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

THE PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering:

a. that the national development is a sustainable process that should at all times be responsive to the varying dynamic among the public;

b. that globalization of information has placed Indonesia as part of the world's information community, therefore the making of regulation concerning organization of Electronic Information and transactions at the national level is required in order that the development of Information Technology can be carried out in an optimal, distributive, and widespread manner throughout all levels of society to advance the intellectual life of people.

c. that very rapid development and advance of Information Technology have contributed to changes in the people's life activities in the various field that have had direct effect on the emergence of new forms of legal acts;

d. that the use and usage of Information Technology must continuously be developed to foster, maintain, and strengthen the national union and unity under laws and regulations in the national interest.

f. that the Government of necessity supports the development of Information Technology through infrastructure of law and its regulation in order that the Information Technology usage is carried out securely to prevent its misuse with due regard to religious and social-cultural values of the Indonesian society;

g. that based on consideration as intended by point a, point b, point c, point d, point e, and point f, it is necessary to make Law concerning Electronic Information and Transactions.

Bearing in mind:

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

With the Joint Consent of
THE HOUSE OF REPRESENTATIVES OF THE REPUBLIC OF INDONESIA
and
THE PRESIDENT OF THE REPUBLIC OF INDONESIA

HAS DECIDED:

To enact: LAW CONCERNING ELECTRONIC INFORMATION AND TRANSACTIONS.

CHAPTER 1
GENERAL PROVISIONS
Article 1

In this law:

1. "Electronic Information" means one cluster or clusters of electronic data, including but not limited to writings, sounds, images, maps, drafts, photographs, electronic data interchange (EDI), electronic mails, telegrams, telex, telecopy or the like, letters, signs, figures, Access Codes, symbols or perforations that have been processed for meaning or understandable to persons qualified to understand them.

2. "Electronic Transactions" means a legal act that is committed by the use of Computers, Computer networks, and/or other electronic media.

3. "Information Technology" means a technique to collect, prepare, store, process, announce, analyze, and/or disseminate information.

4. "Electronic Record" means any Electronic Information that is created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical form, or the like, visible, displayable and/or audible via Computers or Electronic Systems, including but not limited to writings, sounds, images, maps, drafts, photographs or the like, letters, signs, figures, Access Codes, symbols or perforations having certain meaning or definition or understandable to persons qualified to understand them.

5. "Electronic System" means a set of electronic devices and procedures that functions to prepare, collect, process, analyze, store, display, announce, send, and/or disseminate Electronic Information.

6. "Provision of Electronic System" means an Electronic System usage by the state administrators, Persons, Business Entities, and/or the public.

7. "Electronic System Network" means a closed or open connection of two Electronic Systems or more.

8. "Electronic Agent" means an automated electronic means that is used to initiate an action to certain Electronic Information, which is operated by Persons.

9. “Electronic Certificate” means a certificate in electronic nature that bears an Electronic Signature and identity, demonstrating a status of a legal subject of parties to an Electronic Transaction issued by Certification Service Providers.

10. “Electronic Certification Service Provider” means a legal entity that acts as a reliable party, issues and audits Electronic Certificates.

11. “Trustworthiness Certification Body” means an independent institution that is formed by professionals acknowledged, certified, and supervised by the Government, whose authority is to audit and issue trustworthiness certificates for Electronic Transactions.

12. “Electronic Signature” means a signature that contains Electronic Information that is attached to, associated or linked with other Electronic Information that is used for means of verification and authentication.

13. “Signatory/Signer” means a legal subject associated or linked with an Electronic Signature.

14. “Computer” means an electronic, magnetic, optical data processing device, or a system that performs logic, arithmetic, and storage functions.

15. “Access” means an activity to make interaction with independent or network Electronic Systems.

16. “Access Code” means a figure, letter, symbol, other character or a combination thereof, which is a key to enable Access to Computers and/or other Electronic Systems.

17. “Electronic Contract” means an agreement of parties entered into by means of Electronic Systems.

18. “Sender/Originator” means a legal subject that sends Electronic Information and/or Electronic Records.

19. “Recipient/Addressee” means a legal subject that receives Electronic Information and/or Electronic Records from Senders/Originators.

20. “Domain Name” means an internet address of a state administrator, Person, Business Entity, and/or the public that can be used for communication over the internet, in the form of unique character code or set to identify a certain location on the internet.

21. “Person” means an individual, whether an Indonesian citizen, foreign citizen, or legal entity.

22. “Business Entity” means a sole proprietorship or partnership of both legal entity and nonlegal entity.

23. “Government” means a Minister(s) or other official(s) the President designates.

