The Legal 500 Country Comparative Guides

Indonesia: Technology

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

For a full list of jurisdictional Q&As visit here

Contributing Firm

ABNR Counsellors at Law

Authors

Agus Ahadi Deradjat
Partner
The Legal 500
aderadjat@abnrlaw.com

Mahiswara Timur
Associate
mtimur@abnrlaw.com

1. **What is the regulatory regime for technology?**

   Generally, technology is regulated by the electronic information and transactions regulatory regime, which is subject to Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016 ("**EIT Law**"), and its implementation regulations. The EIT Law is the "umbrella regulation" governing the utilization of information technology in Indonesia.

   However, sector-specific technology industries are subject to specific laws and regulations, such as:

   - Law No. 36 of 1999 on Telecommunications ("**Telco Law**"), which specifically governs the provision of telecommunications;
   - Government Regulation No. 80 of 2019 on E-Commerce, which is applicable to the use of technology in trading/e-commerce;
   - the provision of financial technology services is subject to regulations under the Financial Services Authority (*Otoritas Jasa Keuangan*, "**OJK**");
   - payment transactions systems are subject to the regulations of Bank Indonesia (Indonesia's central bank).

2. **Are communications networks or services regulated?**

   Yes, the provision of telecommunications networks and services are regulated under the Telco Law and its implementation regulations. The Telco Law is further administered through a number of implementing regulations, which include:

   - Government Regulation No. 52 of 2000 on Provision of Telecommunications ("**GR 52/2000**");
   - Government Regulation No. 53 of 2000 on Utilisation of Radio Frequency Spectrum and Satellite Orbit ("**GR 53/2000**"); and
   - Law No. 32 of 2002 on Broadcasting (the Broadcasting Law).

3. **If so, what activities are covered and what licences or authorisations are required?**

   The Telco Law classifies the provision of telecommunications into:

   a) Provision of telecommunications services

   Provision of telecommunications services is defined as the provision of telecommunications services that allow telecommunications to be carried out, comprising:

   i) Basic Telephony Services, which include:

   - Telephony;

- Facsimile;
- Short message service; and
- Multimedia messaging service.

ii) Value-Added Telephony Services, including:

- Call center;
- Calling card;
- Internet Telephony for Public Interest (known as Voice over Internet Protocol or VOIP); and
- Content services.

iii) Multimedia Services

- Internet access (also known as Internet Services Providers or ISPs);
- Network access point providers;
- Data communication system; and
- Internet Protocol Television.

b) Provision of telecommunications network

Provision of telecommunications network is defined as the provision of a telecommunications network that allows telecommunications to be carried out, comprising:

i) Fixed Network

- Fixed-local network;
- Fixed-long distance connection network;
- Fixed-international connection network; and
- Fixed-closed network.

ii) Mobile Network

- Mobile terrestrial network;
- Mobile cellular network; and
- Mobile satellite network.

c) Provision of special telecommunications

This is defined as the provision of telecommunications that have a special nature, purpose, or operation. Special telecommunications may be provided for the following purposes:

i) Self-purpose, which may be in the form of amateur radio, inter-citizen radio

communication, or other activities that:

1. Require telecommunications that cannot be fulfilled by telecommunications network and/or services providers;
2. The location of the activity has not been reached by telecommunications network and/or services providers; and
3. Require a dedicated and separated telecommunications network;

ii) State security;

iii) Broadcasting.

On the licensing requirement, generally the provision of telecommunications must be based on a telecommunications provision license from the MCIT, which is applied for via the Online Single Submission ("**OSS**") system. Initially, the telecommunications license will be issued conditionally, in which the applicant must satisfy certain conditions within 9 – 12 months of its issuance. At the end of the validity of the conditional telecommunications license, the applicant must undergo an Operational Worthiness Test. Upon its completion, a permanent telecommunications license will be issued.

Depending on the type of telecommunications network or services that will be provided, the operator might be required to obtain another technical license, such as a radio frequency spectrum utilization, or radio station license, or landing right, as applicable.

4. **Is there any specific regulator for the provisions of communications-related services?**

The Minister of Communications and Information Technology (MCIT) is responsible for administering telecommunications, including the telecommunications network, telecommunications services, and special telecommunications.

The MCIT has also established the Indonesian Telecommunications Regulatory Body (BRTI) to assist in the administration of the telecommunications sector. The MCIT has specifically delegated its authority to regulate, supervise and control the provision of telecommunications networks and services to the BRTI, while maintaining the authority to formulate policies, regulate, supervise and control other fields of the telecommunications sector.

