DFDL

2026 EDITION



SERIES I

AI-RELATED DISPUTES IN ASIA

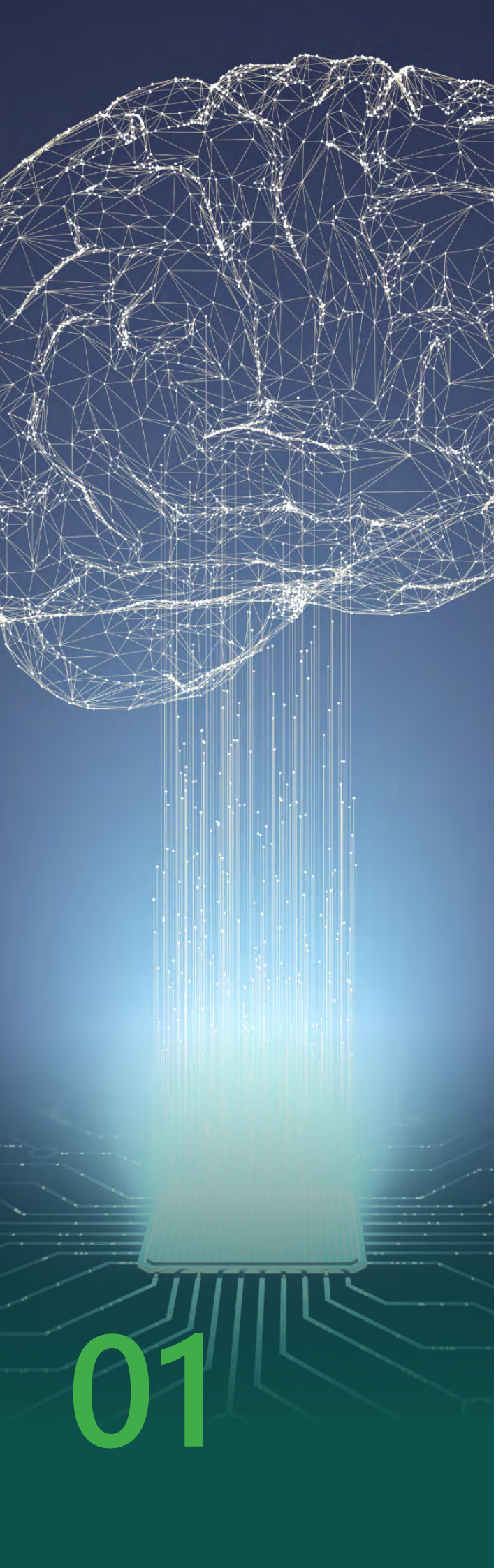
NOT SO ARTIFICIALLY INTELLIGENT

SHARE • LEARN • INFORM

WWW.DFDL.COM

CONTENTS

01	Is there a dedicated AI law in your jurisdiction? What general and sector-specific laws are currently being applied to AI issues?	3
02	Is there any AI-related law, regulation, guideline, code of practice, or soft law currently in the pipeline?	9
03	Would an AI-related dispute in your jurisdiction most likely be handled by: (a) the courts, (b) a regulator, or (c) both, depending on the issue?	14
04	In practice, are AI-related disputes more likely to be resolved through: (a) litigation, (b) regulatory enforcement, or (c) negotiated/ contractual resolution (e.g. arbitration)?	18
05	Under general civil/tort/contract principles, would liability for AI-caused harm most likely fall on: (a) the developer, (b) the deployer, (c) the end user, or (d) shared or unclear?	23
06	Does the lack of transparency in AI decision-making create a real risk that a claimant cannot prove causation/fault?	28
07	Would courts likely uphold a vendor's liability cap/indemnity for AI risks (hallucinations, erroneous outputs, bias, security failures)?	32
08	Could an AI vendor's standard limitation of liability or accuracy disclaimer be challenged as an unfair/unenforceable term under consumer or contract law?	37
09	Does characterising an AI system as a "tool" rather than a "service" change the applicable liability regime?	41
10	Is there any realistic basis under current law to treat the AI system itself (not its developer/deployer/ user) as legally responsible?	45



01

Is there a dedicated AI law in your jurisdiction? What general and sector-specific laws are currently being applied to AI issues?

BANGLADESH

No. Bangladesh has no dedicated AI law, and nothing in any statute defines "artificial intelligence". The Cyber Security Act 2026 comes closest: it creates offences that plainly assume the involvement of AI, but it does not define the term.

The Cyber Security Ordinance 2025 was the first instrument in Bangladesh to treat AI-enabled cybercrime as an offence. It was repealed and replaced by the Cyber Security Act 2026, which carries substantially the same offences forward.

What the Act does instead is punish conduct carried out with AI: hacking critical information infrastructure using AI tools or agents, and using AI-generated content for blackmail, sexual harassment and obscenity.

Regulatory activity has been directed at how the State and regulated entities use AI rather than at the vendors supplying it:

a. Bangladesh Bank issued its Cyber Security Framework, Version 1.0 (2026) in March. It binds banks, finance companies, MFS providers and payment operators, and compliance is due by 31 December 2026. It prohibits staff from entering confidential banking data into generative AI tools and requires prior institutional approval before AI is used for work purposes.

b. Telecommunications law was amended in 2025 to cover intermediaries, OTT, cloud and AI services, bringing them within the BTRC's reach.

01

CAMBODIA

No. Cambodia does not have dedicated AI legislation. AI-related issues are governed by existing legal frameworks, including the Civil Code and the laws on consumer protection, e-commerce, telecommunications, intellectual property, and cybersecurity. These frameworks may be applied to AI-related disputes depending on the circumstances.

Cambodia is actively developing its AI governance framework through several key strategies: the Cambodia Digital Government Policy 2022–2035 (January 2022), which sets out the national roadmap for digital transformation and the integration of emerging technologies into government operations; the Cambodia Digital Economy and Society Policy Framework 2021–2035 (May 2021), which establishes the policy vision for Cambodia's digital economy transition; and the Draft National Artificial Intelligence Strategy 2025–2030 (June 2025), prepared by the Ministry of Post and Telecommunications ("MPTC"), which identifies ethical and responsible AI as a national priority and contemplates a dedicated AI governance framework. In parallel, the MPTC has prepared a Draft Law on Personal Data Protection and a Draft Law on Cybersecurity, both under governmental review. Once enacted, these are expected to form part of the broader legal framework governing AI.

INDONESIA

No. Indonesia has not enacted a standalone, binding statute or regulation dedicated specifically to artificial intelligence. The principal AI-specific instrument currently in force is Circular Letter of the Minister of Communication and Informatics No. 9 of 2023 on AI Ethics, dated 19 December 2023. It is non-binding guidance rather than a regulation, and is directed mainly to companies whose business activities fall under KBLI 62015, private electronic system operators, and public electronic system operators.

The following general and sector-specific laws are currently applied to AI issues:

- Law No. 27 of 2022 on Personal Data Protection ("**PDP** Law") applies to any processing of personal data regardless of the technology used, and therefore governs AI systems to the extent they process personal data (including in training, inference and outputs).
- Law No. 11 of 2008 on Electronic Information and Transactions, as last amended by Law No. 1 of 2024 (**"ITE Law"**), governs electronic systems generally and applies to AI-related conduct, including unauthorised access, unlawful content, and platform sanctions.
- Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions (**"Government Regulation 71/2019"**), as the implementing regulation of the ITE Law, sets out electronic system and electronic data governance requirements. It requires public electronic system operators to place electronic systems and electronic data in Indonesia, while private electronic system operators may place them onshore or offshore, subject to regulatory access, supervision, and sector-specific requirements. These rules may apply to AI systems to the extent they form part of an electronic system processing Indonesian data.
- OJK's AI Governance for Indonesian Banking is non-binding guidance providing a minimum reference for banks on responsible AI development and deployment. It complements OJK's broader digital banking and technology risk framework, including the Digital Banking Transformation Blueprint and applicable OJK/SEOJK rules on digital banking, information technology, and cyber resilience.
- The 2023 Fintech AI Code of Ethics addresses algorithmic bias in digital lending.
- Press Council Regulation No. 1/Peraturan-DP/I/2025 on Guidelines for the Use of Artificial Intelligence in Journalistic Works, issued on 22 January 2025.

LAO PDR

No. Lao PDR does not have a dedicated AI law. As of mid-2026, the country has not passed any AI-specific statute, has not created a standalone AI regulator, and has not yet finalised a National AI Strategy.

General and sector-specific laws are currently being applied to AI-related issues. The most significant is the Civil Code (No.55/NA, 6 December 2018) (the **"Civil Code"**), whose Part VI (Tort, Articles 470–495) provides the general framework for civil liability, including tort liability for violations arising from wilful acts, neglect, or lack of due care (Article 472), product liability for sub-standard products or goods that damage consumers (Article 493), employer liability for acts of employees in the performance of assigned tasks (Article 486), and liability for hazardous materials (Article 494). On the criminal side, the Penal Code (No.26/NA, 17 May 2017) (the **"Penal Code"**) contains cybercrime provisions in Articles 164–173, criminalising illegal access to computer systems (Article 165), data theft from computer systems (Article 167), interference with computer systems (Article 171), modification and destruction of computer data (Articles 171 and 172), and general cybercrimes (Article 173).

Additional applicable legislation includes the Law on Electronic Data Protection (No.25/NA, 12 May 2017), which governs the collection and use of electronic personal data; the Law on Prevention and Combating Cyber Crime (No.61/NA, 15 July 2015) (the **"Cybercrime Law"**), which criminalises illegal access, data and system interference, and provides procedural and cooperation rules; and the Law on Consumer Protection (No.02/NA, 30 June 2010) (the **"Consumer Protection Law"**), which sets out general principles on consumer rights, though it is considered too general to be implemented effectively in practice.

The Law on High Technology (No.07/NA, 16 November 2021) (the **"High Technology Law"**) governs the high technology, which includes AI. The High Technology Law defines "Artificial Intelligence" only as "a branch of computer science concerned with creating systems capable of learning, reasoning, adapting, and improving their own performance over time without direct human intervention". AI activities fall under the general high-technology framework. The law applies to anyone conducting high-technology activities in Lao PDR and requires a licence from the high-technology management agency before conducting such work. AI use in services (trade, transport, finance, health, education, tourism) is expressly promoted as part of service-sector high-tech development. Technology transfer involving AI must also comply with the Law on Technology Transfer, and investment and business activity are subject to the Law on Investment Promotion and the Law on Enterprises. General prohibitions and penalties under the High Technology Law (unlicensed activity, harmful or substandard technology, misappropriation of research) apply equally to AI-related conduct.

The Law on Telecommunications (Amended) (No.05/NA, 16 November 2021) and related ICT laws also apply. Notably, the Decision on Digital Technology Business Operations (No.3643/MOTC, 29 September 2025) (the **"DTBO Decision"**), issued by the Ministry of Technology and Communications, expressly covers AI as one of the regulated digital technology business operations, requiring businesses operating in the AI sector to comply with its principles and measures. This is the first binding regulatory instrument in Lao PDR that explicitly names AI.

The Ministry of Technology and Communications serves as the central regulatory authority for telecommunications, ICT, data protection, and the digital agenda. There is no separate AI regulator.

MYANMAR

No. Myanmar has not enacted a dedicated law regulating Artificial Intelligence (**"AI"**). Existing general and sector-specific legislation nevertheless applies to AI-related activities depending on the nature and use of the AI system. The instruments most likely to be engaged are: (i) the Contract Act 1872 (**"Contract Act"**); (ii) the Penal Code (**"Penal Code"**); (iii) the Evidence Act 1872, as amended by Union Law No. 73/2015 (**"Evidence Act"**); (iv) the Consumer Protection Law of 2019 (**"CPL"**); (v) the

Electronic Transactions Law of 2004, as amended by State Administration Council Law No. 7/2021 (**"ETL"**); (vi) the Telecommunications Law of 2013 (**"TCL"**); (vii) the Cybersecurity Law of 2025 (**"CSL"**); (viii) the Law Protecting Citizens' Privacy and Security of 2017, as amended by National Defence and Security Council Law No. 1/2025 and Law No. 4/2026 (**"Privacy Law**"); (ix) the Arbitration Law of 2016 (**"Arbitration Law"**); and (x) the Code of Civil Procedure 1908 (**"CPC"**). Sector-specific statutes such as the Anti-Online Scam Law of 2026 (**"AOSL"**) may also apply where AI is used in connection with online scams or related offences. None of these instruments defines "AI" or expressly regulates AI-generated content; instead, they regulate broader concepts (information, electronic records, cyber resources, personal data, goods and services) that Myanmar courts would apply by analogy or general application to AI-related facts, as developed in Questions 3 to 10 below.

PHILIPPINES

No. The Philippines does not have a dedicated artificial intelligence (**"AI"**) law. Several AI-related bills were filed during the 19th Congress in the Philippines, but none were enacted into laws prior to the conclusion of the session. Some of these bills include House Bill (**"HB"**) Nos. 7396,[1] 7913,[2] and 7983,[3] which were all filed in 2023. These bills sought to establish a comprehensive regulatory framework, but none of them passed the committee level.

Yes, in the absence of a comprehensive regulatory framework, general and sector-specific laws apply to AI-related issues.

General laws

The following provisions of the Civil Code of the Philippines may apply to AI-related issues: *Torts and Quasi-Delicts* (Article 2176), where damage is caused to another by the use of AI with fault or negligence; *Abuse of Rights* (Articles 19, 20 and 21), where the AI is deployed in bad faith, in a manner that causes unjust harm, or to generate deepfakes; and *Contract Law* (Article 1306), where there are stipulations on who is liable, whether the developer, deployer, or end user.

The following provisions of the Revised Penal Code may also apply to AI-related issues: *Estafa/Swindling* (Article 315), if the AI was used as a tool to commit fraud; *Libel* (Articles 353 to 355), if the defamatory content was AI-generated or spread through AI; *Falsification of Documents* (Articles 171 to 176), if the AI was used to manufacture documents, which may include the possession of implements for falsification; theft (Article 308), if committed using AI,[4] just to name a few.

The relevant provisions of the Cybercrime Prevention Act may also apply where AI is used to commit illegal access, computer-related fraud, identity theft, data interference, cyber libel, or other cyber-related offences.

Sector-specific laws and regulations

The following sector-specific laws and regulations may apply to AI-related issues:

First, the Data Privacy Act (**"DPA"**) and its Implementing Rules and Regulations (**"IRR"**) apply when an AI system collects, uses, or process personal and sensitive personal information. The National Privacy Commission (**"NPC"**) issued NPC Advisory No. 2024-04 (**"Advisory"**) which outlines the guidelines on how the DPA applies to AI systems processing of personal data.

The Advisory highlights that the obligations of Personal Information Controllers and Personal Information Processors under the DPA and its IRR should be maintained - particularly transparency, accountability, fairness, accuracy, data minimization, and lawful basis for processing apply insofar as the AI systems involve the processing of personal data.[5]

More recently, on 11 August 2026, the NPC issued a notice to the public and considers the use of a real person's face or likeness to generate synthetic images

1 https://issuances-library.senate.gov.ph/bills/house-bill-no-7396-19th-congress (last accessed, 31 August 2026).

2 https://issuances-library.senate.gov.ph/bills/house-bill-no-7913-19th-congress (last accessed, 31 August 2026).

3 https://issuances-library.senate.gov.ph/bills/house-bill-no-7983-19th-congress (last accessed, 31 August 2026).

4 See for instance, *Laurel v. Abrogar*, G.R. No. 155076, 13 January 2009, where the Philippine Supreme Court *En Banc* ruled that the use of the communication facilities without the consent of the owner constitutes the crime of theft. This case may find special significance in AI-related criminal cases.

