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

BY THE GRACE OF GOD ALMIGHTY

THE PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering:

a. that national development is a continuous process that shall always be responsive to the various dynamics that occur in society;

b. that information globalization has placed Indonesia as part of the world's information society, thus requiring the establishment of regulations on the management of Electronic Information and Transactions at the national level so that the development of Information Technology can be carried out optimally, evenly, and spread to all levels of society in order to enrich the life of the nation;

c. that the rapid development and progress of Information Technology has led to changes in the activities of human life in various sectors which have directly affected the birth of new forms of legal act.

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

e. that the utilization of Information Technology has an important role in trade and national economic growth to realize public welfare;

f. that the government needs to support the development of Information Technology through legal infrastructure and its regulations so that the utilization of Information Technology is conducted safely to prevent its misuse by taking into account the religious and socio-cultural values of Indonesian people;

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

Observing:

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

With the Mutual Consent of

THE HOUSE OF REPRESENTATIVES OF THE REPUBLIC OF INDONESIA

and

THE PRESIDENT OF THE REPUBLIC OF INDONESIA

HAS DECIDED:

To enact:

LAW ON ELECTRONIC INFORMATION AND TRANSACTIONS.

CHAPTER I

GENERAL PROVISIONS

Article 1

Under this Law the following definitions are employed:

1. Electronic Information is one or a set of electronic data, including but not limited to text, voice, image, map, design, photo, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, letter, sign, number, Access Code, symbol, or perforation which has been processed and which has meaning or may be understood by people who are able to understand it.
2. Electronic Transaction is a legal act which is conducted by using a Computer, Computer network, and/or other electronic media.
3. Information Technology is a technique to collect, prepare, store, process, announce, analyze, and/or disseminate information.
4. Electronic Document is any Electronic Information that is made, forwarded, transmitted, received, or stored in analog, digital, electromagnetic, optical, or similar format, and which may be seen, displayed and/or heard through a Computer or an Electronic System including but not limited to text, voice, image, design map, photo or the like, letter, sign, number, Access Code, symbol, or perforation which has meaning or definition or may be understood by people who are able to understand it.
5. Electronic System is a series of electronic procedures and devices that serve to prepare, collect, process, analyze, store, display, announce, send, and/or disseminate Electronic Information.
6. Electronic System Organization is the utilization of Electronic System by state administrator, Person, Business Entity, and/or the public.
7. Electronic System Network is the connection of two or more Electronic Systems, which are closed or open.
8. Electronic Agent is a device of an Electronic System made to automatically perform an action on certain Electronic Information which is operated by a Person.
9. Electronic Certificate is an electronic certificate containing Digital Signature and identity which shows the legal subject status of the parties in an Electronic Transaction which is issued by an Electronic Certification Provider.
10. Electronic Certification Provider is a legal entity that serve as a trustworthy party, and which provides and audits an Electronic Certificate.
11. Reliability Certification Body is an independent body that is established by recognized professionals, validated, and supervised by the Government with authority to audit and issue a Reliability Certificate in an Electronic Transaction.
12. Electronic Signature is a signature consisting of Electronic Information that is attached, associated or related to other Electronic Information, and that is used as a verification and authentication tool.
13. Signer is the legal subject associated or related to the Electronic Signature.
14. Computer is a device to process electronic, magnetic, optical data, or a system that carry out logic, arithmetic, and storage functions.
15. Access is an activity to conduct interaction with an Electronic System which is a stand-alone or in a network.
16. Access Code is a number, letter, symbol, other character or a combination thereof, which are keys to be able to access Computer and/or other Electronic System.
17. Electronic Contract is an agreement between the parties made through an Electronic System.

18. Sender is the legal subject that send Electronic Information and/or Electronic Document.
19. Recipient is the legal subject that receive Electronic Information and/or Electronic Document from Sender.
20. Domain Name is the internet address of a state administrator, Person, Business Entity, and/or public, which may be utilized in communication through the internet, which is in the form of unique code or character arrangement to go to a certain location on the internet.
21. Person is an individual, either an Indonesian citizen, a foreign citizen, or legal entity.
22. Business Entity is a private company or a partnership company, both incorporated and unincorporated.
23. Government is the Minister or other officials appointed by the President.

Article 2

This Law is applicable to every Person who commits legal act as regulated under this Law, both who are within Indonesian jurisdiction and outside of Indonesian jurisdiction, and which has legal consequences in Indonesian jurisdiction and/or outside of Indonesian jurisdiction and which is detrimental to Indonesia's interest.

CHAPTER II
PRINCIPLES AND PURPOSES

Article 3

The utilization of Information Technology and Electronic Transaction shall be implemented based on the principle of legal certainty, benefit, prudence, good faith, and freedom to choose technology or technology-neutral.

Article 4

The utilization of Information Technology and Electronic Transaction shall be implemented for the following purposes:

a. enrich the life of the nation as a part of world's information society;
b. develop national trading and economy in order to improve public welfare;
c. increase the effectiveness and efficiency of public services;
d. open the widest possible opportunity for every Person to advance their thinking and abilities in the field of the use and utilization of Information Technology in the most optimal and responsible manner; and
e. provide a sense of security, fairness, and legal certainty for Information technology users and operators.

CHAPTER III
ELECTRONIC INFORMATION, DOCUMENT, AND SIGNATURE

Article 5

(1) Electronic Information and/or Electronic Document and/or its printout are valid legal forms of evidence (alat bukti hukum yang sah).

