LAW OF THE REPUBLIC OF INDONESIA
NUMBER 11 OF 2008
ON
ELECTRONIC INFORMATION AND TRANSACTIONS[1]

AS CONSOLIDATED WITH:
LAW NUMBER 19 OF 2016 ON AMENDMENT TO LAW NUMBER 11 OF 2008 ON ELECTRONIC INFORMATION AND TRANSACTIONS

BY THE GRACE OF GOD ALMIGHTY

PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering:

a. that national development is a sustainable process which should always be responsive against various dynamics which happen in the public;

b. that globalization of information has put Indonesia as a part of global information society, therefore it requires the establishment of regulation on management of Electronic Information and Transaction on national level, thus the development of Information Technology may be performed in optimum manner, equally distributed, and spread to all strata of the society in order to educate the nation's life;

c. that development and advancement of Information Technology which is so rapid has caused alteration to activities of human's lives in various sectors, which directly have affected the inception of new forms of legal acts;

d. that the use and utilization of Information Technology should continue to be developed in order to protect, maintain, and strengthen national unity based on Laws and Regulations for the purpose of national interest;

---

[*] This translation is created with the best effort as can be offered and by any means, does not constitute and should not be treated as official translation or sworn translation for legal proceeding purposes. The copyright owner: 1) Should not be held liable for any error which occurs in the source document; 2) Reserves the right to change and modify this translation, with subsequent notifications given to every clients in timely manner; and 3) May seek redress for any unlawful or unauthorized transfer or disclosure of this translation against any party.

e. that utilization of Information Technology takes pivotal role in national trading and economic growth in order to realize public welfare;

f. that government is required to support the development of Information Technology through legal infrastructures and its regulation, therefore the utilization of Information Technology is performed in secure manner in bid to prevent its misuse by regarding the values of religion and socio-culture of the Indonesian society;

g. that based on considerations as referred to in letter a, letter b, letter c, letter d, letter e, and letter f, it is deemed necessary to enact Law on Electronic Information and Transactions.

LAW NUMBER 19 OF 2016 ON AMENDMENT TO LAW NUMBER 11 OF 2008 ON ELECTRONIC INFORMATION AND TRANSACTION

Considering:

a. that in order to guarantee recognition, as well as respect toward rights and freedom of others and in order to fulfill fair demand in accordance with considerations of security and public order in a democratic society, amendment to Law Number 11 of 2008 on Electronic Information and Transactions is deemed necessary to be made, so that fairness, public order, and legal certainty can be realized;

b. that based on consideration as referred to in letter a, it is deemed necessary to enact Law on Amendment to Law Number 11 of 2008 on Electronic Information and Transactions;

In view of:

Article 5 paragraph (1) and Article 20 of the 1945 Constitution of the Republic of Indonesia;

LAW NUMBER 19 OF 2016 ON AMENDMENT TO LAW NUMBER 11 OF 2008 ON ELECTRONIC INFORMATION AND TRANSACTION

In view of:

1. Article 5 paragraph (1), Article 20, Article 25A, Article 28D paragraph (1), Article 28E paragraph (2), Article 28E paragraph (3), Article 28F, Article 28G paragraph (1), Article 28J paragraph (2), and Article 33 paragraph (2) of the 1945 Constitution of the Republic of Indonesia;
2. Law Number 11 of 2008 on Electronic Information and Transactions (State gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843);

With the Mutual Agreement of

HOUSE OF REPRESENTATIVES OF THE REPUBLIC OF INDONESIA

and

PRESIDENT OF THE REPUBLIC OF INDONESIA

HAVE DECIDED:

To enact:

LAW ON ELECTRONIC INFORMATION AND TRANSACTIONS.

CHAPTER 1
GENERAL PROVISIONS

Article 1*

Under this Law, the following definitions are employed:

1. Electronic Information is one or a group of electronic data, including but not limited to text, sound, image, map, design, photo, electronic data interchange (EDI), electronic mail (*surat elektronik*), telegram, telex, telecopy or its equivalent, letter,

mark, number, Access Code, symbol, or perforation which has been processed and having meaning or understandable by the person who is capable of understanding it.

2. Electronic Transaction is legal act which is performed by using Computer, Computer network, and/or other electronic media.
3. Information Technology is a technique to collect, prepare, store, process, publish, analyze, and/or disseminate information.
4. Electronic Document is any Electronic Information which is produced, forwarded, sent, received, or stored in the forms of analogue, digital, electromagnetic, optical, or its equivalent, which may be viewed, published, and/or listened to via Computer or Electronic System, including but not limited to text, sound, image, map, design, photo or its equivalent, letter, mark, number, Access Code, symbol or perforation which having meaning or definition or understandable by the person who is capable of understanding it.
5. Electronic System is a set of electronic devices and procedures which function to prepare, collect, process, analyze, store, display, publish, send, and/or disseminate Electronic Information.
6. Organization of Electronic System is utilization of Electronic System by state organizer, Person, Enterprise, and/or the public.

6a Electronic System Provider is any Person, state organizer, Enterprise, and the public who provide, manage, and/or operate Electronic System, either independently or collectively, to Electronic System user, for its own and/or other's needs.

7. Electronic System Network is the connection between two or more Electronic Systems, which are closed or open.
8. Electronic Agent is device of an Electronic System which is created to perform an act against a certain Electronic Information automatically as organized by Person.
9. Digital Certificate is certificate that is electronic in nature which contains Digital Signature and identity that shows legal subject status of the parties to Electronic Transaction which is issued by Digital Certification Provider.

10. Digital Certification Provider is incorporated entity which functions as the trusted party, who grants and audits Digital Certificate.
11. Reliability Certification Agency is independent agency which is established by acknowledged professionals, legalized, and supervised by the Government, with the authority to audit and issue reliability certificate in Electronic Transaction.
12. Digital Signature is signature which consists of Electronic Information that is affixed, associated or related to other Electronic Information which is used as verification and authentication tool.
13. Signor is legal subject who is associated with or related to Digital Signature.
14. Computer is tool for processing of electronic, magnetic, optical data, or system which performs logical, arithmetical, and repository functions.
15. Access is an act of performing interaction with Electronic System which is independent or within the network.
16. Access Code is number, letter, symbol, other character or combination of them, which becomes the key to be able to access Computer and/or other Electronic System.
17. Electronic Contract is agreement of the parties which is made through Electronic System.
18. Sender is legal subject who sends Electronic Information and/or Electronic Document.
19. Acceptor is legal subject who accepts Electronic Information and/or Electronic Document from the Sender.
20. Domain Name is internet address of state organizer, Person, Enterprise, and/or the public, which may be used to communicate through internet, in the forms of code or composition of unique characters to show certain location on the internet.
21. Person is individual, either Indonesian citizen, foreign citizen, or incorporated entity.
22. Enterprise is individual company or partnership company, either taking form as incorporated entity or unincorporated entity.
23. Government is Minister or other official who is appointed by the President.

Article 2

This Law prevails for any Person who performs legal act as addressed under this Law, either residing in Indonesia's jurisdiction or outside of Indonesia's jurisdiction, which having legal consequence within Indonesia's jurisdiction and/or outside of Indonesia's jurisdiction and injuring Indonesia's interests.

CHAPTER II
PRINCIPLES AND PURPOSES

Article 3

The utilization of Information Technology and Electronic Transaction is performed based on the principles of legal certainty, benefit, precautionary, good faith, and freedom to choose technology or technology-neutral.

Article 4

The utilization of Information Technology and Electronic Transaction is performed with the purposes to:

a. educate nation's life as a part of global information society;
b. develop national trading and economy in the event of increasing public welfare;
c. increase the effectiveness and efficiency of public services;
d. open opportunities as broad as possible to any Person to advance the thinking and ability within the sectors of the use and utilization of Information Technology as optimal as possible and accountable; and
e. provide the feeling of secure, fairness, and legal certainty for the user and provider of Information Technology.