5 Section 2, NPC Advisory No. 2024-04.

or videos and the posting or sharing of that content as a form of personal data processing. Depending on the circumstances, the unauthorized AI-generated content may result in administrative, civil, or criminal liability under the DPA and related laws.[6]

Second, the Consumer Act, the Internet Transactions Act, the Electronic Commerce Act, and rules against unfair or deceptive practices may apply to AI-powered products, chatbots, recommendations, automated pricing, misleading synthetic advertising, and false representations regarding an AI system's capabilities.

Third, the Intellectual Property Code may apply to the use of copyrighted works, trademarks, patents, and trade secrets in connection with AI. The Intellectual Property Office of the Philippines ("**IPOPHL**") released its Examination Guidelines of Inventions, Utility Model, and Industrial Design Applications Relating to Artificial Intelligence which state that AI can neither be an Applicant or Inventor/Maker/Designer under the IP Code of the Philippines since these positions must be a "person" as recognized in the Philippine jurisdiction.[7]

While AI alone cannot be granted protection under the IP Code, AI-related inventions, along with Core and Applied AI Technologies, enjoys protection. Specifically, AI-related inventions are considered as a subset of "computer-implemented inventions" and therefore, must demonstrate a "technical contribution" or "technical effect" to the known art.[8] It must also contain one (1) or more independent and dependent claim.[9]

Fourth, the Commission on Elections ("**COMELEC**") released Resolution No. 11064 ("**Resolution**"), which required the transparency and disclosure requirements on the use of AI in both election propaganda and campaign materials.[10] The disclosure requirements include the fact of its use and the appropriate technology employed in order to identify its authenticity and legitimate source.[11] The failure to disclose will result to the concerned candidate or party and their respective social media campaign managers being required to explain why a complaint for violation of the guidelines should not be filed against them.[12] The Resolution therefore prohibits any AI content that does not comply with the transparency and disclosure requirements.[13]

Lastly, the Philippine Supreme Court issued A.M. No. 25-11-28-SC or the Governance Framework on the use of Human-Centered Augmented Intelligence in the Philippine Judiciary ("**Governance Framework**"), which governs the use of AI by members of the judiciary, court officials and employees, court users, and vendors, third-party contractors, or organizations engaged in the design, developments, and utilization of AI tools by or on behalf of the judiciary. Court users refer to "the members of the public, including members of the Bar, who seek relief from, transact, or interact with the courts or offices of the Judiciary, whether on their own behalf or for another person or entity".[14]

The Governance Framework emphasizes that the use of AI must be human-centered[15] and that harm must be avoided at all times.[16] Additionally, the use of AI must be understandable and intelligible to the public, and therefore, transparent.[17] At all times, the human user is accountable for any use of AI and therefore, is subject to disciplinary or ethical actions.[18] The following principles should also be observed: [1] Fairness and non-discrimination;[19] [2] Privacy and data protection;[20]

[3] Security, safety, and robustness;[21] and [4] Sustainability of resources and environmental impact.[22]

The Governance Framework also establishes a permanent AI committee which is designated as an advisory body that will provide guidance on the AI tools that will be designed and used within the

6 https://privacy.gov.ph/notice-to-the-public-use-of-real-persons-likenesses-in-ai-generated-images/?utm_source=chatgpt.com_(last accessed, 31 August 2026).

7 Section IV(3), Examination Guidelines of Inventions, Utility Model, and Industrial Design Applications Relating to Artificial Intelligence.

8 Section V(1), Examination Guidelines of Inventions, Utility Model, and Industrial Design Applications Relating to Artificial Intelligence.

9 Section VII(1.1.2), Examination Guidelines of Inventions, Utility Model, and Industrial Design Applications Relating to Artificial Intelligence.

10 Article IV, COMELEC Resolution No. 11064.

11 *Id* at Section 1, Article IV.

12 *Id* at Section 4, Article IV.

13 *Id* at Section 1(6), Article V.

14 Part I(C)(9), A.M. No. 25-11-28-SC.

15 *Id*, at Part II(1).

16 *Id*, at Part II(2).

17 *Id*, at Part II(3).

18 *Id*, at Part II(4).

19 *Id*, at Part II(5).

20 *Id*, at Part II(6).

21 *Id*, at Part II(7).

22 *Id*, at Part II(8).

Judiciary.[23] In addition to the design and use, there shall also be a systematic risk management approach throughout the life cycle of the AI systems.[24]

THAILAND

No. Thailand does not currently have a dedicated, standalone AI law in force. AI-related activities are presently governed through existing laws of general application and sector-specific regulatory frameworks.

For example, the Civil and Commercial Code may apply to contractual disputes, negligence claims, and liability arising from damage caused by AI-assisted decisions or services. The Personal Data Protection Act (PDPA) may apply where AI systems collect, process, profile, or otherwise use personal data. The Cybersecurity Act and related regulations may be relevant where AI systems create cybersecurity risks or are involved in incidents affecting critical information infrastructure. Depending on the circumstances, AI-related conduct may also be subject to laws governing consumer protection, electronic transactions, intellectual property rights, product liability, competition and unfair trade practices, as well as industry-specific regulations in sectors such as finance, healthcare, telecommunications, and insurance.

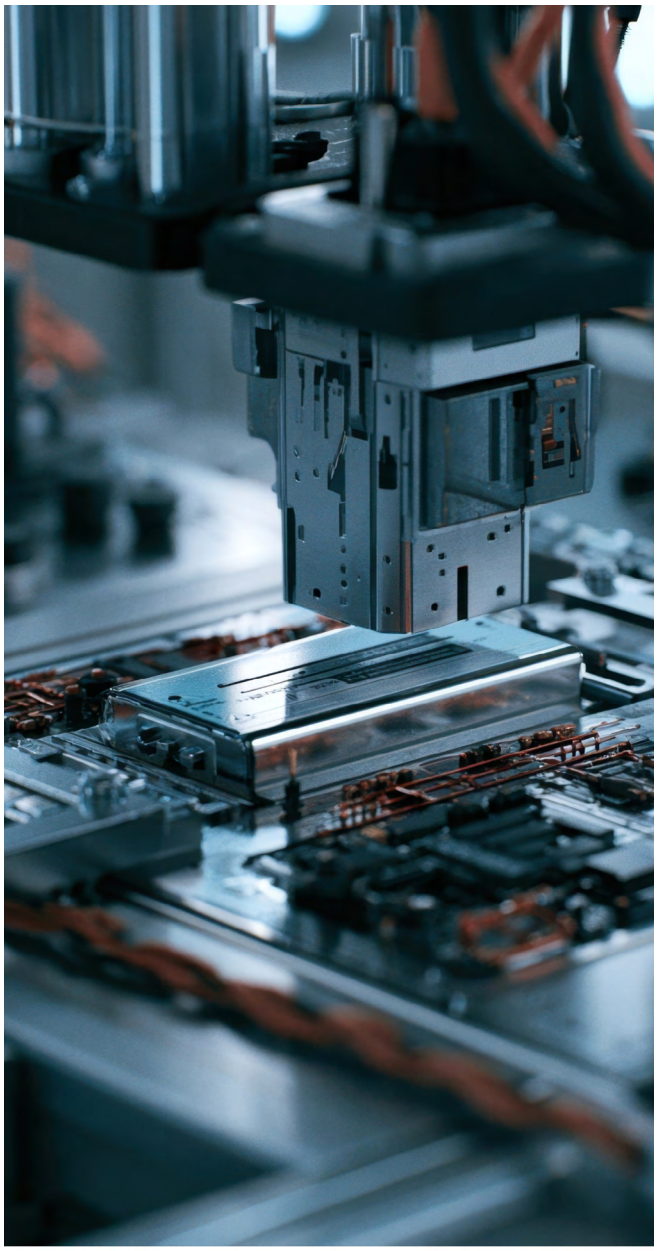
As a result, AI-related legal issues in Thailand are currently addressed through the application and interpretation of existing legal principles rather than by reference to a dedicated AI statute. Consequently, questions relating to liability, transparency, bias, safety, data use, and regulatory compliance are generally assessed under traditional legal doctrines and regulatory requirements on a case-by-case basis, taking into account the specific facts and circumstances of each matter.

23 *Id*, at Part III(1)(B).

24 *Id*, at Part III(1)(B)(5).

VIETNAM

Yes. Vietnam enacted a dedicated AI law (Law No. 134/2025/QH15) on 10 December 2025, effective from 1 March 2026 (the "**AI Law**"). The AI Law regulates the full lifecycle of AI systems, including research, development, provision, deployment, and use, and introduces a three-tier risk classification (high, medium, and low) with graduated obligations on developers, providers, and deployers. It imposes transparency and labelling duties (including for deepfakes), establishes a liability framework for AI-caused harm, and creates a regulatory sandbox together with a supporting infrastructure and data regime.





02

Is there any AI-related law, regulation, guideline, code of practice, or soft law currently in the pipeline?

BANGLADESH

Yes. A national AI policy is already in draft, and it sets a target of enacting a full AI statute by 2028.

The main features of the draft Policy are as follows:

a. a **risk-based classification** into prohibited, high-risk, limited-risk and low-risk systems;

b. **mandatory algorithmic impact assessments** for significant public-sector systems and private high-risk systems;

c. **prohibitions** on social scoring, biometric mass surveillance without lawful authority, manipulative systems, and AI-generated election disinformation;

d. **children's data rules**, including no collection below 16 without parental consent and no use of children's data to train models;

e. **algorithmic disgorgement** — a deployer that trains on unlawful data must unlearn it, or pull the model and retrain, and must prove it has done so;

f. **regulatory sandboxes**, with renewable one-year waivers subject to transparency and incident reporting;

g. the **National Data Governance Authority (NDGA)** as the central AI regulator, able to set standards, certify high-risk systems and oversee impact assessments; and

h. an **Independent Oversight Committee** able to demand algorithmic documentation and training-data disclosure, and to recommend withdrawal of unsafe systems.

On timing, the draft gives the Ministry of Law, Justice and Parliamentary Affairs two separate mandates, both for 2028: comprehensive AI liability legislation covering insurance, apportionment along the value chain and cross-border harm; and the drafting of a comprehensive Artificial Intelligence Act. Until one of those instruments is enacted, the draft Policy accepts that liability for AI-caused harm continues to be governed by an interim regime drawn from the existing law of tort and administrative law.

CAMBODIA

Yes. Cambodia is developing several AI-related and digital governance instruments, although none currently constitute binding AI-specific legislation. Key initiatives include the Draft National Artificial Intelligence Strategy 2025–2030, the proposed National AI Governance Framework, the Draft Law on Personal Data Protection, and the Draft Cybersecurity Law. The Draft AI Strategy identifies ethical and responsible AI as a national priority and contemplates the development of AI governance measures, risk management frameworks, and sector-specific guidance to support the responsible adoption and deployment of AI technologies. Cambodia also participates in non-binding regional initiatives, including the ASEAN Guide on AI Governance and Ethics. In addition, the Cambodia Digital Government Policy 2022–2035 and the Cambodia Digital Economy and Society Policy Framework 2021–2035 provide the broader policy foundation for the adoption and governance of emerging technologies, including AI.

Expected timeline: unclear, although significant developments are likely within the next one to two years. The Draft AI Strategy and National AI Governance Framework remain under development and consultation, while the Draft Law on Personal Data Protection and the Draft Cybersecurity Law are still undergoing governmental review. At present, Cambodia's AI governance framework remains largely policy-driven and based on soft-law principles rather than binding AI-specific regulation.

INDONESIA

Yes. Several AI instruments are in the pipeline, as follows:

- Presidential Regulation on AI Ethics, listed in the 2026 Presidential Regulation drafting programme under Presidential Decree No. 38 of 2025 on the 2026 Presidential Regulation drafting programme (**"Keppres 38/2025"**). **Timeline:** originally targeted for Q1 or Q2 2026 promulgation; however, as of August 2026 it remains unsigned and no official promulgation date has been announced.
- Presidential Regulation on the National AI Roadmap (stated horizon in the current draft: 2026–2030; earlier drafts referenced 2026–2029), in the same signature queue as the AI Ethics Presidential Regulation and likewise listed in Keppres 38/2025 for 2026 promulgation. **Timeline:** originally targeted for Q1 or Q2 2026 promulgation; as of August 2026 it remains unsigned and no official promulgation date has been announced.
- Draft AI Bill: an early-stage House of Representatives (**"DPR"**) legislative priority with no confirmed drafting schedule. **Timeline:** one to two years, or unclear.
- Sector-specific AI rules (in areas such as health and education, beyond OJK's banking guide) are expected to follow once the two Presidential Regulations are signed. **Timeline:** unclear.

LAO PDR

Yes. Although there is no AI-specific statute currently in the legislative pipeline, several significant developments are underway.

The most notable is the formulation of a National AI Strategy. In January 2026, the Lao PDR Government Communications and UNESCO. The Government announced that its forthcoming National AI Strategy will be guided by the UNESCO ethics framework. The Strategy is currently in formulation, and the expected timeline for its adoption remains unclear, likely 1–2 years.

In terms of binding regulation, the DTBO Decision already expressly lists AI as one of the regulated categories of digital technology business operations. While not an AI-specific statute, this represents the first binding regulatory instrument in Lao PDR that explicitly names AI.

The Government has also proposed amendments to the Cybercrime Law and the Law on Information Communication Technology (No.02/NA, 7 November 2016), both under the Ministry of Technology and Communications, which were put forward in 2025 and may address AI-related issues in the digital space.

On the bilateral cooperation front, in April 2025 the Ministry of Technology and Communications signed an MOU with Chinese partners to establish a Lao-China AI Innovation Cooperation Centre, which will focus on building AI processing infrastructure, a large-scale Lao language information system, and industrial AI models in medicine, agriculture, education, and trade.

At the regional and international level, Lao PDR participates in the voluntary, principles-based ASEAN Guide on AI Governance and Ethics, which was endorsed in 2024 when Lao PDR held the ASEAN chair.

Lao PDR is also a founding member of the World Artificial Intelligence Cooperation Organisation ("**WAICO**"), an intergovernmental body established in 2026.

However, at the regional level, Lao PDR sits within ASEAN's voluntary approach rather than any binding AI-specific regime.

MYANMAR

No draft AI-related law, regulation, guideline, code of practice, or soft law has been officially declared as being in the pipeline.

The Ministry of Science and Technology established the National AI Strategy and National AI Policy Drafting Committee in July 2024. According to a social media post by a member of the Drafting Committee, the Myanmar National AI Strategy (2024–2030) and the Myanmar National AI Development Policy were issued and took effect on 27 February 2026. However, we have been unable to locate any official confirmation of their issuance from the Ministry or any gazette notification.

Based on the social media post, the Myanmar National AI Strategy (2024–2030) is structured around six pillars: AI governance, infrastructure and investment, education and capacity building, ecosystem development, research and innovation, and AI business and start-up promotion. The Myanmar National AI Development Policy addresses AI governance frameworks, international cooperation, sustainable AI ecosystem development, rules for AI system development and deployment, and compliance with intellectual property rights and ethical standards.

The Supervisory Committee on Legal Knowledge Dissemination via Artificial Intelligence was established under Notification No. 120/2025 and subsequently reformed under the President's Office Notification No. 53/2026 as a joint initiative between the Ministry of Legal Affairs and the National AI Development Project. Legal knowledge data is being integrated into the Myanmar Legal Assistant AI Model, which will initially focus on five legal domains during the 100-day plan.

The Supreme Court of the Union has formed implementation committees for AI Technology and e-Government Processes and for a Case Management System, indicating that AI implementation within the justice sector is progressing alongside broader policy development.

02

PHILIPPINES

Yes, following the failure to pass a comprehensive AI-related law during the last Congress, the lower house (House of Representatives) and the upper house (Senate) of Congress have pending AI bills in the 20th Congress.