Article 2

This Law shall apply to any Person who commits legal acts as governed by this Law, both within jurisdiction of Indonesia and outside jurisdiction of Indonesia, having legal effect within jurisdiction of Indonesia and/or outside jurisdiction of Indonesia and detrimental to the interest of Indonesia.

CHAPTER II
PRINCIPLES AND OBJECTIVES

Article 3

Information Technology and Electronic Transaction usage shall be implemented under the principles of legal certainty, benefit, prudence, good faith, and freedom to choose technology or technology neutrality.

Article 4

Information Technology and Electronic Transaction usage shall be implemented with the objectives to:

a. advance the intellectual life of the people as part of the world information community;
b. develop the national trade and economy in order to improve public welfare;
c. improve the effectiveness and efficiency of public services;
d. give as wide opportunities as possible to any Person to cultivate his/her insight and capability in the optimal and responsible use and usage of Information Technology; and
e. give senses of security, justice, and legal certainty for Information Technology users and providers.

CHAPTER III
ELECTRONIC INFORMATION, RECORDS, AND SIGNATURES

Article 5

1) Electronic Information and/or Electronic Records and/or the printouts thereof shall be lawful means of proof.
2) Electronic Information and/or Electronic Records and/or the printouts thereof as intended by section (1) shall be the expansion of lawful means of proof in accordance with the Law of Procedure applicable in Indonesia.
3) Electronic Information and/or Electronic Records shall be declared to be lawful if using Electronic Systems in accordance with provisions as governed by this Law.
4) Provisions on Electronic Information and/or Electronic Records as intended by section (1) shall not apply to:
   a. certificates that under Laws must be made in writing form; and
   b. certificates together with their papers that under Laws must be made in notarial deed or deed made by land conveyances.

Article 6

Where other provisions are in place other than those regulated in Article 5 section (4) requiring that information must be in writing or original form, Electronic Information and/or Electronic Records shall be deemed to be lawful to the extent information contained therein is accessible, displayable, assured as to its integrity, and accountable in order to be explanatory.

Article 7

Any Person who asserts rights, affirms existing rights, or denies other Persons' rights with respect to the existence of Electronic Information and/or Electronic Records must ensure that Electronic Information and/or Electronic Records with him/her originate in Electronic Systems eligible under Laws and Regulations.

Article 8

(1) Unless agreed otherwise, time of sending of Electronic Information and/or Electronic Records shall be determined at the time the Electronic Information and/or Electronic Records have been sent to the proper address by the Senders/Originators to Electronic Systems the Recipients/Addressees designate or use, and have entered Electronic Systems outside the control of the Senders/Originators.

(2) Unless agreed otherwise, the time of receipt of Electronic Information and/or Electronic Records shall be determined at the time the Electronic Information and/or Electronic Records enter Electronic Systems under the control of the authorized Recipients/Addressees.

(3) Where Recipients/Addressees have designated certain Electronic Systems to receive Electronic Information, reception shall occur at the time Electronic Information and/or Electronic Records enter designated Electronic Systems.

(4) Where there are two or more information systems used in the sending or reception of Electronic Information and/or Electronic Records, then:
a. the time of sending shall be the time when Electronic Information and/or Electronic Records enter a first information system outside the control of the Senders/Originators.
b. the time of receipt shall be the time when Electronic Information and/or Electronic Records enter a last information system under the control of the Recipients/Addressees.

Article 9

Business actors that offer products through Electronic Systems must make available full and true information about contractual conditions, producers, and offered products.

Article 10

(1) Any business actor who conducts Electronic Transactions may be certified by Trustworthiness Certification Bodies.

(2) Provisions on formation of Trustworthiness Certification Bodies as intended by section (1) shall be regulated by Government Regulation.

Article 11

(1) Electronic Signatures shall have lawful legal force and legal effect to the extent satisfying the following requirements:

a. Electronic Signature-creation data shall be associated only with the Signatories/ Signers;
b. Electronic Signature-creation data at the time the electronic signing process shall be only in the power of the Signatories/ Signers;
c. Any alteration in Electronic Signatures that occur after the signing time is knowable;
d. Any alteration in Electronic Information associated with the Electronic Signatures after the signing time is knowable;
e. There are certain methods adopted to identify the identity of the Signatories/ Signers; and
f. There are certain methods to demonstrate that the Signatories/Signers have given consent to the associated Electronic Information;

(2) Further provisions on Electronic Signatures as intended by section (1) shall be regulated by Government Regulation.