5. **Are they independent of the government control?**

No. The BRTI is established by the MCIT and must report on its performance to the MCIT. Further, the organization, working relations, membership, duties, and authorities of BRTI are governed by the MCIT.

6. **Are platform providers (social media, content sharing, information search engines) regulated?**

   Yes, digital platform providers are also subject to the EIT Law and its implementation regulations.

   Pursuant to Government Regulation No. 71 of 2019 on the Provision of Electronic Systems ("**GR 71/2019**"), digital platform providers fall under the definition of "Electronic Systems Operators or **ESOs**". An ESO is defined as a person, state administrator, business entity, or the public, that provides, processes or operates electronic systems with an electronic systems user in its own or other parties' interest.

7. **If so, does the reach of the regulator extend outside your jurisdiction?**

   Article 2 of the EIT Law stipulates that the EIT Law will apply to any person (whether an individual or legal entity) that engages in legal action either within or outside the jurisdiction of Indonesia, and has legal effect within and/or outside the jurisdiction of Indonesia that is detrimental to the interests of Indonesia. Further, as GR 71/2019 is the implementing regulations of the EIT Law, the provisions under GR 71/2019 also have extra-territorial effect.

   However, regardless of the extra-territorial effect of the EIT Law and the implementing regulations, the authorities acknowledge that the enforcement of these provisions on a foreign entity is subject to voluntary compliance of the entity and diplomatic relations.

8. **Does a telecoms operator need to be domiciled in the country?**

   Yes. Under the Telco Law, telecommunications network and services providers must be one of the following legal entities:

   - State-owned company;
   - Regional government-owned company;
   - Indonesian private business entity; or
   - Cooperative entity.

   Further, the provision of special telecommunications can be performed by:

   - Individuals;
   - Government institutions; or
   - Legal entities other than a telecommunications network or services operator

9. **Are there any restrictions on foreign ownership of telecoms operators?**

   Presidential Regulation No. 44 of 2016 on Lines of Business that are Closed and Lines of Business that are Conditionally Open to Investment (Negative List on Investments) imposes

the foreign shareholding restrictions with maximum 67% foreign ownership for a foreign investment company in the telecommunications sector in general, which includes those engaged in the following business activities:

an operator of a telecommunication network, covering the provision of fixed network and mobile network operations (cellular, satellite, or terrestrial);

- an operator of telecommunication services, covering:
- basic telephony services providers (telephony, facsimile, short message services, and/or multimedia messaging services);
  - content service providers (ringtones, premium short message services, etc);
  - internet service providers;
  - data communications system providers;
  - telephony internet service providers for the public;
  - internet interconnection services (network access point) providers; and
  - other multimedia services providers; and
- an operator of a telecommunications network that is integrated with telecommunications services.

Nevertheless, on the provision of telecommunication network and infrastructure, the Negative List on Investment imposes further restrictions on the provision of telecommunication towers, in which a telecommunications tower may only be provided and managed by a local (non-foreign investment/not foreign-owned) company. The Investment Coordinating Board should be consulted on shareholding restrictions applicable to other lines of business in the communications and informatics sectors on a case-by-case basis.

10. **Are there any regulations covering interconnection between operators?**

Yes, interconnection is regulated under the Telco Law, GR 52/2000, and MCIT Regulation No. 08/Per/M.KOMINFO/02/2006 on Interconnection ("**MCIT Reg 08/2006**"). In general, the Telco Law and its implementation regulations require telecommunications network operators to ensure the availability of interconnection.

11. **If so are these different for operators with market power?**

The Telco Law and its implementation regulations do not provide different rules towards operators with market power. However, MCIT Reg 08/2006 expressly requires telecommunications network operators to implement transparent and non-discriminatory practices in the provision of interconnection. Additionally, operators with market power are also subject to the provisions under Law No. 5 of 1999 on the Prohibitions of Monopolistic and Unfair Business Competition Practices.

12. **What are the principal consumer protection regulations that apply specifically to**

telecoms services?

Consumer protection in the telecommunications sector is subject to the general rules under Law No. 8 of 1999 on Consumer Protection. Additionally, sector-specific regulations also provide consumer protection rules, such as MCIT Regulation No. 01/PER/M.KOMINFO/01/2010 on Provision of Telecommunications Networks, as amended several times, last by MCIT Regulation No. 7 of 2015 and MCIT Regulation No. 13 of 2019 on Provision of Telecommunications Services.