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

(3) Electronic Information and/or Electronic Document shall be deemed valid if using the Electronic System that is in accordance with the provisions regulated under this Law.

(4) Provisions regarding Electronic Information and/or Electronic Document as referred to in paragraph (1) are not applicable for:

a. a letter that according to Law shall be made in written form; and

b. a letter along with its document that according to Law shall be made in the form of notarial deed or deed made by the deed-making officials.

Article 6

In the event that there are provisions other than those regulated under Article 5 paragraph (4) which require that information shall be in written or oral form, Electronic Information and/or Electronic Document shall be deemed valid so long that the information contained in it can be accessed, displayed, have its completeness guaranteed, and can be accounted for so that it explains a situation.

Article 7

Every Person who declares rights, strengthens existing rights, or rejects the rights of other Person based on the existence of Electronic Information and/or Electronic Document must ensure that the Electronic Information and/or Electronic Document in their possession come from the Electronic System that meets the requirements under the Laws and Regulations.

Article 8

(1) Unless agreed otherwise, the delivery time of Electronic Information and/or Electronic Document shall be determined as the time after the Electronic Information and/or Electronic Document have been sent with the correct address by the Sender, to an Electronic System appointed or used by the Recipient and has entered into the Electronic System that is beyond the Sender's control.

(2) Unless agreed otherwise, the time of receipt of Electronic Information and/or Electronic Document shall be determined as the time when the Electronic Information and/or Electronic Document entered the Electronic System under the control of the entitled Recipient.

(3) In the event that the Recipient has appointed certain Electronic System to receive Electronic Information, the receipt occurs at the time the Electronic Information and/or Electronic Document entered the appointed Electronic System.

(4) In the event that there are two or more information systems used in the delivery or receipt of Electronic Information and/or Electronic Document, then:

a. the delivery time shall be when the Electronic Information and/or Electronic Document entered the first information system that is beyond the Sender's control;

b. the time of receipt shall be when the Electronic Information and/or Electronic Document entered the last information system that is under the Recipient's control.

Article 9

Businesses that offer products through Electronic System shall provide complete and valid information related to the requirements of contract, producer, and product offered.

Article 10

(1) Every business that organizes Electronic Transaction may be certified by the Reliability Certification Body.

(2) Provisions regarding the establishment of Reliability Certification Body as referred to in paragraph (1) shall be regulated in a Regulation of the Government.

Article 11

(1) Electronic Signature has valid legal force and legal consequences as long as the following requirements are met:

a. the Electronic Signature creation data is only related to the Signer;

b. the Electronic Signature creation data at the time of the electronic signing process is only in the Signer's possession;

c. all changes to the Electronic Signature which happen after the signing are discoverable;

d. all changes to the Electronic Information which are related to the said Electronic Signature which happens after the signing are discoverable;

e. there is certain method that is used to identify who is the Signer; and

f. there is certain method that can disclose that the Signer has granted their approval in regards to the relevant Electronic Information.

(2) Further provisions regarding Electronic Signature as referred to in paragraph (1) shall be regulated in a Regulation of the Government.

Article 12

(1) Every Person who is involved with the Electronic Signature has the obligation to provide security in regards to the Electronic Signature that they used.

(2) Electronic Signature security as referred to in paragraph (1) shall at least include:

a. a system that cannot be accessed by other Person with no right;

b. the Signer shall implement the principle of prudence to prevent illegal use of the data related to Electronic Signature creation;

c. the Signer without delay shall implement the method recommended by Electronic Signature provider or other methods that are proper and appropriate and shall immediately notify someone whom the Signer deems to trust the Electronic Signature or the party supporting the Electronic Signature services if:

1. the Signer is aware that the Electronic Signature creation data has been compromised; or

2. there is a circumstance that is known to the Signer may present significant risks, possibly due to the compromised Electronic Signature creation data; and

d. in the event that the Electronic Certificate is used to support Electronic Signature, the Signer shall ensure the validity and completeness of all information related to the Electronic Certificate in question.

(3) Every Person who violates the provisions as referred to in paragraph (1), is responsible for all losses and legal consequences incurred.

CHAPTER IV

THE ORGANIZATION OF ELECTRONIC CERTIFICATION AND ELECTRONIC SYSTEM

Division One

The Organization of Electronic Certification

Article 13

(1) Every Person has the right to use the service of Electronic Certification Provider to create Electronic Signature.

(2) Electronic Certification Provider shall ensure the relationship of an Electronic Signature with its owner.

(3) Electronic Certification Provider comprises of:

a. Indonesian Electronic Certification Provider; and

b. foreign Electronic Certification Provider.

(4) Indonesian Electronic Certification Provider shall be Indonesian incorporated entity and is domiciled in Indonesia.

(5) Foreign Electronic Certification Provider that operates in Indonesia shall be registered in Indonesia.

(6) Further provisions regarding Electronic Certification Provider as referred to in paragraph (1) shall be regulated in a Regulation of the Government.

Article 14

Electronic Certification Provider as referred to in Article 13 paragraph (1) to paragraph (5) shall provide accurate, clear, and definite information to every services user, which encompass:

a. the method uses to identify Signer;

b. the things that can be used to identify the personal identity of Electronic Signature's creator; and

c. the things that can be used to present the validity and security of the Electronic Signature.

