directly support companies and enterprises operating in the digital economy, such as commitments on simplifying procedures for supporting startups and investors in the digital economy sector.

Vietnam's participation in DEFA has created momentum for the country to improve its tech policies to align with the commitments. Legal documents issued in 2025 — such as the Law on E-Commerce, the Cybersecurity Law, the Digital Economy Law, the Intellectual Property Law, as well as organizing the signing ceremony for the Hanoi Convention — reflect Vietnam's efforts and readiness in negotiating and signing the Agreement.

5.6.4. Moving Forward

Digital transformation, along with science, technology, and innovation, is becoming a powerful driver shaping the future. Accordingly, it is necessary to continue innovating in the formulation and improvement of tech policies to promote technological development and the digital economy. In the coming period, tech policies should focus on the following efforts:

- Incorporating the provisions of the Hanoi Convention, DEFA into domestic legal regulations.
- Strengthening international cooperation, especially with ASEAN countries, to share practices and expertise in digital economic development, cybersecurity, and in improving technology and innovation institutions and policies.
- Encouraging public-private partnership models in technology development.
- Attracting private sector participation in improving technology institutions and policies
- Creating a safe and flexible legal environment for innovation, including encouraging the application of regulatory sandboxes, and eliminating the mindset that if something cannot be managed, it should be banned in policymaking.

Appendix

List of leading ministries and key agencies that oversee different policy areas within digital economy (within the scope of this report)

Area	Indonesia	Malaysia	Philippines	Singapore	Thailand	Vietnam
AI	Communication and Digital Ministry (KOMDIGI)	National AI Office (NAIO) under Ministry of Digital	Department of Information and Communications Technology (DICT)	Infocomm Media Development Authority (IMDA) under Ministry of Digital Development and Information (MDDI)	National AI Committee Electronic Transactions Development Agency (ETDA) under Ministry of Digital Economy and Society (MDES)	Ministry of Science and Technology (MOST)
Digital content	Communication and Digital Ministry (KOMDIGI)	Malaysian Communications and Multimedia Commission (MCMC)	Department of Information and Communications Technology (DICT)	Infocomm Media Development Authority (IMDA) under Ministry of Digital Development and Information (MDDI)	Ministry of Digital Economy and Society (MDES)	Ministry of Science and Technology (MOST)
Cyber security	National Cyber and Crypto Agency (NCCA)	National Cyber Security Agency (NACSA)	Cybercrime Investigation and Coordinating Center (CICC)	Cyber Security Agency of Singapore (CSA) Ministry of Digital Development and Information (MDDI)	National Cyber Security Committee (NCSC) Cyber Security Regulatory Committee (CSRC) National Cyber Security Agency (NCSA)	Ministry of Public Security (MOPS)
Commerce/ E-commerce	Ministry of Trade (MOT)	Ministry of International Trade and Industry (MITI)	Department of Trade and Industry	Competition and Consumer Commission of Singapore (CCCS) Ministry of Trade and Industry (MTI)	Trade Competition Commission of Thailand (TCCT) Ministry of Commerce (MOC)	Ministry of Industry and Trade (MOIT)
Labour rights	Ministry of Manpower (MOM)	Ministry of Human Resources (MOHR)	Department of Labor and Employment (DOLE)	Ministry of Manpower (MOM)	Ministry of Labour	Ministry of Finance Ministry of Labour – Invalids and Social Affairs (MOLISA)
Taxation	Ministry of Finance (MOF)	Ministry of Finance (MOF)	Department of Finance (DOF)	Ministry of Finance (MOF)	Ministry of Finance (MOF)	Ministry of Finance (MOF)
Finance	Ministry of Finance (MOF) Financial Services Authority (OJK) Bank Indonesia (BI)	Ministry of Finance (MOF) Bank Negara Malaysia (BNM)	Department of Finance (DOF) Bangko Sentral ng Pilipinas (BSP)	Ministry of Finance (MOF) Monetary Authority of Singapore (MAS)	Ministry of Finance (MOF) Bank of Thailand (BOT)	Ministry of Finance (MOF) State Bank of Vietnam (SBV)
Digital transformation	Communication and Digital Ministry (KOMDIGI)	Ministry of Digital MyDigital Corporation Malaysia Digital Economy Corporation (MDEC)	Department of Information and Communications Technology (DICT)	Ministry of Digital Development and Information (MDDI)	Ministry of Digital Economy and Society (MDES)	National Committee on Digital Transformation Ministry of Science and Technology (MOST)

* Note: The list is not exhaustive.

References

1	Spotlight on Southeast Asia: Evolution of Tech Regulation in the Digital Economy. (2024, January 29). *Tech For Good Institute*. https://techforgoodinstitute.org/research/tfgi-reports/spotlight-of-southeast-asia-evolution-of-tech-regulation-in-the-digital-economy/
2	The Evolution of Tech Governance in Southeast Asia-6. (2025, March 26). *Tech For Good Institute*. https://techforgoodinstitute.org/research/tfgi-reports/the-evolution-of-tech-governance-in-southeast-asia-6/
3	*e-Conomy SEA 2025 report: ASEAN's digital economy poised to surpass $300 billion in GMV by 2025, fueled by 7.4x GMV and 11.2x revenue growth in a decade.* (n.d.). Bain. Retrieved 20 February 2026, from https://www.bain.com/about/media-center/press-releases/sea/e-conomy-sea-2025/
4	ibid
5	ibid
6	ibid
7	*Digital Nations 2025: Sustaining progress in Asia Pacific through investment—GSMA Asia Pacific.* (n.d.). Retrieved January 22, 2026, from https://www.gsma.com/about-us/regions/asia-pacific/gsma_resources/digital-nation-apac-2025/
8	ibid
9	ibid
10	ibid
11	Lam, T. (2025, September 5). Artificial Intelligence (AI) in Southeast Asia 2025-2026—(Free Report) AI Investment. *Source of Asia*. https://www.sourceofasia.com/ai-in-southeast-asia-2025-2026/
12	Communications, M. &. (2025, September 10). *Southeast Asia AI Market Growth Doubles by 2030.* Market Research Southeast Asia | Consulting Firm. https://marketresearchsoutheastasia.com/insights/articles/southeast-asia-ai-market-growth-double-2030
13	*Private funding in Southeast Asia digital economy lags global level, report says | Reuters.* (n.d.). Retrieved January 22, 2026, from https://www.reuters.com/business/retail-consumer/private-funding-southeast-asia-digital-economy-lags-global-level-report-says-2025-11-11/
14	ibid

15	ibid
16	Chính phủ C. T. tin điện tử C. (n.d.). *Luật số 71/2025/QH15 của Quốc hội: Luật Công nghiệp công nghệ số.* Retrieved 22 January 2026, from http://vanban.chinhphu.vn/?pageid=27160&docid=214609&classid=1&typegroupid=3
17	Chính phủ C. T. tin điện tử C. (n.d.). *Luật số 134/2025/QH15 của Quốc hội: Luật Trí tuệ nhân tạo.* Retrieved 22 January 2026, from http://vanban.chinhphu.vn/?pageid=27160&docid=216334&classid=1&orggroupid=1
18	*Senate of the Philippines.* (n.d.). Retrieved 22 January 2026, from https://senate.gov.ph/legislative-documents/bills/594456
19	*SG Unveils Insights from World's First Technical Testing of Real World Applications of GenAI.* (n.d.). Infocomm Media Development Authority. Retrieved 22 January 2026, from https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/sg-unveils-insights-from-worlds-first-technical-testing-of-real-world-applications-of-genai
20	ibid
21	MALAYSIA - National Artificial Intelligence (AI) Action Plan 2030
22	Thirteenth Malaysia Plan 2026 - 2030
23	*Digital Ministry targets tabling AI law late next year | The Star.* (n.d.). Retrieved 22 January 2026, from https://www.thestar.com.my/news/nation/2025/10/09/digital-ministry-targets-tabling-ai-law-late-next-year
24	*Kementerian Komunikasi dan Digital.* (n.d.). Retrieved 22 January 2026, from https://www.komdigi.go.id/berita/pengumuman/detail/konsultasi-publik-buku-putih-peta-jalan-kecerdasan-artifisial-nasional-dan-konsep-pedoman-etika-kecerdasan-artifisial
25	*EU AI Act: First regulation on artificial intelligence.* (2023, August 6). Topics | European Parliament. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
26	*Kementerian Komunikasi dan Digital.* (n.d.). Retrieved 22 January 2026, from https://www.komdigi.go.id/berita/pengumuman/detail/konsultasi-publik-buku-putih-peta-jalan-kecerdasan-artifisial-nasional-dan-konsep-pedoman-etika-kecerdasan-artifisial
27	*Komdigi: AI Rules are being Drafted.* (n.d.). Retrieved 22 January 2026, from https://www.kompas.id/artikel/en-komdigi-aturan-ai-sedang-disusun
28	*Consultation Paper on Proposed Guidelines on Artificial Intelligence Risk Management for Financial Institutions.* (n.d.). Retrieved 22 January 2026, from https://www.mas.gov.sg/publications/consultations/2025/consultation-paper-on-guidelines-on-artificial-intelligence-risk-management
29	*AI Security Guidelines_Published_30092025(1).pdf.* (n.d.). NCSA Drive. Retrieved 22 January 2026, from https://drive.ncsa.or.th/s/Le37SrkAWo97q6g

30	Thailand Drafts AI Risk Management Guidelines for Financial Service Providers. (n.d.). *Tilleke & Gibbins*. Retrieved 22 January 2026, from https://www.tilleke.com/insights/thailand-drafts-ai-risk-management-guidelines-for-financial-service-providers/
31	*Digital AgTech.* (n.d.). Retrieved 1 February 2026, from https://www.mdec.my/digitalagtech https://www.digital.gov.my/en-GB/siaran/Sabah-Negeri-Kedua-Tertinggi-Di-Malaysia-Dalam-Penggunaan-Sistem-Digital-AGTECH
32	*Naga City secures ₱6.7-M grant to develop PH's first AI-powered city planning system*. (n.d.). Retrieved 22 January 2026, from https://newsbytes.ph/2025/11/20/naga-city-secures-%e2%82%b16-7-m-grant-to-develop-phs-first-ai-powered-city-planning-system/
33	*Establishing a national AI supercomputing center, making AI a universal "intelligent assistant" for the people.* (n.d.). Retrieved January 22, 2026, from https://www.vietnam.vn/en/xay-dung-trung-tam-sieu-tinh-toan-ai-quoc-gia-dua-ai-tro-thanh-tro-ly-tri-tue-pho-cap-cho-nguoi-dan
34	*National Data Center No. 1 opens in Ha Noi.* (n.d.). Retrieved January 22, 2026, from https://en.baochinhphu.vn/national-data-center-no-1-opens-in-ha-noi-111250819164321883.htm
35	*Indonesia unveils national AI roadmap.* (n.d.). Retrieved January 22, 2026, from https://govinsider.asia/intl-en/article/indonesia-unveils-national-ai-roadmap
36	*Bangkok Post—B25 billion approved for AI development.* (n.d.). Retrieved January 22, 2026, from https://www.bangkokpost.com/business/general/3078438/b25-billion-approved-for-ai-development
37	*Malaysia to reap economic benefits from Sovereign AI Cloud development.* (n.d.). Retrieved January 22, 2026, from https://www.nst.com.my/business/economy/2025/10/1294502/malaysia-reap-economic-benefits-sovereign-ai-cloud-development
38	Perdana, S., & Complex, S. P. (n.d.). *MALAYSIA DIGITAL ECONOMY BLUEPRINT.*
39	APEC Cross-Border Privacy Rules (CBPR) System. (n.d.). Infocomm Media Development Authority. Retrieved January 22, 2026, from https://www.imda.gov.sg/how-we-can-help/cross-border-privacy-rules-certification
40	*Republic Act No. 12234.* (n.d.). Retrieved 22 January 2026, from https://lawphil.net/statutes/repacts/ra2025/ra_12234_2025.html
41	*Permendikdasmen No. 13 Tahun 2025.* (n.d.). Database Peraturan | JDIH BPK. Retrieved 22 January 2026, from http://peraturan.bpk.go.id/Details/322506/permendikdasmen-no-13-tahun-2025
42	*TalentCorp and MyDIGITAL Launch MyMahir National AI Council for Industry to Accelerate Workforce Readiness.* (n.d.). Retrieved 22 January 2026, from https://www.talentcorp.com.my/resources/press-releases/talentcorp-and-mydigital-launch-mymahir-national-ai-council-for-industry-to-accelerate-workforce-readiness/
43	*Thai Academy—Thai Academy*. (n.d.). Retrieved 22 January 2026, from https://thai-academy.com/en/
44	*DepEd launches AI center for education | Department of Education.* (n.d.). Retrieved 22 January 2026, from https://www.deped.gov.ph/2025/02/20/deped-launches-ai-center-for-education/
45	*Shaping the future of quantum intelligence.* (n.d.). Retrieved 22 January 2026, from https://theedgemalaysia.com/content/advertise/shaping-the-future-of-quantum-intelligence