CHAPTER III
ELECTRONIC INFORMATION, DOCUMENT, AND SIGNATURE

Article 5*

(1) Electronic Information and/or Electronic Document and/or its hardcopy are valid legal evidence.

(2) Electronic Information and/or Electronic Document and/or its hardcopy as referred to in paragraph (1) are expansion of valid evidence in accordance with the prevailing Procedural Law in Indonesia.

(3) Electronic Information and/or Electronic Document are declared valid if using Electronic System in accordance with provisions as addressed under this Law.

(4) Provisions on Electronic Information and/or Electronic Document as referred to in paragraph (1) do not apply for:

a. letter, of which, according to the Law should be made in writing; and

b. letter, as well as its documents, of which, according to the Law should be made in the forms of notarial deed or deed which is made by notary [*pejabat pembuat akta*].

Article 6

In case there are provisions other than as addressed under Article 5 paragraph (4) which require that an information should be in the forms of writing or its authentic version, Electronic Information and/or Electronic Document are deemed to be valid, provided that information as addressed in it may be accessed, displayed, guaranteed on its integrity, and accountable, hence it explains a condition.

Article 7

Any Person who declares a right, strengthens existing right, or reject right of other Person based on the existence of Electronic Information and/or Electronic Document, should ascertain that Electronic Information and/or Electronic Document under its possession are originated from Electronic System which fulfills requirements based on Laws and Regulations.

Article 8

(1) Unless agreed otherwise, delivery time of an Electronic Information and/or Electronic Document is determined when Electronic Information and/or Electronic Document is determined when Electronic Information and/or Electronic Document have been sent to the correct address by the Sender to an Electronic System which is appointed or used by the Acceptor and has entered Electronic System which is beyond the control of the Sender.

(2) Unless agreed otherwise, acceptance time of an Electronic Information and/or Electronic Document is determined when Electronic Information and/or Electronic Document enter Electronic System which is under the control of eligible Acceptor.

(3) In case the Acceptor has appointed a certain Electronic System to accept Electronic Information, acceptance occurs when Electronic Information and/or Electronic Document enter the appointed Electronic System.

(4) In case there are two or more information systems which are used for the delivery or acceptance of Electronic Information and/or Electronic Document, then:

a. delivery time is when Electronic Information and/or Electronic Document enter the first information system which exists beyond the control of the Sender;

b. acceptance time is when Electronic Information and/or Electronic Document enter the final information system which exists under the control of the Acceptor.

Article 9

Businesses who offer product through Electronic System should provide complete and veracious information relating to the conditions of contract, producer, and offered product.

Article 10

(1) Any businesses which organize Electronic Transaction may be certified by Reliability Certification Agency.

(2) Provisions on establishment of Reliability Certification Agency as referred to in paragraph (1) are addressed under Regulation of the Government.

Article 11

(1) Digital Signature possesses valid legal power and legal consequence insofar it fulfills the following requirements:
   a. generation data on Digital Signature is related only to the Signor;
   b. generation data on Digital Signature during the process of electronic singing only exists within the control of the Signor;
   c. any alteration to Digital Signature which occurs subsequent to the signing period may be known;
   d. any alteration to Electronic Information relating to such Digital Signature subsequent to the signing period may be known;
   e. there is certain method which is used to identify who the Signor is; and
   f. there is certain method which shows that the Signor has given its consent to related Electronic Information.

(2) Further provisions on Digital Signature as referred to in paragraph (1) are addressed under Regulation of the Government.

Article 12

(1) Any Person who is involved in Digital Signature is obliged to provide security of Digital Signature which is used by it.

(2) Security of Digital Signature as referred to in paragraph (1) at least encompasses:
   a. system is inaccessible by another ineligible Person;
   b. Signor should implement precautionary principles in order to prevent invalid use of data relating to the generation of Digital Signature;
   c. Signor should, without any delay, use the method which is advised by Digital Signature provider or other method which is proper and should have immediately notified someone whom by the Signor is considered to trust Digital Signature or to the party as the supporter of Digital Signature services, if:
      1. Signor knows that the generation data on Digital Signature has been breached; or
      2. condition which is known by the Signor may raise significant risk, probably due to the breach of generation data on Digital Signature; and

d. in case Digital Certificate is used to support Digital Signature, the Signor should guarantee the veracity and integrity of all information relating to such Digital Certificate.

(3) Any Person who commits violation of provisions as referred to in paragraph (1), is held liable for any incurred losses and legal consequences.

CHAPTER IV
DIGITAL CERTIFICATION PRACTICE AND ELECTRONIC SYSTEM

First Division
Digital Certification Practice

Article 13

(1) Any Person is entitled to use the service of Digital Certification Provider for the generation of Digital Signature.

(2) Digital Certification Provider should guarantee interconnectedness of a Digital Signature with its owner.

(3) Digital Certification Provider consists of:
   a. Indonesian Digital Certification Provider; and
   b. foreign Digital Certification Provider.

(4) Indonesian Digital Certification Provider takes form as Indonesian incorporated entity and is domiciled in Indonesia.

(5) Foreign Digital Certification Provider which operates in Indonesia should be registered in Indonesia.

(6) Further provisions on Digital Certification Provider as referred to in paragraph (3) are addressed under Regulation of the Government.

Article 14

Digital Certification Provider as referred to under Article 13 paragraph (1) up to paragraph (5) should provide accurate, clear, and certain information to every service user, encompassing:

a. method that is used to identify the Signor;
b. matter which may be used to know the identity of generator of Digital Signature; and
c. matter which may be used to show the validity and security of Digital Signature.

Second Division
Organization of Electronic System

Article 15

(1) Any Electronic System Provider should organize Electronic System in reliable and secure manners, as well as held responsible for the proper operation of Electronic System.
(2) Electronic System Provider is held liable for the Organization of its Electronic System.
(3) Provisions as referred to in paragraph (2) do not apply in case the occurrence of force majeure [*keadaan memaksa*], error, and/or negligence from Electronic System user can be proven.

Article 16

(1) Insofar that it is not deemed otherwise under separate law, any Electronic System Provider must operate Electronic System which fulfills the following minimum requirements:
    a. able to redisplay Electronic Information and/or Electronic Document in integrated manner in accordance with the retention period as established under Laws and Regulations;
    b. able to protect the availability, integrity, authenticity, confidentiality, and accessibility of Electronic Information in the course of such Organization of Electronic System;
    c. able to operate in accordance with procedure or guideline in the course of such Organization of Electronic System;

d. be equipped with procedure or guideline which is published using language, information, or symbol which may be understood by the party in connection with such Organization of Electronic System; and

e. owns sustainable mechanism to maintain the recency, clarity, and accountability of procedure or guideline.

(2) Further provisions on Organization of Electronic System as referred to in paragraph (1) are addressed under Regulation of the Government.

CHAPTER V
ELECTRONIC TRANSACTION

Article 17

(1) Organization of Electronic Transaction may be performed within public or private scope.

(2) The parties who perform Electronic Transaction as referred to in paragraph (1) must be in good faith in the course of performing interaction and/or exchange of Electronic Information and/or Electronic Document during the ongoing transaction.

(3) Further provisions on organization of Electronic Transaction as referred to in paragraph (1) are addressed under Regulation of the Government.

Article 18

(1) Electronic Transaction which is incorporated in the forms of Electronic Contract binds the parties.

(2) The parties have the authority to make choice of law for international Electronic Transaction which is made by them.

(3) If the parties do not make choice of law for international Electronic Transaction, the prevailing law is based on the principles of Private International Law.