Division Two

The Organization of Electronic System

Article 15

(1) Every Electronic System Organizer shall organize their Electronic System reliably and safely and be responsible for the proper operation of the Electronic System.

(2) Electronic System Organizer shall be responsible for the Organization of its Electronic System.

(3) The provision as referred to in paragraph (2) is not applicable in the event that it can be proven that there is a situation that forces an error, and/or negligence of the Electronic Systems' user.

Article 16

(1) Unless otherwise determined in a separate law, every Electronic System Organizer must operate an Electronic System that fulfills the following minimum requirements:

a. able to redisplay the Electronic Information and/or Electronic Document in full in accordance with the retention period stipulated by the Laws and Regulations;

b. able to protect the availability, completeness, authenticity, confidentiality and accessibility of

Electronic Information in said Electronic System Organization;

c. may operate in accordance with the procedures or instructions in said Electronic System Organization;

d. equipped with procedures or instructions announced in the language, information, or symbol that can be understood by the party concerned with said Electronic System Organization; and

e. has continuous mechanism to maintain the novelty, clarity, and accountability of procedures or instructions.

(2) Further provisions regarding Electronic System Organization as referred to in paragraph (1) shall be regulated in a Regulation of the Government.

CHAPTER V

ELECTRONIC TRANSACTIONS

Article 17

(1) The organization of Electronic Transactions may be conducted within either public or private sphere.

(2) The parties that conduct Electronic Transaction as referred to in paragraph (1) must have good faith in conducting interaction and/or exchange of Electronic Information and/or Electronic Document during the transaction.

(3) Further provisions regarding the organization of Electronic Transactions as referred to in paragraph (1) shall be regulated in a Regulation of the Government.

Article 18

(1) Electronic Transaction which are made into an Electronic Contract are binding on the parties.

(2) The parties are authorized to choose the law applicable to the international Electronic Transaction they made.

(3) If the parties do not make a choice of law in international Electronic Transaction, the law that applies shall be based on the principles of Private International Law.

(4) The parties are authorized to determine the court, arbitration forum, or other alternative dispute resolution agencies that are authorized to settle disputes that may arise from the international Electronic Transaction they made.

(5) If the parties do not make a choice of forum as referred to in paragraph (4), the determination of the authority of the court, arbitration forum, or other alternative dispute resolution agencies that are authorized to settle dispute that may arise from said transaction, shall be based on the principles of Private International Law.

Article 19

The parties that conduct Electronic Transaction shall use the agreed Electronic System.

Article 20

(1) Unless determined otherwise by the parties, Electronic Transaction shall occur at the time that the transaction offer that is sent by Sender is received and approved by Recipient.

(2) Approval on Electronic Transaction as referred to in paragraph (1) shall be conducted through an electronic acceptance statement.

Article 21

(1) Sender or Recipient may conduct Electronic Transaction by themselves, through a party authorized by them, or through Electronic Agent.

(2) The party responsible for all legal consequences in the Electronic Transaction as referred to in paragraph (1) shall be regulated as follows:

a. if conducted themselves, all legal consequences in the Electronic Transaction shall be the responsibility of the transacting parties;

b. if conducted through the granting of power of attorney, all legal consequences in the Electronic Transaction shall be the responsibility of the principal (pemberi kuasa); or

c. if conducted by Electronic Agent, all legal consequences in the Electronic Transaction shall be the responsibility of the Electronic Agent organizer.

(3) If the loss of Electronic Transaction is due to the failure of the operation of the Electronic Agent due to the action of a third party directly against the Electronic System, all legal consequences are the responsibility of the Electronic Agent organizer.

(4) If the loss of Electronic Transaction is due to the failure of the operation of the Electronic Agent due to service user's negligence, all legal consequences are the responsibility of the service user.

(5) The provision as referred to in paragraph (2) are not applicable in the event that it can be proven that there is a compelling situation, error, and/or negligence of the Electronic System' user.

Article 22

(1) Certain Electronic Agent organizers shall provide a feature in the Electronic Agent they operate that allows its user to make changes to information that is still in the transaction process.

(2) Further provisions regarding certain Electronic Agent organization as referred to in paragraph (1) shall be regulated in a Regulation of the Government.

CHAPTER VI

DOMAIN NAME, INTELLECTUAL PROPERTY, AND PROTECTION OF PERSONAL RIGHTS

Article 23

(1) Every state administrator, Person, Business Entity, and/or the public has the right to own a Domain Name based on the principle of the first registrant.

(2) The ownership and usage of Domain Name as referred to in paragraph (1) shall be based on good faith, do not violates the principles of fair business competition, and do not violates the rights of another person.

(3) Every state administrator, Person, Business Entity, or the public who is harmed by the illegal use of Domain Name by another Person, has the right to file a lawsuit for the cancellation of said Domain Name.

Article 24

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

(2) In the event that there is a Domain Name management dispute by the public, the Government has the right to temporarily take over the management of the disputed Domain Name.

(3) The existence of a Domain Name manager who is outside of Indonesian territory and their registered domain Name shall be acknowledged so long as it does not conflict with Laws and Regulations.

(4) Further provisions regarding Domain Name management as referred to in paragraph (1), paragraph (2), and paragraph (3) shall be regulated in a Regulation of the Government.

