Legal 500
Country Comparative Guides 2025

Indonesia
Artificial Intelligence

Contributor

ABNR Counsellors at Law

Ayik Candrawulan Gunadi

Partner | agunadi@abnrlaw.com

Mahiswara Timur

Senior Associate | mtimur@abnrlaw.com

Marshel Miyata

Associate | mmiyata@abnrlaw.com

This country-specific Q&A provides an overview of artificial intelligence laws and regulations applicable in Indonesia.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Indonesia: Artificial Intelligence

1. What are your countries legal definitions of "artificial intelligence"?

Indonesia has yet to issue any laws or regulations that specifically define artificial intelligence. To date, the only guidance has been issued by the Minister of Communications and Digital ("**MOCD**", formerly the Minister of Communications and Informatics) through Circular Letter No. 9 of 2023 on Artificial Intelligence Ethics ("**CL 9/2023**"). Under this CL 9/2023, artificial intelligence is defined as "a form of programming on a computer device to carry out accurate data processing and/or analysis." While this definition might not accurately or specifically cover "artificial intelligence", CL 9/2023 further elaborates that artificial intelligence includes subsets such as machine learning, natural language processing, expert systems, deep learning, robotics, neural networks, and other related fields.

It could be indicated from the above that there is no specific and uniform legal definition that sufficiently covers artificial intelligence yet.

2. Has your country developed a national strategy for artificial intelligence? If so, has there been any progress in its implementation? Are there plans for updates or revisions?

Yes, in July 2020, Indonesia published a national strategy on artificial intelligence, titled "Artificial Intelligence National Strategy for Indonesia 2020 – 2045: AI Towards Indonesia Vision 2045." The national strategy sets out key strategic issues and initiatives programs for the following focus areas:

a. Artificial intelligence ethics and policy
b. Artificial intelligence talent development
c. Data and infrastructure
d. Industry research and innovation

The main objective of the strategy is to effectively promote the development of artificial intelligence in support of the broader '2045 Indonesia Vision', which aspires to realize a nation that is sovereign, advanced, just, and prosperous. To achieve this, the strategy outlines various programs and actions, including but not limited to the formulation of laws and regulations on data protection, artificial intelligence, cybersecurity, and resilience; the establishment of an AI ethics commission; talent development through the creation of competency standards; ensuring data security and privacy; promoting widespread and equitable infrastructure development; and advancing research and innovation.

Healthcare, bureaucratic reform, education and research, food security, and mobility and smart cities, are identified in the strategy as 'priority sectors' for the development and application of artificial intelligence. These priority sectors are included in the short-term roadmap for 2020–2024 and long-term roadmap for 2024–2045.

The national strategy is intended to be enacted through a presidential regulation. However, no significant progress has been made on this aspect. Nevertheless, there has been some development in terms of program implementation. For instance, the Data Protection Law has been enacted in 2022, and a government regulation regulating the implementation of such law is currently in preparation.

No plans for updates or revisions to the national strategy have been observed in the foreseeable future.

3. Has your country implemented rules or guidelines (including voluntary standards and ethical principles) on artificial intelligence? If so, please provide a brief overview of said rules or guidelines. If no rules on artificial intelligence are in force in your jurisdiction, please (i) provide a short overview of the existing laws that potentially could be applied to artificial intelligence and the use of artificial intelligence, (ii) briefly outline the main difficulties in interpreting such existing laws to suit the peculiarities of artificial intelligence, and (iii) summarize any draft laws, or legislative initiatives, on artificial intelligence.

Indonesia has not implemented any regulations on artificial intelligence. However, AI is arguably captured within the definition of an 'electronic agent,' which is defined in the Electronic Information and Transactions, as lastly amended by Law No. 1 of 2024 ("**EIT Law**") and Government Regulation No. 71 of 2019 on the Provision

of Electronic Systems and Transactions ("**GR 71**") as a device within an electronic system created to perform certain actions on specific electronic information automatically which is operated by a person. The forms of electronic agents include (i) visual (e.g., graphic display of a website), (ii) audio (e.g., telemarketing service), (iii) electronic data (e.g., electronic data capture (EDC), barcode recognition), and (iv) other forms. We understand that this definition might not be perfectly fit to define AI, as: (i) AI is not only "automatic", but often "autonomous", particularly considering that AI may not entirely think based on binary rules (despite of being operated on a binary computational system), but rather based on a spectrum; and (ii) AI is not necessarily a part of an electronic system, but it can be deemed as its own electronic system itself. However, given the broad and vague language of the EIT Law and GR 71, there is still a possibility to expand the interpretation to also capture AI.