(4) The parties have the authority to determine the forum of court, arbitration, or other alternative dispute resolution body which is competent to handle the dispute which might occur from international Electronic Transaction which is made by them.

(5) If the parties do not make choice of forum as referred to in paragraph (4), determination of competence of court, arbitration, or other alternative dispute resolution body which is competent to handle the dispute which might occur from such transaction, is based on the principles of Private International Law.

Article 19

The parties who perform Electronic Transaction should use Electronic System which is agreed.

Article 20

(1) Unless deemed otherwise by the parties, Electronic Transaction takes place when the offering of transaction which is sent by the Sender has been accepted and agreed by the Acceptor.

(2) Agreement to offering of Electronic Transaction as referred to in paragraph (1) should be performed by electronic acceptance statement.

Article 21

(1) Sender or Acceptor may perform Electronic Transaction by itself, through the party who is authorized by it, or through Electronic Agent.

(2) Party who is held liable for any legal consequences for the performance of Electronic Transaction as referred to in paragraph (1) is addressed as follows:

a. if it is performed by itself, any legal consequences for the performance of Electronic Transaction become the liability of the parties to transaction;

b. if it is performed through the granting of authorization, any legal consequences for the performance of Electronic Transaction become the liability of principal; or

c. if it is performed through Electronic Agent, any legal consequences for the performance of Electronic Transaction become the liability of Electronic Agent provider.

(3) If losses of Electronic Transaction are caused by the failure of operation of Electronic Agent due to a direct act of third party toward Electronic System, any legal consequences become the liability of Electronic Agent provider.

(4) If losses of Electronic Transaction are caused by the failure of operation of Electronic Agent due to negligence of the service user, any legal consequences become the liability of service user.

(5) Provisions as referred to in paragraph (2) do not apply in case the occurrence of force majeure [*keadaan memaksa*], error, and/or negligence from Electronic System user can be proven.

Article 22

(1) Certain Electronic Agent provider should accommodate feature for Electronic Agent which is operated by it, which enables its user to perform modification to information which is still undergoing the transaction process.

(2) Further provisions on certain Electronic Agent provider as referred to in paragraph (1) are addressed under Regulation of the Government.

CHAPTER VI
DOMAIN NAMES, INTELLECTUAL PROPERTY RIGHTS, AND PROTECTION OF INDIVIDUAL RIGHTS

Article 23

(1) Any state organizer, Person, Enterprise, and/or the public are entitled to own Domain Name based on the first-come-first-serve principle.

(2) Ownership and use of Domain Name as referred to in paragraph (1) should be based on good faith, not violating fair business competition principles, and not violating rights of another Person.

(3) Any state organizer, Person, Enterprise, or the public who is injured due to unauthorized use of Domain Name by other Person, is entitled to file a lawsuit for cancellation of Domain Name in question.

Article 24

(1) Domain Name Registry is Government and/or the public.

(2) In case dispute occurs relating to the registry of Domain Name by the public, Government is authorized to temporarily take over registry of Domain Name which is disputed.

(3) Domain Name Registry which exists outside of Indonesian territories and Domain Name which is registered by it, its existence is acknowledged, provided that it is not in contradictory with Laws and Regulations.

(4) Further provisions on registry of Domain Name as referred to in paragraph (1), paragraph (2), and paragraph (3) are addressed under Regulation of the Government.

Article 25

Electronic Information and/or Electronic Document which are composed into intellectual creation, internet site, and intellectual creation which exists within it is protected as Intellectual Property Right based on provisions under Laws and Regulations.

Article 26*

(1) Unless deemed otherwise under laws and regulations, the use of any information through electronic media in connection with personal data of an individual should be performed based on consent of Person in question.

(2) Any Person whose right is violated as referred to in paragraph (1) may file a lawsuit for incurred losses based on this Law.

(3) Any Electronic System Provider must erase Electronic Information and/or Electronic Document which are irrelevant that are under its control upon request from person in question based on court stipulation.

(4) Any Electronic System Provider must provide mechanism for the erasure of Electronic Information and/or Electronic Document which are no longer relevant in accordance with provisions under laws and regulations.

(5) Provisions on procedures for the erasure of Electronic Information and/or Electronic Document as referred to in paragraph (3) and paragraph (4) are addressed under regulation of the government.

CHAPTER VII
PROHIBITED ACTS

Article 27*

(1) Any Person who deliberately and unlawfully distributes and/or transmits and/or makes the accessibility of Electronic Information and/or Electronic Document containing contents which violate decency.

(2) Any Person who deliberately and unlawfully distributes and/or transmits and/or makes the accessibility of Electronic Information and/or Electronic Document containing contents on gambling.

(3) Any Person who deliberately and unlawfully distributes and/or transmits and/or makes the accessibility of Electronic Information and/or Electronic Document containing contents on insult and/or defamation.

(4) Any Person who deliberately and unlawfully distributes and/or transmits and/or makes the accessibility of Electronic Information and/or Electronic Document containing contents on extortion and/or threat.

Article 28

(1) Any Person who deliberately and unlawfully disseminates hoax and misleading news which inflict losses for consumers to Electronic Transaction.

(2) Any Person who deliberately and unlawfully disseminates information which is aimed to create hatred or hostility toward certain individual and/or group of society based on ethnicity, religion, race, and inter-group relation (*Suku, Agama, Ras, dan Antargolongan* – SARA).

Article 29

Any Person who deliberately and unlawfully sends Electronic Information and/or Electronic Document containing violence threat or frightening which is addressed personally.

Article 30

(1) Any Person who deliberately and unlawfully or illegally accesses Computer and/or Electronic System as owned by another Person by all means.

(2) Any Person who deliberately and unlawfully or illegally accesses Computer and/or Electronic System by all means with the purpose of obtaining Electronic Information and/or Electronic Document.

(3) Any Person who deliberately and unlawfully or illegally accesses Computer and/or Electronic System by all means by violating, breaching, trespassing, or penetrating security system.

Article 31*

(1) Any Person who deliberately and unlawfully or illegally performs interception or wiretapping of Electronic Information and/or Electronic Document in a Computer and/or certain Electronic System as owned by another Person.

(2) Any Person who deliberately and unlawfully or illegally performs interception of transmission of Electronic Information and/or Electronic Document which is not public in nature, from, to, and within a Computer and/or certain Electronic System as owned by another Person, both not causing any alteration or causing any alteration, deletion, and/or cessation of Electronic Information and/or Electronic Document which are being transmitted.

(3) Provisions as referred to in paragraph (1) and paragraph (2) do not apply against interception or wiretapping as performed in the event of law enforcement upon request from police, public prosecutor's office, or another institution which authorities are established based on law.

(4) Further provisions on procedures for interception as referred to in paragraph (3) are addressed under a law.

Article 32

(1) Any Person who deliberately and unlawfully or illegally, by all means, alters, adds, reduces, performs transmission, damages, deletes, moves, hides an Electronic Information and/or Electronic Document as owned by another Person or owned by the public.

(2) Any Person who deliberately and unlawfully or illegally, by all means, moves or transfers Electronic Information and/or Electronic Document to Electronic System of another Person who is ineligible.

(3) Against act as referred to in paragraph (1) which causes the disclosure of an Electronic Information and/or Electronic Document which is confidential in nature to be accessible by the public with the improper data integrity.

Article 33

Any Person who deliberately and unlawfully or illegally performs any act which causes the interference of Electronic System and/or causes Electronic System to not properly in operation.