Article 25

Electronic Information and/or Electronic Document formed into an intellectual work, internet site, and intellectual work contained within are protected as Intellectual Property Right based on the provisions of Laws and Regulations.

Article 26

(1) Unless determined otherwise by Laws and Regulations, the use of any information through electronic media which is related to the personal data of a person shall be conducted with consent from the Person concerned.

(2) Every person whose right is violated as referred to in paragraph (1) may file a lawsuit for the loss incurred based on this Law.

CHAPTER VII

PROHIBITED ACTIONS

Article 27

(1) Any Person who intentionally and illegally distributes and/or transmits and/or made accessible Electronic Information and/or Electronic Document which contain content that violates decency.

(2) Any person who intentionally and illegally distributes and/or transmits and/or made accessible Electronic Information and/or Electronic Document which contain gambling.

(3) Any person who intentionally and illegally distributes and/or transmits and/or made accessible Electronic Information and/or Electronic Document which contain offensive and/or defamation content.

(4) Any person who intentionally and illegally distributes and/or transmits and/or made accessible Electronic Information and/or Electronic Document which contain extortion and/or threat.

Article 28

(1) Any Person who intentionally and illegally spreads false and misleading news resulting in consumer losses in Electronic Transaction.

(2) Any Person who intentionally and illegally spreads information intended to cause hatred or hostility to certain individuals and / or certain groups of people based on ethnicity, religion, race and inter-groups (suku, agama, ras, dan antar golongan/SARA).

Article 29

Any Person who intentionally and illegally send Electronic Information and/or Electronic Document that contain personally aimed threats of violence or intimidation.

Article 30

(1) Any Person who intentionally and illegally or unlawfully access a Computer and/or Electronic System that belongs to another Person in any way.

(2) Any Person who intentionally and illegally or unlawfully access a Computer and/or Electronic System in any way in order to obtain Electronic Information and/or Electronic Document.

(3) Any Person who intentionally and illegally or unlawfully access a Computer and/or Electronic System in any way by violating, breaching, bypassing, or breaking through the security system.

Article 31

(1) Any Person who intentionally and illegally or unlawfully intercept or tap the Electronic Information and/or Electronic Document in certain Computer and/or Electronic System that belongs to another person.

(2) Any Person who intentionally and illegally or unlawfully intercept the transmission of non-public Electronic Information and/or Electronic Document from, to, and in certain Computer and/or Electronic System that belong to another person, both that do not cause any change and that cause change, removal, and/or termination of the Electronic Information and/or Electronic Document that is being transmitted.

(3) With the exception of the interception as referred to in paragraph (1) and paragraph (2), interception conducted for law enforcement purposes requested by the police, prosecutor, and/or other law enforcement agencies stipulated based on law.

(4) Further provisions regarding procedures for the interception as referred to in paragraph (3) shall be regulated in a Regulation of the Government.

Article 32

(1) Any Person who intentionally and illegally or unlawfully in any way changes, adds, reduces, transmits, damages, omits, moves, hides any Electronic Information and/or Electronic Document that belongs to another Person or owned by the public.

(2) Any Person who intentionally and illegally or unlawfully in any way moves or transfers Electronic Information and/or Electronic Document to the Electronic System of unauthorized Person.

(3) Toward the actions as referred to in paragraph (1) resulting in the disclosure of confidential Electronic Information and/or Electronic Document, to be accessible to the public with data completeness that is not appropriate.

Article 33

Any Person who intentionally and illegally or unlawfully takes any action that disrupts Electronic System and/or causes Electronic System to not be able to function properly.

Article 34

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

a. Computer hardware or software that is designed or specifically developed to facilitate the actions as referred to in Article 27 to Article 23;

b. Computer password, Access Code, or anything similar that is intended so that the Electronic System can be accessed for the purpose of facilitating the actions as referred to in Article 27 to Article 23.

(2) Actions as referred to in paragraph (1) are not criminal actions if intended for research, Electronic

System testing activities, protecting the Electronic System itself and are conducted legally and lawfully.

Article 35

Any Person who intentionally and illegally or unlawfully manipulates, creates, alters, omits, damages Electronic Information and/or Electronic Document so that said Electronic Information and/or Electronic Document is considered as if the data were authentic.

Article 36

Any Person who intentionally and illegally or unlawfully commits actions as referred to Article 27 to Article 34 which causes losses to another person.

Article 37

Any Person who intentionally commits prohibited actions as referred to Article 27 to Article 36 from outside of Indonesian territory against Electronic Systems located within Indonesian jurisdictions.

CHAPTER VIII
DISPUTE SETTLEMENT

Article 38

(1) Any Person may file a lawsuit against a party that organizes an Electronic System and/or uses Information Technology that incur losses.

(2) The public may file a lawsuit through a proxy against that organizes an Electronic System and/or uses Information Technology which incur losses to the public, in accordance with the provisions of Laws and Regulations.

Article 39

(1) Civil lawsuit shall be implemented in accordance with the provisions of Laws and Regulations.

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

CHAPTER IX
THE ROLES OF THE GOVERNMENT AND THE ROLES OF THE PUBLIC

Article 40

(1) Government shall facilitate the utilization of Information Technology and Electronic Transaction in accordance with the provisions of Laws and Regulations.

(2) Government shall protect public interests from any type of disruptions as the result of Information Technology and Electronic Transaction misuse that disrupt public order, in accordance with the provisions of Laws and Regulations.