GR 71 outlines several principles that must be observed and implemented in the operation of electronic agents, namely: (i) prudence; (ii) information technology system security and integration; (iii) security control of electronic transaction activities; (iv) cost-effectiveness and efficiency; and (v) consumer protection.

The principles for security control of user and electronic transactions include: (i) confidentiality; (ii) integrity; (iii) availability; (iv) authenticity; (v) authorization; and (vi) non-repudiation.

For reference, the term 'electronic transaction' refers to any legal action conducted using computers, computer networks, and/or other electronic media.

Further, MOCD issued CL 9/2023 to provide ethics guideline in the formulation of internal policies of companies regarding data and ethics of artificial intelligence and the implementation of artificial intelligence-based activities. It mainly provides general definition and general guidance on the values, ethics, and control of artificial intelligence-based consultation, analysis, and programming activities by business actors and electronic system operators.

Under CL 9/2023, the operation of artificial intelligence technology shall uphold ethical values, including values of inclusivity, humanity, security, accessibility, transparency, credibility and accountability, personal data protection, sustainable development and environment, and intellectual property. With these values in mind, artificial intelligence operators are expected to:

i. take responsibility for safeguarding society in the use of data;
ii. ensure that artificial intelligence is not used as a policy maker or decision maker on matters concerning humanity;
iii. prevent racism and other harmful actions against humans;
iv. promote innovation and problem-solving capabilities;
v. comply with regulatory obligations to protect user rights and safety in digital media;
vi. ensure transparency of information to users, the Ministry of Communication and Digital Affairs, and the public; and
vii. take into account risk management and crisis management.

Guidelines have also been issued by authorities from various sectors. The Indonesian Financial Services Authority (OJK) has released a Guideline on the Code of Ethics for Responsible and Trustworthy Artificial Intelligence in the Financial Technology Industry, which sets out the key principles for the use of AI by financial technology providers. In addition, the Press Council has published Press Council Regulation No. 1/PERATURAN-DP/I/2025 on Guidelines for the Use of Artificial Intelligence in Journalistic Creations. This guideline stresses the necessity of human oversight and verification throughout the entire process of using artificial intelligence and mandates that any artificial intelligence generated content, including images, personalized materials, or advertisements, must clearly disclose the use of artificial intelligence in its creation.

4. Which rules apply to defective artificial intelligence systems, i.e. artificial intelligence systems that do not provide the safety that the public at large is entitled to expect?

Under Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, every Electronic System Operator is required to ensure that its system operates in a reliable and secure manner and is legally accountable for its proper functioning. In particular, Article 31 of the regulation requires operators to safeguard both users and the general public from any harm or losses resulting from the operation of their electronic systems.

If a defective artificial intelligence system arises due to the operator's failure to meet these obligations, the liabilities would lies with the operator or developer of the defective artificial intelligence system. In this instance, the operator or developer would be subject to administrative sanctions, including written warnings, administrative fines, temporary suspension of operations,

termination of access, and/or removal from the official registry of providers. The imposition of administrative sanctions does not eliminate the possibility of criminal or civil liability. However, liability may be waived if the operator can demonstrate that the harm resulted from force majeure circumstances or from the fault or negligence of the user.

5. Please describe any civil and criminal liability rules that may apply in case of damages caused by artificial intelligence systems. Have there been any court decisions or legislative developments clarifying liability frameworks applied to artificial intelligence?

There are currently no specific rules in Indonesia governing liability for damages caused by artificial intelligence systems. Therefore, in the absence of specific rules, liability is determined based on existing broader legal frameworks under Indonesian law.