The following AI-related bills are pending in the House of Representatives:

- HB No. 2827, or the proposed *Artificial Intelligence Development and Regulation Act*, which is a measure to protect the citizens from algorithmic bias, deepfakes, and privacy violations.
- HB No. 252 or the proposed *AI Regulation Act*,[25] which proposes the creation of an Artificial Intelligence Bureau, which shall, among others, develop a national AI development and regulation strategy and develop a framework of governance over the introduction of AI-powered systems in the public and private sectors, the academe, and the workplace.
- HB No. 10362, or the proposed *AI Governance Act*, seeks to establish a national framework for responsible AI use and worker protection.
- HB No. 387, or the proposed *Protection of Labor Against Artificial Intelligence (AI) Automation Act*,[26] which seeks to strike a balance between the rights of business owners to use AI and the preservation of employment opportunities for workers.
- HB No. 659, or the proposed *Artificial Intelligence Development Act*,[27] which proposes the establishment of a National Center for Artificial Intelligence Research, which shall be the primary policy-making research body concerned with the development of AI and allied emergent technologies in the Philippines.

The following AI-related bills are pending in the Senate:

Senate Bill No. 25, or the proposed *Artificial Intelligence Regulation Act (AIRA)*, which seeks to create a National AI Commission ("**NAIC**"), which shall have original and exclusive jurisdiction over all matters pertaining to AI, including its development, promotion, registration, and regulation.

Under the bill, NAIC will handle the registration of any entity which seeks to deploy, import, distribute, and/or use an AI system commercially.[28] It also provides for different classifications of risk in AI systems depending on how much influence it will affect the public.[29]

The bill also prohibits and penalizes, among others, the deployment of unregistered AI systems, the use of AI systems to commit fraud, crimes, or cause harm, and manipulate public opinion, spread disinformation, or conduct unlawful surveillance.[30]

It is unclear whether the Philippine Congress will be able to pass any of these bills before the next Congress in 2028 given the current political climate.

Meanwhile, the Philippine Supreme Court states in Governance Framework that it may adopt and localize principles and best practices from the AI governance frameworks of other jurisdictions,[31] and that domestically, it may pursue cooperation with the following authorities to develop national AI policies:

[1] The Department of Science and Technology, in relation to the National AI Strategy for the Philippines;

[2] The Department of Trade and Industry, in relation to the National AI Strategy Roadmap 2.0;

[3] The Department of Information and Communications Technology, in relation to its efforts (with the Civil Service Commission), to

25 https://docs.congress.hrep.online/legisdocs/basic_20/HB00252.pdf (last accessed, 31 August 2026).

26 https://docs.congress.hrep.online/legisdocs/basic_20/HB00387.pdf (last accessed, 31 August 2026).

27 https://docs.congress.hrep.online/legisdocs/basic_20/HB00659.pdf (last accessed, 31 August 2026).

28 *Id.*, Section 13.

29 *Id.*, Section 16.

30 *Id.*, Section 20.

31 Governance Framework, at Part III(1)[7].

draft the Principles and Guidelines for an Ethical and Trustworthy Use of AI in the Government;

[4] The National Privacy Commission, for the data protection aspect of AI; and

[5] Other regulatory or research bodies on AI to be created by law or regulation in the future.[32]

The Governance Framework does not indicate any expected timeline on the adoption and localization of AI governance frameworks of other jurisdictions, or the development of national AI policies.

THAILAND

Yes. Thailand is currently developing a comprehensive AI regulatory framework. Most notably, the Ministry of Digital Economy and Society (MDES) and the Electronic Transactions Development Agency (ETDA) have proposed the draft Artificial Intelligence Act, which is intended to become Thailand's first dedicated AI legislation.

According to publicly available information, the draft law adopts a risk-based regulatory approach, focusing primarily on the regulation of high-risk AI systems rather than imposing blanket regulation on all AI applications. The draft framework also contemplates obligations for AI providers and deployers, governance measures for high-risk AI, transparency requirements relating to AI-generated content and deepfakes, AI regulatory sandboxes, and sector-specific oversight by relevant regulators.

In parallel, Thailand has already introduced a number of AI-related soft law instruments and sector-specific guidelines. For example, in 2025, the Bank of Thailand issued its AI Risk Management Policy, which provides guidance to financial service providers on the governance and management of risks arising from the use of AI. In the insurance sector, the Office of Insurance Commission published the AI Governance Guideline for Insurance Companies B.E. 2568 (2025), establishing a governance framework for the systematic adoption and oversight of AI technologies within insurance businesses. In addition, the Securities and Exchange Commission of Thailand has introduced a regulatory framework governing the use of Artificial Intelligence and Machine Learning in the capital markets, reflecting a broader trend towards sector-specific AI governance.

VIETNAM

Not strictly applicable, as a dedicated law already exists (though its rollout is still phasing in). The AI Law itself took effect on 1 March 2026 and its implementing Decree No. 142/2026/ND-CP on 1 May 2026. Transitional periods apply to systems already in operation before the effective date: 18 months for AI systems in healthcare, education, and finance, and 12 months for all others. Subordinate instruments still to be issued include the Prime Minister's list of high-risk AI systems, the national AI ethics framework, and various ministerial technical guidance and standards referenced throughout the Law and the Decree.



32 *Id.*



03

Would an AI-related dispute in your jurisdiction most likely be handled by: (a) the courts, (b) a regulator, or (c) both, depending on the issue?

BANGLADESH

Both, though the balance tips towards the courts. There is no specialist AI, technology or data tribunal. A civil claim would be filed in the ordinary civil courts under the Code of Civil Procedure 1908 and decided by a generalist judge applying contract and tort. The draft Policy proposes a "Digital Rights Court" to hear takedown applications, but no such court yet exists.

For now, the forum is determined by the cause of action rather than by the technology involved: a claim is filed in whichever court or before whichever regulator ordinarily has jurisdiction over that cause of action, and the fact that the harm was caused by an AI system does not alter that allocation.

CAMBODIA

Both, depending on the issue. Private disputes involving AI, such as contractual, negligence, or other civil liability claims, would generally be resolved by the courts or through arbitration where the parties have so agreed. Regulatory aspects of AI-related disputes, particularly those involving telecommunications, e-commerce, consumer protection, cybersecurity, or data governance, may fall within the jurisdiction of relevant regulators, including the MPTC and the Ministry of Commerce. As Cambodia does not yet have a dedicated AI regulator or an AI-specific dispute resolution framework, jurisdiction will depend on the nature of the claim. To date, there appear to be no reported Cambodian court decisions

in which AI has been a material issue, making this an evolving and largely untested area.

INDONESIA

Both, depending on the issue.

Indonesia has no dedicated AI court or AI regulator yet. Its AI governance is still transitioning from non-binding ethical guidance toward a formal framework (a Presidential Regulation on AI Ethics and Safety and the Draft AI Bill remain pending), so disputes fall to whichever existing regime covers the underlying harm:

- **Data protection issues** fall to PDP Law administrative enforcement (fines of up to 2% of annual revenue, warnings, suspension), with appeals to the Administrative Court and criminal cases to the ordinary criminal courts.
- **Financial-sector AI** (credit scoring, robo-advice, fintech) is subject to OJK supervisory or licensing action under its sectoral AI ethics guidance.
- **Platform or electronic-system-operator compliance** falls to the Ministry of Communication and Digital Affairs (**"MoCD"**) administrative action, including under Article 40A of the amended ITE Law, with Article 21 of the ITE Law providing the operative rule that the party procuring or using an electronic agent bears the legal consequences of transactions executed through it.
- **IP, contract, and civil liability disputes over AI** fall to the ordinary civil courts, as no AI-specific liability regime exists yet.
- **Criminal conduct** (data misuse, unauthorised access, disruptive AI content) falls to the criminal courts.

LAO PDR

Both, depending on the issue.

An AI-related dispute involving civil liability, such as damages caused by AI systems, contractual disputes over AI products or services, or product liability claims, would be handled by the People's Courts through the civil and commercial chambers under the Law on Civil Procedure (Amended) (No.67/NA, 11 December 2024) (the "**Civil Procedure Law**"). The civil chamber has jurisdiction over disputes relating to compensation for damages (Article 33), while the commercial chamber handles business and commercial contract disputes, intellectual property disputes, and consumer protection matters (Article 35). The court system operates on a three-tier trial basis comprising primary, appellate, and cassation levels (Article 10).

On the regulatory side, the Ministry of Technology and Communications oversees telecommunications, ICT, and digital technology business operations, including AI pursuant to the DTBO Decision. Regulatory enforcement actions for data protection violations, cybercrime, or non-compliance with ICT and digital regulations would be handled administratively by the relevant government agencies. Criminal matters, such as cybercrimes under Articles 164–173 of the Penal Code, would be prosecuted through the criminal courts.

However, given the absence of a dedicated AI regulator and the limited enforcement capacity of existing regulatory bodies, most substantive AI-related disputes would likely end up before the courts rather than being resolved through administrative or regulatory channels.

03

MYANMAR

Based on Myanmar's current legal practice, litigation before the courts would be the primary mechanism for resolving AI-related disputes. As noted above, Myanmar has not enacted a dedicated AI law, nor is any AI-specific legislation currently in the pipeline. Disputes would therefore be addressed within the existing legal and institutional framework, taking into account Myanmar's current stage of technological development.

In the absence of dedicated AI legislation, AI-related issues would be addressed under the existing framework identified in Question 1, namely the Contract Act, CPL, Penal Code, Evidence Act, ETL, TCL, CSL, Privacy Law, Arbitration Law and CPC (together with the AOSL where relevant). These laws do not contain specific definitions or provisions referring to AI-generated or AI-processed content; instead, they regulate broader concepts such as information, electronic data messages, electronic records, cyber resources, personal data, goods, services and dishonest or fraudulent conduct. Courts would apply these provisions by analogy or general application to AI-related facts, with the Contract Act, CPL, and Penal Code supplying most substantive rights and duties, and the Evidence Act, CPC, and Arbitration Law supplying the procedural framework.

Where the use of an AI system results in the commission of a civil wrong or criminal offence, the relevant existing laws apply depending on the nature of the conduct. Illustratively, an AI output used to deceive a person into parting with property may attract Sections 415 to 420 of the Penal Code (cheating and cheating by personation); AI-generated documents used to support a false claim may attract Sections 463 to 471 (forgery); AI-generated content that harms reputation may attract Sections 499 to 500 (defamation); and misuse of information handled through AI systems may attract Sections 405 to 409 (criminal breach of trust). Cyber misuse involving AI resources may separately fall within Sections 36 and 66 to 68 of the CSL, and unauthorised use or disclosure of personal data processed by an AI system may fall within Section 38(b) of the ETL (as inserted by the 2021 amendment).

Any of these laws may provide for penalties including imprisonment, fines, or both, imposed by the competent courts. There is currently no AI-specific regulator or regulatory enforcement mechanism in Myanmar, which further reinforces litigation as the more likely dispute-resolution pathway.

PHILIPPINES

An AI-related dispute would most likely be handled by both the courts (or an alternative dispute resolution mechanism) and a regulator, depending on the issue.

As the Philippines does not yet have a single, comprehensive AI law or dedicated AI regulator, disputes are handled under existing general and sector-specific laws.

Regulators are empowered to handle AI disputes through their existing statutory mandate. AI is treated only as the instrument through which an existing legal violation may have been committed. In the Philippines, regulators may exercise quasi-legislative, quasi-judicial, supervisory, and enforcement functions.

Within the limits of a regulator's mandate, it may receive complaints, conduct hearings, determine liability, and order the payment of administrative fines and penalties. Regulators therefore have the power to determine questions of fact to which the legislative policy is to apply, in accordance with the standards laid down by the law. This necessarily involves the exercise of discretion in determining the rights and liabilities of the parties.[33]

If an AI dispute involves contractual liability, negligence, damages, cybercrime, or a civil or criminal matter, the dispute may be litigated before the ordinary courts.

As such, a dispute may begin before a regulator and later reach the courts through judicial review, and appeal, and enforcement proceedings, or it can start as a separate civil or criminal action. By way of example, under the DPA, the NPC has administrative authority while courts retain jurisdiction over civil and criminal consequences.[34]

33 *Alliance for the Family Foundation v. Hon. Garin*, G.R. No. 217872, 26 April 2017.

34 Chapter II, Sec. 7(b) and 7(i), R.A. 10173.

Despite the first contact of the dispute to be lodged with an administrative agency with a quasi-judicial function, the Rules of Court allow judgments or final orders of quasi-judicial agencies to be appealed to the Court of Appeals.[35] However, despite the allowance of such appeal, it is a well-settled rule that the findings of fact of quasi-judicial agencies are accorded great respect even by the Supreme Court and that without any tainting of grave abuse of discretion, the judgment should be upheld.[36]

Therefore, since a survey of pending House and Senate bills show that an agency is sought to be established, then a quasi-judicial function should allow "all controversies relating to the subject matter pertaining to its specialization are deemed to be included within the jurisdiction of said administrative agency or body."[37]

THAILAND

Both, depending on the issue.

AI-related disputes in Thailand may be handled by both the courts and regulatory authorities, depending on the nature of the dispute. Private law disputes, such as claims arising from contractual breaches, negligence, product liability, intellectual property infringement, data privacy violations, or damages caused by the use of AI systems, would generally fall within the jurisdiction of the courts. Parties may also resolve such disputes through arbitration where a valid arbitration agreement exists.

On the other hand, regulatory issues concerning the development, deployment, or operation of AI systems may fall within the authority of sector-specific regulators. For example, the Personal Data Protection Committee may oversee issues involving personal data processing, the Securities and Exchange Commission may supervise the use of AI in capital markets, the Bank of Thailand may oversee AI-related risks within the financial sector, and the Office of Insurance Commission may regulate AI use in the insurance industry.

The proposed draft Artificial Intelligence Act further supports a decentralised regulatory model, under which existing sectoral regulators would retain primary responsibility for overseeing AI systems within their respective sectors, while a national AI governance framework would provide overarching coordination. The draft therefore suggests that regulatory enforcement will play an increasingly important role, particularly in relation to high-risk AI systems. However, claims for compensation, contractual disputes, and other private law claims would continue to be adjudicated by the courts.

Accordingly, AI-related disputes in Thailand are most likely to be handled by both the courts and relevant regulators, depending on the subject matter and the nature of the alleged harm. Regulatory authorities would generally address compliance and enforcement issues, while the courts would remain the primary forum for resolving civil liability and compensation claims.

VIETNAM

Both, depending on the issue.

Private disputes concerning contractual performance, tortious harm, IP infringement, or consumer claims arising from AI fall to the ordinary courts (or arbitration, where agreed) under the Civil Code and the Civil Procedure Code. Separately, the AI Law creates a dedicated regulatory enforcement track: the Ministry of Science and Technology (as lead state-management authority) and relevant line ministries may inspect, investigate, and require the suspension or recall of non-compliant AI systems, and may refer serious violations for administrative or criminal sanction. A single fact pattern (for example, a harmful AI-generated output) could therefore trigger both a private civil claim and parallel regulatory action.

35 Rules of Court, Rule 43.

36 *South Cotabato Communications Corporation v. Hon. Sto Tomas*, G.R. No. 217575, 15 June 2016.

37 *Sto. Tomas v. Del Valle*, G.R. No. 223637, 28 August 2019.



04

In practice, are AI-related disputes more likely to be resolved through: (a) litigation, (b) regulatory enforcement, or (c) negotiated/ contractual resolution (e.g. arbitration)?

BANGLADESH

As noted above, Bangladesh currently has no AI-specific courts, so AI-related litigation has not yet surfaced. Because there is no AI-specific law, there is also no dedicated enforcement agency, although law enforcement does take action against cybercrime under the Cyber Security Act and other applicable laws. In practice, commercial disputes are resolved through contract and arbitration, and consumer and public-sector disputes through regulatory pressure. Litigation is the least likely of the three, for three reasons:

a. The counterparty is usually offshore. Bangladesh consumes AI rather than building it. Banks, telecoms operators, e-commerce platforms, and government agencies license systems from foreign vendors under foreign-law contracts with foreign-seated arbitration. Any dispute is therefore unlikely to land in a Bangladeshi forum at all.

b. Domestic litigation is slow and the remedies are thin. Disposal times are long, damages awards are modest, and there is no mechanism for class or representative consumer claims. Arbitration is the credible alternative. Bangladesh has been a New York Convention party since 1992, and the Bangladesh International Arbitration Centre offers an institutional route, though no AI-specific arbitration has surfaced yet.

c. Activity so far has been supervisory, not adversarial. The Bangladesh Bank framework and office order, the Cabinet Division's directions, and the judiciary's own warnings are all instruction rather than enforcement. Taken together, the disputes that matter are being resolved in arbitration clauses drafted abroad, or quietly managed by regulators at home.

