

Legal 500

Country Comparative Guides 2026

Indonesia

Artificial Intelligence

Contributor

**ABNR Counsellors at
Law**



Ayik Candrawulan Gunadi

Partner | agunadi@abnrlaw.com

Mahiswara Timur

Partner | 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 is the legal definition of "artificial intelligence" in your jurisdiction, if any? If no definition exists, how do regulators or courts typically describe 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 currently there is no specific and uniform legal definition under the regulations that sufficiently covers artificial intelligence yet.

We have also yet to see Indonesian courts provide a definition or descriptive framing of artificial intelligence, as AI-related litigation remains scarce. Even in existing AI-related court judgments, judges have not included any delineation or formal statement describing what constitutes artificial intelligence. Contextual usage of the term "artificial intelligence" throughout these rulings generally refers to automated systems that assist humans in performing tasks, such as platforms that generate deepfake content.

Nevertheless, the MOCD released an AI Ethics Guidelines Framework in mid-2025 ("AI Ethics Guidelines"), which sets forth a definition of AI. Under this framework, artificial intelligence refers to technology centred on developing systems built with explicit or implicit objectives. These systems are capable of autonomously or semi-autonomously processing data and information from a wide range of input variables to generate outputs including predictions, recommendations, synthetic content, or other decisions that carry implications for both physical and digital environments.

In the absence of a codified statutory definition of AI under current regulations, this MOCD framing is expected to act as the main interpretive reference point for regulators and courts going forward.

2. Has your country developed a national strategy for artificial intelligence? If yes, what progress has been made 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 initiative 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 to create legally binding obligations for each stakeholder to achieve the targets established thereunder. However, no significant progress

has been made on this aspect. Nevertheless, there has been some development in terms of program implementation. For instance, the PDP Law was enacted in 2022, and a government regulation regulating the implementation of such law is currently in preparation.

Due to the rapid development and evolving dynamics of AI in recent years, particularly following the emergence of generative AI technologies, the government is currently preparing a draft Presidential Regulation on the 2026–2029 AI Roadmap to align policy directions and update the national strategy with these developments. The details of the proposed adjustments are not yet known, however, the draft Presidential Regulation is reportedly complete and is expected to be enacted in the near future.

3. Has your jurisdiction adopted any AI-specific laws, regulations, voluntary standards, or ethical guidelines? If so, please provide a brief overview. If not, which existing laws could be/applied to artificial intelligence and the use of artificial intelligence, what are the main interpretive challenges, and are there any pending artificial intelligence legislative initiatives?

AI-specific laws and regulations

Indonesia has not implemented any specific laws and regulations on artificial intelligence. However, AI is arguably captured within the definition of an 'electronic agent,' which is defined Law No. 11 of 2008 on Electronic Information and Transactions, as last amended by Law No. 1 of 2026 ("EIT Law"), and Government Regulation No. 71 of 2019 on the Provision of Electronic Systems and Transactions ("GR 71/2019") 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 a perfect 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 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 71/2019, there is still a possibility to expand the interpretation to also capture AI.

GR 71/2019 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.

AI standards or guidelines

Notwithstanding the absence of specific laws and regulations, MOCD has issued CL 9/2023 to provide ethics guidelines in the formulation of internal policies of companies regarding data and ethics of artificial intelligence and the implementation of artificial intelligence-based activities. It is worth noting that such circular letter is categorized as soft law, which in nature serves only as guidance and does not constitute a regulation issued under the formal law-making hierarchy. As such, it does not create legally binding obligations for the public. CL 9/2023 mainly provides general definitions 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 MOCD, and the public; and

vii. take into account risk management and crisis management.