Article 34

(1) Any Person who deliberately and unlawfully or illegally produces, sells, procures for use purposes, imports, distributes, provides or possesses:

   a. hardware or software of Computer which is designed or specifically developed to facilitate an act as referred to under Article 27 up to Article 33;

   b. password of Computer, Access Code, or matter which is similar to it, with an aim for Electronic System to be accessible with the purpose of facilitating an act as referred to under Article 27 up to Article 33.

(2) Act as referred to in paragraph (1) is not a criminal act if it is aimed to perform the activities in regards to research, testing of Electronic System, for protection of the Electronic System itself in lawful and legal manners.

Article 35

Any Person who deliberately and unlawfully or illegally performs manipulation, creation, alteration, deletion, damaging of Electronic Information and/or Electronic Document with the aim that such Electronic Information and/or Electronic Document is deemed to be as if it is the authentic data.

Article 36

Any Person who deliberately and unlawfully or illegally performs an act as referred to under Article 27 up to Article 34 which inflicts losses to another Person.

Article 37

Any Person who deliberately performs prohibited acts as referred to under Article 27 up to Article 36 outside of Indonesia's territories against Electronic System which exists in Indonesia's jurisdictions.

CHAPTER VIII
DISPUTE RESOLUTION

Article 38

(1) Any Person may file a lawsuit against the party who organizes Electronic System and/or uses Information Technology which inflicts losses.

(2) The public may file a lawsuit through class action [*perwakilan*] against the party who organizes Electronic System and/or uses Information Technology which causes losses for the public, in accordance with provisions under Laws and Regulations.

Article 39

(1) Civil lawsuit is performed in accordance with provisions under Laws and Regulations.

(2) Other than resolution through civil lawsuit as referred to in paragraph (1), the parties may resolve the dispute through arbitration, or other alternative dispute resolution body in accordance with provisions under Laws and Regulations.

CHAPTER IX
GOVERNMENT'S ROLES AND PUBLIC ROLES

Article 40*

(1) Government facilitates the utilization of Information Technology and Electronic Transaction in accordance with provisions under laws and regulations.

(2) Government protects public interest from any types of interferences as a consequence of misuse of Electronic Information and Electronic Transaction which disturbs public order, in accordance with provisions under laws and regulations.

(2a) Government must perform prevention of dissemination and use of Electronic Information and/or Electronic Document containing prohibited contents in accordance with provisions under laws and regulations.

(2b) In the course of performing prevention as referred to in paragraph (2a), Government is authorized to perform termination of access and/or order Electronic System Provider to perform termination of access against Electronic Information and/or Electronic Document containing illegal contents.

(3) Government determines body or institution which possesses strategic electronic data which must be protected.

(4) Body or institution as referred to in paragraph (3) should produce Electronic Document and its electronic backup record, as well as connect it to certain data center for data security purposes.

(5) Body or institution other than as addressed in paragraph (3) produces Electronic Document and its electronic backup record in accordance with the needs of protection of data as possessed by it.

(6) Further provisions on role of the Government as referred to in paragraph (1), paragraph (2), paragraph (2a), paragraph (2b), and paragraph (3) are addressed under regulation of the government.

Article 41

(1) The public may take role in the increase in utilization of Information Technology through the use and Organization of Electronic System and Electronic Transaction in accordance with provisions under this Law

(2) Public role as referred to in paragraph (1) may be organized through an agency as established by the public.

(3) Agency as referred to in paragraph (2) may possess consultation and mediation functions.

CHAPTER X
INVESTIGATION

Article 42

Investigation against criminal act as referred to under this Law, is performed based on provisions under Criminal Procedural Law and provisions under this Law.

Article 43*

(1) In addition to Indonesian National Police Investigator, certain Civil Servant Officer within the scope of the Government whose scope of its duties and responsibilities is within the sectors of Information Technology and Electronic Transaction, is granted special authority as investigator under the Law on Criminal Procedural Law in order to perform investigation of criminal act within the sectors of Information Technology and Electronic Transaction.

(2) Investigation within the sector of Information Technology and Electronic Transaction as referred to in paragraph (1) is performed by considering protection of privacy, confidentiality, smoothness of public services, and integrity or wholeness of data in accordance with provisions under laws and regulations.

(3) Search [*penggeledahan*] and/or confiscation of Electronic System which relates to allegation of criminal act within the sectors of Information Technology and Electronic Transaction are performed in accordance with the provisions of criminal procedural law.

(4) In the course of performing search and/or confiscation as referred to in paragraph (3), investigator must keep the maintenance of public-service interests.

(5) Civil Servant Investigator as referred to in paragraph (1) is authorized to:

a. solicit report or complaint from an individual on the occurrence of criminal act within the sectors of Information Technology and Electronic Transaction;

b. summon any Person or other party to be heard and examined as suspect or witness in connection with the occurrence of allegation of criminal act within the sectors of Information Technology and Electronic Transaction;

c. perform examination on veracity of report or statement in relation to criminal act within the sectors of Information Technology and Electronic Transaction;

d. perform examination against Person and/or Enterprise which is reasonably alleged to commit criminal act within the sectors of Information Technology and Electronic Transaction;

e. perform examination against tools and/or means relating to Information Technology activities which are alleged to be used to commit criminal act within the sectors of Information Technology and Electronic Transaction;

f. perform search against certain places which are alleged to be used as the place to commit criminal act within the sectors of Information Technology and Electronic Transaction;

g. perform sealing and confiscation against tools and/or means of Information Technology activities which are alleged to be used in incompliance from provisions under laws and regulations;

h. produce a data and/or Electronic System relating to criminal act within the sectors of Information Technology and Electronic Transaction, so that it is inaccessible;

i. request information which exists within Electronic System or information which is produced by Electronic System from Electronic System Provider which is related to criminal act within the sectors of Information Technology and Electronic Transaction;

j. request expert assistance which is required for investigation of criminal act within the sectors of Information Technology and Electronic Transaction; and/or

k. conduct cessation of investigation of criminal act within the sectors of Information Technology and Electronic Transaction in accordance with provisions of criminal procedural law.

(6) Arrest and detainment of perpetrator of criminal act within the sectors of Information Technology and Electronic Transaction are performed in accordance with provisions of criminal procedural law.

(7) Civil Servant Officer Investigator as referred to in paragraph (1), in the course of performing its duties, notifies the commencement of investigation to Public Prosecutor through Indonesian National Police Investigator.

(7a) In case investigation has been concluded, Civil Servant Officer Investigator as referred to in paragraph (1) submits its investigation result to Public Prosecutor through Indonesian National Police Investigator.

(8) In the event of unveiling criminal act of Electronic Information and Electronic Transaction, investigator may enter into cooperation with investigator from other state in order to exchange information and evidence in accordance with provisions under laws and regulations.

Article 44

Evidence for investigation, prosecution and examination in court proceedings according to provisions under this Law, are as follows:

a. evidence as referred to in provisions under Laws and Regulations; and

b. other evidence in the forms of Electronic Information and/or Electronic Document as referred to under Article 1 point 1 and point 4, as well as Article 5 paragraph (1), paragraph (2), and paragraph (3).

CHAPTER XI
CRIMINAL PROVISIONS

Article 45*

(1) Any Person who deliberately and unlawfully distributes and/or transmits and/or causes the access of Electronic Information and/or Electronic Document containing contents which violate decency as referred to under Article 27 paragraph (1) is sentenced with imprisonment for 6 (six) years at maximum and/or fines in sum of IDR 1,000,000,000.00 (one billion rupiahs) at maximum.

(2) Any Person who deliberately and unlawfully distributes and/or transmits and/or causes the access of Electronic Information and/or Electronic Document containing contents on gambling as referred to under Article 27 paragraph (2) is sentenced with imprisonment for 6 (six) years at maximum and/or fines in sum of IDR 1,000,000,000.00 (one billion rupiahs) at maximum.