13. **What legal protections are offered in relation to the creators of computer software?**

Under the Law No. 28 of 2014 on Copyright ("**Copyright Law**"), computer programs, including software, are an object of copyright. Therefore, the creators of computer software are entitled to legal protection for their creation under the Copyright Law, which includes moral and economic rights in their creations.

14. **Do you recognise specific intellectual property rights in respect of data/databases?**

Yes, the Copyright Law acknowledge compilation of data in computer-readable or other media format as an object of copyright protection.

15. **What key protections exist for personal data?**

Currently, there are no general provisions on data privacy, applicable to all sectors. The technical requirements on personal data protection are still subject to the sectoral regulations that are applicable for each type of business.

Nevertheless, within the context of electronic systems, the EIT Law, GR 71/2019, and MCIT Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("**Regulation 20/2016**") are currently considered the umbrella regulations for the management of personal data. As such, they are applicable to the operation of electronic systems in any field of business. The EIT Law and its implementation regulations emphasize the requirement to obtain consent for the use of information through electronic media that involves personal data, unless provided otherwise by relevant laws and regulations.

As regulated in GR 71/2019, in principle, personal data handling is subject to the following requirements:

1. the collection of personal data must be conducted in a limited and specific manner, lawfully, fairly, and with the acknowledgment and approval of data subject;
2. must be carried out in accordance with its purposes;
3. must ensure the rights of data subject;
4. must be conducted in an accurate, complete, non-misleading, up-to-date, and accountable manner, and by taking into account the purpose of personal data processing;

5. must be carried out by protecting the security of personal data from loss, misuse, unauthorized access, and disclosure, as well as from change or damage;
6. must conform with the need to notify the purposes of collection, processing activity, and failure in the protection of personal data; and
7. must be destroyed or deleted unless remaining in a retention period following the needs based on the provisions of laws and regulations.

In addition to the consent requirement, GR 71/2019 stipulates that personal data processing must be conducted in compliance with the applicable requirements:

- Performance of contractual obligations where the data subject is party to the contract or in order to fulfil a request of the data subject prior to entering into the contract;
- Compliance with legal obligation that is imposed on the data controller based on the laws and regulations;
- Fulfilment of the vital interests of the data subject;
- Exercise of authority vested in the data controller by the laws and regulations;
- Fulfilment of a public service obligation to which the data controller is subject in the public interest; and/or
- Pursuit of a legitimate interest of the data controller and/or the data subject.

16. **Are there restrictions on the transfer of personal data overseas?**

The requirements on cross-border data are regulated specifically under Regulation 20/2016. In addition to the need to obtain consent from the data subject, the transfer of the personal data to a territory outside of Indonesia must:

a) be coordinated with the Minister or the authorized official/agency

The coordination is implemented in the following form: (a) reporting the personal data transfer plan, specifying at least the full name of the destination country, the full name of the recipient, the date of transfer, and the reasons/purposes for which the personal data are transferred; (b) seeking advocacy, if necessary; and (c) reporting the results of the activity.

b) apply the provisions of the laws and regulations on cross-border personal data exchange.

Please note that, based on newly issued regulation on e-commerce, Government Regulation No. 80 of 2019 on E-Commerce, cross-border personal data transfer from Indonesia to other countries or regions outside Indonesian jurisdiction is prohibited, unless the country or region has been declared by the Minister of Trade as maintaining equal protection standards and levels with Indonesia.

17. **What is the maximum fine that can be applied for breach of data protection laws?**

Data breach can be subjected to administrative and criminal sanction, as elaborated below:

Administrative sanctions

GR 71/2019 stipulates that, the failure to protect personal data from loss, misuse, unauthorized access and disclosure, alteration, or damage towards the personal data is subject to administrative sanctions in the form of:

- written warning;
- administrative fine;
- temporary suspension;
- termination of access; and/or
- exclusion from a registry maintained by MCIT.

However, GR 71/2019 does not stipulate the maximum administrative fine for this violation.

Criminal Sanctions

Pursuant to the EIT Law, the following activities are subject to criminal sanction:

- intentionally and without authorization or unlawfully to alter, add, reduce, transmit, tamper with, delete, move, hide in any manner whatsoever electronic information and/or electronic documents belonging to other persons or the public, is subject to criminal sanctions in the form of imprisonment of up to 8 years and/or criminal fine of up to IDR 2 billion;
- intentionally and without authorization or unlawfully to move or transfer in any manner whatsoever electronic information and/or electronic records to electronic systems of unauthorized persons is subject to criminal sanction in the form of imprisonment of up to 9 years and/or criminal fine of up to IDR 3 billion
- intentionally and without authorization or unlawfully to alter, add, reduce, transmit, tamper with, delete, move, hide in any manner whatsoever electronic information and/or electronic documents belonging to other persons or the public that causes the disclosure of confidential electronic information and/or electronic document to become publicly accessible, is subject to criminal sanction in the form of imprisonment of up to10 years and/or criminal fine of up to IDR 5 billion.