(3) Government shall determine the agency or institution that owns strategic electronic data that must be protected.

(4) Agency or institution as referred to in paragraph (3) shall prepare Electronic Document and its electronic backup as well as connects it to certain data centers for data security purposes.

(5) Agency or institution other than which is regulated under paragraph (3) shall prepare Electronic Document and its electronic backup in accordance with its data protection requirements.

(6) Further provisions regarding the roles of the Government as referred to in paragraph (1), paragraph (2), and paragraph (3) shall be regulated in a Regulation of the Government.

Article 41

(1) The public may play a role in improving Information Technology utilization, through the use and Organization of Electronic System and Electronic Transaction in accordance with the provisions of this Law.

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

(3) The agency as referred to in paragraph (2) may have consultation and mediation functions.

CHAPTER X

INVESTIGATION

Article 42

Investigation on the criminal act as referred to in this Law, shall be conducted based on the provisions in Criminal Procedural Law and provisions of this Law.

Article 43

(1) Other than Indonesian National Police Investigator Officials, certain Civil Servant Officials in the Government whose scope of duties and responsibilities is in the Information Technology and Electronic Transaction sector shall be granted special authority as an investigator as referred to in Criminal Procedural Law to conduct criminal act investigation in the Information Technology and Electronic Transaction sector.

(2) Investigation in the Information Technology and Electronic Transaction sector as referred to in paragraph (1) shall be conducted by taking into consideration the protection of privacy, confidentiality, smooth public service, data integrity, or data completeness in accordance with the provisions of Laws and Regulations.

(3) Search and/or confiscation of an electronic system related to an alleged criminal act shall be conducted with the permission of the head of the local district court.

(4) In conducting search and/or confiscation as referred to in paragraph (3), investigator must maintain the interests of public services.

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

a. receive report or complaint from anyone regarding the existence of criminal act based on the provisions of this Law;

b. summon every goods or another party for hearing and/or inspection as suspect or witness related to the suspected criminal act in the sectors related to the provisions of this Law;

c. review the validity of the report or information related to the criminal act based on the provisions of this Law;

d. investigate the Person and/or Business Entity who are reasonably suspected of committing a

criminal act based on this Law;

e. examine the equipment and/or facilities related to Information Technology activities suspected to be used for committing a criminal act based on this Law;

f. search certain places suspected to be used as places for committing a criminal act based on this Law;

g. seal and confiscate equipment and/or facilities of Information Technology activities suspected to be used in a way that violates the provisions of the Laws and Regulations;

h. request assistance from expert needed in the investigation of criminal act based on this Law; and/or

i. stop investigation of criminal act based on this Law in accordance with the applicable provisions of the criminal procedural law.

(6) In the event of arrest and detainment, investigator through public prosecutor must request determination of the head of local district court by no later than twenty four hours.

(7) Civil Servant Investigators as referred to in paragraph (1) in coordination with Indonesian National Police Investigator Officials shall notify the start of investigation and submit the result to the public prosecutor.

(8) In order to uncover Electronic Information and Electronic Transaction criminal act, investigator may cooperate with other country's investigator to share information and forms of evidence.

Article 44

Forms of evidence of investigation, prosecution and examination in court proceedings, based on the provisions of this Law are as follows:

a. forms of evidence as referred to in the provisions of Laws and Regulations; and

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

CHAPTER XI
CRIMINAL PROVISIONS

Article 45

(1) Any Person who fulfilled the elements as referred to in Article 27 paragraph (1), paragraph (2), paragraph (3), or paragraph (4) will be subject to imprisonment for a maximum of 6 (six) years and/or a maximum fine of IDR1,000,000,000.00 (one billion rupiah).

(2) Any Person who fulfilled the elements as referred to in Article 28 paragraph (1) or paragraph (2) will be subject to imprisonment for a maximum of 6 (six) years and/or a maximum fine of IDR1,000,000,000.00 (one billion rupiah).

(3) Any Person who fulfilled the elements as referred to in Article 29 will be subject to imprisonment for a maximum of 12 (twelve) years and/or a maximum fine of IDR2,000,000,000.00 (two billion rupiahs).

Article 46

(1) Any Person who fulfilled the elements as referred to in Article 30 paragraph (1) will be subject to imprisonment for a maximum of 6 (six) years and/or a maximum fine of IDR600,000,000.00 (six hundred million rupiahs).

(2) Any Person who fulfilled the elements as referred to in Article 30 paragraph (2) will be subject to imprisonment for a maximum of 7 (seven) years and/or a maximum fine of IDR700,000,000.00 (seven hundred million rupiahs).

(3) Any Person who fulfilled the elements as referred to in Article 30 paragraph (3) will be subject to imprisonment for a maximum of 8 (eight) years and/or a maximum fine of IDR800,000,000.00 (eight hundred million rupiahs).

Article 47

Any Person who fulfilled the elements as referred to in Article 31 paragraph (1) or paragraph (2) will be subject to imprisonment for a maximum of 10 (ten) years and/or a maximum fine of IDR800,000,000.00 (eight hundred million rupiahs).

Article 48

(1) Any Person who fulfilled the elements as referred to in Article 32 paragraph (1) will be subject to imprisonment for a maximum of 8 (eight) years and/or a maximum fine of IDR2,000,000,000.00 (two billion rupiahs).