Guidelines have also been issued by authorities from various sectors, including:

i. Banking and financial sector

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, as well as a guideline book titled Artificial Intelligence Governance for Indonesian Banking, which outlines the guiding principles, risk management and governance framework, and implementation guidelines tailored for the banking sector.

ii. Mass media sector

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.

iii. Education sector

Seven ministers, i.e. the Minister of Home Affairs, the Minister of Religious Affairs, the Minister of Primary and Secondary Education, the Minister of Higher Education, Science and Technology, the Minister of Communication and Digital Affairs, the Minister of Population and Family Development/Head of the National Population and Family Planning Agency, and the Minister of Women's Empowerment and Child Protection, jointly issued a Joint Decree on Guidelines for the Utilization and Learning of Digital Technology and Artificial Intelligence in Formal, Non-formal, and Informal Education. This Joint Decree provides guiding principles, addresses child protection in the digital space, outlines the role of families in supervising the use of AI, and sets out guidelines and limitations on the use of AI across different levels of education.

Upcoming AI-related regulations

The Indonesian government is in the process of

developing regulations to govern AI, i.e. Presidential Regulation on AI Ethics. This regulation is intended to establish a clear governance framework to promote the development of AI that is ethical, transparent, and accountable, while ensuring that innovation can continue to grow within a trusted environment. Based on the current draft, the scope of the regulation will include the roles and responsibilities of users, developers, and relevant ministries, and will adopt the ethical values set out in CL 9/2023. Additionally, the regulation is expected to introduce a risk-based classification of AI use across several levels, along with requirements to implement mitigation measures for identified risks. Business actors will also be required to conduct periodic self-assessments of the risks associated with their AI and report the results to the relevant authorities.

As of June 2026, publicly available information suggests that the draft regulation has been consulted with various stakeholders and is substantially finalized, pending formal enactment. Therefore, the regulation is expected to be issued in the near term.

4. Are there legal requirements for artificial intelligence transparency, explainability, or audits? Are there obligations to disclose the use of artificial intelligence to customers/clients?

From the perspective of existing laws and regulations, as there is currently no specific regulation governing artificial intelligence in Indonesia, there are no provisions that expressly mandate AI systems to ensure transparency, explainability, or audits. However, some obligations such as transparency and audits may be inferred from more general regulatory frameworks, including the following:

1. Transparency

Where AI is used to process personal data, such processing is subject to Law No. 27 of 2022 on Personal Data Protection ("PDP Law"), which requires transparency. In this regard, data controllers must ensure that data subjects are informed of the personal data being processed and the manner in which such data is processed. Accordingly, where AI is used in personal data processing, such as in automated decision-making or where personal data is processed for AI-related purposes, the transparency requirement under the PDP Law would apply.

2. Audits

Under GR 71, an electronic agent is required to have

governance policies, operational procedures, and audit mechanisms, including periodic audits of its electronic system. Additionally, an electronic agent is required to maintain audit trails of all activities relating to the operation of the electronic system for the purposes of supervision, law enforcement, dispute resolution, verification, testing, and other examinations, including mitigation or incident response purposes. Such audit trail mechanisms include:

- maintaining transaction logs in accordance with the operator's data retention policy and applicable laws and regulations;
- providing notifications to consumers upon the successful completion of a transaction;
- ensuring the availability of audit trail functions capable of detecting attempted or actual system intrusions, which must be periodically reviewed or evaluated; and
- where the processing system and audit trail are managed by a third party, ensuring that such audit trail processes comply with the standards established by the operator.

As elaborated in our response to Question No. 3, given that AI may also be considered an electronic agent under GR 71/2019, these obligations may also be considered applicable to AI, such that periodic audit mechanisms and audit trails would be expected to be in place.

There are also no direct legal obligations to disclose the use of artificial intelligence to customers/clients. However, customers/clients generally have the right to obtain accurate, clear, and honest information under Law No. 8 of 1999 on Consumer Protection, as last amended by Law No. 1 of 2026 ("Consumer Protection Law"). Such a right may support a general expectation of transparency, including in relation to the use of AI. While this does not constitute an explicit legal requirement to disclose AI, we view that such disclosure would be required where the use of AI materially affects the characteristics, functioning, or outcomes of the relevant product or service, such that failure to disclose could be considered misleading.

Meanwhile, from the perspective of the forthcoming presidential regulation on AI ethics, based on the AI Ethics Guidelines, which further elaborate the ethical values set out in CL 9/2023, and may provide an indication of the likely scope and interpretation of the forthcoming presidential regulation, obligations relating to transparency, explainability, audit, and disclosure of AI use do not appear to be uniformly mandated under the anticipated framework.