(3) Any Person who deliberately and unlawfully distributes and/or transmits and/or causes the access of Electronic Information and/or Electronic Document containing contents on insult and/or defamation as referred to under Article 27 paragraph (3) is sentenced with imprisonment for 4 (four) years at maximum and/or fines in sum of IDR 750,000,000.00 (seven hundred and fifty million rupiahs) at maximum.

(4) Any Person who deliberately and unlawfully distributes and/or transmits and/or causes the access of Electronic Information and/or Electronic Document containing contents on extortion and/or threat as referred to under Article 27 paragraph (4) is sentenced with imprisonment for 6 (six) years at maximum and/or fines in sum of IDR 1,000,000,000.00 (one billion rupiahs) at maximum.

(5) Provisions as referred to in paragraph (3) are complaint offense.

Article 45A*

(1) Any Person who deliberately and unlawfully disseminates hoax and misleading news which inflict losses for consumers to Electronic Transaction as referred to under Article 28 paragraph (1) is sentenced with imprisonment for 6 (six) years at

maximum and/or fines in sum of IDR 1,000,000,000.00 (one billion rupiahs) at maximum.

(2) Any Person who deliberately and unlawfully disseminates information which is aimed to create hatred or hostility toward certain individual and/or group of society based on ethnicity, religion, race, and inter-group relation (SARA) as referred to under Article 28 paragraph (2) is sentenced with imprisonment for 6 (six) years at maximum and/or fines in sum of IDR 1,000,000,000.00 (one billion rupiahs) at maximum.

Article 45B*

Any Person who deliberately and unlawfully sends Electronic Information and/or Electronic Document containing violence threat or frightening which is addressed personally as referred to under Article 29 is sentenced with imprisonment for 4 (four) years at maximum and/or fines in sum of IDR 750,000,000.00 (seven hundred and fifty million rupiahs) at maximum.

Article 46

(1) Any Person who fulfills elements as referred to under Article 30 paragraph (1) is sentenced with imprisonment for 6 (six) years at maximum and/or fines in sum of IDR 600,000,000.00 (six hundred million rupiahs) at maximum.

(2) Any Person who fulfills elements as referred to under Article 30 paragraph (2) is sentenced with imprisonment for 7 (seven) years at maximum and/or fines in sum of IDR 700,000,000.00 (seven hundred million rupiahs) at maximum.

(3) Any Person who fulfills elements as referred to under Article 30 paragraph (3) is sentenced with imprisonment for 8 (eight) years at maximum and/or fines in sum of IDR 800,000,000.00 (eight hundred million rupiahs) at maximum.

Article 47

Any Person who fulfills elements as referred to under Article 31 paragraph (1) or paragraph (2) is sentenced with imprisonment for 10 (ten) years at maximum and/or fines in sum of IDR 800,000,000.00 (eight hundred million rupiahs) at maximum.

Article 48

(1) Any Person who fulfills elements as referred to under Article 32 paragraph (1) is sentenced with imprisonment for 8 (eight) years at maximum and/or fines in sum of IDR 2,000,000,000.00 (two billion rupiahs) at maximum.

(2) Any Person who fulfills elements as referred to under Article 32 paragraph (2) is sentenced with imprisonment for 9 (nine) years at maximum and/or fines in sum of IDR 3,000,000,000.00 (three billion rupiahs) at maximum.

(3) Any Person who fulfills elements as referred to under Article 32 paragraph (3) is sentenced with imprisonment for 10 (ten) years at maximum and/or fines in sum of IDR 5,000,000,000.00 (five billion rupiahs) at maximum.

Article 49

Any Person who fulfills elements as referred to under Article 33, is sentenced with imprisonment for 10 (ten) years at maximum and/or fines in sum of IDR 10,000,000,000.00 (ten billion rupiahs) at maximum.

Article 50

Any Person who fulfills elements as referred to under Article 34 paragraph (1) is sentenced with imprisonment for 10 (ten) years at maximum and/or fines in sum of IDR 10,000,000,000.00 (ten billion rupiahs) at maximum.

Article 51

(1) Any Person who fulfills elements as referred to under Article 35 is sentenced with imprisonment for 12 (twelve) years at maximum and/or fines in sum of IDR 12,000,000,000.00 (twelve billion rupiahs) at maximum.

(2) Any Person who fulfills elements as referred to under Article 36 is sentenced with imprisonment for 12 (twelve) years at maximum and/or fines in sum of IDR 12,000,000,000.00 (twelve billion rupiahs) at maximum.

Article 52

(1) In case criminal act as referred to under Article 27 paragraph (1) relates to decency or sexual exploitation in regards to child, a one-third additional sentence of primary sentence is imposed.

(2) In case act as referred to under Article 30 up to Article 37 is addressed to Computer and/or Electronic System, as well as Electronic Information and/or Electronic Document as owned by the Government and/or which is used for public services, it is sentenced with primary sentence and one-third additional sentence.

(3) In case act as referred to under Article 30 up to Article 37 is addressed to Computer and/or Electronic System, as well as Electronic Information and/or Electronic Document as owned by the Government and/or strategic body, including and not limited to defence agency, central bank, banking, finance, international body, aviation authority, it is threatened with the maximum sentence of primary sentence of each Article, added with two-third additional sentence.

(4) In case criminal act as referred to under Article 27 up to Article 37 is committed by corporation, it is sentenced with primary sentence and two-third additional sentence.

CHAPTER XII
TRANSITIONAL PROVISIONS

Article 53

When this Law enters into force, all Laws and Regulations and institutional aspect in connection with utilization of Information Technology which are not in contradictory with this Law are declared to continue to prevail.

CHAPTER XIII
FINAL PROVISIONS

Article 54

(1) This Law enters into force on its promulgation date.

(2) Regulation of the Government should have been established no later than 2 (two) years after the promulgation of this Law.

For the purposes of public cognizance, it has been ordered that the promulgation of this Law should be achieved through its publication in the State Gazette of the Republic of Indonesia.

LAW NUMBER 19 OF 2016 ON AMENDMENT TO LAW NUMBER 11 OF 2008 ON ELECTRONIC INFORMATION AND TRANSACTION

Article II

This Law enters into force on its promulgation date.

For the purposes of public cognizance, it has been ordered that the promulgation of this Law should be achieved through its publication in the State Gazette of the Republic of Indonesia.

Enacted in Jakarta
on 21 April 2008
PRESIDENT OF THE REPUBLIC OF INDONESIA,

DR. H. SUSILO BAMBANG YUDHOYONO

Promulgated in Jakarta
on 21 April 2008

MINISTER OF LAW AND HUMAN RIGHTS
OF THE REPUBLIC OF INDONESIA,

ANDI MATTALATA

STATE GAZETTE OF THE REPUBLIC OF INDONESIA OF 2008 NUMBER 58

LAW NUMBER 19 OF 2016 ON AMENDMENT TO LAW NUMBER 11 OF 2008 ON ELECTRONIC INFORMATION AND TRANSACTION

Enacted in Jakarta
On 25 November 2016
PRESIDENT OF THE REPUBLIC OF INDONESIA,
signed
JOKO WIDODO

Promulgated in Jakarta
On 25 November 2016
MINSITER OF LAW AND HUMAN RIGHTS OF
THE REPUBLIC OF INDONESIA
signed
YASONNA H. LAOLY

STATE GAZETTE OF THE REPUBLIC OF INDONESIA OF 2016 NUMBER 251

ELUCIDATION OF

LAW OF THE REPUBLIC OF INDONESIA

NUMBER 11 OF 2008

ON

ELECTRONIC INFORMAITON AND TRANSACTIONS

I. GENERAL

The utilization of Information Technology, media, and communication has changed both global behavior of the society and human civilization. Development of information technology and communication has also caused the world relationship to be borderless (*tanpa batas*) and caused significant changes in social, economy, and culture in very fast manner. Information Technology is currently being a double-edged sword, because asides from giving contribution for the increase in welfare, advancement and human civilization, it also becomes an effective mean for illegal act.