(2) Any Person who fulfilled the elements as referred to in Article 32 paragraph (2) will be subject to imprisonment for a maximum of 9 (nine) years and/or a maximum fine of IDR3,000,000,000.00 (three billion rupiahs).

(3) Any Person who fulfilled the elements as referred to in Article 32 paragraph (3) will be subject to imprisonment for a maximum of 10 (ten) years and/or a maximum fine of IDR5,000,000,000.00 (five billion rupiahs).

Article 49

Any Person who fulfilled the elements as referred to in Article 33, will be subject to imprisonment for a maximum of 10 (ten) years and/or a maximum fine of IDR10,000,000,000.00 (ten billion rupiahs).

Article 50

Any Person who fulfilled the elements as referred to in Article 34 paragraph (1), will be subject to imprisonment for a maximum of 10 (ten) years and/or a maximum fine of IDR10,000,000,000.00 (ten billion rupiahs).

Article 51

(1) Any Person who fulfilled the elements as referred to in Article 35, will be subject to imprisonment for a maximum of 12 (twelve) years and/or a maximum fine of IDR12,000,000,000.00 (twelve billion rupiahs).

(2) Any Person who fulfilled the elements as referred to in Article 36, will be subject to imprisonment for a maximum of 12 (twelve) years and/or a maximum fine of IDR12,000,000,000.00 (twelve billion rupiahs).

Article 52

(1) In the event that the criminal act as referred to in Article 27 paragraph (1) is related to decency or sexual exploitation of children, shall be subject to an aggravation of one third of the principal sentence.

(2) In the event that the acts as referred to in Article 30 to Article 37 are aimed to Computer and/or

Electronic System as well as Electronic Information and/or Electronic Document that belongs to the Government and/or used for public services, will be sentenced to the principal sentence plus one third.

(3) In the event that the acts as referred to in Article 30 to Article 37 are aimed to Computer and/or Electronic System as well as Electronic Information and/or Electronic Document that belongs to the Government and/or strategic agencies including but not limited to defense agency, central bank, banking, finance, international agency, aviation authority will be sentenced to a maximum of principal criminal sentence of each Article plus two-third.

(4) In the event that the acts as referred to in Article 30 to Article 37 are conducted by corporates, will be sentenced to the principal sentence plus two-third.

CHAPTER XII

TRANSITIONAL PROVISIONS

Article 53

At the time this Law comes into force, all Laws and Regulations and institutions related to the utilization of Information Technology that do not conflict this Law shall remain valid.

CHAPTER XIII

CLOSING PROVISIONS

Article 54

(1) This Law comes into force from the date of its promulgation.

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

For public cognizance, it is hereby ordered that this Law be promulgated in the State Gazette of the Republic of Indonesia.

Enacted in Jakarta,

On 21 April 2008

THE PRESIDENT OF THE REPUBLIC OF INDONESIA,

Signed

DR. H. SUSILO BAMBANG YUDHOYONO

Promulgated in Jakarta,

On 21 April 2008

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

Signed

ANDI MATTALATTA

STATE GAZETTE OF THE REPUBLIC OF INDONESIA OF 2008 NUMBER 58

ELUCIDATION OF
LAW OF THE REPUBLIC OF INDONESIA
NUMBER 11 OF 2008
ON
ELECTRONIC INFORMATION AND TRANSACTIONS

I. GENERAL

The use of information technology, media and communication has changed both the behavior of society and human civilization globally. The development of information and communication technology has also caused world relations to be borderless and caused significant social, economic and cultural changes to take place so rapidly. Information technology is currently a double-edged sword because in addition to contributing to the improvement of human welfare, progress and civilization, it is also an effective means of unlawful acts.

Currently, a new legal regime has been born, which is known as cyber law or telematics law. Cyber law is internationally used for legal terms related to the use of information and communication technology. Likewise, telematics law is the embodiment of the convergence of telecommunications law, media law and informatics law. Other terms that are also used are law of information technology, virtual world law, and cybercrime law. These terms were born through consideration paid to the activities carried out through computer systems networks and communication systems both locally and globally (Internet) by utilizing computer system-based information technology which is an electronic system that can be seen virtually. Legal problems that are often encountered are when it comes to the delivery of information, communication, and/or transactions electronically, especially in terms of evidence and matters related to legal acts carried out through electronic systems.

What is meant by electronic system is a computer system in a broad sense, which does not only include computer hardware and software, but also includes telecommunications networks and/or electronic communication systems. Software; or a computer program is a set of instructions embodied in the form of language, code, scheme, or other forms, which when combined with computer-readable media will be able to make the computer work to perform special functions or to achieve specific results, including preparation in designing these instructions.

Electronic systems are also used to explain the existence of an information system which is the application of information technology based on telecommunications networks and electronic media, which functions to design, process, analyze, display, and transmit or disseminate electronic information. In a technical and management manner, information systems are actually the embodiment of the application of information technology products into a form of organization and management in accordance with the characteristics of the needs at the said organization and in accordance with their intended purposes. On the other hand, technically and functionally information systems are integrated systems between humans and machines that include components of hardware, software, procedures, human resources, and substance of information which in their utilization include input, process, output, storage and communication functions.