18. **What additional protections have been implemented, over and above the GDPR requirements?**

Currently, the EIT Law, GR 71/2019, and Regulation 20/2016 set out the main rules for personal data protection in Indonesia. Although there are some indications that the GR 71/2019 and Regulation 20/2016 are influenced by the GDPR, these regulations must be deemed a separate and independent regulation regime from GDPR. The GDPR is directly applicable in Indonesia, unless certain criteria under the GDPR are satisfied (e.g., if an Indonesian company processes personal data of EU citizens).

The Indonesian government is currently preparing a bill on personal data protection ("**Privacy Bill**"), which is intended to be the main governing law for personal data protection in all sectors. The Privacy Bill indicates more significant influence of GDPR in data protection rules in Indonesia in the future, for example: (i) adoption of the "data processor" and "data controller" concept and differentiation; (ii) exemption from mandatory consent requirement for personal data processing based on certain legitimate bases; and (iii) an obligation to appoint Data Protection Officer under certain circumstances.

19. **Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?**

In general, the provision and use of cloud-based services would be subject to the EIT Law and GR 71/2019. In this case, there is no restriction on providing and using cloud-based services. However, Public ESOs, which are ESOs in the form of state administrative institutions and entities appointed by state administrative institutions, are required to manage, process, and/or store electronic information and/or data in Indonesia. Thus, Public ESOs can only use cloud-based services with data storage/processing facilities in Indonesia.

20. **Are there specific requirements for the validity of an electronic signature?**

Based on GR 71/2019, there are 2 types of e-signature:

- certified e-signature; and
- non-certified e-signature.

Regardless of the type of e-signature, they are deemed valid and shall have equal weight to manual signatures, thus having legal force and effect, if meeting the following requirements:

- the data related to the creation of the e-signature ("**Creation Data**") must be associated only with the signor (signature owner); during the electronic signing process, the Creation Data must be in the sole possession of the signor;
- any alteration to the e-signature, after signing, is clearly accessible;
- any alteration to the electronic information associated with the e-signature after signing, is clearly accessible;
- a specific method is adopted to identify the signatory; and
- there is a specific method to demonstrate that the signatory has given consent to the electronic information related to the transaction.

21. **In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?**

No, outsourcing of IT services does not automatically trigger the transfer of employees, assets or third-party contracts. It may be accepted by the parties to an agreement that there will be a transfer of employees, assets or third-party contracts; however, the transfer might need to be finalized with further legal documents (e.g., agreement for the assignment of

assets and employments agreements).

However, from an Indonesian labor law perspective, there may be an issue related to outsourcing services. Generally, a company (an assignor) cannot outsource its core activities to another party/entity (an assignee), failing which, the risk would be that the employees performing the outsourced activities (the assignee) can be deemed as employees of the assignor. In addition, only non-core activities (auxiliary activities) can be outsourced, and the determination on whether an activity is core or non-core would be done by a business association where the assignor falls under.

22. **If a software program which purports to be a form of A.I. malfunctions, who is liable?**

Indonesian laws and regulations have not regulated responsibility for A.I. yet.

The determination on liability would depend on the actual operation of the A.I. software itself. There might be scenarios where the developer of the A.I. or the end user of the A.I. software would be liable.

However, a party that suffers damages from the malfunctions may be able to claim to the party responsible for the malfunctions. The claim would depend on whether or not there is a contractual relationship between the party suffering the damages and the party responsible for the malfunctions.

If there is a contractual relationship, the claim can be submitted as a contractual claim, for so long as there is a contractual right therein. A non-defaulting party can claim for damages for so long as the damages are direct and foreseeable to the default concerned.

In case there is no contract, a party suffering the damages can submit a claim based on tort. Based on the general civil liability principles under Article 1365 of the Indonesian Civil Code, a party shall be liable for providing compensation for damages that result from that party's unlawful action (tort). Please note that, the unlawful action as stipulated herein includes action that violates:

- Laws and regulations;
- Other party's subjective rights;
- Legal obligation;
- Propriety/decency; and/or
- Reasonable care.