Currently, a new legal regime has been born, which is known as cyber law or telematic law. Cyber law or *hukum siber*, is internationally used for legal definition relating to utilization of information and communication technology. In addition, telematic law is the manifestation of convergence of telecommunication law, media law, and informatics law. Another definition which is also used is law of information technology (*hukum teknologi informasi*), virtual world law (*hukum dunia maya*), and cyberspace law (*hukum mayantara*). Such definitions exist considering activities which are performed through the networks of computer system and communication system, both within the local and global scopes (Internet) by utilizing computer-system-based information technology which is electronic system, may be viewed virtually. Legal dispute which is often encountered is when relating to delivery of information, communication, and/or transaction in electronic manner, specifically in regards to inquisitorial process and matters relating to legal act which is performed through electronic system.

Electronic system refers to computer system in a broad manner, which not only encompasses hardware and software of computer, but also encompasses

telecommunication network and/or electronic communication system. Software or program of computer is a set of instructions which are incorporated in the forms of language, code, scheme, or other forms, of which, if it is combined with media which is readable using computer, it will make computer to work in order to perform special function or to reach special outcome, including preparation for designing such instruction.

Electronic system is also used to explain the existence of information system which is implementation of information technology that is based on telecommunication network and electronic media, which functions to design, process, analyze, display, and send or disseminate electronic information. Information system, from technical and management perspectives, is actually the incorporation of implementation of information technology product into a form of organization and management in accordance with the characteristic of needs of such organization and in accordance with its designation purpose. On the other hand, information system, from technical and functional perspectives, is the integrity of system between human and machine which encompasses the components of hardware, software, procedure, human resources, and substance of information, of which, the utilization encompasses the functions of input, process, output, storage, and communication.

In connection with that, legal society actually has broadened the interpretation of its principles and norms when encountering the issue on intangible goods since a long time ago, for instance, in the case of electricity theft as criminal act. In reality, cyber activity is no longer simple because its activity is no longer limited by territories of a state, that is easily to be accesses whenever and wherever. Losses may incur both toward parties to transactions and toward other persons who have never performed transaction, for instance, stealing credit-card funds through shopping on the Internet. Asides from that, inquisitorial process is quintessential factor, considering electronic information is not only not yet accommodated in Indonesia's procedural law system in comprehensive manner, but also it is very prone to be altered, wiretapped, forged, and sent to all over the world within seconds. Thus, consequence which is impacted can be so complex and complicated.

A much broader issue within civil sector is because electronic transaction for trading activity through electronic system (electronic commerce) has become a part of national and international commerce. This reality shows that convergence within the sectors of information technology, media, and informatics (telematic) continuously developes and cannot be restrained, alongside with the invention of new development within the sectors of information technology, media, and communication.

Activities through electronic system media, which is also termed as cyber space (*ruang siber*), although it is virtual in nature, it may be categorized as actual legal conduct or act. Legally, activities on cyber space cannot be approached by only using conventional legal parameter and qualification because if this method is followed, there will be too many obstacles and loopholes from law enforcement. Activities on cyber space are virtual activities which have very actual impact, although its evidence is electronic in nature.

Hence, the subject of its actor should also be qualified as Person who has performed actual legal act. In regards to e-commerce activities, *inter alia*, it is known that the existence of electronic document, of which, its standing is equivalent with document as produced on the paper.

In relation to that matter, the aspects of security and legal certainty in the course of utilization of information technology, media, and communication are required to be regarded, so that they may be optimally developed. Therefore, there are three approaches to maintain security on cyber space, namely approaches from legal aspect, technology aspect, social, cultural, and ethical aspect. In bid to overcome security interference in the course of organization of system in electronic manner, legal approach is absolute in nature, because without any legal certainty, issue on utilization of information technology will be not optimum.

LAW NUMBER 19 OF 2016 ON AMENDMENT TO LAW NUMBER 11 OF 2008 ON ELECTRONIC INFORMATION AND TRANSACTION

That the independence declares freedom of thought and speech, as well as right to obtain information through the use and utilization of Information Technology and communication are aimed to advance public welfare, and educate the nation's life, as well as providing the feeling of security, fairness, and legal certainty for user and Electronic System Provider.

In the life as society, nation, and state, right and freedom through the use and utilization of such Information Technology are performed by considering derogation which has been established under the law with the sole intention to guarantee recognition, as well as respect toward right and freedom of another person and in order to fulfill fair demand in accordance with the considerations of moral, religious values, security, and public order in a democratic society.

Law Number 11 of 2008 on Electronic Information and Transaction (UU ITE) is the first law within the sectors of Information Technology and Electronic Transaction as legislative product which is very needed and has become the pioneer which puts the foundation for the regulation within the sectors of utilization of Information Technology and Electronic Transaction. Nevertheless, in its reality, the journey of implementation of UU ITE encountered issues.

Firstly, against this Law, several judicial reviews at Constitutional Court had been filed with Constitutional Court Decision Number 50/PUU-VI/2008, Number 2/PUU-VII/2009, Number 5/PUU-VIII/2010, and Number 20/PUU-XIV/2016.

Based on Constitutional Court Decision Number 50/PUU-VI/2008 and Number 2/PUU-VII/2009, insult and defamation criminal acts within the sectors of Electronic Information and Electronic Transaction are not merely deemed as general criminal act, but as complaint offense. Emphasis on complaint offense is intended to be in line with the principles of legal certainty and the feeling of public justice.

Based on Constitutional Court Decision Number 5/PUU-VIII/2010, Constitutional Court is on the opinion that activities and authorities of wiretapping

are very sensitive matters, because on one hand, it is derogation of human right, but on the other hand, it has the legal interest aspect. Therefore, regulation (*pengaturan*) on legality of wiretapping should be enacted and formulated precisely in accordance with the 1945 Constitution of the Republic of Indonesia. Asides from that, the Court is on the opinion that since wiretapping is violation of human right, as stressed under Article 28J paragraph (2) of the 1945 Constitution of the Republic of Indonesia, it is very reasonable and rightly so if the state wishes to deviate from such privacy right of citizen, the state should have deviated in the forms of law and not in the forms of regulation of the government.

In addition, based on Constitutional Court Decision Number 20/PUU-XOV/2016, Constitutional Court is on the opinion that in order to prevent the existence of multi-interpretation of Article 5 paragraph (1) and paragraph (2) of UU ITE, the Court stresses that any interception should be performed lawfully, moreover, in the event of law enforcement. Therefore, the Court, in its verdict, adds the word or phrase "specifically" to the phrase "Electronic Information and/or Electronic Document". In order to avoid interpretation that such decision will narrow-down the meaning or definition which exists in Article 5 paragraph (1) and paragraph (2) of UU ITE, in order to provide legal certainty on existence of Electronic Information and/or Electronic Document as evidence, it is deemed necessary to re-emphasize it under Elucidation of Article 5 of UU ITE.

Secondly, provisions on search, confiscation, arrest, and detainment as addressed under UU ITE raise issue for investigator, because criminal act within the sectors of Information Technology and Electronic Transaction happens [*sic*] so fast and the perpetrator may easily obscure the act or evidence of crime.