CAMBODIA

Negotiated or contractual resolution, with litigation or regulatory enforcement arising depending on the nature of the dispute and the applicable legal framework.

Litigation remains available where no arbitration agreement exists, but there is currently little or no reported AI-specific jurisprudence in Cambodia. Similarly, AI-specific regulatory enforcement remains largely untested due to the absence of a dedicated AI regulatory regime. As Cambodia's digital governance framework develops, regulatory enforcement is likely to focus on areas such as data protection, cybersecurity, consumer protection, and online fraud rather than AI itself.

In practice, AI-related disputes in Cambodia are most likely to be resolved through contractual mechanisms, including negotiation, mediation, or arbitration, particularly in commercial relationships where the parties have agreed on risk allocation, liability caps, indemnities, and dispute resolution clauses. Cambodia has an established arbitration framework under the Law on Commercial Arbitration and the National Commercial Arbitration Centre ("**NCAC**"), making arbitration a common mechanism for resolving complex technology and cross-border commercial disputes.

INDONESIA

In practice, based on current Indonesian dispute-resolution patterns, negotiated or contractual resolution (including arbitration) is likely for commercial disputes; regulatory enforcement will address compliance-type issues separately; and litigation remains the fallback.

- Most commercial AI disputes (vendor and licensing disputes, IT service failures, and data-driven fintech products) arise from technology contracts, and Indonesian and cross-border technology agreements routinely carry arbitration clauses (commonly BANI, SIAC, or ICC), because arbitration offers confidentiality and reliable cross-border enforcement under the New York Convention. However, Article 18A of the ITE Law (as last amended by Law No. 1 of 2024) mandates Indonesian law and Indonesian dispute settlement for international electronic contracts with adhesion clauses where the user is in Indonesia or the electronic system provider conducts business activities in Indonesia, narrowing party autonomy for mass-market AI SaaS and consumer-facing contracts.
- Regulatory enforcement (MoCD or OJK administrative action) is the default route for compliance-type issues, such as AI ethics, data protection, and licensing or registration, since regulators act directly on operators rather than on parties suing each other.
- Litigation is comparatively less used for the commercial substance of AI disputes, but remains necessary for (i) claims not covered by an arbitration clause, (ii) interim or emergency relief, (iii) criminal matters, and (iv) appeals from regulatory decisions (Administrative Court or Constitutional Court).

04

LAO PDR

Negotiated/contractual resolution is most likely in practice.

In practice, AI-related disputes in Lao PDR are most likely to be resolved through negotiated or contractual resolution mechanisms rather than through litigation or regulatory enforcement. Under the Law on Economic Dispute Resolution, the Centre for Economic Dispute Resolution ("**CEDR**") and the Offices for Economic Dispute Resolution ("**OEDRs**") handle commercial and business disputes where the parties have agreed to submit their dispute to arbitration or mediation. Lao PDR has been a party to the New York Convention since 1998, and foreign arbitral awards can be recognised and enforced through the Lao courts.

Court-mediated settlement is also strongly encouraged under the Civil Procedure Law. The courts have a duty to mediate litigants at all levels of proceedings (Article 20), and the commercial chamber is required to seek mediation before proceeding to trial (Article 39).

In practice, direct negotiation between the parties remains the most common resolution mechanism, particularly in technology-related matters where international technology vendors and their Lao clients typically prefer contractual dispute resolution clauses such as arbitration or mediation.

Litigation and regulatory enforcement remain less common for AI-related matters, largely due to the absence of AI-specific regulations, limited judicial experience with technology disputes, and the constrained enforcement capacity of regulatory bodies.

MYANMAR

AI-related disputes in Myanmar are currently most likely to be resolved through litigation before the ordinary courts. There is no dedicated AI dispute-resolution mechanism, specialised tribunal, or AI-specific regulatory enforcement framework. Contractual resolution (including arbitration) is the second most likely pathway, but only for parties who have addressed AI risk in advance in a valid agreement. Regulatory enforcement is a distant third and, at present, is limited to sector-specific administrative action rather than substantive AI supervision.

Litigation: Where an AI-related dispute arises, such as breach of contract, civil liability for AI-caused harm, or misuse of electronic information, the aggrieved party would generally bring a claim before the competent court under the existing legal framework.

Regulatory Enforcement: Myanmar does not have an AI-specific regulator or regulatory enforcement framework. Sector-specific regulators can nevertheless impose administrative orders that would reach AI operators falling within their remit. Under the CSL, the department may impose warnings, fines, temporary or permanent licence suspension, and blacklisting on cybersecurity service providers and digital platform service providers (Sections 51 and 52). Under the CPL, the Consumer Affairs Committee and the Department may issue warnings, compensation orders, fines, product-sale prohibitions and licence revocations against non-compliant entrepreneurs (Sections 52 to 54). Under ETL, the Control Board may impose administrative orders on certification authorities for licence violations; and under the TCL, the Post and Telecommunications Department (PTD) may impose administrative orders on telecommunications licensees. These mechanisms are narrow in scope and are not designed to address AI-related disputes generally. Regulatory enforcement is therefore unlikely to be the primary pathway for resolving AI-related disputes in practice, but may proceed in parallel with litigation.

Negotiated/ Contractual Resolution (Arbitration): Under Section 28 of the Contract Act, parties may agree to resolve disputes through arbitration or negotiation as a recognised exception to the general prohibition against ousting the ordinary courts. Where the seat is in Myanmar, the Arbitration Law 2016 applies and, in a domestic arbitration, the tribunal must decide according to the substantive law in force in Myanmar (Section 32(a)(1)); in an international commercial arbitration the tribunal may apply the law chosen by the parties (Section 32(a)(2)). Foreign awards are enforceable in Myanmar under the New York Convention regime in Chapter 10 of the Arbitration Law, subject to the standard grounds for refusal. Arbitration is unlikely to be available for the entire dispute where the underlying claim engages non-arbitrable subject matter: consumer disputes are channelled to the CPL's mediation and administrative regime under Sections 44 to 56 (Section 77 of the CPL disapplies other laws to matters governed by that regime), and criminal offences (including under the Penal Code, CSL and ETL) cannot be settled by arbitration. In practice, arbitration is realistic only where the parties are commercial actors of comparable bargaining power and the dispute is a pure contract or commercial-tort claim.

Jurisdictional and enforcement risk: Most AI systems used in Myanmar are supplied by foreign vendors with no local establishment, which creates three practical layers of risk. First, service of process on a foreign defendant must be effected through the mechanisms in Order V and Order XXIX of the CPC and may materially delay proceedings absent a Myanmar-facing agent for service. Second, an award or judgment obtained in Myanmar against a foreign vendor may need to be recognised and enforced abroad, and any award obtained abroad in favour of a Myanmar claimant must be enforced in Myanmar under Chapter 10 of the Arbitration Law (if arbitral) or through the ordinary courts (if a judgment), each with its own procedural constraints. Third, under the CSL, the Ministry retains a power under Section 42 to inspect or exercise control over digital platform service operations for national defence, security or public interest, and under Section 43 to temporarily suspend, control or close such services with the agreement of the Union Government. These CSL powers add a layer of regulatory jurisdictional risk that is unique to platform-based AI services and that cannot be contracted out of.

The practical enforceability of a Myanmar judgment or regulatory order against an offshore AI vendor, and the statutory grounds on which recognition or enforcement can be resisted, are examined in Question 14 of the companion publication (Series II).

PHILIPPINES

Given the lack of a dedicated AI regulatory agency that will exercise jurisdiction over AI-related disputes, and considering the rapidly evolving AI technologies, regulatory enforcement may likely be the first point of contact in resolving AI-related disputes because of the existing regulatory mandates of Philippine regulators over data privacy, such as disputes involving the unauthorized processing of personal data through AI systems, which fall under the jurisdiction of the NPC; intellectual property, such as disputes over ownership, licensing, and infringement of AI-generated content, which fall under the jurisdiction of the IPOPHL; and consumer protection, such as consumer complaints arising from defective or misleading AI products and services, which fall under the jurisdiction of the Department of Trade and Industry.

If an AI-related dispute arises between businesses, including those arising from AI vendor agreements, the use of AI software-as-a-service ("**SaaS**") contracts, or technology licensing arrangements, it is more likely that the dispute will be resolved through negotiated or contractual mechanisms, as these agreements typically contain alternative dispute resolution clauses such as negotiation, mediation, or arbitration.

Where the AI-related dispute involves torts or quasi-delict claims, abuse of rights issues, criminal liability, or high-value damages claims, the dispute is more likely to be resolved through litigation.

04

THAILAND

In practice, AI-related disputes in Thailand are currently more likely to arise through regulatory enforcement proceedings or to be resolved through negotiated or contractual mechanisms, including settlement discussions, mediation, or arbitration, depending on the parties involved and the underlying contractual arrangements. Given the absence of substantial AI-specific case law and the relatively early stage of AI regulation in Thailand, litigation before the courts remains comparatively untested. Regulatory action may arise where the use of AI implicates existing laws, particularly in areas such as personal data protection, cybersecurity, consumer protection, or sector-specific compliance requirements.

VIETNAM

At this early stage, negotiated or contractual resolution is likely to remain the dominant pathway, as the AI Law is only newly in force and there is no AI-specific case law to guide litigants. Litigation before the courts, or arbitration under the Commercial Arbitration Law (Law No. 54/2010/QH12) where the parties have an arbitration agreement, remains available on ordinary civil and commercial principles. Regulatory enforcement under the AI Law is likely to address systemic or public-interest harms (for example, serious incidents, deepfakes, and non-compliant high-risk systems) rather than individual compensation claims, which claimants would still need to pursue through the courts.





05

Under general civil/tort/ contract principles, would liability for AI-caused harm most likely fall on: (a) the developer, (b) the deployer, (c) the end user, or (d) shared or unclear?

BANGLADESH

Shared or unclear, but in practice the risk sits with the deployer. The deployer is the organisation that puts the system into use under its own authority and acts on what it produces, not the developer that built the model, and not the end user on the receiving end of the decision.

There is no product liability statute, so a claimant falls back on contract or negligence, and both fail at the same point. Contract only reaches the immediate counterparty, so anyone harmed by a system supplied through an intermediary has no contract with the developer. Tort law in Bangladesh remains underdeveloped: negligence is available in principle, but no decision has extended a duty of care to a foreign developer, and serving, proving and funding such a claim would be a demanding exercise.

A deployer cannot deflect liability onto the system itself. An agent must be a person under section 182 of the Contract Act, so an AI system cannot be one — and the deployer cannot say the system acted on its own account. Liability for a system that it chose and relied upon therefore follows.

The draft Policy makes this explicit, imposing strict liability on the deployer of a high-risk system regardless of fault, covering financial loss, injury, discrimination and wrongful refusal of services. If enacted, the Bangladeshi customer carries first-line liability for a foreign vendor's model, and everything turns on the indemnity. Buyers here will have to negotiate AI contracts on that footing rather than signing vendor standard terms, because

the liability stops with them long before it reaches whoever built the model.

Consumer protection adds a further layer. Under the Consumer Rights Protection Act 2009, a supplier of goods or services is responsible for ensuring quality, safety and accurate information. A deployer that offers an AI-powered product or service to Bangladeshi consumers cannot disclaim its way out of these obligations, and the Directorate of National Consumer Rights Protection has the power to receive complaints and order remedies. Where the AI system is consumer-facing, the deployer's exposure under this legislation runs alongside its tort and contract liability, regardless of what the vendor agreement says.

CAMBODIA

Shared or unclear. Cambodia does not have specific rules governing liability for harm caused by AI. Instead, liability would likely be determined under general laws, including the Civil Code and the parties' contractual arrangements. Responsibility will depend on the facts of each case. Deployers and end users may be liable where they control, implement, or rely on AI-generated outputs, while developers or vendors may be liable where harm results from defects, negligent design, inadequate safeguards, or breach of contractual obligations. Given the absence of AI-specific legislation or judicial precedent, liability is likely to be assessed on a case-by-case basis and may be shared among multiple parties.

For example, where an AI-enabled platform processes personal data, the operator may be responsible for complying with Article 32 of the E-Commerce Law 2019, which requires persons holding personal information in electronic form to implement reasonable security safeguards against loss, unauthorised access, use, modification, leakage, or disclosure of such data. This suggests that liability may attach to the party operating or controlling the system, even where the underlying issue involves AI.

INDONESIA

Shared or unclear, with no fixed rule under current Indonesian law.

Indonesian law has no dedicated AI liability regime. AI is not a legal subject, so liability attaches to the natural or legal persons behind it. Under Articles 1365 and 1367 of the Indonesian Civil Code (**"ICC"**) (unlawful acts, and liability for the acts of persons or things under one's supervision), together with Article 21 of the ITE Law (under which the party conducting an electronic transaction through an electronic agent is responsible for the legal consequences of that agent's operation, subject to statutory exceptions) and Government Regulation 71/2019 (which treats an electronic agent as part of an electronic system), fault-based liability may fall on the developer, deployer, operator, or negligent user, depending on whose act or omission caused the harm. The framework was not designed for autonomous, black-box systems.

LAO PDR

Shared or unclear.

Under Lao law, there is no AI-specific liability regime. Liability for AI-caused harm would be determined by applying general civil, tort, and contract principles under the Civil Code, and the likely allocation would depend heavily on the specific factual circumstances.

A developer could potentially be held liable under Article 493 (Liability for Damages Caused by Products or Goods), which provides that businesses that operate and produce sub-standard products or goods that damage consumers or customers are liable for the resulting damages. If an AI system is characterised as a product, its developer could face liability under this provision. A deployer, on the other hand, could face liability under Article 486 (Liability of an Employer), which provides that an employer is liable for damages arising from the acts of its employees in the performance of assigned tasks. By analogy, a deployer that uses AI in its business operations could be held vicariously liable for harm caused by the AI system's

outputs to third parties. Similarly, under Article 489, owners or possessors of materials or property are liable for damages resulting from their wrongful acts.

The general tort provision under Article 472 requires proof of wilful acts, neglect, or lack of due care in violation of law, together with a causal relationship between the event and the damages (Article 474). This fault-based standard could in principle apply to any party in the AI value chain.

In addition, Article 494 (Liability for Hazardous Materials) imposes a heightened standard of liability on owners or possessors of hazardous materials, including vehicles operating on engines and industrial processing plants, which could potentially be applied by analogy to certain high-risk AI systems.

In the absence of clear AI-specific rules, the allocation of liability among the developer, deployer, and end user remains uncertain, and would depend on the court's interpretation of the existing general provisions in the light of the particular facts.

MYANMAR

Liability is likely to be shared or unclear, and may fall on more than one actor. Myanmar law does not treat the developer, deployer and end-user of an AI system as interchangeable: each attracts a different combination of contractual, product-liability, data-protection and attribution rules, and the allocation of liability therefore depends on the cause of action, the contractual arrangements and the specific role of each party in producing the harm.