23. **What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of hacking/DDOS attacks?**

a) The EIT Law and GR 71/2019 stipulate general provisions on cybersecurity. The EIT Law

requires electronic systems operators to provide electronic systems in a reliable and secure manner, and take responsibility for the proper operation of the electronic systems. Further, GR 71/2019 elaborates that the security aspect shall cover the protection of electronic systems physically and non-physically, which shall include the security of hardware and software. Further, the GR 71/2019 also requires ESOs to maintain and implement a security procedure, facility, and system to prevent and mitigate security threats and attacks.

b) The EIT Law prohibits certain activities which in technical terms may constitute hacking:

- intentionally and without authorization or unlawfully to access in any manner whatsoever computers and/or electronic systems belonging to other persons is subject to criminal sanction in the form of imprisonment of up to 6 years and/or criminal fine of up to IDR 600 million
- intentionally and without authorization or unlawfully to access Computers and/or Electronic Systems in any manner whatsoever with intent to obtain electronic information and/or electronic documents is subject to criminal sanction in the form of imprisonment of up to 7 years and/or a criminal fine of up to IDR 700 million
- intentionally and without authorization or unlawfully to access computers and/or electronic systems in any manner whatsoever to breach, infiltrate, trespass into, or break through security systems are subject to criminal sanction in the form of imprisonment of up to 8 years and/or criminal fine of up to IDR 800 million

The EIT Law also includes a general prohibition of intentionally and without authorization or unlawfully to commits any act that results in interference on electronic systems and/or malfunction of electronic systems, which based on its nature, would include DDOS attacks. This activity is liable to criminal sanction in the form of imprisonment for up to 10 years and/or criminal fine of up to IDR 10 billion.

24. **What technology development will create the most legal change in your jurisdiction?**

The development of A.I. and user profiling would be a great challenge for Indonesian regulations, as automated decision-making by a computer is a deviation from the conventional liability concept under Indonesian laws and regulations. In this case, it would be necessary to have a certain threshold or criteria in order the determine the liable party if a decision is causing damage, and to mitigate the risk. Additionally, the vast practice of consumer profiling would be a challenge as it may be intrusive of human rights, since the use of machine-learning can be used to predict and/or shape consumer behaviour.

Further, the provision of cloud-based services would also be a challenge to Indonesian investment law, as, currently, services can be provided remotely and the need to establish an entity in Indonesia could be mitigated. From the business enterprise perspective, this would be viewed as an opportunity to expand their business with minimal cost. However, the government is greatly concerned about consumer protection and taxation aspects of this type

of service.

In the telecommunications sector, emerging OTT services, especially instant messaging, voice, and video chat services would be a challenge for the government to protect existing telecommunications service providers. We understand the OTT services are providing communications services via internet provided by licensed telecommunications operators, which are probably also providing text and voice communications services. However, there is a discrepancy in legal obligations of telecommunications operators and OTT services providers, where OTT services providers are not subject to the same or similar obligations, although providing similar services.

25. **Which current legal provision/regime creates the greatest impediment to economic development/ commerce?**

In general, the government is currently acknowledging the cross-territorial nature of technology services. We observe that the government is now more open to the provision of services by foreign entities, without requiring them to establish an Indonesian entity. This would boost the introduction of new technology services in Indonesia.

Further, the GR 71/2019 currently allows electronic systems operators for private scope to use data processing and storage facilities outside Indonesia, which would increase efficiency from a business perspective.

The government also issued Government Regulation No. 80 of 2019 on E-Commerce ("**GR 80/2019**"), which stipulates the general rules and requirements for e-commerce business operating in Indonesia. As GR 80/2019 acknowledges and allows the provision of e-commerce by foreign entities, we believe that this could expand the great commercial potential of large and micro, small, and medium enterprises in Indonesia.

26. **Do you believe your legal system specifically encourages or hinders digital services?**

The EIT Law adopts a technology-neutral approach and the freedom to choose technology principles in its provisions and implementation regulations. Thus, in principle, the government allows and encourages digital services to develop their technology, as long as it is not detrimental to Indonesia or customers.

However, in some cases, digital services are often being viewed or treated as conventional services, and are subject to the same compliance requirements for conventional services. This is often caused by the gap between the development of the digital services and the extant regulations. Although this seldom occurs, this practical issue could potentially become a challenge in Indonesia.

27. **To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?**

As previously explained, the EIT Law generally adopts a technology-neutral approach and freedom to choose technology principles in its provisions and implementation regulations. Thus, there is an opportunity to benefit from and develop A.I. in Indonesia. However, the laws and regulations currently do not provide a detailed elaboration on the limitation and liability aspects of A.I. We view that the issue of determining responsibility of a legal subject in the utilization of A.I. would need to be further assessed and regulated, to catch up with worldwide practice.