Article 12

(1) Any Person involved in electronic signing is required to provide security of Electronic Signatures he/she uses;

(2) Security of Electronic Signatures as intended by section (1) shall include at least:

a. the systems are not accessible to unauthorized Persons;
b. the Signatories/Signers must apply the principle of prudence to avoid unauthorized uses of Electronic Signature-creation data;
c. the Signatories/Signers must without delay adopt methods recommended by Electronic Signature providers, or other appropriate methods and should promptly notify Persons whom the Signatories/Signers consider to be relying on the Electronic Signatures or notify parties that support Electronic Signature services if:
− the Signatories/Signers know that the Electronic Signature-creation data has been compromised; or
− circumstances known to the Signatories/Signers may pose considerable risks due likely to the compromised Electronic Signature-creation data; and
d. where Electronic Certificates are used to support Electronic Signatures, the Signatories/Signers must confirm the truth and integrity of all information in connection with the Electronic Certificates.

(3) Any Person in violation of the provisions as intended by section (1) shall be responsible for any damage and legal consequence incurred.

CHAPTER IV
PROVISION OF ELECTRONIC CERTIFICATION AND ELECTRONIC SYSTEMS

Part One
Provision of Electronic Certification

Article 13

(1) Any Person shall be entitled to engage the service of Electronic Certification Service Providers for creating Electronic Signatures.

(2) Electronic Certification Service Providers must confirm the attribution of an Electronic Signature to the owner.

(3) Electronic Certification Service Providers shall include:
a. Indonesian Electronic Certification Service Providers; and
b. foreign Electronic Certification Service Providers.

(4) Indonesian Electronic Certification Service Providers shall be an Indonesian legal entity and domiciled in Indonesia.

(5) Foreign Electronic Certification Service Providers that operate in Indonesia must be registered in Indonesia.

(6) Further provisions on Electronic Certification Service Providers as intended by section (3) shall be regulated by Government Regulation.

Article 14

Electronic Certification Service Providers as intended by Article 13 section (1) through section

(5) must make available to any service user accurate, clear, and definite information that includes:
a. methods that are adopted to identify the Signatories/Signers;
b. things that can be used to recognize Electronic Signature-creation personal data;
c. things that can demonstrate the validity and security of Electronic Signatures;

Part Two
Provision of Electronic Systems

Article 15

(1) Any Electronic System Provider must provide Electronic Systems in reliable and secure manner and shall be responsible for the proper operation of the Electronic Systems.
(2) Electronic System providers shall be responsible for their Provision of Electronic Systems.

(3) The provision as intended by section (2) shall not apply where it is verifiable that there occur compelling circumstances, fault, and/or negligence on the part of the Electronic System users.

Article 16

(1) To the extent not provided otherwise by separate laws, any Electronic System Provider is required to operate Electronic Systems in compliance with the following minimal requirements:
a. can redisplay Electronic Information and/or Electronic Records in their entirety in accordance with the retention period as provided for by Laws and Regulations;
b. can protect the availability, entirety, authenticity, confidentiality, and accessibility of Electronic Information in the Provision of Electronic Systems;
c. can operate in compliance with procedures or guidelines for the Provision of Electronic Systems;
d. are furnished with procedures or guidelines that are announced with languages, information, or symbols that are understandable to parties attributed to the Provision of Electronic Systems; and
e. adopt sustainable mechanism in order to maintain updates, clarity, and accountability for the procedures or guidelines;

(2) Further provisions on Provision of Electronic Systems as intended by section (1) shall be regulated by Government Regulation.

CHAPTER V
ELECTRONIC TRANSACTIONS

Article 17

(1) Provision of Electronic Transactions may be carried out within a public or private scope.
(2) Parties that conduct Electronic Transactions as intended by section (1) must be in good faith in making interaction and/or exchange of Electronic Information and/or Electronic Records during the transactions.
(3) Further provisions on provision of Electronic Transactions as intended by section (1) shall be regulated by Government Regulation.

Article 18

(1) Electronic Transactions that are stated in Electronic Contracts shall bind on parties.
(2) Parties shall have the power to choose law applicable to international Electronic Transactions they enter.
(3) If parties do not make choice of law in international Electronic Transactions, the applicable law shall be under the principles of the Private International Law.
(4) Parties shall have the powers to determine forums of court, arbitration, or other alternative dispute resolution institutions with jurisdiction to handle disputes that may arise from international Electronic Transactions they enter.
(5) If parties do not make choice of forum as intended by section (4), the jurisdiction of court, arbitration, or other alternative dispute resolution institution with jurisdiction to handle

disputes that may arise from such transactions shall be determined under the principles of the Private International Law.

Article 19

Parties that conduct Electronic Transactions must adopt agreed-on Electronic Systems.

Article 20

(1) Unless provided otherwise by parties, Electronic Transactions shall occur at the time the transaction offers sent by Senders/Originators have been received and accepted by Recipients/Addressees.
(2) Acceptance on the Electronic Transaction offers as intended by section (1) must be made with an electronic acknowledgement of receipt.