46	*Programme details.* (n.d.). Retrieved 22 January 2026, from https://www.disg.gov.sg/enterprise-compute-initiative/
47	Briefing, V. (2025, July 15). Vietnam Law on Personal Data Protection: Overview. *Vietnam Briefing News.* https://www.vietnam-briefing.com/news/vietnam-law-on-personal-data-protection-latest-developments-and-insights.html/
48	https://english.luatvietnam.vn, & LuatVietnam. (n.d.). *Draft Cybersecurity Law to strengthen cyberattack prevention.* LuatVietnam. Retrieved 23 January 2026, from https://english.luatvietnam.vn/legal-updates/draft-cybersecurity-law-to-strengthen-cyberattack-prevention-address-ai-risks-892-105216-article.html
49	*CSA's Cyber Essentials and Cyber Trust Marks expanded to Include Cloud Security, Artificial Intelligence and Operational Technology.* (n.d.). Cyber Security Agency of Singapore. Retrieved 23 January 2026, from https://www.csa.gov.sg/news-events/press-releases/csa-s-cyber-essentials-and-cyber-trust-marks-expanded-to-include-cloud-security--artificial-intelligence-and-operational-technology/
50	*Public Consultation—Quantum-Safe Handbook and Quantum Readiness Index.* (n.d.). Cyber Security Agency of Singapore. Retrieved 23 January 2026, from https://www.csa.gov.sg/resources/publications/quantum-safe-handbook-and-quantum-readiness-index/
51	BERNAMA. (2025, March 14). *NACSA Strengthens National Cyber Security Preparedness With NCCMP.* BERNAMA. https://bernama.com/en/news.php?id=2402253
52	*Peraturan BSSN No. 5 Tahun 2025.* (n.d.). Database Peraturan | JDIH BPK. Retrieved 22 January 2026, from http://peraturan.bpk.go.id/Details/315044/peraturan-bssn-no-5-tahun-2025
53	*BERNAMA - NACSA Finalising Malaysia's Cybersecurity Strategy 2025-2030—Digital Ministry.* (n.d.). Retrieved 22 January 2026, from https://www.bernama.com/en/news.php?id=2451273
54	*New Cyber Crime Bill and RM32 Million Boost to Tackle Scams in Malaysia.* (n.d.). Retrieved 22 January 2026, from https://fintechnews.my/54535/security/malaysia-cybersecurity-budget-2026-cyber-crime-bill-national-scam/
55	*NACSA | National Cyber Crisis Management Plan.* (n.d.). Retrieved 23 January 2026, from https://www.nacsa.gov.my/nccmp.php
56	*Malaysia: Prime Minister publishes Cybersecurity (Exemption) Order 2025 | News*. (n.d.). DataGuidance. Retrieved 22 January 2026, from https://www.dataguidance.com/news/malaysia-prime-minister-publishes-cybersecurity
57	DICT Mandates ISO Cybersecurity Standards for Telecom Firms. (2025, September 30). *eLegal Philippines*. https://elegal.ph/dict-mandates-iso-cybersecurity-standards-for-telecom-firms/
58	https://english.luatvietnam.vn, & LuatVietnam. (n.d.). *Draft Cybersecurity Law to strengthen cyberattack prevention*. LuatVietnam. Retrieved 23 January 2026, from https://english.luatvietnam.vn/legal-updates/draft-cybersecurity-law-to-strengthen-cyberattack-prevention-address-ai-risks-892-105216-article.html
59	Online N. D. (2025, February 28). *Cybersecurity protection function handed over to Public Security Ministry*. Nhan Dan Online. https://en.nhandan.vn/cybersecurity-protection-function-handed-over-to-public-security-ministry-post144665.html

60	Briefing, V. (2025, July 15). Vietnam Law on Personal Data Protection: Overview. *Vietnam Briefing News*. https://www.vietnam-briefing.com/news/vietnam-law-on-personal-data-protection-latest-developments-and-insights.html/
61	*Law on E-Transactions.* (n.d.). Vietnamlawmagazine.Vn. Retrieved 23 January 2026, from https://vietnamlawmagazine.vn/law-on-e-transactions-71419.html
62	*Provisions in the Cybersecurity (Amendment) Act to Come Into Force on 31 October 2025.* (n.d.). Cyber Security Agency of Singapore. Retrieved 23 January 2026, from https://www.csa.gov.sg/news-events/press-releases/provisions-in-the-cybersecurity--amendment--act-to-come-into-force-on-31-october-2025/
63	*Public Consultation on Amendments to the Public Sector (Governance) Act.* (n.d.). REACH (Reaching Everyone for Active Citizenry @ Home). Retrieved 23 January 2026, from https://www.reach.gov.sg/latest-happenings/public-consultation-pages/2025/public-consultation-on-amendments-to-the-public-sector--governance--act/
64	*The Royal Decree on Measures for Prevention and Suppression of Technology Crimes B.E. 2566 (2023) and the Draft Cyber Security Maintenance Act. : มหาวิทยาลัยพะเยา.* (n.d.). Retrieved 23 January 2026, from https://www.up.ac.th/NewsRead.aspx?itemID=34578
65	*Protection from Scams Act 2025—Singapore Statutes Online.* (n.d.). Retrieved 23 January 2026, from https://sso.agc.gov.sg/Act/PSA2025from https://sso.agc.gov.sg/Act/PSA2025
66	Aureada, Y. (2025, September 7). *Understanding the Anti-Financial Account Scamming Act (AFASA)*. Aureada CPA Law Firm. https://www.aureadalaw.com/post/understanding-the-anti-financial-account-scamming-act-afasa
67	*E-Conomy SEA 2023 report: Southeast Asia's digital economy hits $100 billion in revenue. Businesses now focusing on boosting profitability; widening digital participation remains critical | Bain & Company.* (n.d.). Retrieved 22 January 2026, from https://www.bain.com/about/media-center/press-releases/sea/e-conomy-sea-2025/
68	ibid
69	ibid
70	*From protests to politics: How gig workers are reshaping Southeast Asia's power balance—CNA*. (n.d.). Retrieved 22 January 2026, from https://www.channelnewsasia.com/asia/indonesia-delivery-riders-grab-gojek-southeast-asia-malaysia-thailand-protests-political-force-5368301
71	tfgi.editor. (2022, June 13). MSMEs Critical for a Greener Future in Southeast Asia. *Tech For Good Institute*. https://techforgoodinstitute.org/blog/perspectives/msmes-critical-for-a-greener-future-in-southeast-asia/
72	ASEAN Economic Community Council Statement on the Substantial Conclusion of the ASEAN DEFA Negotiations. (2025, October 24). *ASEAN Main Portal.* https://asean.org/asean-economic-community-council-statement-on-the-substantial-conclusion-of-the-asean-defa-negotiations/ Portal. https://asean.org/asean-economic-community-council-statement-on-the-substantial-conclusion-of-the-asean-defa-negotiations/

73	Digital Economy Framework Agreement (DEFA): ASEAN to leap forward its digital economy and unlock US$2 Tn by 2030. (2023, August 19). *ASEAN Main Portal*. https://asean.org/asean-defa-study-projects-digital-economy-leap-to-us2tn-by-2030/ary 2026, from https://www.dataguidance.com/news/malaysia-online-safety-act-enters-effect
74	ASEAN takes major step toward landmark digital economy pact | World Economic Forum. (n.d.). Retrieved 22 January 2026, from https://www.weforum.org/stories/2025/10/asean-defa-digital-economy-pact-negotiations/
75	*Malaysia: Online Safety Act enters into effect | News.* (n.d.). DataGuidance. Retrieved 22 January 2026, from https://www.dataguidance.com/news/malaysia-online-safety-act-enters-effect
76	Post, T. J. (n.d.). *Indonesia to start restricting children's social media access in 2026.* Retrieved 22 January 2026, from https://asianews.network/indonesia-to-start-restricting-childrens-social-media-access-in-2026/
77	*New Online Safety Code of Practice for App Distribution Services Enhances Protection for Singapore Users.* (n.d.). Retrieved 22 January 2026, from https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/online-safety-code-of-practice-for-app-distribution-services
78	Thailand Establishes 24-Hour Takedown Obligation for Social Media Platforms. (n.d.). *Tilleke & Gibbins*. Retrieved 22 January 2026, from https://www.tilleke.com/insights/thailand-establishes-24-hour-takedown-obligation-for-social-media-platforms/
79	*Protection from Scams Act 2025—Singapore Statutes Online.* (n.d.). Retrieved 22 January 2026, from https://sso.agc.gov.sg/Act/PSA2025
80	Thailand Amends Emergency Decree on Technology Crime. (n.d.). *Tilleke & Gibbins*. Retrieved 22 January 2026, from https://www.tilleke.com/insights/thailand-amends-emergency-decree-on-technology-crime/
81	Thailand Introduces New Obligations for Online Marketplaces. (n.d.). *Tilleke & Gibbins*. Retrieved 22 January 2026, from https://www.tilleke.com/insights/thailand-introduces-new-obligations-for-online-marketplaces/
82	Chính phủ C. T. tin điện tử C. (n.d.). *Luật số 122/2025/QH15 của Quốc hội: Luật Thương mại điện tử.* Retrieved 22 January 2026, from http://vanban.chinhphu.vn/?pageid=27160&docid=216503&classid=1&orggroupid=1
83	*Republic Act No. 11967 or the Internet Transactions Act of 2023 | DTI ECommerce.* (n.d.). Retrieved 22 January 2026, from https://ecommerce.dti.gov.ph/internet-transactions-act-of-2023/
84	*Manila Bulletin—DTI to mandate digital trustmark for all online businesses.* (n.d.). Retrieved 22 January 2026, from https://mb.com.ph/2025/09/12/dti-to-mandate-digital-trustmark-for-all-online-businesses
85	*Parlementaria Terkini—JDIH SETJEN DPR.* (n.d.). Retrieved 22 January 2026, from https://jdih.dpr.go.id/berita/detail/id/60969/t/RUU+Perlindungan+Konsumen+Akan+Hadirkan+Keseimbangan+Kepentingan+dan+Kepastian+Hukum
86	*PMK 37 / 2025—Indonesia E-Commerce Income Tax Regulation | Alvarez & Marsal | Management Consulting | Professional Services.* (n.d.). Retrieved 22 January 2026, from https://www.alvarezandmarsal.com/thought-leadership/pmk-37-2025-new-indonesia-regulation-on-withholding-of-article-22-income-tax-by-e-commerce-platforms