Currently, artificial intelligence systems are not recognized as legal subjects under Indonesian law. As such, liability cannot attach to the artificial intelligence system itself, but rather to the parties who design, deploy, or use it. Under Law No. 11 of 2008 on Electronic Information and Transactions, as lastly amended by Law No. 1 of 2024 ("**EIT Law**"), civil liability may arise for the person who causes harm to others. In particular, liability may result from an unlawful act committed by an electronic system operator or a user that causes loss to another party. Liability can also stem from contractual obligations, where a party may be held liable for damages resulting from a breach of contract or negligence, depending on the terms of the agreement.

In terms of criminal liability, the general principle under Article 55 of the Indonesian Criminal Code applies. Only those who commit, order the commission of, or participate in the unlawful act can be held criminally responsible. This implies that a human actor must be identifiable in connection with the offense. For example, if an artificial intelligence system is designed in a way allowing it to or designed in a manner that disrupts another electronic system or causes it to malfunction, this may constitute a violation of Article 33 of the EIT Law, which prohibits any act that disrupts or causes an electronic system to operate improperly. This offense is subject to criminal sanctions, including imprisonment of up to 10 years or a maximum fine of IDR 10 billion. Under the EIT Law, criminal liability applies to any person who intentionally and without authority commits such an act. Accordingly, if the artificial intelligence system is deliberately designed to carry out such actions, the liability would rest with the operator. Conversely, if the artificial intelligence system is abused by a user to commit the offense, then the user would bear responsibility. In addition, certain offenses under the EIT Law may give rise to further criminal liability if they result in material losses to another person. The existence of such criminal liability also does not automatically eliminate potential civil liability.

To date, there have been no court decisions or legal developments in Indonesia that specifically address or clarify the issue of liability arising from the use of artificial intelligence.

6. Who is responsible for any harm caused by an AI system? And how is the liability allocated between the developer, the deployer, the user and the victim?

As explained in number 5 above, the party held responsible will generally be the one deemed to have caused or committed the act resulting in harm. Thus, the burden of liability would need to be assessed on a case-by-case basis, as to whether or not the liability should be borne by the developer, deployer, and user.

For example, if a self-driving car hits someone due to the user's failure to operate the system as instructed, liability would rest with the user. Conversely, if the accident is caused by a defect or error in the car's system, the liability would lies with the manufacturer or developer of the system.

Conceptually, parties in a contractual relationship may also allocate responsibility for artificial intelligence related harm.

7. What burden of proof will have to be satisfied for the victim of the damage to obtain compensation?

Under the Indonesian Civil Code and the Civil Procedure Code, the concept of liability for damages caused by another person is governed by Article 1365 of the Civil Code, which states:

> *"Every unlawful act that causes harm to another person obliges the person at fault to compensate for the loss."*

Based on Article 1365, there are four elements that must be satisfied and proven by a claimant seeking compensation, which are: (i) the existence of an unlawful

act, (ii) fault on the part of the defendant, (iii) actual damage or loss suffered, and (iv) a causal link between the defendant's act and the resulting damage.

Each of these elements must be established individually, as follows:

(i) Existence of an unlawful act

This element concerns actions that violate legal norms applicable within society. Such violations may include contraventions of statutory provisions, breaches of propriety, a lack of due care, or conduct that is contrary to accepted moral standards, whether in relation to others or to their property.

(ii) Fault on the part of the defendant

Fault may arise from either an affirmative act or a failure to act (omission). For instance, a defendant may be held liable for intentionally permitting an artificial intelligence system to cause harm to others.

(iii) Actual damage or loss suffered

Losses are divided into two categories, i.e. material and immaterial losses. Material losses refer to tangible, quantifiable damage suffered by the claimant. Immaterial losses refer to the loss of expected benefits or opportunities that could have reasonably been obtained in the future.

(iv) Causal link

This element requires proof of a direct causal connection between the defendant's conduct and the claimant's loss. In essence, the harm suffered must be a direct consequence of the defendant's unlawful act.

Nonetheless, there are specific instances where the burden of proof is reversed, meaning the defendant is required to prove the absence of fault. One notable example is in consumer protection cases. Under Law No. 8 of 1999 on Consumer Protection, if the victim is a consumer, the burden of proving whether or not there was fault lies with the business undertaking.

Therefore, it is important to clearly delineate the rules for using artificial intelligence, including prohibited uses of the artificial intelligence system in a contractual arrangement with the users. This is important to establish the 'fault' to the user in cases of misuse.