Transparency is expressly recognized as one of the core ethical values under CL 9/2023 and the AI Ethics Guidelines. This includes ensuring that users understand how AI processes their data, have access to information regarding such processing, and are provided with transparency in relation to AI systems, including explanations for decisions made. In addition, the ethical values of credibility and accountability emphasize that users are entitled to reliable and accountable information, as well as ease of access to clear explanations. These principles may, in practice, support expectations around explainability and disclosure of AI use.

Audit obligations are not expressly reflected as an ethical value. The AI Ethics Guidelines instead emphasize the implementation of self-assessment mechanisms to evaluate compliance with AI ethical principles. As such, it appears that the forthcoming AI-specific regulation is unlikely to impose a formal audit requirement, at least based on the current framework.

5. Are there legal requirements or best practice expectations for human oversight and human-in-the-loop in artificial intelligence systems?

There are currently no explicit legal requirements in Indonesia mandating human oversight or human-in-the-loop mechanisms in artificial intelligence systems. Existing regulations, including GR 71/2019 and the PDP Law, generally impose obligations relating to accountability, governance, and risk management, but do not specifically require human intervention in AI decision-making processes. Similarly, while CL 9/2023 sets out general ethical principles for the use of AI, human oversight and human-in-the-loop mechanisms are not expressly identified as standalone ethical values.

However, the AI Ethics Guidelines include human oversight as one of the measures that may be implemented to mitigate the multidimensional risks arising from AI systems. Such measures emphasize governance and control 'by humans, for humans, and under human oversight', particularly by (i) ensuring that AI systems remain under human control and are not permitted to make final decisions autonomously in matters that significantly affect human rights, life, or well-being, (ii) establishing governance processes that ensure meaningful human oversight at all stages of the development, deployment, and use of AI, (iii) developing policies, guidelines, and organizational structures that enable collective, participatory, and democratic decision-making regarding the direction of AI technologies, and (iv) engaging relevant stakeholders in the formulation of AI governance frameworks.

At present, as these measures are not set out in a binding legal framework, they serve only as best practice guidance. However, these measures are expected to be incorporated into the forthcoming Presidential Regulation on AI Ethics, where they are likely to be positioned as minimum safeguards to mitigate AI-related risks. Should such provisions be enacted under the Presidential Regulation, these measures would become binding legal requirements that must be implemented as part of AI risk mitigation.

6. Are there specific legal or regulatory requirements addressing algorithmic bias, discrimination, or fairness in AI systems (including gender bias)?

There are currently no specific legal or regulatory requirements in Indonesia addressing bias, discrimination, or fairness particularly in AI systems. As with other issues, relevant obligations are currently derived from general regulatory frameworks rather than AI-specific rules.

GR 71/2019 provides that personal data must be collected in a fair manner. To the extent that an AI system involves the collection of personal data, the requirement for fair data collection under GR 71/2019 would apply. This includes ensuring that the data collection process is not conducted in a biased or discriminatory manner, such as selectively collecting or disproportionately processing data from certain groups of individuals in a way that may lead to unequal or discriminatory outcomes.

In addition, the Consumer Protection Law requires business undertakings to treat consumers properly, honestly, and without discrimination, including on the basis of ethnicity, religion, culture, region, education, wealth, or other social status. In this context, AI system providers, as well as business actors that use AI in delivering their services, should ensure that the use of AI does not result in unfair or discriminatory treatment of consumers, as this could potentially be viewed as inconsistent with the fairness and non-discrimination obligation under the Consumer Protection Law.

While not constituting binding legal requirements, it is worth noting that issues relating to bias, discrimination, and fairness are addressed in CL 9/2023. CL 9/2023 embodies ethical principles, particularly inclusivity and humanity, by emphasizing that the development, deployment, and use of AI should uphold equality, fairness, and human values. This is further reflected in expectations to reduce bias in data and algorithms, ensure that AI systems operate without discrimination,

and promote the fair distribution of AI-generated benefits. Given that similar values from CL 9/2023 are expected to be incorporated into the forthcoming Presidential Regulation on AI Ethics, once enacted, they may potentially give rise to binding legal requirements that specifically address issues of bias, discrimination, and fairness in AI.