In this regard, the world of law has long since broadened the interpretation of its principles and norms when dealing with intangible material problems, for example in the case of theft of electricity as a criminal act. In reality, cyber activities are no longer simple, because their activities are no longer limited by the territory of a country, which can be easily accessed anytime and from anywhere. Losses can occur both to transactors and to other people who have never made a transaction, for example theft of credit card funds through shopping on the Internet. In addition, proof is a very important factor considering that electronic information has yet to be accommodated comprehensively within Indonesia's procedural law system, but is also very susceptible to being changed, tapped, falsified, and sent to various parts of the world within seconds. Thus, the resulting impacts can be complex and intricate.

A wider problem occurs in the civil sector because electronic transactions for trading activities through

electronic systems (electronic commerce) have become part of national and international commerce. This fact shows that the convergence in the field of information technology, media and informatics (telematics) continues to grow without much resistance, along with the discovery of new developments in the fields of information, media and communication technology.

Activities through electronic media systems, which are also called cyberspace, although virtual in nature can be categorized as real legal acts or measures, Judicially, activities in cyberspace cannot be solely approached with conventional legal standards and qualifications because if this method is taken, there will be too much trouble and things that will escape the enforcement of the law. Activities in cyberspace are virtual activities that have a very real impact even though the forms of evidence is electronic.

Thus, the subject of the perpetrator must also be qualified as a Person who has actually committed a legal act. In e-commerce activities, among others, there are electronic documents of which the position is equal to documents made on paper.

In this regard, it is necessary to pay attention to the aspects of security and legal certainty in the use of information, media, and communication technology in order for it to develop optimally. Therefore, there are three approaches to maintain security in cyber space, namely the approach of legal aspects, technological aspects, social, cultural, and ethical aspects. In order to overcome security problems in electronic system operation, the legal approach is absolute because without legal certainty, the problem of utilizing information technology is not optimal.

II. ARTICLE BY ARTICLE

Article 1

Self-explanatory.

Article 2

This Law has the scope of jurisdiction which is not solely for legal acts that apply in Indonesia and/or committed by Indonesian citizens, but also applies to legal acts committed outside the jurisdiction of Indonesia by both Indonesian citizens and citizens of foreign countries or Indonesian legal entities or foreign legal entities that have legal consequences in Indonesia, considering that the use of Information Technology for Electronic Information and Electronic Transaction can be cross-territorial or universal.

“detrimental to Indonesia’s interest” include but not limited to detrimental to national economic interests, strategic data protection, the dignity of the nation, state defense and security, state sovereignty, citizens, as well as Indonesian legal entities.

Article 3

“principle of legal certainty” means the legal basis for the utilization of Information Technology and Electronic Transaction as well as all anything that supports their operation that has legal recognition inside and outside the court.

“principle of benefit” means the principle for the utilization of Information Technology and Electronic Transaction shall be endeavored to support the information process so as to improve public welfare.

”principle of prudence” means the basis for the relevant party which shall take into account all aspects that may potentially incur losses, both for themselves and for another party in the utilization of Information Technology and Electronic Transaction.

“principle of good faith” means the basis used by the parties that in conducting Electronic Transaction without the purpose to intentionally and illegally or unlawfully cause harm to the another party without the knowledge of the other party.

“principle of freedom to choose technology or technology-neutral” means that the principle of the utilization of Information Technology and Electronic Transaction is not focused on the use of certain technology So that it can follow future developments.

Article 4

Self-explanatory.

Article 5

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Letter a

Letter which is based on law shall be made in written form includes but not limited to securities, valuable documents, documents used in the process of enforcing civil, criminal and state administrative procedural laws.

Letter b

Self-explanatory.

Article 6

So far, written form is identical to information and/or documents that are written on paper only, even though in essence, information and/or documents may be made into any media, including electronic media. In the scope of Electronic System, the original information with its copy is no longer relevant to be differentiated because the Electronic System basically operates by way of duplication which results in the original information being indistinguishable from the copy.

Article 7

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

Article 8

Self-explanatory.

Article 9

“complete and valid information” include:

a. information that contains the identity and status of legal subjects and their competence, either as a producer, supplier, organizer or intermediary;

b. other information that states certain matters which become the requirement for an agreement to be

valid as well explain the goods and/or services offered, such as name, address, and description of goods/services.

Article 10

Paragraph (1)

Reliability Certification is intended as proof that businesses conducting electronic trading are fit to do business after going through an assessment and audit from the authorized body. Proof of Reliability Certification is shown through a certification logo in the form of a trust mark on the relevant business' home page.

Paragraph (2)

Self-explanatory.

Article 11

Paragraph (1)

This Law grants recognition on duty that even though it is only a code, Electronic Signature has the same position as manual signatures in general which have legal force and legal consequences.

The requirements referred to in this Article are the minimum requirements that shall be fulfilled in every Electronic Signature. This provision opens the widest possible opportunity for anyone to develop methods, techniques, or processes to create Electronic Signature.

Paragraph (2)

The relevant Regulation of the Government shall, among others, regulate the techniques, methods, facilities, and process to create Electronic Signature.

Article 12

Self-explanatory.

Article 13

Self-explanatory.

Article 14

Information as referred to in this Article is the minimum information that shall be fulfilled by every Electronic Signature organizer.

Article 15

Paragraph (1)

“Reliably” means that the Electronic System has abilities that are suitable for the needs of its user.

“Safely” means that the Electronic System is protected both physically and non-physically.

“Proper operation” means that the Electronic System has abilities that are suitable for its specification.