87	Bureau of Internal Revenue. (n.d.). Retrieved 22 January 2026, from https://www.bir.gov.ph/vat-on-ds
88	Chính phủ C. T. tin điện tử C. (n.d.). *Luật số 67/2025/QH15 của Quốc hội: Luật Thuế thu nhập doanh nghiệp.* Retrieved 22 January 2026, from http://vanban.chinhphu.vn/?pageid=27160&docid=214607&classid=1&typegroupid=3
89	Chính phủ C. T. tin điện tử C. (n.d.). *Luật số 122/2025/QH15 của Quốc hội: Luật Thương mại điện tử.* Retrieved 22 January 2026, from http://vanban.chinhphu.vn/?pageid=27160&docid=216503&classid=1&orggroupid=1
90	*TCCT to introduce new rules to curb e-commerce giants, protect small retailers*. (n.d.). Retrieved 22 January 2026, from https://www.nationthailand.com/business/economy/40055547
91	*Enhanced E-commerce Guidelines to Safeguard Consumer Trust and Foster Competitive E-commerce Market.* (n.d.). Competition and Consumer Commission of Singapore. Retrieved 22 January 2026, from https://www.ccs.gov.sg/media-and-events/newsroom/announcements-and-media-releases/enhanced-e-commerce-guidelines-to-safeguard-consumer-trust-and-foster-competitive-e-commerce-market/
92	*Official Portal of The Parliament of Malaysia—Bills.* (n.d.). Retrieved 22 January 2026, from https://www.parlimen.gov.my/bills-dewan-rakyat.html?uweb=dr& Gig Workers Bill 2025
93	*Platform Workers Act: What it covers.* (n.d.). Retrieved 22 January 2026, from https://www.mom.gov.sg/employment-practices/platform-workers-act/what-it-covers
94	ASEAN Digital Masterplan 2025. (n.d.). *ASEAN Main Portal*. Retrieved 2 February 2026, from https://asean.org/book/asean-digital-masterplan-2025/
95	ASEAN Economic Community Council Statement on the Substantial Conclusion of the ASEAN DEFA Negotiations. (2025, October 24). *ASEAN Main Portal*. https://asean.org/asean-economic-community-council-statement-on-the-substantial-conclusion-of-the-asean-defa-negotiations/
96	ร่าง พรบ ไซเบอร์ (๒๗ ตค ๖๘).pdf. (n.d.). NCSA Drive. Retrieved 30 January 2026, from https://drive.ncsa.or.th/s/QNpzAw3QT8QDpLn
97	*Republic Act No. 12234.* (n.d.). Retrieved 22 January 2026, from https://lawphil.net/statutes/repacts/ra2025/ra_12234_2025.html
98	*Republic Act No. 12252.* (n.d.). Retrieved 2 February 2026, from https://lawphil.net/statutes/repacts/ra2025/ra_12252_2025.html
99	*National Data Center No. 1 opens in Ha Noi.* (n.d.). Retrieved January 22, 2026, from https://en.baochinhphu.vn/national-data-center-no-1-opens-in-ha-noi-111250819164321883.htm
100	*Quyết định 20/2025/QĐ-TTg danh mục dữ liệu quan trọng, dữ liệu cốt lõi.* (n.d.). Retrieved 30 January 2026, from https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Decision-20-2025-QD-TTg-issuance-of-the-list-of-important-data-and-core-data-667084.aspx?tab=1
101	Chính phủ C. T. tin điện tử C. (n.d.). *Luật số 122/2025/QH15 của Quốc hội: Luật Thương mại điện tử.* Retrieved 22 January 2026, from http://vanban.chinhphu.vn/?pageid=27160&docid=216503&classid=1&orggroupid=1

102	*DJED.* (n.d.). Retrieved 22 January 2026, from https://djed.komdigi.go.id/about/aju-widya-sari
103	*Kementerian Komunikasi dan Digital.* (n.d.). Retrieved 22 January 2026, from https://www.komdigi.go.id/profil/daftar-pejabat
104	*Shaping the future of quantum intelligence.* (n.d.). Retrieved 22 January 2026, from https://theedgemalaysia.com/content/advertise/shaping-the-future-of-quantum-intelligence
105	HARI ISNIN : 25 OGOS 2025 MESYUARAT KEDUA, PENGGAL KEEMPAT PARLIMEN KELIMA BELAS 2025
106	baochinhphu.vn. (2025, March 22). *Ra mắt Hiệp hội Dữ liệu Quốc gia.* baochinhphu.vn. https://baochinhphu.vn/ra-mat-hiep-hoi-du-lieu-quoc-gia-102250322102622812.htm
107	thuvienphapluat.vn. (2025, June 19). *Quyết định 728/QĐ-BKHCN 2025 chức năng Trung tâm Dữ liệu quốc gia về khoa học và công nghệ.* THƯ VIỆN PHÁP LUẬT. https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Quyet-dinh-728-QD-BKHCN-2025-chuc-nang-Trung-tam-Du-lieu-quoc-gia-ve-khoa-hoc-va-cong-nghe-655330.aspxliệu quốc gia về khoa học và công nghệ. THƯ VIỆN PHÁP LUẬT.
108	thuvienphapluat.vn. (2025, June 19). *Quyết định 728/QĐ-BKHCN 2025 chức năng Trung tâm Dữ liệu quốc gia về khoa học và công nghệ.* THƯ VIỆN PHÁP LUẬT. https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Quyet-dinh-728-QD-BKHCN-2025-chuc-nang-Trung-tam-Du-lieu-quoc-gia-ve-khoa-hoc-va-cong-nghe-655330.aspx
109	DepEd launches AI center for education. (2025, February 20). *Department of Education*. https://www.deped.gov.ph/2025/02/20/deped-launches-ai-center-for-education/
110	*Kementerian Komunikasi dan Digital.* (n.d.). Retrieved 22 January 2026, from https://www.komdigi.go.id/berita/pengumuman/detail/konsultasi-publik-buku-putih-peta-jalan-kecerdasan-artifisial-nasional-dan-konsep-pedoman-etika-kecerdasan-artifisial
111	*Coordinating Minister for Human Development and Culture Leads the First Meeting of the AI Talent Task Force, Encouraging Policy Harmonization and Ecosystem Strengthening | Coordinating Ministry for Human Development and Culture.* (n.d.). Retrieved 22 January 2026, from https://www.kemenkopmk.go.id/pimpin-temu-perdana-gugus-tugas-talenta-ai-menko-pmk-dorong-harmonisasi-kebijakan-dan-penguatan
112	*Perpres No. 83 Tahun 2025.* (n.d.). Database Peraturan | JDIH BPK. Retrieved 22 January 2026, from http://peraturan.bpk.go.id/Details/329002/perpres-no-83-tahun-2025
113	*TalentCorp and MyDIGITAL Launch MyMahir National AI Council for Industry to Accelerate Workforce Readiness.* (n.d.). Retrieved 22 January 2026, from https://www.talentcorp.com.my/resources/press-releases/talentcorp-and-mydigital-launch-mymahir-national-ai-council-for-industry-to-accelerate-workforce-readiness/
114	*Azalina: Govt to establish Online Safety Committee under new Act to address harmful content, protect users | Malay Mail.* (n.d.). Retrieved 22 January 2026, from https://www.malaymail.com/news/malaysia/2025/11/13/azalina-govt-to-establish-online-safety-committee-under-new-act-to-address-harmful-content-protect-users/198272
115	*Gig Workers Bill passed in Dewan Negara.* (n.d.). Retrieved 22 January 2026, from https://www.nst.com.my/news/nation/2025/09/1272694/gig-workers-bill-passed-dewan-negara
116	*Thailand establishes National AI Committee to boost competitiveness.* (2025, April 3). Nationthailand. https://www.nationthailand.com/business/tech/40048295

117	*Thailand Launches National Committee to Tackle Cybercrime.* (n.d.). Retrieved 22 January 2026, from https://thailand.prd.go.th/en/content/category/detail/id/2078/iid/432955
118	xaydungchinhsach.chinhphu.vn. (2025, January 13). *Lập BCĐ về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số.* xaydungchinhsach.chinhphu.vn. https://xaydungchinhsach.chinhphu.vn/thanh-lap-ban-chi-dao-trung-uong-ve-phat-trien-khoa-hoc-cong-nghe-doi-moi-sang-tao-va-chuyen-doi-so-119250113123121466.htm
119	Chính phủ C. T. tin điện tử C. (n.d.). *Quyết định số 2319/QĐ-TTg của Thủ tướng Chính phủ: Thành lập Ban Chỉ đạo quốc gia về dữ liệu.* Retrieved 22 January 2026, from http://vanban.chinhphu.vn/?pageid=27160&docid=215666
120	*What is the Online Safety (Relief and Accountability) Bill (OSRA)? | gov.sg.* (n.d.). Retrieved 22 January 2026, from https://www.gov.sg/explainers/parliament-nov2025/
121	*The historic reshuffle of Vietnam's administrative divisions.* (n.d.). Retrieved 22 January 2026, from https://vietnamnet.vn/en/the-historic-reshuffle-of-vietnam-s-administrative-divisions-2475007.html
122	*PBBM signs law reorganizing NEDA into new department.* (n.d.). Retrieved 22 January 2026, from http://www.pids.gov.ph/details/news/in-the-news/pbbm-signs-law-reorganizing-neda-into-new-department
123	*DTU di setiap kementerian, perkukuh agenda pendigitalan sektor awam—Malaysia MADANI.* (n.d.). Retrieved 22 January 2026, from https://malaysiamadani.gov.my/2025/12/dtu-di-setiap-kementerian-perkukuh-agenda-pendigitalan-sektor-awam/
124	*CCCS Expands Consumer Protection Mandate. (n.d.). Competition and Consumer Commission of Singapore*. Retrieved 22 January 2026, from https://www.ccs.gov.sg/media-and-events/newsroom/announcements-and-media-releases/cccs-expands-consumer-protection-mandate/
125	*Digital Economy Framework Agreement (DEFA): ASEAN to leap forward its digital economy and unlock US$2 Tn by 2030—ASEAN Main Portal*. (n.d.). Retrieved 22 January 2026, from https://asean.org/asean-defa-study-projects-digital-economy-leap-to-us2tn-by-2030/
126	ASEAN Economic Community Council Statement on the Substantial Conclusion of the ASEAN DEFA Negotiations. (2025, October 24). *ASEAN Main Portal*. https://asean.org/asean-economic-community-council-statement-on-the-substantial-conclusion-of-the-asean-defa-negotiations/
127	*Digital Economy Framework Agreement (DEFA): ASEAN to leap forward its digital economy and unlock US$2 Tn by 2030—ASEAN Main Portal.* (n.d.). Retrieved 22 January 2026, from https://asean.org/asean-defa-study-projects-digital-economy-leap-to-us2tn-by-2030/
128	theinvestor.vn. (n.d.). *Malaysia to push for conclusion of ASEAN Digital Economy Framework Agreement*. Retrieved 22 January 2026, from https://theinvestor.vn/malaysia-to-push-for-conclusion-of-asean-digital-economy-framework-agreement-d16706.html
129	Pascual, J. (2025, November 25). *DTI shares economic deliverables for ASEAN 2026 | ABS-CBN News.* ABS-CBN. https://www.abs-cbn.com/news/business/2025/11/25/dti-shares-economic-deliverables-for-asean-2026-1129
130	*Ekspansi QRIS Lintas Negara, Sebaran dalam 9 Negara per Agustus 2025.* (n.d.). Retrieved 22 January 2026, from https://qris.interactive.co.id/homepage/blog-detail.php?lang=id&page=MjE4-ekspansi-qris-lintas-negara-sebaran-dalam-9-negara-per-agustus-2025
131	BERNAMA. (2025, February 12). *Unlocking ASEAN's Digital Trade With Digital Business Identity*. BERNAMA. https://asean.bernama.com/news.php?id=2497863