7. What legal frameworks apply to AI-related harm and defective artificial intelligence systems? Who can be held liable (developer, deployer, victim of the damage, others), how is liability allocated, and what burden of proof applies to victims?

Applicable legal frameworks and allocation of liability

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 the 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 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 that allow or cause disruption to another electronic system, 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.

Burden of proof

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.

In civil cases, the burden of proof generally lies with the party who asserts a right or claim. Meanwhile, in criminal cases, the burden of proof rests with the prosecutor. The prosecutor must establish the guilt of the accused beyond a reasonable doubt, which is a significantly higher standard of proof than in civil proceedings. The accused benefits from the presumption of innocence and is not required to prove their innocence. Any doubt regarding the guilt of the accused must be resolved in their favor. 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 the Consumer Protection Law, 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. What cybersecurity obligations apply to AI systems?

Cybersecurity obligations applicable to AI systems are set out under regulations issued by the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara or "BSSN"), as follows:

1. Implementation of Security Measures

Under BSSN Regulation No. 8 of 2020 on Security Systems in the Electronic System Operation, electronic systems operators in general, which would include AI providers, are required to implement an information security management system commensurate with the risk level of the system. Prior to implementing such security measures, the provider must conduct an independent assessment to determine the risk classification of the system, whether it falls within the strategic, high, or low risk category, in accordance with the self-assessment format prescribed by BSSN. The results of this self-assessment must then be submitted to BSSN for verification. Based on the verification outcome, the electronic systems operator is required to implement an information security management system, including compliance with SNI ISO/IEC 27001 (Indonesian National Standard (SNI) that adopts ISO/IEC 27001). In addition, depending on the applicable risk level, the

electronic systems operator may also be required to implement other security standards as stipulated by BSSN or relevant ministries/agencies.

2. Cyber Incident Response

BSSN Regulation No. 1 of 2024 requires the establishment of an internal cyber incident response team within an organization. This team is responsible for handling cyber incidents, including mitigation and recovery efforts, dissemination of information on cyber incidents to relevant stakeholders, and the issuance of guidance aimed at preventing or minimizing the impact of such incidents. The regulation further requires that the organization's incident response team be registered with the national cyber incident response team administered by BSSN.

9. Is the use of artificial intelligence insured and/or insurable in your jurisdiction, including with cyber policies? Are there market trends, or limitations?

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.

At present, the products that are beginning to emerge are cyber insurance, which generally covers risks such as cybersecurity breaches, data breaches, and other cyber incidents, as well as information and communication technology (ICT) liability insurance, which typically combines elements of professional indemnity and public/product liability insurance, covering, among others, errors and omissions in the provision of IT services, personal injury and property damage, as well as legal defence costs. However, we note that, in practice, insurance products specifically covering artificial intelligence-related risks have yet to be offered by insurance companies in Indonesia.

10. Can artificial intelligence be named as an inventor in a patent application filed in your jurisdiction? If not, what is the current legal position?

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.

Therefore, in an AI-assisted invention, the inventor shall be the human who made the intellectual contribution to the invention, even if AI was used as a tool. However, in the absence of specific guidance on AI-assisted innovation and given the lack of established precedent, it remains unclear which human party would qualify as the inventor. It is likewise uncertain how the relevant authorities or courts would approach this issue. Nevertheless, we are of the view that the inventor would most likely be the individual who makes a substantive contribution to the inventive concept, such as by formulating the problem, directing the use of the AI system, and selecting or refining the output into a patentable invention.

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

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 ("DGIP") 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.

In this regard, the DGIP takes the position that works generated entirely autonomously by AI are not eligible for copyright protection. Conversely, AI-assisted works that exhibit substantial human intellectual contribution may remain eligible for legal protection. In such cases, authorship is attributed to the individual who can demonstrate a sufficient level of intellectual contribution to the creation of the work.