Under general contract principles (Sections 10 and 73 of the Contract Act), liability turns on the parties' respective obligations, the agreed allocation of risk and the causal link between breach and loss. Beyond contract, three regimes overlay the allocation exercise. First, Section 35 of the CPL imposes a chain of responsibility for consumer damage on the seller of goods or service operator, the manufacturer of goods, the trademark authority, the redistributor, the importer and "the person who operates services for the domestic consumers at either Myanmar or foreign country", the last limb is significant for foreign AI providers, who cannot invoke a lack of Myanmar presence to defeat consumer claims. Second, where the AI system processes personal data, the deployer (and any downstream data handler) will typically be a "Personal Data Holder" under Section 2(m) of the ETL (as inserted by the 2021 amendment) and must comply with the management, protection and deletion duties in Section 27-a; failure attracts imprisonment and fines under Section 38(a). Third, where the AI system is delivered through a digital platform with 100,000 or more users in Myanmar, the deployer is a "digital platform service provider" under Section 4(l) of the CSL and must meet the retention, content-moderation and reporting duties in Sections 30 to 34, on pain of the administrative sanctions in Section 52 and the criminal penalty in Section 64. Applying these rules to a typical AI value chain: the developer (design and training) is most exposed to product-liability-style claims under Section 35(b) of the CPL and to contractual claims from its deployer counterparties; the deployer (integration and customer-facing supply) is most exposed to consumer claims under Section 35(a) and (f) of the CPL, personal-data claims under Section 38(a) of the ETL and platform-obligation claims under the CSL; and the end-user is most exposed to attribution under Section 22 of the ETL (discussed in Questions 9 and 10) and to direct liability for the acts they cause the AI to perform.

Hypothetical A (consumer chatbot). A Myanmar retail bank deploys a chatbot supplied by a foreign vendor. The chatbot generates an incorrect representation about interest rates that causes a customer to enter into a losing transaction. The customer is a "consumer" under Section 2(b) of the CPL. Under Section 35 of the CPL, the bank is the service operator (Section 35(a)); the vendor is the manufacturer of the underlying goods (Section 35(b)) and, as a foreign supplier of services to Myanmar consumers, is also caught by Section 35(f); and Section 40 makes them jointly or severally liable. Section 22 of the ETL treats the chatbot output as that of the bank, which programmed (or caused to be programmed on its behalf) the system to operate automatically.

Hypothetical B (enterprise HR AI). A private employer licenses a resume-screening AI from a foreign SaaS provider under a click-through agreement capping the vendor's liability at USD 10. The algorithm rejects candidates on grounds that

expose the employer to labour and reputational claims. The employer has direct exposure to the affected candidates (with whom it has no privity to any AI-vendor cap), and its recourse against the vendor is limited by the click-through cap. The cap is nevertheless exposed to challenge under Section 16(3) of the Contract Act (burden-shift where the transaction is unconscionable), Section 23 (public policy) and Section 74 (reasonable compensation notwithstanding a stipulated sum). Depending on how the AI is deployed, the employer may also be a "Personal Data Holder" under Section 2(m) of ETL and must comply with Section 27-a in processing candidate data.

Hypothetical C (generative-AI defamation). An AI-generated article falsely accuses a Myanmar company of criminal conduct. The publisher (the deployer) faces exposure under Sections 499 and 500 of the Penal Code and to a civil claim for damage to reputation under Section 2(k) of the CPL where the target qualifies as a consumer. The developer's exposure depends on the degree of control it retained over the model's outputs at deployment (Section 22 of the ETL) and on the presence of a contractual indemnity in favour of the publisher (Sections 124 and 125 of the Contract Act). If the platform on which the article is published has more than 100,000 users in Myanmar, the platform provider must also block, remove or suspend the content under Sections 31 and 32 of the CSL on pain of the administrative and criminal sanctions in Sections 52 and 64.

PHILIPPINES

Under general civil, tort, and contract principles, liability for AI-caused harm will depend on the cause of action of the aggrieved party.

Under the Civil Code, whoever causes damage to another by act or omission, there being fault or negligence, is obliged to pay for the damage done.[38] To sustain a claim based on tort / quasi-delict, the following requisites must concur: [1] there is damage that is suffered by the plaintiff; [2] fault or negligence of the defendant; and [3] connection of cause and effect (or proximate cause) between the fault or negligence of the defendant and the damage incurred by the plaintiff.[39]

Additionally, proximate cause is defined as that cause, "which, in natural and continuous sequence, unbroken by any efficient intervening cause, produces the injury, and without which the result would not have occurred."[40]

A situation may therefore arise where the damage suffered by the plaintiff results from the defendant's act or omission involving AI, whether because the defendant relied on, used, or was assisted by an AI system in causing the harm.

To illustrate, if the proximate cause of the harm is the coding of the AI software, then the developer may be liable. The deployer, who is the entity that puts the AI system into operation for a particular use, may be liable if it fails to implement adequate safeguards, human oversight, or verification protocols, and the failure caused damage to the aggrieved party. Finally, the end-user may be liable if the person who utilized the AI-generated output (such as a lawyer who submits an AI-drafted pleading) failed to exercise independent judgment or due diligence in reviewing the AI output before its release.

Apart from tort, liability may also be governed by the provisions of contract law under the Civil Code.

Therefore, as long as the contract is not contrary to law, morals, good customs, public order, or public policy, the parties are free to place whatever stipulations they deem necessary and convenient, including who may be liable for any AI-caused harm, whether it may be the developer, deployer, or the end-user.[41]

Beyond tort and contract, liability may also apply depending on the characterization of the AI system under the Consumer Code of the Philippines.[42]

If the AI system is treated as a product and if there is damage caused to consumers by defects resulting from the creation of the products or "insufficient or inadequate information on the use and hazards

38 Civil Code, Article 2176.

39 *Andamo v. IAC*, G.R. No. 74761, 06 November 1990.

40 *Vda. De Bataclan v. Medina*, G.R. No. L-10126, 22 October 1957.

41 Art. 1306, Civil Code of the Philippines.

42 R.A. No. 7394, 13 April 1992.

thereof", then under the law, the Filipino or foreign manufacturer, producer, and importer shall be liable for redress for the same – independently of fault.[43]

The provision provides parameters on the term "defective" by taking all the relevant circumstances into consideration, including but not limited to: [1] Presentation of product; [2] Use and hazards reasonably expected of it; [3] The time it was put into circulation.[44]

However, if the classification of the system is "service", then only the service supplier is liable for redress, independently of fault, for damages caused to consumers by defects relating to the rendering of the service, "as well as for insufficient or inadequate information on the fruition and hazards thereof".[45]

Similarly, the parameters on the term "defective" also takes into consideration all the relevant circumstances, including but not limited to: [1] way it is provided; [2] result of hazards which may reasonably be expected of it; and [3] time when it was provided.[46]

The laws above show that there is still no general governance framework for the liability of AI-caused harm. The Supreme Court, through the Governance Framework, warns that "responsibility ultimately falls on the designer, developer, or user of an AI tool."[47] In a recent case, the anti-corruption court in the Philippines, *i.e.*, the *Sandiganbayan*, has warned a lawyer to fact-check AI-generated information to avoid incorrect citations. The anti-corruption court ruled that the "ultimate responsibility of the misquotations ultimately fell on her shoulders as she signed the same" even if it was the previous counsel who crafted such AI-generated pleading.

Ultimately, it is important to view the facts surrounding the harm meticulously to determine the proximate cause of the AI-related harm and determine liability.

THAILAND

Under current Thai law, there is no AI-specific liability regime allocating responsibility among developers, deployers, or end users of AI systems. Liability would therefore be determined under existing legal principles, including contract, tort, product liability, consumer protection, and other applicable laws, depending on the facts of the case.

As a result, liability may potentially fall on the developer, deployer, end user, or multiple parties, depending on factors such as the nature of the AI system, the degree of control exercised by each party, any contractual allocation of risk, the foreseeability of the harm, and whether a party acted negligently or failed to comply with applicable legal obligations. Given the absence of AI-specific legislation or judicial precedents directly addressing these issues, the allocation of liability in AI-related cases remains largely untested and would likely be assessed on a case-by-case basis.

VIETNAM

Primarily the deployer (bên triển khai), with contractual recourse against the developer or provider only where separately agreed. Article 29(2) of the AI Law provides that where a high-risk AI system is properly managed, operated, and used in compliance with the law but nonetheless causes damage, the deployer bears compensation liability to the victim and may seek reimbursement from the provider or developer only if there is a prior agreement to that effect. Where a third party unlawfully hijacks or interferes with the system, that third party is liable, with joint liability for the deployer or provider if they were at fault in permitting the intrusion (Article 29(4)).

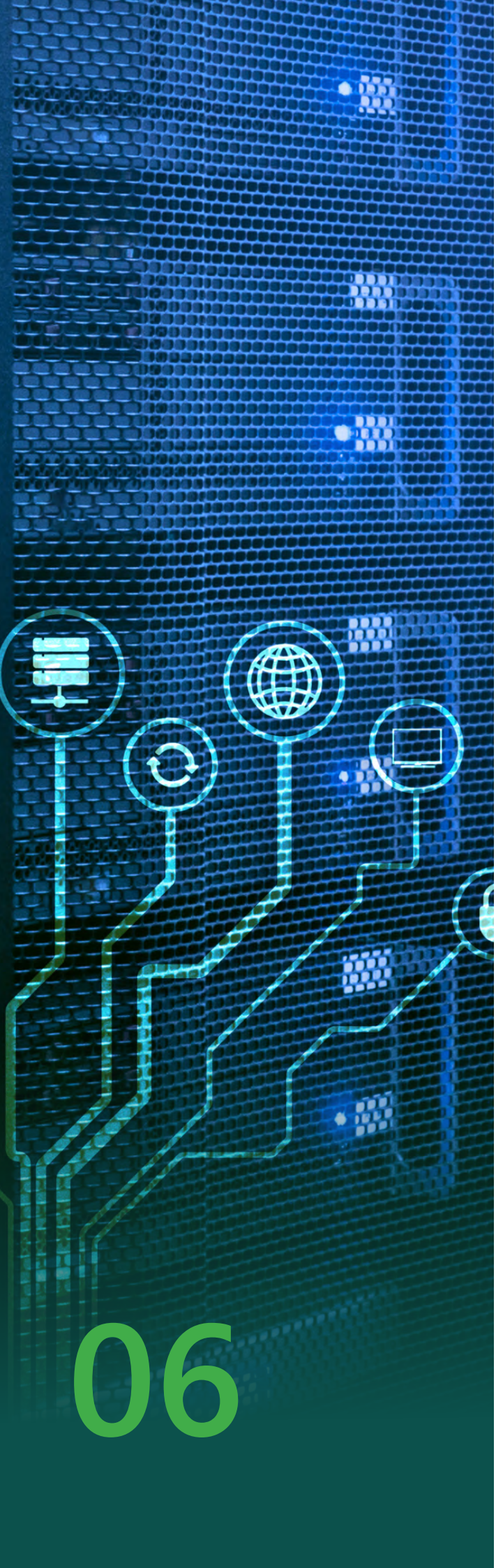
43 Chapter V, Art. 97, R.A. No. 7394.

44 *Id*.

45 *Id* at Art. 99.

46 *Id*.

47 Part II(4), A.M. No. 25-11-28-SC.



06

Does the lack of transparency in AI decision-making create a real risk that a claimant cannot prove causation/ fault?

BANGLADESH

The Cyber Security Act 2026 makes AI-generated outputs admissible as electronic evidence, and sections 3 and 36 of the Evidence Act (as amended up to date) allow electronic records to be produced, but admissibility is not the same as explainability. A claimant can put the output before the court; proving how the system arrived at it is another matter entirely.

Two things may soften the position in time. First, the draft National AI Policy 2026–2030 proposes mandatory algorithmic impact assessments for high-risk systems and an Independent Oversight Committee with power to demand algorithmic documentation and training-data disclosure. If enacted, these would give claimants a documentary trail that does not exist today. Second, the Consumer Rights Protection Act 2009 already places obligations on suppliers of goods and services to provide accurate information and to bear responsibility for defective products, which may provide an alternative route in consumer-facing AI disputes. But until the policy becomes law, a claimant suing over an opaque AI decision is left with general evidence rules designed for a world in which the decision-maker could be put on the stand.

CAMBODIA

Yes. The lack of transparency in AI decision-making may make it difficult for claimants to prove causation, fault, or the source of a harmful output. Under Cambodian law, a claimant generally bears the burden of proving the

wrongful act, damage, and the link between them. As Cambodia currently has no AI-specific transparency, disclosure, or evidentiary rules, claimants may face practical challenges in obtaining the technical information needed to understand how an AI system reached a particular decision, particularly where such information is controlled by the developer or deployer.

INDONESIA

Yes. The fault-based liability structure under Articles 1365 and 1367 of the ICC struggles to accommodate autonomous, black-box AI systems, because proving whose fault caused the harm becomes difficult when the AI's decision-making process is opaque. It should be noted, however, that this is currently a doctrinal or scholarly conclusion; no Indonesian court has yet decided a black-box AI causation case, so the gap has not been judicially tested.

Under current Indonesian law specifically:

- Article 1365 requires the claimant to prove an unlawful act, fault or negligence, loss, and a causal link between the act and the loss. Where the AI's internal reasoning is not explainable, the claimant may struggle to identify whether the harm was caused by a design flaw, defective training data, a deployment or configuration error, a third-party integration issue, or user misuse, undermining both the fault and causation elements.
- Because AI is not a legal subject, liability must be pinned on the developer, deployer, or user behind it, so the claimant also carries the added burden of proving which of these parties actually controlled the harmful conduct.
- The closest statutory proxy, the "electronic agent" concept under the ITE Law and Government Regulation 71/2019, was not designed for algorithmic decision-making or black-box systems and therefore provides no evidentiary shortcut (for example, no presumption of fault or reversal of the burden of proof) to ease this difficulty.
- This gap is why Indonesian commentators have proposed strict, risk-based, or control-based liability models for AI deployers or principals as possible reforms to the current fault-based regime.

LAO PDR

Yes. The lack of transparency in AI decision-making, commonly referred to as the "black box" problem, creates a real risk that a claimant cannot prove causation or fault under Lao law.

Under Article 474 of the Civil Code, the claimant must demonstrate a causal relationship between the event and the damages by proving three elements: that the event is a reason for the cause of damages, that the event occurred before the damages, and that the event is the direct cause of the damages. The requirement to prove a "direct cause" is particularly challenging when AI systems make decisions through opaque, multi-layered processes whose internal logic may not be traceable or explainable even to the system's developers.

The fault requirement compounds this difficulty. Under Article 472, the claimant must prove that the violator acted through wilful acts, neglect, or lack of due care. Given the complexity and autonomy of AI systems, it may be extremely difficult for a claimant to identify and demonstrate what specific act of negligence or lack of due care by the developer, deployer, or user caused the AI to produce the harmful output. The evidentiary burden further exacerbates the problem. Under Article 12 of the Civil Procedure Law, the plaintiff bears responsibility for finding and collecting information and evidence related to the case and submitting it to the court in a complete manner. There is no reversal of the burden of proof for technology-related claims, making it even more difficult for claimants to satisfy the evidentiary threshold when facing opaque AI systems.

Unlike some jurisdictions that are developing AI transparency or explainability requirements, Lao PDR has no such obligations in its current legal framework.

The combination of a fault-based liability regime, the requirement to prove direct causation, the plaintiff's evidentiary burden, and the absence of AI-specific transparency or explainability obligations creates significant evidentiary barriers for claimants seeking to establish liability for AI-caused harm.

MYANMAR

Yes. The lack of transparency in AI decision-making creates a real risk that a claimant cannot prove causation or fault under Myanmar's existing evidentiary framework. Under the Evidence Act, the general rule is that the party asserting a fact bears the burden of proving it (Sections 101 and 102), and, in an AI-related dispute, a claimant would ordinarily need to prove fault or wrongful conduct and establish a causal connection between that conduct and the harm suffered.