Thirdly, characteristic on visuality of cyber space enables illegal contents, such as Electronic Information and/or Document containing contents which violate decency, gambling, insult or defamation, extortion and/or threat, dissemination of hoax and misleading news, thus inflicting losses for consumers to Electronic Transaction, as well as an act of spreading hate or hostility based on ethnicity, religion, race, and inter-group relation, and sending of violence threat or frightening as addressed personally, may be accessed, distributed, transmitted,

copied, stored for re-dissemination from anywhere and anytime. In the event of protecting public interest from any types of interference as a result of misuse of Electronic Information and Electronic Transaction, emphasis on Government's role in preventing dissemination of illegal content is required, by performing an act of termination of access to Electronic Information and/or Electronic Document containing contents which are illegal, so that they are inaccessible from Indonesia's jurisdiction, as well as authority is required by investigator to request information which exists at Electronic System Provider for criminal law enforcement purpose within the sectors of Information Technology and Electronic Transaction.

Fourthly, the use of any information through media or Electronic System in relation to personal data of an individual should be performed based on consent of person in question. Therefore, guarantee on fulfillment of protection of oneself by obliging any Electronic System provider to erase irrelevant Electronic Information and/or Electronic Document under its control upon request from Person in question based on court stipulation is needed.

Based on such consideration, it is deemed necessary to enact Law on Amendment to Law Number 11 of 2008 on Electronic Information and Transaction which re-emphasizes provisions on existence of Electronic Information and/or Electronic Document under Elucidation of Article 5, adding provisions on obligation for erasure of Electronic Information and/or Electronic Document which are irrelevant under Article 26, amending provisions under Article 31 paragraph (4) on delegation of formulation of interception procedures into a law, adding Government's roles in the course of performing prevention of dissemination and use of Electronic Information and/or Electronic Document which containing prohibited contents under Article 40, amending several provisions on investigation relating to allegation of criminal act within the sectors of Information Technology and Electronic Transaction under Article 43, and adding elucidation of Article 27 paragraph (1), paragraph (3), and paragraph (4), so that it is better harmonized with material criminal law system as addressed in Indonesia.

II. ARTICLE BY ARTICLE

Article 1

Self-explanatory.

Article 2

This Law has scope of jurisdiction which is not merely for legal act that prevails in Indonesia and/or performed by Indonesian citizen, but also prevails for legal act as performed outside of jurisdiction (*wilayah hukum*) of Indonesia, either by Indonesian citizen or foreign citizen or Indonesian incorporated entity or foreign incorporated entity, which is having legal consequence in Indonesia, considering the utilization of Information Technology for Electronic Information and Electronic Transaction may be cross-territories or universal.

"Injuring Indonesia's interests" refers to, including but not limited to injuring the interests of national economy, protection of strategic data, nation's dignity and standards, state defence and security, state sovereignty, citizen, as well as Indonesian incorporated entity.

Article 3

"Principle of legal certainty" refers to legal ground for utilization of Information Technology and Electronic Transaction, as well as any matters which support its organization which obtains legal recognition inside and outside of court.

"Principle of benefit" refer to principle for the utilization of Information Technology and Electronic Transaction is strived for supporting the informing process, therefore it may increase public welfare.

"Principle of precautionary" refers to ground for parties in question that they [*sic*] should take regard the entire aspects which are having potentials to inflict losses, either for themselves or another party in the course of utilization of Information Technology and Electronic Transaction.

“Principle of good faith” refers to principle which is used by the parties in the course of performing Electronic Transaction does not has the purpose to deliberately and unlawfully or illegally inflict losses for another party without the knowledge of such party.

“Principle of freedom to choose technology or technology-neutral” refers to principle for the utilization of Information Technology and Electronic Transaction is not focused on the use of certain technology, hence it may follow development in the future period.

Article 4

Self-explanatory.

Article 5*

Paragraph (1)

That existence of Electronic Information and/or Electronic Document binds and be recognized as valid evidence in order to provide legal certainty against the Organization of Electronic System and Electronic Transaction, specifically for the inquisitorial process and matters relating to legal act which is performed through Electronic System.

Paragraph (2)

Specifically for Electronic Information and/or Electronic Document in the forms of result of interception or wiretapping or recording which is a part of wiretapping that should be performed in the event of law enforcement upon request from police, public prosecutor, and/or other institution, of which, its authority is addressed based on law.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Letter a

Letter, of which, according to the law should be made in writing, including but not limited to negotiable instrument, letter of value [*surat yang berharga*],

and letter that is used in the civil, criminal, and state administrative procedural law enforcement process.

Letter b

Self-explanatory.

Article 6

Up until the current condition, written form is identical with information and/or document as merely incorporated on the paper, however, fundamentally, information and/or document may be incorporated into any media, including electronic media. Within the scope of Electronic System, authentic information and its copy is no longer relevant to be differentiated since Electronic System basically operates through the way of duplication which causes the authentic information can no longer be differentiated from its copy.

Article 7

This provision denotes that an Electronic Information and/or Electronic Document may be used as the reason for the inception of a right.

Article 8

Self-explanatory.

Article 9

“Complete and veracious information” refers to, encompassing:

a. information containing identity, as well as status of legal subject and its competence, either as producer, supplier, provider or intermediary;
b. other information explaining certain matter which becomes the condition for validity of agreement, as well as explaining goods and/or services which are offered, such as name, address, and description of goods/services.

Article 10

Paragraph (1)

Reliability Certification is intended as proof that businesses which perform electronic trading are eligible to operate business after undergoing assessment and audit from authorized body. Proof that Reliability Certification has been performed is shown with the existence of certification logo in the forms of trust mark on the home page (*laman*) of such businesses.

Paragraph (2)

Self-explanatory.

Article 11

Paragraph (1)

This Law only provides explicit recognition that, although it is only a code, Digital Signature possesses the same standing with manual signature which generally possesses legal power and legal consequence.

Requirements as referred to under this Article are minimum requirements which must be fulfilled by each Digital Signature. This provision opens opportunities as broad as possible to anyone to develop method, technique, or process for the generation of Digital Signature.

Paragraph (2)

Regulation of the Government in question, *inter alia*, addresses technique, method, mean, and process for the generation of Digital Signature.

Article 12

Self-explanatory.

Article 13

Self-explanatory.

Article 14

Information as referred to under this Article is minimum information which should be fulfilled by any Digital Signature provider.

Article 15

Paragraph (1)

"Reliable" denotes that Electronic System possesses capability which is in accordance with the purposes of its use.

"Secure" denotes that Electronic System is protected physically and non-physically.

"Proper operation" denotes that Electronic System possesses capability which is in accordance with its specification.

Paragraph (2)

"Held liable" denotes that there is legal subject who is legally held liable against such Organization of Electronic System.

Paragraph (3)

Self-explanatory.

Article 16

Self-explanatory.

Article 17

Paragraph (1)

This Law provides opportunity for the utilization of Information Technology by state organizer, Person, Enterprise, and/or the public.

Utilization of Information Technology should be performed well, wisely, responsibly, effectively, and efficient, hence the utmost benefit for the public may be reached.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 18

Paragraph (1)

Self-explanatory.

Paragraph (2)

Choice of law is performed by the parties to international contract, including those which are performed electronically, is known as *pilihan hukum*. This law binds as the law which prevails for such contract.

Choice of law in Electronic Transaction may only be performed if there is foreign element in the contract and its implementation should be in line with the principles of private international law (*Hukum Perdata Internasional* – HPI).

Paragraph (3)

In case the choice of law is absent, determination of prevailing law which is based on principles or rules of private international law will be determined as the law which prevails to such contract.

Paragraph (4)

Forum which is competent to adjudicate international contract dispute, including those which are performed electronically, is forum which is chosen by the parties. Such forum may take form as court, arbitration, or other alternative dispute resolution body.

Paragraph (5)

In case the parties do not make choice of forum, the competence of forum prevails based on principles or rules of private international law. Such rules are known as the domicile of the defendant (the basis of presence) rule and effectiveness which emphasizes on the location where assets of the defendant lie (principle of effectiveness).