12. What are the main issues to consider when using artificial intelligence systems in the workplace? Have any new regulations, or guidelines, 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 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.

13. What are the main privacy/data protection issues arising from artificial intelligence development and use (including training data)? Have data protection authorities issued guidelines or rulings on artificial intelligence, and what are the key takeaways?

The involvement of personal data in the development and use of AI may give rise to several key privacy and data protection issues, particularly in relation to compliance with the PDP Law:

1. Unclear or Invalid Legal Basis for Processing The use of personal data for training AI systems may be carried out without a clear or valid legal basis. This is particularly relevant where personal data is scraped from publicly available sources or collected from user inputs into AI systems. In both cases, the availability of data does not automatically render it freely usable for any purpose, including AI training, under the PDP Law. A valid legal basis, such as consent or another recognized ground, must still be established, and the subsequent use must remain consistent with the original purpose of collection. Where data is repurposed for AI training without proper legal basis, this may result in unlawful processing.

2. Lack of Transparency There is a risk of non-compliance with transparency obligations under the PDP Law. Individuals may not be adequately informed that their personal data is being used to train or operate AI systems, and the complexity of such systems may make it difficult to provide clear and meaningful disclosures regarding how personal data is collected, processed, and utilized.

3. Purpose Limitation and Data Minimization Risks AI systems often require large volumes of data, which may create a tendency toward excessive data collection or the use of data beyond the original purpose for which it was obtained. This may contravene the PDP Law principles of purpose limitation and data minimization, which require that personal data be processed only for specific,

legitimate purposes and limited to what is necessary.

4. Data Security Risks The use of AI involves the aggregation and processing of significant volumes of data, increasing the risk of data breaches, unauthorized access, or cyber incidents. Ensuring adequate technical and organizational security measures is therefore critical to comply with the PDP Law and to mitigate potential harm arising from such incidents

The MOCD, as the authority currently acting as the data protection authority, has not yet issued any specific guidelines or rulings addressing data protection issues in the context of artificial intelligence.

14. How is data scraping regulated in your jurisdiction from an IP, privacy and competition perspective? Are there recent precedents addressing the legality of data scraping for training of artificial intelligence systems?

– Intellectual property

From the perspective of intellectual property, the 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.

15. 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.

16. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence? What are its powers and enforcement tools?

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. In addition, the cybersecurity aspects of AI are overseen by the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara or "BSSN"), which is responsible for cybersecurity matters, including the establishment of standards and the handling of cyber incidents. Other sectoral regulators may also be relevant depending on the use case. For instance, in the financial sector, the OJK supervises the use of AI, particularly in relation to risk management, consumer protection, and governance.

The powers and enforcement tools of these authorities derive from their respective enabling regulations and generally include the authority to issue implementing regulations and guidelines, conduct supervision and

audits, request information and documentation, and impose administrative sanctions.

17. How widespread is the adoption of artificial intelligence in businesses in your jurisdiction, and which sectors are leading?

We have seen a significant increase in the deployment of artificial intelligence by businesses 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 financial services (such as for credit scoring, KYC, fraud detection), e-commerce and technology sectors (such as cloud computing, AI-based consumer service, stock management).

As of 2026, the MOCD claimed that the adoption rate of AI in Indonesia has reached 92% (<https://www.komdigi.go.id/berita/siaran-pers/detail/adopsi-ai-92-persen-pemerintah-jadikan-ai-pilar-produktivitas-nasional>).

18. How is artificial intelligence used in the legal sector, by lawyers and/or in-house counsels? Are AI-driven legal tools widely adopted, and what are the main regulatory concerns?

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.

19. 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.

20. 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. The most imminent developments are two Presidential Regulations, namely the Presidential Regulation on the 2026–2029 AI Roadmap and the

Presidential Regulation on AI Ethics. Both regulations are reportedly in the final stages of preparation and pending signature by the President, and are expected to be enacted within this year. 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
Partner

mtimur@abnrlaw.com



Marshel Miyata
Associate

mmiyata@abnrlaw.com