The 2015 amendment to the Evidence Act expressly extended the definition of "document" to include electronic records and any record generated, sent, received or stored by electronic, magnetic, optical or similar technologies (Section 3, Illustration (7)). Section 60A permits evidence to be given through a video conferencing or live television link in specified circumstances, and Section 114A creates presumptions in relation to electronic records including that a properly used device or process is presumed to have accurately produced or communicated the electronic record in question, and that an electronic record generated in the ordinary course of business by a neutral third party is presumed authentic. These presumptions cut both ways in an AI-related dispute: they may help a claimant admit AI-generated logs as evidence, but they may equally help a defendant insulate opaque AI outputs from challenge. In either case, they do not address the deeper problem that a claimant may have difficulty obtaining or interpreting the information necessary to establish how an AI system reached a particular decision or output, and whether that decision or output caused the alleged harm.

Accordingly, where relevant AI system information is inaccessible or difficult to interpret, the lack of transparency creates a significant practical obstacle for a claimant seeking to prove causation or fault. Myanmar currently has no AI-specific evidentiary rules, disclosure requirements or presumptions that would specifically alleviate this burden. A claimant would need to rely on the general discovery and inspection powers of the ordinary courts under the CPC, and, in cybersecurity-related matters, on the seizure and forensic-analysis powers of the CSL Investigation Unit (Sections 45 to 50), whose findings are admissible as expert evidence. The related explainability and access-to-model-logs issues are considered further in Question 11 of the companion publication (Series II).

PHILIPPINES

Yes. The lack of transparency in AI decision-making creates an evidentiary risk, particularly where the claimant must prove both fault and causation. The claimant bears the burden of proving the material allegations of the complaint, and that burden does not automatically shift merely because the defendant used an AI system.

The lack of transparency may prevent the claimant from establishing which actor (developer, data provider, or end user) was responsible. It will also be challenging to establish whether human intervention took place in the review of AI-related results.

However, the lack of transparency does not necessarily make the claim impossible. The claimant may rely on discovery, evidentiary presumptions, or expert witnesses to prove its cause of action.

Under the existing sector-specific legal frameworks, liability, responsibility, and accountability generally attach to the person or entity that deploys, operates, or benefits from the AI system. Accordingly, a complete understanding of the AI system's internal reasoning or decision-making process may not always be necessary to establish liability. Nevertheless, the claimant must still prove proximate causation. This requires determining whether the harm resulted from the end user's inputs, prompts, or manner of using the AI system, or from a defect in the system's design, development, coding, training, or operation. Although the lack of transparency may complicate this inquiry, it does not necessarily prevent a claimant from proving causation or fault through other evidence.

THAILAND

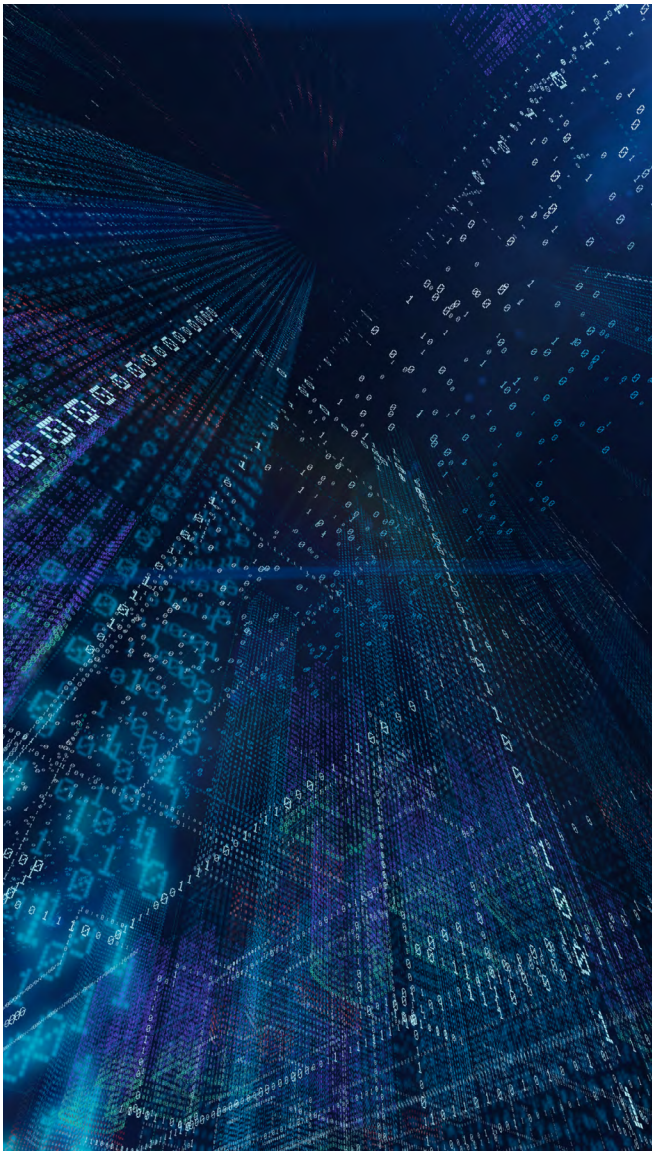
Yes. The lack of transparency in AI decision-making may create a genuine risk that a claimant is unable to establish causation or fault, particularly in complex cases involving autonomous or machine-learning systems. While this issue has not yet been extensively tested before Thai courts, it is likely to present evidentiary challenges under existing Thai legal principles.

Under Thai law, a claimant generally bears the burden of proving damage, fault, and causation. Where an AI system reaches an outcome through opaque decision-making processes, it may be difficult to determine whether the harm resulted from defects in the model, training data, implementation, human oversight failures, or misuse by the end user. This may complicate the claimant's ability to satisfy the required evidentiary standard.

However, this does not necessarily prevent recovery. Thai courts have broad discretion in assessing evidence and may rely on circumstantial evidence, expert testimony, contractual obligations, and the parties' overall conduct. Nevertheless, AI-generated outputs are unlikely to be accepted at face value without supporting documentation, source data, audit trails, or other verifiable evidence. Accordingly, where the operation of an AI system cannot be adequately explained or independently verified, parties may face practical difficulties in establishing causation or fault.

VIETNAM

Yes, this is a recognised risk. The AI Law expressly shields developers and deployers from having to disclose source code, detailed algorithms, model parameters, or raw training data when explaining a system's outputs, even to regulators, which limits the technical detail available to a claimant. Under the Civil Procedure Code, the burden of proof falls on the party asserting a claim, so a claimant alleging AI-caused harm must ordinarily prove fault and causation. Vietnam's consumer protection law reverses that burden where the claimant is a consumer, which partly mitigates the risk in business-to-consumer AI disputes. For all other claimants, the opacity of AI decision-making remains a genuine evidentiary obstacle.





07

Would courts likely uphold a vendor's liability cap/ indemnity for AI risks (hallucinations, erroneous outputs, bias, security failures)?

BANGLADESH

Untested. No Bangladeshi court has ruled on a liability cap or indemnity clause drafted specifically for AI risks. The answer must therefore be taken from the Contract Act 1872 and the general law of contract.

Freedom of contract is the starting point. Under section 10 of the Contract Act, all agreements made by the free consent of competent parties, for a lawful consideration and with a lawful object, are enforceable. A clearly drafted liability cap in a negotiated commercial agreement between parties of comparable bargaining power is likely to be upheld, subject to two constraints:

a. Section 74 of the Contract Act caps damages at the sum named in the contract as payable on breach, but only to the extent the court considers the amount "reasonable compensation". A nominal cap is vulnerable to being treated as disproportionate and adjusted upward to what the court considers reasonable.

b. Section 23 voids any agreement whose object or consideration is unlawful, including anything the court regards as opposed to public policy. A cap that immunises a vendor from liability for foreseeable physical injury, fraud, or criminal conduct would face serious challenge on this ground.

The draft National AI Policy, if enacted, would change the picture materially. It proposes strict liability for deployers of high-risk systems regardless of fault, together with comprehensive AI liability legislation covering insurance

and apportionment along the value chain. A vendor's contractual cap would then sit alongside a statutory liability floor, and the cap could not contract below it.

Until then, the practical answer is that a proportionate, negotiated cap for ordinary AI errors will probably survive; a blanket exclusion for hallucinations, bias or security failures in a standard-form agreement is exposed to challenge under sections 23, 74 and 16 of the Contract Act, particularly where the counterparty is a consumer or a party of materially weaker bargaining position.

CAMBODIA

Untested. Cambodian courts would likely uphold contractual liability caps and indemnities, as the Civil Code generally recognises the parties' freedom to allocate risk by agreement. However, provisions seeking to exclude liability for intentional misconduct or gross negligence are unlikely to be enforceable. As there is no reported Cambodian case addressing AI-specific liability caps or indemnities, the position remains largely untested.

INDONESIA

Untested for AI-specific risks, but likely upheld for ordinary negligence under general Indonesian contract law.

Parties are generally free to include exclusion or limitation of liability clauses under the freedom-of-contract principle in Article 1338 of the Indonesian Civil Code. However, that freedom is bounded by Article 1339 (fairness, custom, and law), mandatory statutory rules, and public-order considerations. Clauses that seek to exclude liability for intentional misconduct or gross negligence may be challenged or disregarded, particularly in standard-form or unequal-bargaining contexts. Indonesian authority on AI-specific caps remains undeveloped, so this conclusion should be framed as an extrapolation from general contract, consumer-protection, and public-policy principles rather than settled AI case law. In addition, under Article 18 of Law No. 8 of 1999 on Consumer Protection (**"Consumer Protection Law"**), standard-form clauses that shift a business actor's responsibility, eliminate a consumer's right to sue, or grant one-sided authority to the business are declared null and void by operation of law under Article 18(3). This is directly relevant where the AI vendor's counterparty qualifies as a consumer under Article 1 of the Consumer Protection Law, but does not necessarily apply to B2B contracts, which revert mainly to the Civil Code and sector-specific rules.

Applied to AI risks specifically:

- **Ordinary or foreseeable errors** (occasional inaccuracies, non-critical bugs): a properly drafted cap or exclusion would likely be upheld, consistent with normal commercial risk allocation.
- **Hallucinations, bias, or security failures amounting to gross negligence or wilful misconduct** (for example, known defects not disclosed, reckless deployment without basic safeguards, or failure to patch known vulnerabilities): a cap or indemnity attempting to exclude liability for these would likely be struck down or disregarded by an Indonesian court, consistent with the gross-negligence carve-out doctrine.
- **Consumer-facing AI** products: any clause that eliminates the consumer's right to claim compensation risks being void under Article 18 of the Consumer Protection Law, regardless of how it is framed.

No Indonesian court has yet ruled on an AI-specific liability cap (whether for hallucination, algorithmic bias, or an AI security failure); this is genuinely untested territory. The likely outcome, extrapolated from the well-established gross-negligence and public-policy carve-out applied to ordinary limitation-of-liability clauses, is that caps would be enforced for negligent AI errors but not for conduct that a court characterises as gross negligence or wilful disregard of known AI risks (for example, deploying a system known to hallucinate in a high-stakes context without adequate warnings or safeguards).

07

LAO PDR

Untested. There is no reported Lao case law or judicial guidance on whether courts would uphold a vendor's liability cap or indemnity specifically for AI-related risks such as hallucinations, erroneous outputs, bias, or security failures.

In principle, the Civil Code supports freedom of contract. Under Article 8, participants in civil relationships have freedom to exercise their rights voluntarily, and under Article 9, they may freely perform any act to create rights and obligations for themselves on the basis of legality and compliance with law. This suggests that parties are generally free to negotiate and agree on liability caps and indemnities as part of their contractual arrangements.

However, the Civil Code also provides safeguards that could be used to challenge such clauses. Under Article 24, legal acts made involuntarily, through error, deception, threat, or violence, or "which disadvantage either party" are classified as relatively null (voidable). A significantly one-sided liability cap that heavily favours the vendor at the expense of the other party could potentially be challenged under this provision.

Furthermore, the tort provisions of the Civil Code (Articles 470–495) are statutory obligations, and it remains unclear whether a contractual liability cap could effectively override statutory tort liability, particularly under Article 493 (product liability) or Article 494 (hazardous materials liability).

Given the nascent state of the Lao legal system's engagement with technology disputes and the absence of any AI-specific dispute precedent, the enforceability of vendor liability caps for AI risks remains entirely untested.

MYANMAR

Untested. To the best of our knowledge, no Myanmar court has adjudicated the enforceability of a vendor's liability cap or indemnity clause specifically in relation to AI risks such as hallucinations, erroneous outputs, bias or security failures. A Myanmar court would examine the contractual terms against Sections 10, 16, 23, 73, 74, 124 and 125 of the Contract Act, with the outcome depending on the drafting of the clause, the nature of the AI-related risk, the parties' relative bargaining power and the consumer or commercial character of the transaction.

A clearly drafted liability cap or indemnity in a commercial agreement between parties of comparable bargaining power may be enforceable in principle. Under Section 124 of the Contract Act, a contract of indemnity is recognised, and Section 125 entitles the indemnity-holder to recover all damages, costs and sums paid in reasonable compromise within the scope of the indemnity. The quantum of damages recoverable for breach is nevertheless bounded by Section 73 (compensation for loss that arose naturally in the usual course of things or was within the parties' reasonable contemplation, and not for remote or indirect loss) and Section 74 (where the contract names a sum payable on breach, the court awards reasonable compensation not exceeding that sum, whether or not actual loss is proved). A proportionate cap tied to fees paid a common construct in AI vendor agreements is therefore more likely to survive than a nominal cap (e.g., USD 100 for an enterprise deployment) that a court could recharacterise as a penalty or as evidence of an unconscionable bargain. Where the counterparty is in a materially weaker position (e.g., an SME accepting a click-through licence from a global AI vendor), Section 16(3) of the Contract Act shifts the burden of proving that the contract was not induced by undue influence onto the dominant party, and the court retains a discretion to set the transaction aside.

Under Section 23 of the Contract Act, the consideration or object of an agreement is unlawful and the agreement void where it is forbidden by law, would defeat the provisions of any law, is fraudulent, involves injury to the person or property of another, or is regarded by the Court as immoral or opposed to public policy. A liability cap that effectively immunises a party from responsibility for foreseeable AI-related harm may therefore be vulnerable on public-policy grounds, particularly where it would defeat Section 21(h) of the CPL (which requires the entrepreneur to take responsibility for goods or services inconsistent

with the guarantee), the mandatory personal-data duties in Section 27-a of the ETL, or the safety duties on digital platform service providers in Section 30 of the CSL. A cap purporting to exclude liability for personal injury, death, fraud or a criminal offence would face the strongest headwind. Section 27 of the Contract Act (agreements in restraint of trade are void to that extent) should also be considered where the vendor imposes broad usage restrictions on the licensee's downstream activities.

Illustrative application. A Myanmar enterprise licenses a generative-AI service from a foreign vendor at USD 200,000 per year, subject to a click-through terms schedule capping the vendor's aggregate liability at USD 100 and disclaiming all liability for accuracy, bias and third-party claims. A hallucinated output causes the licensee a USD 5 million business loss. The cap is exposed on three grounds: (i) as a penalty-like clause manifestly disproportionate to fees paid and to foreseeable loss (Sections 73 and 74 of the Contract Act); (ii) as evidence of an unconscionable bargain in a materially asymmetric relationship, triggering the burden-shift in Section 16(3); and (iii) as an object opposed to public policy under Section 23, particularly where the loss engages the CPL, ETL or CSL. A proportionate cap (e.g., a multiple of fees paid) negotiated by counsel and coupled with a narrow accuracy carve-out would attract far less scrutiny.

PHILIPPINES

Untested. There appears to be no settled Philippine jurisprudence specifically determining whether liability caps or indemnity clauses covering AI-related risks (such as hallucinations, inaccurate outputs, discriminatory bias, or security failures) are enforceable.

Philippine courts would apply general contract-law principles. Under Article 1306 of the Civil Code, parties may freely allocate contractual risks, provided their stipulations are not contrary to law, morals, good customs, public order, or public policy. A clearly drafted and negotiated liability cap may consequently be upheld, particularly in a commercial agreement between sophisticated parties, and where it covers ordinary breach or negligence. Philippine jurisprudence has recognised that contractual limitations of liability are not inherently invalid.