Article 19

“Agreed” under this article also encompasses the agreed procedure which exists in the Electronic System in question.

Article 20

Paragraph (1)

Electronic Transaction is incepted when there is agreement between the parties which may take form, *inter alia*, checking of data, identity, personal identification number (*nomor identifikasi pribadi/PIN*) or password (*sandi lewat*).

Paragraph (2)

Self-explanatory.

Article 21

Paragraph (1)

"Authorized" under this provision is advised to be declared in power of attorney.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article 22

Paragraph (1)

"Feature" refers to facility which provides opportunity for the user of Electronic Agent to make modification to information which is delivered by it, namely facilities for cancellation (*pembatalan*), edit, and reconfirmation.

Paragraph (2)

Self-explanatory.

Article 23

Paragraph (1)

Domain Name takes form as address or personal identity of state organizer, Person, Enterprise, and/or the public, of which, its collection is based on the first-come-first-serve (*pendaftar pertama*) principle.

The first-come-first-serve principle is different between provisions regarding to Domain name and regarding to the intellectual property right sector, because no substantive examination is needed, such as examination for registration of mark and patent.

Paragraph (2)

"Violating rights of other Person" refers to, for instance, violating registered mark, registered name of incorporated entity, name of prominent Person, and similar name which basically injures another Person.

Paragraph (3)

"Unauthorized use of Domain Name" refers to registration and use of Domain Name which is solely designated to prevent or hinder other Person to use the name which is intuitive with the existence of its name or the name of its product, or in order to benefit from reputation of Person who has been famous or renown, or in order to mislead consumer.

Article 24

Self-explanatory.

Article 25

Electronic Information and/or Electronic Document which are formulated and be registered as intellectual creation, copyright, patent, mark, trade secret, industrial design, and its equivalent, must be protected under this Law by regarding provisions under Laws and Regulations.

Article 26*

Paragraph (1)

In the course of utilization of Information Technology, personal data protection is a part of privacy rights (*hak pribadi*). Privacy rights are defined as follows:

a. Privacy right is right to enjoy personal life and be free from any kind of interference.
b. Privacy right is right to be able to communicate with another Person without any spying act.
c. Privacy right is right to supervise information access on personal life and someone's data.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article 27*

Paragraph (1)

"Distributes" refers to sending and/or disseminating Electronic Information and/or Electronic Document to many Persons or various parties through Electronic System.

"Transmits" refers to sending Electronic Information and/or Electronic Document which is designated to one other party through Electronic System.

"Makes the accessibility" refers to any acts other than distributing and transmitting through Electronic System which cause Electronic Information and/or Electronic Document to be known by another party or the public.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Provisions in this paragraph refer to provisions regarding to defamation and/or slander as addressed under the Criminal Law Code (*Kitab Undang-Undang Hukum Pidana* – KUHP).

Paragraph (4)

Provisions in this paragraph refer to provisions regarding to extortion and/or threat as addressed under the Criminal Law Code (KUHP).

Article 28

Self-explanatory.

Article 29

Self-explanatory.

Article 30

Paragraph (1)

Self-explanatory.

Paragraph (2)

Technically, prohibited act as referred to in this paragraph may be committed, *inter alia*, by:

a. performing communication, sending, broadcasting or deliberately attempting to realize such conditions to anyone who is ineligible to receive it; or
b. deliberately preventing, so that the information in question cannot be or failed to be received by those who are authorized to accept it within the scope of government and/or regional government.

Paragraph (3)

Security system is system which restricts access to Computer or bans access to inside of Computer based on categorization or classification of user, as well as authority level which is determined.

Article 31*

Paragraph (1)

"Interception or wiretapping" refers to activity to listen, record, divert, alter, hinder, and/or take note of transmission of Electronic Information and/or Electronic Document which is not public in nature, either using communication-wire network or wireless network, such as electromagnetic emission or radiofrequency.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 32

Self-explanatory.

Article 33

Self-explanatory.

Article 34

Paragraph (1)

Self-explanatory.

Paragraph (2)

"Activities in regards to research" refer to research that is conducted by licensed research agency.

Article 35

Self-explanatory.

Article 36

Self-explanatory.

Article 37

Self-explanatory.

Article 38

Self-explanatory.

Article 39

Self-explanatory.

Article 40*

Paragraph (1)

Facilitation of utilization of Information Technology, including governance of Information Technology and Electronic Transaction which is secure, ethical, intelligent, creative, productive, and innovative. This provision includes facilitating the general public, governmental body, and businesses in the course of developing products and services relating to Information Technology and communication.

Paragraph (2)

Self-explanatory.

Paragraph (2a)

Self-explanatory.

Paragraph (2b)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Article 42

Self-explanatory.

Article 43*

Paragraph (1)

"Certain Civil Servant Officer" refers to Civil Servant Officer at ministry which organizes governmental affairs within the sectors of communication and informatics who have fulfilled requirements based on provisions under laws and regulations.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Letter g

Self-explanatory.

Letter h

Self-explanatory.

Letter i

Self-explanatory.

Letter j

"Expert" refers to someone who possesses special expertise within the sector of Information Technology which is academically and practically accountable over such knowledge.

Letter k

Self-explanatory.

Paragraph (6)

Self-explanatory.

Paragraph (7)

Self-explanatory.

Paragraph (7a)

Self-explanatory.

Paragraph (8)

Self-explanatory.

Article 44

Self-explanatory.

Article 45*

Self-explanatory.

Article 45A*

Self-explanatory.

Article 45B*

Provisions under this Article also include cyber bullying (*perundungan di dunia siber*) which contains the elements of violence threat or frightening and causing physical, psychological violence, and/or economic losses [*kerugian material*].

Article 46

Self-explanatory.

Article 47

Self-explanatory.

Article 48

Self-explanatory.

Article 49

Self-explanatory.

Article 50

Self-explanatory.

Article 51

Self-explanatory.

Article 52

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

This provision is intended to punish any illegal act which fulfills elements as referred to under Article 27 up to Article 37 which is committed by corporation (corporate crime) and/or by the management and/or staff who has the capacity to:

a. represent corporation;
b. make decision in corporation;
c. perform supervision and control within corporation;
d. perform activity for the profit of corporation.

Article 53

Self-explanatory.

Article 54

Self-explanatory.

SUPPLEMENT TO THE STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER 4843

LAW NUMBER 19 OF 2016 ON AMENDMENT TO LAW NUMBER 11 OF 2008 ON ELECTRONIC INFORMATION AND TRANSACTION

SUPPLEMENT TO THE STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER 5952

TRANSLATOR'S NOTES

The translator is aware that there have been numerous Constitutional Court Decisions which have been filed against this Law. However, most of them have been accommodated under the Law Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transaction, including:

1. Constitutional Court Decision Number 50/PUU-VI/2008;
2. Constitutional Court Decision Number 2/PUU-VII/2009;
3. Constitutional Court Decision Number 5/PUU-VIII/2010; and
4. Constitutional Court Decision Number 20/PUU-XIV/2016,

therefore, consolidation with the abovementioned Constitutional Court Decisions are, needless to say, practically not necessary anymore.

In addition, the translator is also aware that there have been several judicial-review petitions against this Law subsequent to the passing of Law Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transaction, including:

1. Constitutional Court Decision Number 74/PUU-XIV/2016 (withdrawn);
2. Constitutional Court Decision Number 76/PUU-XV/2017 (completely rejected);
3. Constitutional Court Decision Number 64/PUU-XVI/2018 (inadmissible),

considering that all of them are not granted (or at least partially granted), hence the abovementioned Constitutional Court Decisions are, once again, practically not necessary to be consolidated.