Paragraph (2)

“Responsible” means that there is a legal subject that is legally responsible for the Organization of said Electronic System.

Paragraph (3)

Self-explanatory.

Article 16

Self-explanatory.

Article 17

Paragraph (1)

This Law provides opportunities for the use of Information Technology by state administrators, Person, Business Entity, and/or the public.

Utilization of Information Technology must be carried out properly, wisely, responsibly, effectively, and efficiently in order to obtain maximum benefits for the public.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 18

Paragraph (1)

Self-explanatory.

Paragraph (2)

The selection of law made by parties in international contracts, including those made electronically, is known as the choice of law. This law is binding as the law applicable for said contract.

The choice of law in Electronic Transaction may only be conducted if there is foreign element in the contract which implementation shall be in line with the private international law (hukum perdata internasional/HPI) principle.

Paragraph (3)

In the event that there is no choice of law, determination of applicable law shall be based on private international law principles which will be stipulated as the law applicable for said contract.

Paragraph (4)

Forum which is authorized to adjudicate international contract disputes, including those conducted electronically, is the forum selected by the parties. The forum can take the form of a court, arbitration, or other alternative dispute resolution agencies.

Paragraph (5)

In the event that the parties do not make a choice of forum, the forum's authority shall apply based on private international law principles. This principle is known as the basis of presence and the principle of effectiveness.

Article 19

“agreed” in this article shall also include the agreement on the existing procedures in the relevant Electronic System.

Article 20

Paragraph (1)

Electronic Transaction shall occur upon an agreement between the parties which may be in the form of, among others, data, identity, personal identification number (PIN) or password checking.

Paragraph (2)

Self-explanatory.

Article 21

Paragraph (1)

“authorized” in this provision is preferable stated using a power of attorney.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article 22

Paragraph (1)

“feature” is the facility that offers a chance to the user of Electronic Agent to change the information submitted, for example cancel, edit, and reconfirmation facilities.

Paragraph (2)

Self-explanatory.

Article 23

Paragraph (1)

Domain Name shall be in the form of address or identity of a state administrator, Person, Business Entity, and/or the public, the acquisition of which is based on the first come first serve principle.

The first come first serve principle differs between the provisions in Domain Name and in the area of intellectual property rights because no substantive examination is required, such as an examination in trademark and patent registration.

Paragraph (2)

“violates the rights of another person” for example, violating registered marks, names of registered legal entities, names of famous Person, and similar names which are essentially detrimental to other Person.

Paragraph (3)

“illegal use of Domain Name” is the registration and use of a Domain Name which is solely intended to

prevent or hinder another Person from using a name that is intuitive with the existence of their name or product name, or to complement the reputation of a Person who is already famous or well-known, or to mislead consumers.

Article 24

Self-explanatory.

Article 25

Electronic information and/or Electronic Document formed and registered as intellectual works, copyrights, patents, trademarks, trade secrets, industrial designs, and the like must be protected by this Law with due consideration to the provisions of Laws and Regulations.

Article 26

Paragraph (1)

In the utilization of Information Technology, personal data protection is one of the parts of privacy rights. Privacy rights are defined as follows:

a. Privacy rights are the right to enjoy a private life and be free from all kinds of distractions.

b. Privacy rights are the right to be able to communicate with (another Person without being spied on).

c. Privacy rights are the right to supervise information access regarding someone's personal life and data.

Paragraph (2)

Self-explanatory.

Article 27

Self-explanatory.

Article 28

Self-explanatory.

Article 29

Self-explanatory.

Article 30

Paragraph (1)

Self-explanatory.

Paragraph (2)

Technically, prohibited actions as referred to in this article can be conducted, among others, by way of:

a. communicating, sending, broadcasting or intentionally make an effort to realize the aforementioned things to anyone that has no right to receive it; or

b. intentionally prevented the information in question to not be or failed to be accepted by rightful recipients within the government and/or regional governments.

Paragraph (3)

Security system is a System that restricts Computer access or prohibits access to a Computer based on categorization or clarification of users and the specified level of authority.

Article 31

Paragraph (1)

"intercept or tap" is the activity to hear, record, divert, alter, hinder, and/or note down the transmission of Electronic Information and/or Electronic Document with non-public nature, both using communication cable network or wireless networks, such as electromagnetic emission or radio frequency.

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)

"research" is the research 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

Self-explanatory.

Article 41

Paragraph (1)

Self-explanatory.

Paragraph (2)

"an agency established by the public" is an agency that engages in the information technology and electronic transaction sector.

Paragraph (3)

Self-explanatory.

Article 42

Self-explanatory.

Article 43

Paragraph (1)

Self-explanatory.

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

"expert" is a person with specific expertise in Information Technology sector whose expertise can be accounted for both academically and practically.

Letter i

Self-explanatory.

Paragraph (6)

Self-explanatory.

Paragraph (7)

Self-explanatory.

Paragraph (8)

Self-explanatory.

Article 44

Self-explanatory.

Article 45

Self-explanatory.

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 every unlawful act which fulfills the elements as referred to in Article 27 to Article 37 conducted by corporations (corporate crime) and/or management and/or staff with capacity to:

a. represent a corporation;

b. make decision in a corporation;

c. supervise and control in a corporation;

d. carry out activities for the benefit of corporation.

Article 53

Self-explanatory.

Article 54

Self-explanatory.

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