In *William Golangco Construction Corporation v. Philippine Commercial International Bank*,[48] the Supreme Court upheld the provision in the contract providing for a limitation of liability (regard the period of liability). The Court stated that not only was the provision fair and equitable, but it was also necessary. Without the period of limitation, the contractor "would be expected to make a perpetual guarantee on all materials and workmanship."[49]

Applied similarly, it is only reasonable to assert that a limitation of liability regarding the amount will also be upheld since the court hesitates to "undermine a contractual stipulation freely and validly agreed upon."[50] It also "will not relieve a party from the effects of an unwise or unfavorable contract freely entered into."[51]

However, a court may strike down or refuse to enforce a liability cap in any of the following circumstances:

a. The cap effectively excuses future fraud or bad faith.

   Article 1171 of the Civil Code expressly provides that any waiver of liability for future fraud is void. Thus, a vendor cannot rely on a liability cap to shield itself from fraudulent conduct, deliberate concealment, willful misconduct, or negligence so serious that it amounts to bad faith.

b. The cap violates law or public policy.

   Although Article 1306 recognizes freedom of contract, contractual stipulations must not be contrary to law, morals, good customs, public order, or public policy. A cap may therefore be invalid if it defeats a statutory duty, eliminates a legally required standard of care, or effectively allows the vendor to avoid responsibility for conduct that the law makes actionable. A stipulation prohibited by law or public policy is void under Article 1409 of the Civil Code.

48 G.R. No. 142830, 24 March 2006.

49 *Id.*

50 *Id.*

51 *Id.*

c. The cap is unconscionable or grossly one-sided.

   A court may disregard a cap that is so low that it effectively deprives the injured party of any meaningful remedy, despite proof of substantial damage. In *Aznar v. Citibank*,[52] the Supreme Court held unconscionable a provision limiting the bank's liability to ₱1,000 or the actual damages proved, whichever was lower, because it prevented recovery of a greater amount even when the damage was established. The Court stressed that blind adherence is unwarranted when a provision is "obviously too one-sided." [53]

d. It appears in a contract of adhesion and operates oppressively.

   A contract of adhesion is a "take-it-or-leave-it" contract, then there is no bargaining on equal footing in the execution of the contract. Because of this, the user is limited to either taking, in its entirety, the contract of the vendor, or not avail of its services altogether.[54]

Therefore, while it is not prohibited, it is looked at with a stringent treatment against the vendor and for the vendee. This is in consideration of the possibility of the party's disadvantage on account of his "moral dependence, ignorance, indigence, mental weakness, tender age or other handicap, the courts must be vigilant for his protection".[55]

THAILAND

Untested. Thailand does not yet have a developed body of case law specifically addressing liability caps, indemnities, or disclaimers for AI-related risks (such as hallucinations, erroneous outputs, bias, or security failures). Accordingly, the enforceability of such provisions remains largely untested in the AI context.

That said, under general principles of Thai contract law, courts will generally respect contractual allocations of risk between sophisticated commercial parties, including limitations of liability and indemnity provisions, provided that they are clearly drafted and do not conflict with mandatory laws, public policy, or good morals. As a result, a vendor's liability cap or indemnity for AI-related risks would likely be enforceable in many B2B transactions.

However, enforceability may be more limited where the clause purports to exclude liability for willful misconduct, gross negligence, breaches of mandatory statutory obligations, or where consumer protection considerations apply. In addition, the reasonableness and scope of the clause may be scrutinized on a case-by-case basis, particularly where the alleged harm arises from serious system failures, data breaches, or regulatory non-compliance.

VIETNAM

Yes, in principle, but untested for AI-specific risks. Under the Civil Code, parties are generally free to agree penalty and limitation-of-liability clauses, and such clauses are enforceable unless they violate a statutory prohibition or public policy. However, where the cap or disclaimer appears in a standard-form contract or standard trading conditions, the Civil Code renders void any clause that exempts the drafter's liability, expands its own rights, or removes the counterparty's legitimate rights, where imposed unilaterally and unfairly. No AI-specific case law has yet tested these provisions against hallucination, bias, or security-failure exclusions.

52 G.R. No.164273, 28 March 2007.

53 *Id.*

54 *Quiambao v. China Banking Corporation*, G.R. No. 238462, 12 May 2021.

55 *Id.*



08

Could an AI vendor's standard limitation of liability or accuracy disclaimer be challenged as an unfair/unenforceable term under consumer or contract law?

BANGLADESH

Yes, in a consumer-facing context. The position is more nuanced for a negotiated commercial agreement.

The Consumer Rights Protection Act 2009 gives consumers the right to receive correct and complete information about goods and services, the right to safe products, and the right to compensation for defective goods or services. A blanket accuracy disclaimer that purports to relieve an AI vendor of responsibility for erroneous outputs is difficult to reconcile with these statutory rights, particularly where the vendor has marketed the system on the basis of its accuracy or reliability. The Directorate of National Consumer Rights Protection can receive complaints, investigate, and order remedies, and the Act creates specific offences for misleading advertising and the supply of adulterated or defective products.

Under the Contract Act 1872, a standard limitation clause in a consumer-facing contract is additionally vulnerable to challenge under section 16 (undue influence where there is inequality of bargaining power), section 23 (object opposed to public policy) and section 74 (court's power to award only "reasonable compensation" regardless of the stipulated sum). The cumulative effect is that a take-it-or-leave-it disclaimer for hallucinations, bias or security failures, offered to a Bangladeshi consumer who has no opportunity to negotiate, is exposed on multiple grounds.

In a commercial agreement between parties of comparable bargaining power, a clearly worded and proportionate limitation is more likely to be upheld, consistent with the freedom of contract under section 10 of the Contract Act. Even there, however, a clause purporting to exclude liability for fraud, personal injury or criminal conduct would face challenge under section 23.

The draft National AI Policy would tighten this further. Its proposed strict liability regime for high-risk AI deployers, combined with mandatory impact assessments, would create a statutory baseline that no disclaimer could contract below. Until then, the consumer protection and contract law framework already provides grounds for challenge, even if those grounds have not yet been tested in an AI-specific case.

CAMBODIA

Yes. An AI vendor's limitation of liability or accuracy disclaimer could be challenged, particularly in consumer-facing transactions, if it is misleading or unfair. Cambodian law also does not allow a party to exclude liability for intentional misconduct or gross negligence. While such clauses are more likely to be upheld in commercial contracts, their enforceability will depend on the specific circumstances and wording.

INDONESIA

Yes. Under Article 18 of the Consumer Protection Law, standard-form clauses that shift a business actor's responsibility, eliminate a consumer's right to sue, or grant one-sided authority to the business are void by law, even though the rest of the agreement remains valid. An AI vendor's accuracy disclaimer or liability cap in a consumer-facing contract is squarely the type of clause this provision targets.

While Article 1338 of the ICC generally permits limitation and exclusion of liability clauses under freedom of contract, that freedom is bounded by Article 1339 (fairness, custom, and law), and such clauses can be challenged or disregarded where they cover gross negligence or wilful misconduct, or otherwise violate public policy. While there is no established Indonesian AI jurisprudence on liability caps, Indonesian courts have on occasion scrutinised contractual provisions that operate unfairly against weaker parties. The enforceability of broad exclusions of liability therefore remains subject to general principles of fairness, mandatory law, and public policy. Note that Article 18 of the Consumer Protection Law applies only where the counterparty qualifies as a consumer under Article 1 of the Consumer Protection Law (an end user for personal or family use); B2B AI SaaS contracts fall outside Article 18 of the Consumer Protection Law and are tested only against Articles 1338 and 1339 of the ICC and general principles of fairness, public policy, and mandatory law.

LAO PDR

Potentially yes, but enforcement is uncertain.

The Consumer Protection Law sets out general principles on consumer rights, but notably contains no provisions on unfair contract terms. There is no separate legislation on unfair contract terms in Lao PDR, which represents a significant gap in the consumer protection framework.

Notwithstanding this gap, the Civil Code provides certain protections that could theoretically be invoked. Under Article 24, legal acts made involuntarily or "which disadvantage either party" are relatively null (voidable). A standard limitation of liability or accuracy disclaimer that heavily disadvantages the consumer could potentially be challenged as a relatively null legal act under this provision.

Additionally, under Article 23, legal acts that impact "national security, peace and social order" are absolutely null. While this is unlikely to apply to most commercial AI disclaimers, it could theoretically be relevant in cases where AI systems cause widespread public harm.

In practice, however, the general nature of the Consumer Protection Law and the absence of specific unfair contract terms legislation means that the legal basis for challenging such clauses is limited and untested. The enforcement capacity of consumer protection authorities in Lao PDR is also constrained.

While there is a theoretical basis to challenge unfair AI vendor disclaimers under the Civil Code's relatively null legal acts provisions, the practical enforcement of such challenges remains uncertain.

MYANMAR

Yes, in a consumer-facing context; the position is materially more nuanced in a negotiated commercial agreement. Under the CPL, a standard-form limitation of liability or accuracy disclaimer used by an AI vendor in a consumer contract is likely to be challenged as inconsistent with the statutory consumer rights and guarantees. In a business-to-business agreement between parties of comparable bargaining power, the same clause is instead assessed under the general principles of contract law summarised in Question 7, and is more likely to be enforceable if it is proportionate and clearly drafted.

Section 19 of the CPL codifies core consumer rights, including the right to safe use of goods or services, the right to correct and complete information, the right to complain about consumer damage and the right to remedy for such damage. Section 21 imposes correlative duties on the entrepreneur, including providing simple and correct information about the guarantee and requirements of goods or services, treating consumers honestly, and taking responsibility for goods or services inconsistent with the guarantee. Section 22 requires the entrepreneur to explicitly inform consumers of potential changes in the nature of goods that are normally invisible to them an obligation squarely relevant to opaque AI systems. A blanket disclaimer purporting to exclude responsibility for inaccurate or unreliable AI outputs is difficult to reconcile with these duties, and, where the disclaimer is paired with promotional claims of accuracy or reliability, may separately engage the prohibitions on fraudulent advertisement (Section 63), misleading conduct (Section 65) and deception (Section 66) offences that attract imprisonment and fines under Sections 70 to 72. The same conduct may amount to "fraud" as defined in Section 17 of the Contract Act (including the suggestion, as a fact, of that which is not true, and a promise made without any intention of performing it), rendering the underlying contract voidable at the consumer's option under Section 19.

Section 23 of the CPL requires goods to be of acceptable quality, correct in quality and measure, safe, suitable for consumer needs, matching sample, supported by spare parts or replacement, and consistent with labelling and advertising. Section 26 requires services to be provided with correct and complete information, to perfect service standards, conforming with consumer needs and completed within the guaranteed period. Where an AI system is offered as a consumer product or service, a disclaimer that purports to exclude all responsibility for hallucinations, erroneous outputs, bias or security failures is in direct tension with these statutory guarantees and would leave the consumer's Sections 24 and 27 remedies (repair, replacement, refund, compensation) intact.

In addition, under Section 23 of the Contract Act, an agreement whose object is opposed to public policy is void. A standard-form clause that effectively immunises a vendor from all responsibility for foreseeable AI-related harm may therefore be vulnerable on public-policy grounds, independently of the CPL. Consistent with Question 7, a clearly defined and proportionate liability cap in a negotiated commercial agreement between parties of comparable bargaining power is more likely to be upheld than a blanket exclusion in a standard-form consumer contract; a cap purporting to exclude liability for personal injury, fraud or criminal conduct is unlikely to be upheld in either context.

PHILIPPINES

Yes. While the specific scenario has not yet been ruled by the Supreme Court of the Philippines, a similar situation may be useful in terms of comparison through analogous circumstances.

In a situation where the amount insured was approximately PHP 45 million, a stipulation limiting liability to merely PHP 1 million was ruled as unfair and inequitable, especially since negligence on the part of the entity who stipulated a liability limit was established.[56]

56 *Cebu Shipyard and Engineering Works, Inc. v. William Lines, Inc.*, G.R. No. 132607, 05 May 1999.

The Philippine Supreme Court looks upon contracts of adhesion with great scrutiny to protect the interests of the vendee, who is usually the disadvantaged party in such transaction.

THAILAND

Yes. Under Thai law, an AI vendor's limitation of liability clause or accuracy disclaimer could potentially be challenged as unfair or unenforceable, particularly where the clause seeks to exclude liability for intentional misconduct, gross negligence, statutory obligations, or conduct contrary to public order or good morals.

The enforceability of such provisions would generally depend on the nature of the parties, the bargaining power between them, the wording and scope of the clause, and the applicable legal framework. In a business-to-business context, Thai courts generally recognise the principle of freedom of contract and may uphold reasonable limitations of liability negotiated between commercial parties. However, a court may decline to enforce contractual provisions that are considered unfair, unconscionable, contrary to mandatory law, or inconsistent with public policy.

In the consumer context, liability caps and disclaimers are likely to face greater scrutiny under consumer protection laws and the Unfair Contract Terms Act B.E. 2540 (1997). Under that Act, a contractual provision may be deemed unfair where it imposes obligations or allocates risks beyond what a reasonable person would ordinarily expect or otherwise gives one party an excessive advantage over the other. Examples include clauses that exclude or limit liability for breach of contract, impose liabilities beyond those contemplated by law, permit unilateral termination without reasonable grounds, or materially increase one party's obligations after the contract has been concluded. Consequently, an overly broad AI-related liability cap or accuracy disclaimer may be challenged and, depending on the circumstances, held unenforceable in whole or in part.

In addition, an accuracy disclaimer stating that AI-generated outputs may be inaccurate does not necessarily absolve a vendor from liability where the vendor has made specific representations regarding the performance, reliability, safety, or suitability of the AI system, or where liability arises from negligence, defective products, non-compliance with applicable regulations, or breach of contractual obligations.

Accordingly, while liability caps and disclaimers may generally be enforceable, particularly in commercial contracts, they remain subject to judicial scrutiny and may be challenged under the Unfair Contract Terms Act, consumer protection laws, or other mandatory legal principles where they operate unfairly or excessively in favour of the AI vendor.

VIETNAM

Yes. A standard-form limitation of liability or accuracy disclaimer imposed by an AI vendor may be challenged as void under Articles 405–406 of the Civil Code where it unfairly excludes the vendor's liability, expands the vendor's rights, or strips the customer of legitimate rights without genuine negotiation. Where the counterparty is a consumer, Vietnam's consumer protection law provides additional unfair-contract-term protections and shifts the burden of disproving fault to the business. The risk is heightened for non-negotiable AI terms of service presented to individual or SME users.





09

Does characterising an AI system as a “tool” rather than a “service” change the applicable liability regime?

BANGLADESH

Yes, but the operative distinction is between goods and services rather than between tools and services.

Goods carry implied terms as to quality and fitness under the Sale of Goods Act 1930, but those terms can be contracted out of, so the protection is thin against a well-drafted agreement. Services attract none of them, leaving the buyer with the contract, negligence and consumer legislation. Anything delivered through the cloud falls into the second and weaker category. Characterisation also decides tax treatment and withholding on cross-border payments. More importantly, now that telecoms regulation has been widened to reach AI services, characterisation may decide whether a provider is caught by a licensing regime it never expected.

CAMBODIA

Yes, potentially. The classification of an AI system as a “tool” or a “service” may affect the legal framework applied. However, Cambodian courts would likely focus on the actual role and conduct of the parties rather than the label used, and there are currently no AI-specific rules or precedents addressing this distinction.

09

INDONESIA

Not by itself. Characterising an AI system as a "tool" rather than a "service" may affect how the relationship is analysed, but does not create a separate AI-specific liability regime under Indonesian law. The applicable regime depends primarily on the parties, transaction structure, and statutory context: consumer-facing AI offerings may trigger the Consumer Protection Law whether framed as goods or services, while B2B deployments generally fall back on contract, tort, electronic-system, and sector-specific rules. The label is therefore relevant but not determinative.