132	ASEAN. (2025). *Public Summary of Implementation Roadmap to Establish Regionally Comparable and Recognised UBIN in ASEAN*. https://asean.org/wp-content/uploads/2025/04/Public-Summary-of-Implementation-Roadmap-to-Establish-Regionally-Comparable-and-Recognised-UBIN-in-ASEAN-1.pdf
133	*ASEAN's Next Trade Breakthrough: Accelerating Cross-Border Growth Through Interoperable Identity - Home | ASEAN-BAC*. (n.d.). Retrieved 2 February 2026, from https://asean-bac.org/news-and-press-releases/asean%E2%80%99s-next-trade-breakthrough-accelerating-cross-border-growth-through-interoperable-identity
134	Declaration on the Establishment of an ASEAN AI Safety Network (ASEAN AI SAFE). (2025, October 26). *ASEAN Main Portal.* https://asean.org/declaration-on-the-establishment-of-an-asean-ai-safety-network-asean-ai-safe/
135	Thailand unveils AI ethics centre, pledges major investment at UNESCO forum. (2025, June 25). Nationthailand. https://www.nationthailand.com/business/tech/40051737
136	*Homepage—The United Nations Convention.* (n.d.). Retrieved 22 January 2026, from https://hanoiconvention.org/
137	ASEAN Economic Community Council Statement on the Substantial Conclusion of the ASEAN DEFA Negotiations. (2025, October 24). *ASEAN Main Portal.* https://asean.org/asean-economic-community-council-statement-on-the-substantial-conclusion-of-the-asean-defa-negotiations/
138	Indonesia chapter of Global Anti-Scam Alliance launched to combat rising digital scams and protect consumers. (n.d.). Retrieved 2 February 2026, from https://newsroom.mastercard.com/news/ap/en/newsroom/press-releases/en/2025/indonesia-chapter-of-global-anti-scam-alliance-launched-to-combat-rising-digital-scams-and-protect-consumers/
139	Amojelar, D. G. (2025, October 5). Globe Telecom steps up global partnerships against online scams. *Manila Standard*. https://manilastandard.net/?p=314651438
140	*Nexus Global Payments – Fast. Efficient. Safe.* (n.d.). Nexus Global Payments. Retrieved 2 February 2026, from https://www.nexusglobalpayments.org/
141	*Kementerian Komunikasi dan Digital.* (n.d.). Retrieved 22 January 2026, from https://www.komdigi.go.id/berita/pengumuman/detail/konsultasi-publik-buku-putih-peta-jalan-kecerdasan-artifisial-nasional-dan-konsep-pedoman-etika-kecerdasan-artifisial
142	*Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023.* (n.d.). Retrieved 1 February 2026, from https://jdih.komdigi.go.id/produk_hukum/view/id/883/t/surat+edaran+menteri+komunikasi+dan+informatika+nomor+9+tahun+2023
143	*Komdigi: AI Rules are being Drafted.* (n.d.). Retrieved 22 January 2026, from https://www.kompas.id/artikel/en-komdigi-aturan-ai-sedang-disusun
144	*Permendikdasmen No. 13 Tahun 2025*. (n.d.). Database Peraturan | JDIH BPK. Retrieved 22 January 2026, from http://peraturan.bpk.go.id/Details/322506/permendikdasmen-no-13-tahun-2025
145	*Permendikdasmen No. 12 Tahun 2025.* (n.d.). Database Peraturan | JDIH BPK. Retrieved 1 February 2026, from http://peraturan.bpk.go.id/Details/322494/permendikdasmen-no-12-tahun-2025
146	*Perpres No. 83 Tahun 2025.* (n.d.). Database Peraturan | JDIH BPK. Retrieved 22 January 2026, from http://peraturan.bpk.go.id/Details/329002/perpres-no-83-tahun-2025

147	*Permenkomdigi No. 6 Tahun 2025.* (n.d.). Database Peraturan | JDIH BPK. Retrieved 1 February 2026, from http://peraturan.bpk.go.id/Details/317343/permenkomdigi-no-6-tahun-2025
148	*Peraturan BSSN No. 5 Tahun 2025.* (n.d.). Database Peraturan | JDIH BPK. Retrieved 22 January 2026, from http://peraturan.bpk.go.id/Details/315044/peraturan-bssn-no-5-tahun-2025
149	*Permenpar No. 2 Tahun 2025.* (n.d.). Database Peraturan | JDIH BPK. Retrieved 1 February 2026, from http://peraturan.bpk.go.id/Details/329094/permenpar-no-2-tahun-2025
150	*Permenekraf No. 5 Tahun 2025.* (n.d.). Database Peraturan | JDIH BPK. Retrieved 1 February 2026, from http://peraturan.bpk.go.id/Details/328984/permenekraf-no-5-tahun-2025
151	Online, H. (n.d.). *Peraturan Presiden Nomor 68 Tahun 2025—Pusat Data Hukumonline*. Hukumonline.Com. Retrieved 1 February 2026, from https://www.hukumonline.com/pusatdata/detail/lt686b7bb4ce90f/peraturan-presiden-nomor-68-tahun-2025/document/
152	*Prabowo Tunjuk PT Jalin Sebagai Pemungut Pajak Digital Luar Negeri.* (n.d.). Retrieved 1 February 2026, from https://www.cnnindonesia.com/ekonomi/20250711135126-532-1249596/prabowo-tunjuk-pt-jalin-sebagai-pemungut-pajak-digital-luar-negeri
153	*PMK No. 50 Tahun 2025.* (n.d.). Database Peraturan | JDIH BPK. Retrieved 1 February 2026, from http://peraturan.bpk.go.id/Details/326291/pmk-no-50-tahun-2025
154	*Peraturan BI No. 4 Tahun 2025.* (n.d.). Database Peraturan | JDIH BPK. Retrieved 1 February 2026, from http://peraturan.bpk.go.id/Details/317896/peraturan-bi-no-4-tahun-2025
155	*Proyek Garuda: Menavigasi Arsitektur Rupiah Digital.* (n.d.). Retrieved 1 February 2026, from https://www.bi.go.id/id/rupiah/digital-rupiah/default.aspx
156	ibid
157	*QRIS Cross-Border Expansion, Distribution in 9 Countries by August 2025.* (n.d.). Retrieved 1 February 2026, from https://qris.interactive.co.id/homepage/blog-detail.php?lang=id&page=M-jE4-ekspansi-qris-lintas-negara-sebaran-dalam-9-negara-per-agustus-2025
158	Hukumonline. (n.d.). *Hukumonline Pro - Kerangka OJK Baru Perketat Kepatuhan Pihak Utama: Pelanggaran Prinsip Syariah Kini Dapat Memicu Penilaian Kembali. hukumonline.com.* Retrieved 1 February 2026, from https://pro.hukumonline.com/a/lt687ef6ed00c91/kerangka-ojk-baru-perketat-kepatuhan-pihak-utama--pelanggaran-prinsip-syariah-kini-dapat-memicu-penilaian-kembali
159	Penerapan Program Anti Pencucian Uang, Pencegahan Pendanaan Terorisme, dan Pencegahan Pendanaan Proliferasi Senjata Pemusnah Massal bagi Pedagang Aset Keuangan Digital
160	Kementerian Komunikasi dan Digital. (n.d.). Retrieved 22 January 2026, from https://www.komdigi.go.id/berita/pengumuman/detail/konsultasi-publik-buku-putih-peta-jalan-kecerdasan-artifisial-nasional-dan-konsep-pedoman-etika-kecerdasan-artifisial
161	*Coordinating Minister for Human Development and Culture Leads the First Meeting of the AI Talent Task Force, Encouraging Policy Harmonization and Ecosystem Strengthening | Coordinating Ministry for Human Development and Culture.* (n.d.). Retrieved 22 January 2026, from https://www.kemenkopmk.go.id/pimpin-temu-perdana-gugus-tugas-talenta-ai-menko-pmk-dorong-harmonisasi-kebijakan-dan-penguatan
162	Isdarmadji, N. Q. (2025, July 14). *Kolaborasi Jadi Kunci Menuju Pemerintah Digital Berorientasi Kepuasan Pengguna. Kementerian Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi*. https://www.menpan.go.id/site/berita-terkini/kolaborasi-jadi-kunci-menuju-pemerintah-digital-berorientasi-kepuasan-pengguna