8. Is the use of artificial intelligence insured and/or insurable in your jurisdiction?

Pursuant to the Indonesian Commercial Code, interests are generally insurable or can be insured, provided that they (i) can be assessed in monetary terms, (ii) are exposed to risk, and (iii) are not excluded by law. To date, we are not aware of any regulatory provisions that expressly exclude the insurability of risks arising from the use of artificial intelligence.

In addition, insurance coverage is valid if there exists an insurable interest at the time the insurance contract is entered into. This means the insured party must have a legally recognized interest in the subject matter of the insurance.

Accordingly, based on the above principles, risks associated with the use of artificial intelligence are in principle insurable in Indonesia, provided that the requirements above are satisfied. However, we note that, in practice, such insurance products specifically covering artificial intelligence related risks do not yet appear to be offered by insurance companies in Indonesia.

9. Can artificial intelligence be named an inventor in a patent application filed in your jurisdiction?

No. As of now, artificial intelligence cannot be named an inventor in Indonesia. Under Law No. 13 of 2016 on Patents, as last amended by Law No. 65 of 2024, an 'inventor' is defined as a person or group of persons who jointly carry out the idea that results in an invention. In this context, the term 'person' refers to a natural or legal person, and artificial intelligence does not qualify as either. Therefore, the current law does not recognize artificial intelligence as a subject of patent protection, nor does it allow for the possibility of AI being named an inventor.

10. Do images generated by and/or with artificial intelligence benefit from copyright protection in your jurisdiction? If so, who is the authorship attributed to?

No. Law No. 28 of 2014 on Copyright ("**Copyright Law**") is silent on the copyright protection of images generated by artificial intelligence. However, under the Copyright Law, an author or creator is defined as an individual or a group of individuals who, independently or jointly, create a work that is unique and personal in nature. Since artificial intelligence generated images do not have an author or creator who fits this definition, they cannot be considered copyrightable works under Indonesian law.

Furthermore, the Directorate General of Intellectual Property of the Ministry of Law interprets the requirement of being 'personal in nature' as referring to the creator's ability to possess personality, a trait that, by nature, only humans can have. The "unique" and "personal" elements emphasize that a work must be rendered based on a human's ideas and creation. Accordingly, artificial intelligence generated works fall outside the scope of copyright protection.

11. What are the main issues to consider when using artificial intelligence systems in the workplace? Have any new regulations been introduced regarding AI-driven hiring, performance assessment, or employee monitoring?

Artificial intelligence is seeing growing use in Indonesian workplaces, particularly in areas such as recruitment, where it is used for tasks like CV screening and initial candidate selection, as well as in employee monitoring, performance evaluation, employee training and development, and the automation of routine operational tasks.

Key legal issues to consider when using artificial intelligence in such circumstances:

1. Data protection: If an artificial intelligence system processes employees' personal data, employers must ensure compliance with Law No. 27 of 2022 on Personal Data Protection ("PDP Law"). This includes obtaining valid consent where required, implementing appropriate security measures, and ensuring that data subjects are informed of the purpose, scope, and duration of data processing activities. Employers must also ensure that personal data is not used beyond its original purpose without proper justification and safeguards.
2. Automated decision making: The PDP Law grants individuals the right to object to decisions made solely through automated processing, including profiling, if such decisions have legal or significant effects on them. This means that if AI is used to automatically screen candidates, rank employees, or trigger disciplinary actions, employers must ensure that such systems do not operate without human oversight. Individuals must be given an opportunity to seek clarification or challenge the outcome.
3. Ethical use of artificial intelligence: Employers are encouraged to comply with CL 9/2023, which emphasizes the ethical use of artificial intelligence. Adhering to these principles helps ensure that artificial intelligence is used in a manner that respects employees' rights and promotes fairness in the workplace.

Other than the general ethical guidelines issued by the MOCD, Indonesia has not enacted specific regulations governing the use of artificial intelligence in hiring, performance assessment, or employee monitoring.