Practical effect of the characterization:

- Service: triggers Consumer Protection Law protections (void one-sided clauses, and business-actor accountability for service failures), plus potential sector-specific service-provider obligations.
- Tool: liability analysis reverts to ordinary tort or negligence and product-type reasoning under the Civil Code, with the person exercising control or supervision over the tool (developer, deployer, or user) bearing fault-based liability; consumer-facing goods may still attract product-liability rules under Articles 19–23 of the Consumer Protection Law, but the service-specific Consumer Protection Law provisions do not automatically apply.

LAO PDR

Potentially yes, though the distinction is untested for AI.

The characterisation of an AI system as a "tool" (i.e. a product or good) rather than a "service" could alter the applicable liability regime under Lao law. Under the Civil Code, if an AI system is characterised as a product or good, Article 493 (Liability for Damages Caused by Products or Goods) would apply, under which the producer or business operator is liable for damages caused by sub-standard products or goods that damage consumers. This provision focuses on the quality and standard of the product. If the AI system or its underlying equipment falls within the definition of "hazardous materials" under Article 494, which includes vehicles operating on engines, industrial processing plants, and similar items, a heightened standard of liability would apply: the owner or possessor is liable for damages except where such damages do not arise from their wrongful acts.

Conversely, if the AI system is characterised as a service, liability would more likely fall under the general tort provision of Article 472, which requires proof of fault (willful acts, neglect, or lack of due care), or under contractual obligations governed by Part V of the Civil Code. The Civil Code does not contain a distinct strict liability regime for services, making the burden on the claimant heavier in a service context than it might be under the product liability or hazardous materials provisions.

If an AI system is used as a "tool" by an employer or deployer, Article 486 (Liability of an Employer) may also be engaged, under which the employer or work-user could be vicariously liable for damages arising from the tool's use in the performance of assigned tasks.

The characterisation of an AI system as a tool, product, or service could therefore materially affect which liability regime applies, but this distinction has not been tested in Lao courts and would depend on the court's interpretation of the existing legal framework in light of the particular facts.

MYANMAR

Yes, though the outcome turns on the substance of the arrangement rather than the label used. The applicable liability regime depends on whether the AI system is provided in a consumer or commercial context and on the specific statutory framework engaged. Section 2(d) of the CPL defines "goods" as objects that are purchased, used or consumed by a consumer or other person, and Section 2(e) defines "service" as an act which fulfils the need of a consumer in the form of work or performance, with or without consideration definitions broad enough to accommodate both on-premises AI software and cloud-delivered AI services.

Under Section 22 of the ETL, an electronic record or data message is deemed to be that of the originator if it was sent by the originator himself, by a person authorised to act on his behalf, or by an information system programmed by or on behalf of the originator to operate automatically. This provision is significant for the characterisation question and cuts both ways. Where an AI system is provided as a "tool" that operates automatically on the user's behalf, the user (as originator) retains attribution and associated responsibility for the outputs, and the provider is treated as the tool-maker rather than the speaker. Where the same system is instead operated by (or on behalf of) the provider — for example, an AI-driven customer-service platform that responds without meaningful user configuration — the provider is the originator, and cannot outsource the attribution to the user. The characterisation is therefore fact-specific: control, configuration, autonomy and the identity of the party that programmed the automatic operation are the relevant indicia.

Under the CPL, the characterisation of an AI system as a "good" (a tool) or a "service" engages different but overlapping statutory guarantee regimes. Section 23 (goods) requires acceptable quality, safety, suitability and consistency with labelling and advertising; Section 26 (services) requires correct information, perfect service standards, conformity with consumer needs and complete performance within the guaranteed period; Section 39 imposes ongoing post-sale duties (spare parts, necessary services, adherence to guarantees) throughout the usable or guaranteed period. An AI system characterised as a tool primarily attracts the goods regime, while one characterised as a service attracts the more onerous service regime; a hybrid AI product (e.g., licensed software with cloud-based updates and support) will typically attract both. The distinction has practical significance for the consumer's remedies under Sections 24 and 27 and for the vendor's post-sale servicing duties under Section 39.

In a commercial context outside the CPL regime, the characterisation is set by the contractual terms agreed between the parties. If characterised as a tool, the provider may argue that the user retains responsibility for reviewing and relying on outputs (consistent with the attribution principle under Section 22 of the ETL); if characterised as a service, the provider may owe specific contractual obligations regarding performance, accuracy and quality, with corresponding liability for breach measured under Sections 73 and 74 of the Contract Act. In either case, liability caps and indemnity provisions would be assessed against Sections 10, 16, 23, 73, 74, 124 and 125 of the Contract Act, including the public-policy ground under Section 23.

PHILIPPINES

Potentially, yes, the applicable liability regime may change.

If the AI system is characterized as a product or tool, Article 97 of the Consumer Act may apply. A manufacturer, producer, or importer may be liable, independently of fault, for damage caused by defects in design, manufacture, presentation, or inadequate safety information.[57] Sellers have more limited liability under Article 98.

If it is characterized as a service, Article 99 applies instead. The service supplier may be liable, independently of fault, where the service fails to provide the safety that consumers may rightfully expect, including because of inadequate information regarding its use or risks. [58]

THAILAND

No. Under Thai law, characterising an AI system as a "tool" rather than a "service" would not, by itself, fundamentally change the applicable liability regime. Thailand does not currently have an AI-specific legal framework that allocates liability based on such classifications. Instead, liability is generally assessed based on the facts of the case, the parties' relationship, the contractual arrangements, and the applicable legal principles.

That said, the distinction may still be relevant in practice. Where an AI system is provided as a tool and the user retains control over how it is used and makes the relevant decisions, liability may be more likely to

57 Consumer Act, Article 97.

58 *Id.*, Article 99.

rest with the user. Conversely, where the provider plays an active role in delivering AI-enabled services, maintains ongoing control over the system, or makes representations regarding the accuracy, reliability, safety, or suitability of its outputs, the provider may face greater exposure to contractual, tort, regulatory, consumer protection, or product liability claims. In addition, an accuracy disclaimer stating that AI-generated outputs may be inaccurate does not necessarily absolve the provider from liability where it has made specific representations regarding the AI system or where liability arises from negligence, breach of contract, non-compliance with applicable laws, or product defects. To the extent that an AI-enabled product falls within the scope of the Product Liability Act B.E. 2551 (2008), such a disclaimer may also be ineffective in excluding or limiting liability for damage caused by an unsafe product.

Accordingly, the terms "tool" and "service" are not determinative. Thai courts would likely focus on the substance of the arrangement, including the parties' respective roles, level of control, contractual obligations, and the circumstances giving rise to the alleged harm.

VIETNAM

Yes, potentially. The AI Law does not use a binary "tool" versus "service" test, but its liability and compliance framework turns on defined roles (developer, provider, deployer, and user), each carrying different obligations and different exposure under Article 29. An AI system supplied as a self-contained tool under the end user's own control may point toward the user or deployer bearing responsibility for outcomes, whereas an AI system delivered as an ongoing hosted service more clearly casts the provider as an active participant subject to high-risk management duties. Characterisation therefore matters less as a formal legal category and more as a factual driver of which role, and which corresponding duties, a given party is found to occupy.



10

Is there any realistic basis under current law to treat the AI system itself (not its developer/deployer/user) as legally responsible?

BANGLADESH

No, and policy is moving the other way.

Legal personality arises only from statute or from an established legal category, and nothing in Bangladeshi law permits a court to confer it on software. Contractual capacity requires an adult of sound mind. Criminal liability requires a guilty mind. Corporate criminal liability rests with the executive officers of the company.

The draft Policy requires strict human accountability and fixes liability on the deployer. Its response to systems that nobody fully understands is to require identifiable persons to answer for them. The question in Bangladesh is not whether the AI is responsible but which person or company in the chain is, and until legislation says otherwise, the courts will answer it with contract, tort and penal laws, where relevant.

CAMBODIA

No. There is no basis under current Cambodian law to treat an AI system itself as legally responsible. Cambodian law does not recognise AI systems as legal persons and therefore does not provide a basis for holding an AI system liable in its own right. Liability would remain with the natural persons or legal entities involved in the development, deployment, ownership, operation, or use of the AI system. The Draft Cambodia National AI Strategy likewise proceeds on the basis that AI risks, governance, and accountability should be managed through obligations imposed on developers, deployers, service providers, and other stakeholders, rather than on the AI system itself. There is currently no

legal framework that grants AI systems the capacity to hold rights, assume obligations, or be sued in their own name.

INDONESIA

No. AI is not a legal subject under Indonesian law. It has no independent legal capacity to hold rights or obligations and cannot itself bear civil, criminal, or administrative liability. AI systems are better analysed as electronic agents or components of electronic systems under the ITE Law and Government Regulation 71/2019, meaning that legal responsibility is attributed to the natural person, legal entity, operator, provider, deployer, or user whose conduct or control is relevant, and not to the AI system itself.

Only natural persons and legal entities (companies, foundations, and similar) qualify as legal subjects capable of bearing civil, criminal, or administrative liability in Indonesia. There is no statute, regulation, or judicial doctrine recognising an AI system as a legal person or otherwise capable of being sued, fined, or held directly responsible in its own name.

LAO PDR

No. There is no realistic basis under current Lao law to treat an AI system itself as legally responsible. Under Article 14 of the Civil Code, "participants in civil relationships" are liable for damages caused by their wrongful actions or inactions. The Civil Code recognises only individuals (natural persons) and legal entities and organisations as participants in civil relationships (Article 1). An AI system is neither a natural person nor a legal entity, and therefore cannot bear civil liability in its own right.

The same limitation applies in the criminal context. Under the Penal Code, criminal liability applies to natural persons (Article 25, defining "offender") and to legal entities (Chapter 9, Articles 88–96). An AI system cannot be an "offender" under Lao criminal law. The Lao legal system, consistent with its civil law tradition and socialist legal framework, does not contemplate granting legal personhood or legal agency to non-human entities such as AI systems. There are no proposals or discussions in the legislative pipeline to extend legal personality to AI.

Accordingly, liability for AI-caused harm would always attach to a human or corporate actor, whether the developer, deployer, operator, or end user, and not to the AI system itself.

MYANMAR

No. Under Myanmar's current legal framework, there is no realistic basis for treating an AI system itself as an independent legal person capable of bearing legal responsibility. Legal personality is conferred on natural persons and legally recognised entities only. Sections 11 and 12 of the Contract Act reinforce this position for private-law purposes: only a person of the age of majority, of sound mind and not otherwise disqualified is competent to contract, and "soundness of mind" is defined by reference to human cognitive faculties criteria that no AI system can satisfy.

Section 35 of the CPL assigns responsibility for consumer damage to identifiable persons and entrepreneurs, including sellers, manufacturers, trademark authorities, redistributors, importers and service operators (including foreign service operators supplying Myanmar consumers), and Section 40 makes the responsibility joint or several where two or more entrepreneurs are responsible. The AI system itself is not listed.

Section 22 of the ETL confirms that even where an information system operates automatically, the outputs are deemed to be those of the originator who programmed or deployed the system. These provisions anchor responsibility in a human or legal person, not in the system itself. The same principle operates in criminal law: offences turning on "dishonest", "fraudulent" or intentional conduct under the Penal Code (e.g., Sections 415 and 463) presuppose a mental element that only a natural person (or, through attribution rules, a body corporate acting through its officers) can hold.

An AI system may therefore be the instrument through which harm occurs, but it cannot be a

defendant or bear independent legal liability under Myanmar's existing legal framework. Consistent with Question 5, liability must be attributed to a natural person or legally recognised entity connected with the AI system the developer, the deployer or the end-user depending on the applicable cause of action, the contractual arrangements between the parties and the facts of the case.

PHILIPPINES

No. An AI system has no natural or juridical personality or independent rights and obligations under Philippine law.

Article 44 of the Civil Code recognizes juridical personality only for entities constituted or granted personality by law; AI systems are not included. Consequently, an AI system cannot presently be sued, found negligent, held criminally liable, or ordered to pay damages.

AI may be identified as the instrument or mechanism through which the injury occurred, but legal responsibility must ultimately be attributed to a legally recognised person, such as the developer, provider, deployer, owner, or user, depending on who exercised control, breached a duty, supplied the defective system or data, or caused the harmful output.

Since all frameworks discussed above emphasise a human-centred approach to AI systems, the law will not treat the AI system itself as an entity that can be held responsible or accountable for its actions. Accordingly, direct liability of the AI system would require new legislation expressly granting AI systems some form of legal personality and establishing how judgments could be enforced against them. No such legal framework currently exists in the Philippines.

THAILAND

No. Under current Thai law, there is no realistic basis for treating an AI system itself as a legally responsible person or entity. AI systems do not have legal personality and therefore cannot independently bear civil, criminal, or regulatory liability.

Instead, liability would generally be attributed to the relevant persons or entities involved in the development, supply, deployment, operation, or use of the AI system, depending on the facts and applicable legal principles. The degree of autonomy of the AI system may be relevant when assessing issues such as causation or allocation of responsibility, but Thai law does not currently recognize AI as a separate legal subject capable of bearing liability in its own right.

Accordingly, any liability arising from the use of AI would be attributed to the relevant developer, provider, deployer, operator, owner, or user, rather than the AI system itself.

VIETNAM

No. Under the Civil Code, only individuals and juridical persons (i.e. entities with lawful establishment, an organisational structure, independent assets, and capacity to participate in legal relations in their own name under Article 74) can hold civil legal capacity. Vietnamese civil law has no concept of a non-human, non-corporate legal subject, and the AI Law confirms this by channelling all liability for AI-caused harm to the human or corporate actors in the chain (developer, provider, deployer, or intervening third party), rather than to the AI system itself.

AUTHORS

BANGLADESH



Shahwar Nizam
Managing Director
Shahwar.Nizam@dfdl.com



Md. Shakhawat Chowdhury
Associate
Shakhawat.Chowdhury@dfdl.com

CAMBODIA



Guillaume Massin
Partner, Head of EU Desk
Guillaume.Massin@dfdl.com

INDONESIA



Vinay Ahuja
Partner and Managing Director
Vinay.ahuja@dfdl.com



Ika Ayu Puspitaningrum
Legal Adviser
Ayu.puspitaningrum@dfdl.com



Afriyan Rachmad
Partner
Afriyan.Rachmad@dfdl.com

LAO PDR



Kooi Thong Lai
Managing Director
Kooithong.Lai@dfdl.com



Senesakoune Sihanouvong
Deputy Managing Director
Senesakoune.Sihanouvong@dfdl.com

MYANMAR



Nishant K. Choudhary
Managing Director
Nishant.choudhary@dfdl.com



Kyaw Kyaw Han
Senior Adviser
KyawKyaw.Han@dfdl.com

PHILIPPINES

OCAMPO SURALVO
ANTONIO AURELLANO
& JACOBA



Jerard Emanuel R. Afable
Associate
Ocampo & Suralvo Law Offices
JAfable@ocamposuralvo.com



Anthony R.V. Jacoba
Partner
Ocampo & Suralvo Law Offices
AJacoba@ocamposuralvo.com



Ramiila L. Quinto
Senior Associate
Ocampo & Suralvo Law Offices
RQuinto@ocamposuralvo.com

THAILAND



Noppadon Treephetchara
Partner
noppadon@dfdl.com



Pawilai Ploythammachat
Legal Adviser
Pawilai@dfdl.com



Napat Wattanasong
Junior Legal Adviser
Napat.Wattanasong@dfdl.com

VIETNAM



Patrick Keil
Counsel
Patrick.keil@dfdl.com



Honganh Tran
Legal Assistant
Honganh.tran@dfdl.com

EXCELLENCE · CREATIVITY · TRUST

Since 1994

BANGLADESH | CAMBODIA* | INDONESIA* | LAO PDR | MALAYSIA* | MYANMAR | PHILIPPINES* | SINGAPORE | THAILAND | VIETNAM

*DFDL collaborating firms