163	DJED. (n.d.). Retrieved 22 January 2026, from https://djed.komdigi.go.id/about/aju-widya-sari
164	Ministry of Communication and Digital. (n.d.). Retrieved 27 January 2026, from https://www.komdigi.go.id/profil/daftar-pejabat
165	Permen PANRB No. 1 Tahun 2025. (n.d.). Database Peraturan | JDIH BPK. Retrieved 27 January 2026, from http://peraturan.bpk.go.id/Details/314682
166	Kementerian Koordinator Bidang Perekonomian Republik Indonesia. (n.d.). Retrieved 27 January 2026, from https://www.ekon.go.id/struktur-organisasi/6/deputi-iii-perniag-aan-dan-ekonomi-digital
167	ASEAN Economic Community Council Statement on the Substantial Conclusion of the ASEAN DEFA Negotiations. (2025, October 24). ASEAN Main Portal. https://asean.org/asean-economic-community-council-statement-on-the-substantial-conclusion-of-the-asean-defa-negotiations/
168	Framework for Negotiating ASEAN Digital Economy Framework Agreement
169	Peraturan OJK No. 3 Tahun 2024. (n.d.). Database Peraturan | JDIH BPK. Retrieved 1 February 2026, from http://peraturan.bpk.go.id/Details/301678/peraturan-ojk-no-3-tahun-2024
170	RI, S. D. (n.d.). Parlementaria Terkini—JDIH SETJEN DPR. Retrieved 22 January 2026, from https://jdih.dpr.go.id/berita/detail/id/60969/t/RUU+Perlindungan+Konsumen+Akan+Hadirkan+Keseimbangan+Kepentingan+dan+Kepastian+Hukum
171	Presidential Regulation 68/2025: Reforming VAT Collection for Overseas Digital Vendors. (2025, August 11). Alvarez & Marsal | Management Consulting | Professional Services. https://www.alvarezandmarsal.com/thought-leadership/presidential-regulation-68-2025-reforming-vat-collection-for-overseas-digital-vendors
172	UU No. 1 Tahun 2024. (n.d.). Database Peraturan | JDIH BPK. Retrieved 1 February 2026, from http://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024
173	QRIS Cross-Border Expansion, Distribution in 9 Countries by August 2025. (n.d.). Retrieved 1 February 2026, from https://qris.interactive.co.id/homepage/blog-detail.php?lang=id&page=MjE4-ekspansi-qris-lintas-negara-sebaran-dalam-9-negara-per-agustus-2025
174	Proyek Garuda: Menavigasi Arsitektur Rupiah Digital. (n.d.). Retrieved 1 February 2026, from https://www.bi.go.id/id/rupiah/digital-rupiah/default.aspx
175	UU No. 1 Tahun 2024. (n.d.). Database Peraturan | JDIH BPK. Retrieved 1 February 2026, from http://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024
176	UU No. 27 Tahun 2022. (n.d.). Database Peraturan | JDIH BPK. Retrieved 1 February 2026, from http://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022
177	PP No. 17 Tahun 2025. (n.d.). Database Peraturan | JDIH BPK. Retrieved 1 February 2026, from http://peraturan.bpk.go.id/Details/316698/pp-no-17-tahun-2025
178	Peraturan BSSN No. 1 Tahun 2024. (n.d.). Database Peraturan | JDIH BPK. Retrieved 1 February 2026, from http://peraturan.bpk.go.id/Details/291240/peraturan-bssn-no-1-tahun-2024
179	RI, D. (n.d.). Komisi VI Dorong Penguatan Hukum Persaingan Usaha di Era Digital. DPR RI. Retrieved 1 February 2026, from https://www.dpr.go.id/kegiatan-dpr/berita/60615
180	Permendikdasmen No. 13 Tahun 2025. (n.d.). Database Peraturan | JDIH BPK. Retrieved 22 January 2026, from http://peraturan.bpk.go.id/Details/322506/permendikdasmen-no-13-tahun-2025

181	*Coordinating Minister for Human Development and Culture Leads the First Meeting of the AI Talent Task Force, Encouraging Policy Harmonization and Ecosystem Strengthening	Coordinating Ministry for Human Development and Culture.* (n.d.). Retrieved 22 January 2026, from https://www.kemenkopmk.go.id/pimpin-temu-perdana-gugus-tugas-talenta-ai-menko-pmk-dorong-harmonisasi-kebijakan-dan-penguatan
182	Thirteen Malaysia Plan 2026 - 2023
183	MALAYSIA DIGITAL ECONOMY 2024
184	*welfth Malaysia Plan, 2021-2025.* (n.d.). Retrieved 1 February 2026, from https://rmke12.ekonomi.gov.my/en/information/about-twelfth-plan
185	*Hadina. (2025, August 26). Malaysia To Become Aged Nation By 2048—Amir Hamzah*. Kementerian Kewangan. https://mof.gov.my/portal/en/news/press-citations/malaysia-to-become-aged-nation-by-2048-amir-hamzah
186	MESYUARAT KETIGA, PENGGAL KEEMPAT PARLIMEN KELIMA BELAS 2025 HARI SELASA : 2 DISEMBER 2025
187	ibid
188	*MOF: RM16 bil deployed into high-growth, high-value sectors under GEAR-uP programme as of 3Q2025.* (2025, December 3). The Edge Malaysia. https://theedgemalaysia.com/node/784560
189	AGENSI KESELAMATAN SIBER NEGARA (NACSA) ARAHAN KETUA EKSEKUTIF NO.6
190	AGENSI KESELAMATAN SIBER NEGARA (NACSA) ARAHAN KETUA EKSEKUTIF NO. 7
191	AGENSI KESELAMATAN SIBER NEGARA (NACSA) ARAHAN KETUA EKSEKUTIF NO. 8
192	AGENSI KESELAMATAN SIBER NEGARA (NACSA) ARAHAN KETUA EKSEKUTIF NO. 9
193	*Official Portal of The Parliament of Malaysia—Bills.* (n.d.). Retrieved 22 January 2026, from https://www.parlimen.gov.my/bills-dewan-rakyat.html?uweb=dr& Gig Workers Bill 2025
194	*Deputy minister says Putrajaya to include gig economy workers in Employment Act	Malay Mail.* (n.d.). Retrieved 1 February 2026, from https://www.malaymail.com/news/malaysia/2021/12/02/deputy-minister-says-putrajaya-to-include-gig-economy-workers-in-employment/2025392
195	*Gig Workers Bill passed in Dewan Negara.* (n.d.). Retrieved 22 January 2026, from https://www.nst.com.my/news/nation/2025/09/1272694/gig-workers-bill-passed-dewan-negara
196	MESYUARAT KEDUA, PENGGAL KEEMPAT PARLIMEN KELIMA BELAS 2025 HARI KHAMIS : 4 SEPTEMBER
197	*Digital Ministry targets tabling AI law late next year	The Star.* (n.d.). Retrieved 22 January 2026, from https://www.thestar.com.my/news/nation/2025/10/09/digital-ministry-targets-tabling-ai-law-late-next-year
198	HARI ISNIN : 25 OGOS 2025 MESYUARAT KEDUA, PENGGAL KEEMPAT PARLIMEN KELIMA BELAS 2025
199	*Announcements	Ministry of Digital.* (2025, December 2). https://digital.gov.my National Could Computing Policy
200	MESYUARAT KETIGA, PENGGAL KEEMPAT PARLIMEN KELIMA BELAS 2025 HARI KHAMIS : 4 DISEMBER 2025

201	ibid
202	*Rise in school bullying prompts calls for reform and comprehensive prevention in Malaysia	Malay Mail.* (n.d.). Retrieved 1 February 2026, from https://www.malaymail.com/news/malaysia/2025/09/04/rise-in-school-bullying-prompts-calls-for-reform-and-comprehensive-prevention-in-malaysia/189989
203	*Portal Rasmi Parlimen Malaysia—Rang Undang-Undang.* (n.d.). Retrieved 1 February 2026, from https://www.parlimen.gov.my/bills-dewan-rakyat.html?uweb=dr D.R. 41/2025 RANG UNDANG-UNDANG ANTIBULI 2025
204	*Malaysia to ban social media for children under 16 next year	AP News.* (n.d.). Retrieved 1 February 2026, from https://apnews.com/article/malaysia-social-media-ban-under-16-1e9e20321c-8c83c470ff7489139f10b8
205	BERNAMA - *Online Safety Act 2024 To Be Enforced Once Guidelines Are Finalised—Fahmi*. (n.d.). Retrieved 1 February 2026, from https://www.bernama.com/en/news.php/?id=2437909
206	BERNAMA - *BHEUU Welcomes Deeming Provision As Key To Enforcing Online Safety Act 2025*. (n.d.). Retrieved 22 January 2026, from https://www.bernama.com/en/news.php?id=2502966
207	*Azalina: Govt to establish Online Safety Committee under new Act to address harmful content, protect users	Malay Mail.* (n.d.). Retrieved 22 January 2026, from https://www.malaymail.com/news/malaysia/2025/11/13/azalina-govt-to-establish-online-safety-committee-under-new-act-to-address-harmful-content-protect-users/198272
208	*Malaysia takes quantum leap in cybersecurity readiness.* (n.d.). Retrieved 1 February 2026, from https://www.nst.com.my/business/corporate/2025/11/1308127/malaysia-takes-quantum-leap-cybersecurity-readiness
209	BERNAMA. (2025, March 14). NACSA Strengthens National Cyber Security Preparedness With NCCMP. BERNAMA. https://bernama.com/en/news.php?id=2402253
210	*CyberSecurity Malaysia*. (n.d.). Retrieved 1 February 2026, from https://www.cybersecurity.my/portal-main/services/post-quantum-overview
211	*Shaping the future of quantum intelligence.* (n.d.). Retrieved 22 January 2026, from https://theedgemalaysia.com/content/advertise/shaping-the-future-of-quantum-intelligence
212	*Digital AgTech*. (n.d.). Retrieved 1 February 2026, from https://www.mdec.my/digitalagtech https://www.digital.gov.my/en-GB/siaran/Sabah-Negeri-Kedua-Tertinggi-Di-Malaysia-Dalam-Penggunaan-Sistem-Digital-AGTECH
213	MESYUARAT KETIGA, PENGGAL KEEMPAT PARLIMEN KELIMA BELAS 2025 HARI RABU : 3 DISEMBER 2025
214	*TalentCorp and MyDIGITAL Launch MyMahir National AI Council for Industry to Accelerate Workforce Readiness*. (n.d.). Retrieved 22 January 2026, from https://www.talentcorp.com.my/resources/press-releases/talentcorp-and-mydigital-launch-mymahir-national-ai-council-for-industry-to-accelerate-workforce-readiness/
215	editor. (2025, December 9). DTU di setiap kementerian, perkukuh agenda pendigitalan sektor awam. Malaysia MADANI. https://malaysiamadani.gov.my/2025/12/dtu-di-setiap-kementerian-perkukuh-agenda-pendigitalan-sektor-awam/
216	MESYUARAT KETIGA, PENGGAL KEEMPAT PARLIMEN KELIMA BELAS 2025 HARI SELASA : 9 DISEMBER 2025