12. What privacy issues arise from the development (including training) and use of artificial intelligence?

The development and use of artificial intelligence may raise significant privacy issues, primarily during the training stage, which may involve the collection and processing of personal data without the appropriate lawful basis and lack of transparency. Data is often scraped from public sources, which may inadvertently include identifiable or sensitive personal data, collected without the relevant individual's knowledge. Additionally, the lack of transparency in how artificial intelligence models are trained and how personal data is utilized poses further privacy risks. In light of these concerns, the development and use of artificial intelligence must always comply with the principles of personal data protection under the PDP Law.

13. How is data scraping regulated in your jurisdiction from an IP, privacy and competition point of view? Are there any recent precedents addressing the legality of data scraping for AI training?

Intellectual property

From the perspective of intellectual property, Indonesia's Copyright Law protects original works that are expressed in tangible form, including literary works, databases, and software. This includes any original works, even if they are not registered with copyright. If data scraping involves original works or related products and prejudices the legitimate interests of the original creators, it may amount to copyright infringement.

Nevertheless, data scraping can still be performed for non-commercial artificial intelligence training that benefits the creator or if the creator has explicitly stated that they do not object to such use. Under Indonesia's Copyright Law, "commercial use" includes both direct commercial exploitation (e.g., paid use) and the provision of free content services that generate economic gain from third parties who benefit from the use of the

copyrighted works.

Privacy

From the perspective of privacy, when data scraping involves the collection of personal data, it must comply with the personal data protection principles set out under the PDP Law. These include having a lawful basis for processing, ensuring transparency, limiting the use of data to specified purposes, and applying data minimization.

Competition

From a competition perspective, data scraping may be restricted if it leads to anti-competitive behavior. If a dominant company scrapes proprietary data and uses it to replicate services, thereby hindering competition and consumer choice, it could be challenged as an abuse of dominant position and unfair competition.

Cybersecurity

The EIT Law prohibits any person from unlawfully accessing an electronic system in any manner to obtain data, including by breaching, bypassing, or breaking through security systems. These provisions may be relevant in assessing the legality of data scraping activities, depending on how the data is accessed.

14. To what extent is the prohibition of data scraping in the terms of use of a website enforceable?

In Indonesia, the prohibition of data scraping in a website's terms of use is generally enforceable, as it forms a contractual agreement between the website operator and the user. When the user or visitor agrees to the terms, they are legally bound by them, and any violations may lead to legal action for breach of contract.

15. Have the privacy authorities of your jurisdiction issued guidelines on artificial intelligence?

The MOCD, as the current authority on privacy-related matters, has issued a guideline, CL 9/2023, which set out general ethics guidelines for the implementation of artificial intelligence, but not specifically on privacy matters. Law No. 27 of 2022 on Personal Data Protection mandates the establishment of a Data Protection Authority, which has not been established yet. It is possible that the new Data Protection Authority would issue a privacy-specific guidelines on artificial intelligence.

16. Have the privacy authorities of your jurisdiction discussed cases involving artificial intelligence? If yes, what are the key takeaways from these cases?

Yes. The MOCD has, on several occasions, expressed concerns and reminded the public about the potential misuse of artificial intelligence. These concerns include cases involving fraud, forged transfer receipts created using artificial intelligence, and the use of deepfake technology. MOCD has also worked together with the Indonesian National Police to conduct cyber patrols aimed at anticipating the spread of deepfake videos and other artificial intelligence driven digital manipulation.

In response to the increasing risks of misuse, MOCD is said to be currently preparing another national roadmap for AI development, aiming to encourage the responsible and beneficial use of AI while mitigating potential negative impacts in the future.

17. Have your national courts already managed cases involving artificial intelligence? If yes, what are the key takeaways from these cases?

No, we have not seen any Indonesian courts adjudicating cases involving artificial intelligence thus far.

18. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence?

Yes, generally, the MOCD, as the policymaker and regulator in the field of digital infrastructure and the digital ecosystem, is the authority responsible for overseeing the implementation of artificial intelligence. This responsibility falls under the Directorate of Artificial Intelligence and Emerging Technology Ecosystems within the MOCD.

19. How would you define the use of artificial intelligence by businesses in your jurisdiction? Is it widespread or limited? Which sectors have seen the most rapid adoption of AI technologies?