217	MESYUARAT KETIGA, PENGGAL KEEMPAT PARLIMEN KELIMA BELAS 2025 HARI RABU : 3 DISEMBER 2025
218	*Prepare for MyDigital ID integration	The Star.* (n.d.). Retrieved 1 February 2026, from https://www.thestar.com.my/news/nation/2025/12/13/prepare-for-mydigital-id-integration
219	*BERNAMA - Data Commission Key To Strengthening Governance And Protection—Gobind*. (n.d.). Retrieved 1 February 2026, from https://www.bernama.com/en/news.php?id=2458626
220	*Digital Ministry targets tabling AI law late next year	The Star.* (n.d.). Retrieved 22 January 2026, from https://www.thestar.com.my/news/nation/2025/10/09/digital-ministry-targets-tabling-ai-law-late-next-year
221	ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace
222	Kuala Lumpur Declaration on Safe and Responsible Use of Social Media Platforms For ASEAN
223	Vietnam+ (VietnamPlus). (2025, May 8). *Malaysia pushes for ASEAN social media safety guidelines development. Vietnam+ (VietnamPlus)*. https://en.vietnamplus.vn/malaysia-pushes-for-asean-social-media-safety-guidelines-development-post318807.vnp
224	netmore. (2025, October 28). MALAYSIA CHAMPIONS THE ASEAN AI SAFETY NETWORK TO ADVANCE AI SAFETY IN SOUTHEAST ASIA. *MyDIGITAL*. https://www.mydigital.gov.my/malaysia-champions-the-asean-ai-safety-network-to-advance-ai-safety-in-southeast-asia/
225	ASEAN Economic Community Council Statement on the Substantial Conclusion of the ASEAN DEFA Negotiations. (2025, October 24). *ASEAN Main Portal*. https://asean.org/asean-economic-community-council-statement-on-the-substantial-conclusion-of-the-asean-defa-negotiations/
226	Eng, M. C. I. (2025, August 12). *Malaysia to Establish Data Commission, Data Security Strategy—Gobind. MCI Group*. https://mcigroup.my/mci-business/malaysia-to-establish-data-commission-data-security-strategy-gobind/
227	Cigaral, I. N. P. (2025, July 3). *Philippines' 'upper middle-income' dream remains elusive.* INQUIRER.Net. https://business.inquirer.net/533807/ph-upper-middle-income-dream-elusive
228	*World Bank Open Data.* (n.d.). World Bank Open Data. Retrieved 1 February 2026, from https://data.worldbank.org
229	2024 Philippine MSME Statistics. (n.d.). *Department of Trade and Industry Philippines*. Retrieved 1 February 2026, from https://www.dti.gov.ph/dti-knowledge-hub/dti-statistics/dti-msme-statistics
230	Lo, K. (2025, August 6). Recto on all-time high 52.4M Filipinos in the labor force as of June 2025: Not just more jobs, but quality jobs are on the rise. *Department of Finance*. https://www.dof.gov.ph/recto-on-all-time-high-52-4m-filipinos-in-the-labor-force-as-of-june-2025-not-just-more-jobs-but-quality-jobs-are-on-the-rise/
231	*Philippines ICT Market Report	Industry Growth, Size & Analysis Overview. (*2026, January 2). Mordor Intelligence. https://www.mordorintelligence.com/industry-reports/philippines-ict-market
232	*Philippine digital economy balloons to P2.25 trillion	Philstar.com.* (n.d.). Retrieved 1 February 2026, from https://www.philstar.com/business/2025/05/04/2440313/philippine-digital-economy-balloons-p225-trillion
233	*Presidential Speeches—Speech by President Ferdinand R. Marcos Jr. At the Manila Tech Summit 2025*. (2025, August 26). https://pco.gov.ph/presidential-speech/speech-by-president-ferdinand-r-marcos-jr-at-the-manila-tech-summit-2025/

234	*ICT group upbeat about Marcos' plans for sector	GMA News Online.* (n.d.). Retrieved 1 February 2026, from https://www.gmanetwork.com/news/money/economy/839456/ict-group-upbeat-about-marcos-plans-for-sector/story/
235	*Presidential Speeches—Speech by President Ferdinand R. Marcos Jr. At the Manila Tech Summit 2025.* (2025, August 26). https://pco.gov.ph/presidential-speech/speech-by-president-ferdinand-r-marcos-jr-at-the-manila-tech-summit-2025/
236	*Republic Act No. 12234.* (n.d.). Retrieved 22 January 2026, from https://lawphil.net/statutes/repacts/ra2025/ra_12234_2025.html
237	*Konektadong Pinoy Bill – Arangkada Philippines.* (n.d.). Retrieved 1 February 2026, from https://arangkadaphilippines.com/konektadong-pinoy-bill/
238	[MEDIA RELEASE] Business groups applaud enactment of Konektadong Pinoy Act, look forward to full implementation. (2025, August 26). *Arangkada Philippines*. https://arangkadaphilippines.com/media-release-business-groups-applaud-enactment-of-konektadong-pinoy-act-look-forward-to-full-implementation/
239	*Republic Act No. 12252.* (n.d.). Retrieved 2 February 2026, from https://lawphil.net/statutes/repacts/ra2025/ra_12252_2025.html
240	*Republic Act No. 12254.* (n.d.). Retrieved 2 February 2026, from https://lawphil.net/statutes/repacts/ra2025/ra_12254_2025.html
241	*Republic Act No. 12289	GOVPH.* (2025, September 12). Official Gazette of the Republic of the Philippines. https://www.officialgazette.gov.ph/2025/09/12/republic-act-no-12289/
242	*Senate of the Philippines.* (n.d.). Retrieved 1 February 2026, from https://senate.gov.ph
243	Newsbytes.PH. (2025, November 20). Naga City secures ₱6.7-M grant to develop PH's first AI-powered city planning system. Newsbytes.PH. https://newsbytes.ph/2025/11/20/naga-city-secures-₱6-7-m-grant-to-develop-phs-first-ai-powered-city-planning-system/
244	National Cybersecurity Plan 2023-2028
245	NTC Memorandum Circular No. 001-01-2025 GUIDELINES ON THE MANAGEMENT OF INTERNET TRAFFIC AND REPORTING MECHANISM OF INTERNET SERVICE PROVIDERS
246	Department Administrative Order No. 25-07 series of 2025, "Implementing Rules and Regulations on the E-Commerce Philippine Trustmark"
247	*FROM NEDA TO DEPDEV: USHERING IN A NEW ERA OF STRENGTHENED ECONOMIC GOVERNANCE - Department of Economy, Planning, and Development.* (n.d.). Retrieved 1 February 2026, from https://depdev.gov.ph/fromnedatodepdev/
248	*eGovPH.* (n.d.). eGovPH. Retrieved 1 February 2026, from https://e.gov.ph
249	*GUIDE: eGov PH Super App's new features and how to use them • PhilSTAR Life.* (n.d.). Retrieved 1 February 2026, from https://philstarlife.com/news-and-views/348407-how-to-use-bagong-pilipinas-egov-ph-super-app?page=3
250	*You can now view your birth, marriage, death records online. Here's how.	Philstar.com.* (n.d.). Retrieved 1 February 2026, from https://www.philstar.com/lifestyle/2025/09/17/2473490/filipinos-can-now-view-birth-marriage-death-certificates-online-heres-how
251	*Bureau of Internal Revenue.* (n.d.). Retrieved 1 February 2026, from https://www.bir.gov.ph/vaton-ds

252	*Digital Economy Framework Agreement (DEFA): ASEAN to leap forward its digital economy and unlock US$2 Tn by 2030—ASEAN Main Portal.* (n.d.). Retrieved 22 January 2026, from https://asean.org/asean-defa-study-projects-digital-economy-leap-to-us2tn-by-2030/
253	*Homepage—The United Nations Convention.* (n.d.). Retrieved 22 January 2026, from https://hanoiconvention.org/
254	*DepEd launches AI center for education | Department of Education.* (n.d.). Retrieved 22 January 2026, from https://www.deped.gov.ph/2025/02/20/deped-launches-ai-center-for-education/
255	*DICT Cybersecurity.* (n.d.). Retrieved 1 February 2026, from https://www.facebook.com/CYBERSECgovph/posts/icymi-the-dict-cybersecurity-bureau-held-its-first-policy-consultation-on-propos/1157374463088174/
256	*DICT and House ICT Committee Lead Unified Push for Stronger Cybersecurity Law*. (n.d.). Retrieved 27 January 2026, from https://dict.gov.ph/news-and-updates/25023
257	*Advisory Guidelines for Cloud Services and Data Centres*. (n.d.). Infocomm Media Development Authority. Retrieved 1 February 2026, from https://www.imda.gov.sg/regulations-and-licences/regulations/codes-of-practice/advisory-guidelines-of-cloud-services-and-data-centres
258	*CSA's Cyber Essentials and Cyber Trust Marks expanded to Include Cloud Security, Artificial Intelligence and Operational Technology.* (n.d.). Cyber Security Agency of Singapore. Retrieved 23 January 2026, from https://www.csa.gov.sg/news-events/press-releases/csa-s-cyber-essentials-and-cyber-trust-marks-expanded-to-include-cloud-security--artificial-intelligence-and-operational-technology/
259	*Provisions in the Cybersecurity (Amendment) Act to Come Into Force on 31 October 2025.* (n.d.). Cyber Security Agency of Singapore. Retrieved 23 January 2026, from https://www.csa.gov.sg/news-events/press-releases/provisions-in-the-cybersecurity--amendment--act-to-come-into-force-on-31-october-2025/
260	*Singapore and Vietnam sign Letter of Intent to enhance cooperation in cross-border electricity trade for the ASEAN Power Grid.* (n.d.). Ministry of Trade and Industry. Retrieved 1 February 2026, from https://www.mti.gov.sg/newsroom/singapore-and-vietnam-sign-letter-of-intent-to-enhance-cooperation-in-cross-border-electricity-trade-for-the-asean-power-grid/
261	*Singapore and Indonesia sign Three Memoranda of Understanding with Indonesia on Cross-Border Electricity Trade, Carbon Capture and Storage, and Sustainable Industrial Zone.* (n.d.). Ministry of Trade and Industry. Retrieved 1 February 2026, from https://www.mti.gov.sg/newsroom/singapore-and-indonesia-sign-three-memoranda-of-understanding-with-indonesia-on-cross-border-electricity-trade--carbon-capture-and-storage--and-sustainable-industrial-zone/
262	*Commencement of the Protection From Scams Act.* (n.d.). Ministry of Home Affairs. Retrieved 1 February 2026, from https://www.mha.gov.sg/mediaroom/press-releases/commencement-of-the-protection-from-scams-act/
263	*New Online Safety Code of Practice for App Distribution Services Enhances Protection for Singapore Users.* (n.d.). Retrieved 22 January 2026, from https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/online-safety-code-of-practice-for-app-distribution-services
264	*Online Safety Assessment Report.* (n.d.). Infocomm Media Development Authority. Retrieved 1 February 2026, from https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/online-safety-assessment-report
265	*Issuance of Implementation Directive to Meta Under the Online Criminal Harms Act.* (n.d.). Ministry of Home Affairs. Retrieved 1 February 2026, from https://www.mha.gov.sg/mediaroom/press-releases/issuance-of-implementation-directive-to-meta-under-the-online-criminal-harms-act/

266	*Enhanced E-commerce Guidelines to Safeguard Consumer Trust and Foster Competitive E-commerce Market.* (n.d.). Competition and Consumer Commission of Singapore. Retrieved 22 January 2026, from https://www.ccs.gov.sg/media-and-events/newsroom/announcements-and-media-releases/enhanced-e-commerce-guidelines-to-safeguard-consumer-trust-and-foster-competitive-e-commerce-market/
267	*Transfer Of Product Safety And Legal Metrology Functions From Enterprise Singapore To The Competition And Consumer Commission Of Singapore.* (n.d.). Competition and Consumer Commission of Singapore. Retrieved 1 February 2026, from https://www.ccs.gov.sg/media-and-events/newsroom/announcements-and-media-releases/transfer-of-product-safety-and-legal-metrology-functions-from-enterprise-singapore-to-the-competition-and-consumer-commission-of-singapore/
268	*Platform Workers Act: What it covers.* (n.d.). Retrieved 22 January 2026, from https://www.mom.gov.sg/employment-practices/platform-workers-act/what-it-covers
269	*Joint press release by SPF, MAS, IMDA and GovTech on restricting access to facilities for scam mules.* (n.d.). Retrieved 1 February 2026, from https://www.mas.gov.sg/news/media-releases/2025/joint-press-release-by-spf-mas-imda-and-govtech-on-restricting-access-to-facilities-for-scam-mules
270	*MAS Clarifies Regulatory Regime for Digital Token Service Providers.* (n.d.). Retrieved 1 February 2026, from https://www.mas.gov.sg/news/media-releases/2025/mas-clarifies-regulatory-regime-for-digital-token-service-providers
271	*SG Unveils Insights from World's First Technical Testing of Real World Applications of GenAI.* (n.d.). Infocomm Media Development Authority. Retrieved 22 January 2026, from https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/sg-unveils-insights-from-worlds-first-technical-testing-of-real-world-applications-of-genai
272	ibid
273	*Programme details.* (n.d.). Retrieved 22 January 2026, from https://www.disg.gov.sg/enterprise-compute-initiative/
274	*Public Consultation on the Proposed Exemption from Manufacturer's Licensing and Product Registration Requirements for Artificial Intelligence—Software as a Medical Device Developed by Selected Public Healthcare Entities for Use in Public Healthcare.* (2025, May 19). HSA. https://www.hsa.gov.sg/announcements/public-consultation/proposedexemption-AI-SaMD
275	*New HealthX Sandbox 2.0 accelerates HealthTech Innovation.* (n.d.). Retrieved 1 February 2026, from https://www.synapxe.sg/media-releases/innovation/new-healthx-sandbox
276	*Health Information Bill—Singapore Statutes Online.* (n.d.). Retrieved 1 February 2026, from https://sso.agc.gov.sg/Bills-Supp/20-2025/Published/20251105
277	*Ethical Use of Big Data and Artificial Intelligence in Biomedical Research.* (n.d.). Bioethics Advisory Committee. Retrieved 1 February 2026, from https://www.bioethics-singapore.gov.sg/bioethics-resource/publications/bac-bdai-2025/
278	*Circular: New Patents and Trade Marks Acceleration Programmes.* (n.d.). Intellectual Property Office of Singapore. Retrieved 1 February 2026, from https://www.ipos.gov.sg/news/news-collection/circular--new-patents-and-trade-marks-acceleration-programmes/
279	*Consultation Paper on Proposed Guidelines on Artificial Intelligence Risk Management for Financial Institutions.* (n.d.). Retrieved 22 January 2026, from https://www.mas.gov.sg/publications/consultations/2025/consultation-paper-on-guidelines-on-artificial-intelligence-risk-management
280	*EU and Singapore sign landmark digital trade agreement.* (n.d.). [Text]. European Commission - European Commission. Retrieved 1 February 2026, from https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1152

281	*EFTA and Singapore sign Digital Economy Agreement—Joint communiqué	European Free Trade Association.* (n.d.). Retrieved 1 February 2026, from https://www.efta.int/media-resources/news/efta-and-singapore-sign-digital-economy-agreement-joint-communique
282	*PDPC	Three Guides Unveiled at ASEAN Digital Ministers' Meeting (ADGMIN) 2025.* (n.d.). Retrieved 1 February 2026, from https://www.pdpc.gov.sg/news-and-events/announcements/2025/01/three-guides-unveiled-at-asean-digital-ministers-meeting-(adgmin)-2025
283	*ASEAN takes major step toward landmark digital economy pact	World Economic Forum.* (n.d.). Retrieved 22 January 2026, from https://www.weforum.org/stories/2025/10/asean-defa-digital-economy-pact-negotiations/
284	*Electronic Gazette and Legislation Act 2025—Singapore Statutes Online.* (n.d.). Retrieved 1 February 2026, from https://sso.agc.gov.sg/Acts-Supp/5-2025/Published/20250211
285	Singapore Parliament passes online harms Bill after more than eight hours of debate. (2025, November 5). *The Straits Times*. https://www.straitstimes.com/singapore/politics/singapore-parliament-passes-online-harms-bill-after-more-than-eight-hours-of-debate
286	*Protection from Scams Act 2025—Singapore Statutes Online.* (n.d.). Retrieved 23 January 2026, from https://sso.agc.gov.sg/Act/PSA2025
287	*Provisions in the Cybersecurity (Amendment) Act to Come Into Force on 31 October 2025. (n.d.). Cyber Security Agency of Singapore*. Retrieved 23 January 2026, from https://www.csa.gov.sg/news-events/press-releases/provisions-in-the-cybersecurity--amendment--act-to-come-into-force-on-31-october-2025/
288	*Public Sector (Governance) (Amendment) Bill—Singapore Statutes Online.* (n.d.). Retrieved 1 February 2026, from https://sso.agc.gov.sg/Bills-Supp/22-2025/Published/20251105
289	*Second Reading Speech for Electronic Conveyancing and Other Matters Bill, Mr Murali Pillai, Senior Minister of State for Law.* (n.d.). Retrieved 1 February 2026, from https://www.mlaw.gov.sg/second-reading-speech-for-electronic-conveyancing-and-other-matters-bill-mr-murali-pillai/
290	*Joint press release by SPF, MAS, IMDA and GovTech on restricting access to facilities for scam mules.* (n.d.). Retrieved 1 February 2026, from https://www.mas.gov.sg/news/media-releases/2025/joint-press-release-by-spf-mas-imda-and-govtech-on-restricting-access-to-facilities-for-scam-mules
291	*CSA Unveils Safe App Portal Pilot.* (n.d.). Cyber Security Agency of Singapore. Retrieved 1 February 2026, from https://www.csa.gov.sg/news-events/press-releases/csa-unveils-safe-app-portal-pilot/
292	*MOU with App Defense Alliance.* (n.d.). Cyber Security Agency of Singapore. Retrieved 1 February 2026, from https://www.csa.gov.sg/news-events/press-releases/mou-with-app-defense-alliance/
293	*Plans For Establishment Of Cyber Resilience Centre To Provide Support To Organisations.* (n.d.). Cyber Security Agency of Singapore. Retrieved 1 February 2026, from https://www.csa.gov.sg/news-events/press-releases/plans-for-establishment-of-cyber-resilience-centre-to-provide-support-to-organisations/
294	*ILO and Singapore convened Global Dialogue on Digital Platform Work	International Labour Organization.* (2025, September 29). https://www.ilo.org/resource/news/ilo-and-singapore-convened-global-dialogue-digital-platform-work
295	*SME Pro-Enterprise Office.* (n.d.). Retrieved 27 January 2026, from https://www.enterprisesg.gov.sg/smepeo

296	Address concerns over AI's impact on jobs and livelihoods, and help workers adjust: PM Wong. (2025, November 23). *The Straits Times*. https://www.straitstimes.com/singapore/politics/address-concerns-over-ais-impact-on-jobs-and-livelihoods-and-help-workers-adjust-pm-lawrence-wong
297	*Bangkok Post—AI now a key feature of everyday life in Thailand.* (n.d.). Retrieved 1 February 2026, from https://www.bangkokpost.com/business/general/3089163/ai-now-a-key-feature-of-everyday-life-in-thailand
298	*ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ* (thaipoliceonline.com). (n.d.). Retrieved 1 February 2026, from https://www.thaipoliceonline.go.th/
299	*Thailand establishes National AI Committee to boost competitiveness.* (2025, April 3). Nationthailand. https://www.nationthailand.com/business/tech/40048295
300	*Thai Academy—Thai Academy.* (n.d.). Retrieved 22 January 2026, from https://thai-academy.com/en/
301	*TCCT to introduce new rules to curb e-commerce giants, protect small retailers*. (n.d.). Retrieved 22 January 2026, from https://www.nationthailand.com/business/economy/40055547
302	*ร่าง พรบ ไซเบอร์ (๒๗ ตค ๖๘).*pdf. (n.d.). NCSA Drive. Retrieved 1 February 2026, from https://drive.ncsa.or.th/s/QNpzAw3QT8QDpLn
303	*Thailand's New Website Security Standards 2025: Implications for Compliance Under the Cybersecurity Act—Formichella & Sritawat—Attorneys at Law.* (n.d.). Retrieved 1 February 2026, from https://fosrlaw.com/2025/thailand-website-security-standards-2025-cybersecurity-act-compliance/ Website Security Standard
304	*AI Security Guidelines_Published_30092025(1).pdf.* (n.d.). NCSA Drive. Retrieved 22 January 2026, from https://drive.ncsa.or.th/s/Le37SrkAWo97q6g
305	*Thailand Launches National Committee to Tackle Cybercrime.* (n.d.). Retrieved 22 January 2026, from https://thailand.prd.go.th/en/content/category/detail/id/2078/iid/432955
306	Technology-crime Decree
307	*Thailand signs the United Nations Convention against Cybercrime—กระทรวงการต่างประเทศ.* (n.d.). Retrieved 1 February 2026, from https://www.mfa.go.th/en/content/united-nations-convention-against-cybercrime-en
308	Thailand Introduces New Obligations for Online Marketplaces. (https://ratchakitcha.soc.go.th/documents/75751.pdf) (n.d.). *Tilleke & Gibbins*. Retrieved 22 January 2026, from https://www.tilleke.com/insights/thailand-introduces-new-obligations-for-online-marketplaces/
309	Thailand Issues Additional Compliance Requirements (https://ratchakitcha.soc.go.th/documents/74830.pdf) for Ride-Hailing Platforms. (n.d.). *Tilleke & Gibbins*. Retrieved 1 February 2026, from https://www.tilleke.com/insights/thailand-issues-additional-compliance-requirements-for-ride-hailing-platforms/
310	*Announcement of a List of Successful Applicants Approved by the Minister of Finance to Establish a Virtual Bank*. (n.d.). Retrieved 1 February 2026, from https://www.bot.or.th/en/news-and-media/news/news-20250619.html
311	Thailand Drafts AI Risk Management Guidelines for Financial Service Providers. (แนวนโยบายธนาคารแห่งประเทศไทย เรื่อง การบริหารจัดการความเสี่ยงของการใช้งานระบบปัญญาประดิษฐ์) (n.d.). *Tilleke & Gibbins*. Retrieved 22 January 2026, from https://www.tilleke.com/insights/thailand-drafts-ai-risk-management-guidelines-for-financial-service-providers/