We have seen significant increase in the deployment of artificial intelligence by business in Indonesia, including on the main business operation and the supporting

operation aspects. In our observation, the rapid development on the use of artificial intelligence is mainly from the financial services (such as for credit scoring, KYC, fraud detections), e-commerce and technology sectors (such as cloud computing, AI-based consumer service, stock management).

We also have indicated several studies which indicate that artificial intelligence is primarily used by businesses to improve efficiency. A 2024 study by IBM revealed that 62% of companies in the financial services and insurance and manufacturing sectors are actively piloting artificial intelligence, and 23% enterprises already integrating artificial intelligence capabilities across their operations (https://asean.newsroom.ibm.com/Indonesia-leans-into-AI).

20. Is artificial intelligence being used in the legal sector, by lawyers and/or in-house counsels? If so, how? Are AI-driven legal tools widely adopted, and what are the main regulatory concerns surrounding them?

Yes, artificial intelligence is increasingly being used in the legal sector by both lawyers and in-house counsels. One of the most common forms of artificial intelligence adopted is generative artificial intelligence, which is used primarily for repetitive and mundane tasks, such as summarizing lengthy documents, assisting with initial research, and performing various daily administrative tasks. In addition to generative artificial intelligence, artificial intelligence technologies specifically developed to assist in the review of documents, particularly in the context of due diligence, are also gaining traction.

While artificial intelligence driven legal tools are becoming more widely adopted, they also raise significant regulatory concerns, particularly in the area of privacy and confidentiality. The use of artificial intelligence in legal work often involves handling sensitive and confidential information, such as client data and proprietary business information. As a result, it is critical for lawyers and in-house counsels to exercise caution when using artificial intelligence tools to ensure that confidentiality is maintained.

21. What are the 5 key challenges and the 5 key opportunities raised by artificial intelligence for lawyers in your jurisdiction?

Key challenges:

1. Data protection: When lawyers input personal data into artificial intelligence tools, they risk breaching personal data protection if the data is processed without proper safeguards or consent.
2. Inaccurate content: Artificial intelligence generated outputs can include factual or legal errors, which may mislead lawyers if not carefully reviewed.
3. Ethical concerns: Using artificial intelligence may affect lawyers' duties of confidentiality, competence, and transparency, especially if clients are unaware of its use.
4. High cost: Adopting artificial intelligence tools involves significant costs for software, integration, and training, which may burden smaller firms.
5. Cybersecurity risks: Artificial intelligence platforms, especially cloud-based ones, may be vulnerable to cyberattacks or data breaches, putting sensitive data at risk.

Key opportunities:

1. Faster research: Artificial intelligence can speed up initial legal research by quickly surfacing relevant laws or precedents, which would provide general overview and direction for conducting further in-depth research, albeit validation is still imperative.
2. Routine task support: Automating repetitive tasks like data entry allows lawyers to focus on more strategic work.
3. Drafting assistance: Artificial intelligence can help generate first drafts of contracts or legal documents, improving efficiency in drafting processes.
4. Data-heavy assessment: Artificial intelligence would allow lawyers to make practical assessment which is driven by data, to allow more consistent assessment across the firm, as well as more scientific approach assessment, such as by considering game theory in determining legal strategy.
5. Improved client service: Artificial intelligence helps lawyers work more efficiently and cost-effectively, leading to faster response times and better client outcomes.

22. Where do you see the most significant legal developments in artificial intelligence in your jurisdiction in the next 12 months? Are there any ongoing initiatives that could reshape AI governance?

Currently, the government from various sectors is in the process of preparing regulations to govern the use of artificial intelligence. For instance, the MOCD is reportedly preparing specific regulations on artificial intelligence, with plans to finalize them by Q3 2025. Additionally, other

sectors are also working on their own regulations. The Ministry of Health, for example, has formed a special working group on artificial intelligence to regulate its use in supporting medical professionals. However, the timeline for this initiative is still unclear. These regulations are expected to bring more clarity and certainty to artificial intelligence governance.

Contributors

Ayik Candrawulan Gunadi
Partner
agunadi@abnrlaw.com

Mahiswara Timur
Senior Associate
mtimur@abnrlaw.com

Marshel Miyata
Associate
mmiyata@abnrlaw.com