312	*AIS Forges Strategic Alliance to Spearhead Thailand's 'Cyber Security Year'.* (2025, May 9). Nationthailand. https://www.nationthailand.com/pr-news/40049743
313	*Thailand unveils AI ethics centre, pledges major investment at UNESCO forum.* (n.d.). Retrieved 22 January 2026, from https://www.nationthailand.com/business/tech/40051737
314	*ถอดบทเรียนเวทีประชุมนานาชาติ สู่เส้นทาง 'ธรรมาภิบาลแพลตฟอร์มดิจิทัล' ในอาเซียน.* (n.d.). ETDA. Retrieved 1 February 2026, from https://www.etda.or.th/th/pr-news/insight_inter_forum.aspx
315	*Thailand Chairs Push to Finalise $2 Trillion ASEAN Digital Economy Pact.* (2025, October 24). Nationthailand. https://www.nationthailand.com/news/asean/40057265
316	*Kinh tế số Việt Nam đạt 18,72% GDP Quý I 2025, tăng trưởng 10% | Báo Nhân Dân điện tử.* (n.d.). Retrieved 1 February 2026, from https://nhandan.vn/ty-trong-kinh-te-so-tren-gdp-dat-khoang-1872-tiep-tuc-la-dong-luc-tang-truong-quan-trong-post898819.html
317	Bộ Khoa học và Công nghệ. (n.d.). *Kinh tế số tăng tốc, xã hội số lan tỏa: Việt Nam đẩy mạnh triển khai các chương trình trọng điểm*. Cổng Thông tin điện tử Bộ Khoa học và Công nghệ. Retrieved 1 February 2026, from https://mst.gov.vn/kinh-te-so-tang-toc-xa-hoi-so-lan-toa-viet-nam-day-manh-trien-khai-cac-chuong-trinh-trong-diem-197251118185521864.htm
318	Phương H. T. T. (2025, January 3). *Tỷ trọng về thương mại điện tử chiếm 2/3 giá trị của nền kinh tế số Việt Nam. Cổng thông tin điện tử Bộ Công Thương*. moit.gov.vn. https://moit.gov.vn/tin-tuc/hoat-dong/hoat-dong-cua-cac-don-vi/cuc-thuong-mai-dien-tu-va-kinh-te-so-to-chuc-hoi-nghi-tong-ket-cong-tac-nam-2024-va-trien-khai-nhiem-vu-nam-2025.html
319	HuongCNT. (2025, February 18). *Thương mại điện tử Việt Nam năm 2024: Những bước tiến và thách thức*. Cục Thương mại điện tử và Kinh tế số. moit.gov.vn. https://moit.gov.vn/khoa-hoc-va-cong-nghe/thuong-mai-dien-tu-viet-nam-nam-2024-nhung-buoc-tien-va-thach-thuc.html
320	*Thương mại điện tử Việt Nam 9 tháng đầu năm tăng trưởng ấn tượng.* (n.d.). Retrieved 1 February 2026, from https://laodong.vn/cong-nghe/thuong-mai-dien-tu-viet-nam-9-thang-dau-nam-tang-truong-an-tuong-1600077.ldo
321	thuvienphapluat.vn. (2026, January 1). *Luật Bảo vệ dữ liệu cá nhân năm 2025 số 91/2025/QH15.* THƯ VIỆN PHÁP LUẬT. https://thuvienphapluat.vn/van-ban/EN/Bo-may-hanh-chinh/Law-91-2025-QH15-Personal-Data-Protection/665440/tieng-anh.aspx
322	thuvienphapluat.vn. (2025, October 13). *Nghị định 194/2025/NĐ-CP hướng dẫn Luật Giao dịch điện tử về cơ sở dữ liệu quốc gia mới nhất*. THƯ VIỆN PHÁP LUẬT. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-194-2025-ND-CP-huong-dan-Luat-Giao-dich-dien-tu-ve-co-so-du-lieu-quoc-gia-663962.aspx
323	*Quyết định 20/2025/QĐ-TTg danh mục dữ liệu quan trọng, dữ liệu cốt lõi.* (n.d.). Retrieved 1 February 2026, from https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Decision-20-2025-QD-TTg-issuance-of-the-list-of-important-data-and-core-data-667084.aspx?tab=1
324	*Cổng thông tin điện tử Bộ Tài Chính.* (n.d.). Retrieved 1 February 2026, from https://mof.gov.vn/cong-nghe-thong-tin-va-chuyen-doi-so/tin-tuc-su-kien-3/sau-diem-noi-bat-trong-phat-trien-khoa-hoc-cong-nghe-doi-moi-sang-tao-6-thang-dau-nam-2025_
325	thuvienphapluat.vn. (2025, May 19). *Quyết định 06/QĐ-TTg 2022 Đề án phát triển ứng dụng dữ liệu về dân cư 2022 2025.* THƯ VIỆN PHÁP LUẬT. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-06-QD-TTg-2022-De-an-phat-trien-ung-dung-du-lieu-ve-dan-cu-2022-2025-499726.aspx
326	Thương, C. (2025, November 13). *Nhiều điểm mới trong dự thảo Luật Thương mại điện tử. Báo Công Thương.* https://media.congthuong.vn/nhieu-diem-moi-trong-du-thao-luat-thuong-mai-dien-tu-430359.media
327	*Công ước Hà Nội—Khẳng định Việt Nam điểm tựa tin cậy trong hợp tác toàn cầu chống tội phạm mạng.* (n.d.). Retrieved 1 February 2026, from https://baovephapluat.vn/kiem-sat-24h/van-de-su-kien/cong-uoc-ha-noi-khang-dinh-viet-nam-diem-tua-tin-cay-trong-hop-tac-toan-cau-chong-toi-pham-mang-186588.html

328	*Đầu năm 2025 đến nay phát hiện gần 1.500 vụ việc lừa đảo qua mạng—Tuổi Trẻ Online*. (n.d.). Retrieved 1 February 2026, from https://tuoitre.vn/dau-nam-2025-den-nay-phat-hien-gan-1-500-vu-viec-lua-dao-qua-mang-20250805220548384.htm
329	*Báo cáo Tình hình nguy cơ ATTT tại Việt Nam 6 tháng đầu năm 2025*. (2025, May 8). Công ty TNHH MTV An ninh mạng Viettel. https://viettelsecurity.com/vi/resource-report/bao-cao-tinh-hinh-nguy-co-attt-tai-viet-nam-6-thang-dau-nam-2025/
330	*Triển vọng thực thi Công ước Hà Nội tại khu vực Đông Nam Á*. (n.d.). Retrieved 1 February 2026, from https://baophapluat.vn/trien-vong-thuc-thi-cong-uoc-ha-noi-tai-khu-vuc-dong-nam-a.html
331	*The historic reshuffle of Vietnam's administrative divisions*. (n.d.). Retrieved 22 January 2026, from https://vietnamnet.vn/en/the-historic-reshuffle-of-vietnam-s-administrative-divisions-2475007.html
332	xaydungchinhsach.chinhphu.vn. (2025, January 13). *Lập BCĐ về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số*. xaydungchinhsach.chinhphu.vn. https://xaydungchinhsach.chinhphu.vn/thanh-lap-ban-chi-dao-trung-uong-ve-phat-trien-khoa-hoc-cong-nghe-doi-moi-sang-tao-va-chuyen-doi-so-119250113123121466.htm
333	Chính phủ C. T. tin điện tử C. (n.d.). *Quyết định số 2319/QĐ-TTg của Thủ tướng Chính phủ: Thành lập Ban Chỉ đạo quốc gia về dữ liệu*. Retrieved 22 January 2026, from http://vanban.chinhphu.vn/?pageid=27160&docid=215666
334	baochinhphu.vn. (2025, March 22). *Ra mắt Hiệp hội Dữ liệu Quốc gia*. baochinhphu.vn. https://baochinhphu.vn/ra-mat-hiep-hoi-du-lieu-quoc-gia-102250322102622812.htm
335	xaydungchinhsach.chinhphu.vn. (2025, March 1). *Bộ Công an thành lập Trung tâm dữ liệu quốc gia*. xaydungchinhsach.chinhphu.vn. https://xaydungchinhsach.chinhphu.vn/bo-cong-an-thanh-lap-trung-tam-du-lieu-quoc-gia-119250301202252987.htm
336	*Thành lập Liên minh Nhân lực chiến lược thực thi Nghị quyết 57-NQ/TW | Báo Nhân Dân điện tử*. (n.d.). Retrieved 1 February 2026, from https://nhandan.vn/thanh-lap-lien-minh-nhan-luc-chien-luoc-thuc-thi-nghi-quyet-57-nqtw-post877973.html
337	thuvienphapluat.vn. (2025, June 19). *Quyết định 728/QĐ-BKHCN 2025 chức năng Trung tâm Dữ liệu quốc gia về khoa học và công nghệ*. THƯ VIỆN PHÁP LUẬT. https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Quyet-dinh-728-QD-BKHCN-2025-chuc-nang-Trung-tam-Du-lieu-quoc-gia-ve-khoa-hoc-va-cong-nghe-655330.aspx
338	thuvienphapluat.vn. (2024, September 24). *Nghị quyết 52-NQ/TW 2019 chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư*. THƯ VIỆN PHÁP LUẬT. https://thuvienphapluat.vn/van-ban/Dau-tu/Nghi-quyet-52-NQ-TW-2019-chinh-sach-chu-dong-tham-gia-cuoc-Cach-mang-cong-nghiep-lan-thu-tu-425113.aspx
339	thuvienphapluat.vn. (2025, December 8). *Quyết định 942/QĐ-TTg 2021 Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số*. THƯ VIỆN PHÁP LUẬT. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-942-QD-TTg-2021-Chien-luoc-phat-trien-Chinh-phu-dien-tu-huong-toi-Chinh-phu-so-477851.aspx
340	thuvienphapluat.vn. (2025, April 19). *Quyết định 411/QĐ-TTg 2022 phê duyệt Chiến lược quốc gia phát triển kinh tế số và xã hội số*. THƯ VIỆN PHÁP LUẬT. https://thuvienphapluat.vn/van-ban/Thuong-mai/Quyet-dinh-411-QD-TTg-2022-phe-duyet-Chien-luoc-quoc-gia-phat-trien-kinh-te-so-va-xa-hoi-so-508672.aspx
341	thuvienphapluat.vn. (2025, May 13). *Nghị quyết 68-NQ/TW 2025 phát triển kinh tế tư nhân*. THƯ VIỆN PHÁP LUẬT. https://thuvienphapluat.vn/van-ban/Thuong-mai/Nghi-quyet-68-NQ-TW-2025-phat-trien-kinh-te-tu-nhan-655260.aspx

342	thuvienphapluat.vn. (2025, July 25). *Nghị quyết 193/2025/QH15 thí điểm cơ chế đặc biệt tạo đột phá phát triển khoa học công nghệ.* THƯ VIỆN PHÁP LUẬT. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-quyet-193-2025-QH15-thi-diem-co-che-dac-biet-tao-dot-pha-phat-trien-khoa-hoc-cong-nghe-644644.aspx
343	thuvienphapluat.vn. (2025, August 16). *Nghị định 94/2025/NĐ-CP Cơ chế thử nghiệm có kiểm soát trong lĩnh vực ngân hàng mới nhất.* THƯ VIỆN PHÁP LUẬT. https://thuvienphapluat.vn/van-ban/Tien-te-Ngan-hang/Nghi-dinh-94-2025-ND-CP-Co-che-thu-nghiem-co-kiem-soat-trong-linh-vuc-ngan-hang-584706.aspx
344	thuvienphapluat.vn. (2026, January 12). *Luật Khoa học, Công nghệ và Đổi mới sáng tạo 2025 số 71/2025/QH15 mới nhất*. THƯ VIỆN PHÁP LUẬT. https://thuvienphapluat.vn/van-ban/Linh-vuc-khac/Luat-Khoa-hoc-Cong-nghe-va-Doi-moi-sang-tao-2025-so-93-2025-QH15-581164.aspx
345	Chính phủ C. T. tin điện tử C. (n.d.). *Luật số 134/2025/QH15 của Quốc hội: Luật Trí tuệ nhân tạo.* Retrieved 22 January 2026, from http://vanban.chinhphu.vn/?pageid=27160&docid=216334&-classid=1&orggroupid=1
346	Chính phủ C. T. tin điện tử C. (n.d.). *Luật số 148/2025/QH15 của Quốc hội: Luật Chuyển đổi số.* Retrieved 1 February 2026, from http://vanban.chinhphu.vn/?pageid=27160&docid=216335&-classid=1&orggroupid=1
347	Dương, B. (2025, July 3). *New digital platforms to support implementation of Resolution 57 launched. VnEconomy*. https://en.vneconomy.vn/new-digital-platforms-to-support-implementation-of-resolution-57-launched.htm
348	ibid

Tech For Good Institute

www.techforgoodinstitute.org