Article 21

(1) Senders/Originators or Recipients/Addressees may conduct Electronic Transactions in person, or by his/her proxy, or by Electronic Agents.
(2) Parties responsible for any legal effect in the conduct of Electronic Transactions as intended by section (1) shall be regulated as follows:
a. if conducted in person, any legal effect in the conduct of Electronic Transactions shall become the responsibility of parties to a transaction;
b. if conducted by proxy, any legal effect in the conduct of Electronic Transactions shall become the responsibility of the grantors of the proxy; or
c. if conducted by Electronic Agents, any legal effect in the conduct of Electronic Transactions shall become the responsibility of Electronic Agent providers.
(3) If damage of Electronic Transactions is occasioned by failure of the operation of Electronic Agents due to third parties' direct measures against Electronic Systems, any legal effect shall become the responsibility of Electronic Agents.
(4) If damage of Electronic Transactions is occasioned by failure of the operation of Electronic Agents due to negligence of service users, any legal effect shall become the responsibility of the service users.
(5) The provision as intended by section (2) shall not apply if provable that there occur compelling circumstances, fault and/or negligence on the part of the Electronic System users.

Article 22

(1) Certain Electronic Agent Providers must provide features to Electronic Agents they operate to enable their users to alter information still in the process of transaction.
(2) Further provisions on certain Electronic Agent providers as intended by section (1) shall be regulated by Government Regulation.

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

Article 23

(1) Any state administrator, Person, Business Entity, and/or the public shall be entitled to hold Domain Names on a first applicant principle basis.
(2) Holding and use of Domain Names as intended by section (1) must be on the basis of good faith, non-violation of fair business competition, and non-infringement of the rights of other Persons.
(3) Any state administrator, Person, Business Entity, or the public damaged by other Persons' unauthorized use of Domain Names shall be entitled to lodge a claim for canceling such Domain Names.

Article 24

(1) Domain Name administrators shall be the Government and/or the public.
(2) Where a dispute on Domain Name administration by the public occurs, the Government shall be entitled to take over temporarily the Domain Name administration in dispute.
(3) Domain Name administrators residing outside the territory of Indonesia and Domain Names they have registered shall be recognized as to its existence to the extent not against Laws and Regulations.
(4) Further provisions on Domain Name administration as intended by section (1), section (2), and section (3) shall be regulated by Government Regulation.

Article 25

Electronic Information and/or Electronic Records that are created into intellectual works, internet sites, and intellectual works contained therein shall be protected as Intellectual Property Rights under provisions of Laws and Regulations.

Article 26

(1) Unless provided otherwise by Laws and Regulations, use of any information through electronic media that involves personal data of a Person must be made with the consent of the Person concerned.
(2) Any Person whose rights are infringed as intended by section (1) may lodge a claim for damages incurred under this Law.

CHAPTER VII
PROHIBITED ACTS

Article 27

(1) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents against propriety.
(2) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents of gambling.
(3) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents of affronts and/or defamation.
(4) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents of extortion and/or threats.

Article 28

(1) Any Person who knowingly and without authority disseminates false and misleading information resulting in consumer loss in Electronic Transactions.
(2) Any Person who knowingly and without authority disseminates information aimed at inflicting hatred or dissension on individuals and/or certain groups of community based on ethnic groups, religions, races, and intergroups (SARA).

Article 29

Any Person who knowingly and without authority sends Electronic Information and/or Electronic Records that contain violence threats or scares aimed personally.

Article 30

(1) Any Person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Systems of other Persons in any manner whatsoever.
(2) Any Person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Systems in any manner whatsoever with the intent to obtain Electronic Information and/or Electronic Records.
(3) Any Person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Systems in any manner whatsoever by breaching, hacking into, trespassing into, or breaking through security systems.

Article 31

(1) Any Person who knowingly and without authority or unlawfully carries out interception or wiretapping of Electronic Information and/or Electronic Records in certain Computers and/or Electronic Systems of other Persons.
(2) Any Person who knowingly and without authority or unlawfully carries out interception of the transmission of nonpublic Electronic Information and/or Electronic Records from, to, and in certain Computers and/or Electronic Systems of other Persons, whether or not causing alteration, deletion, and/or termination of Electronic Information and/or Electronic Records in transmission.
(3) Interception excepted from one as intended by section (1) and section (2) shall be interception carried out in the scope of law enforcement at the request of the police, prosecutor's office, and/or other law enforcement institutions as stated by laws.
(4) Further provisions on procedures for interception as intended by section (3) shall be regulated by Government Regulation.

Article 32

(1) Any Person who knowingly and without authority or unlawfully in any manner whatsoever alters, adds, reduces, transmits, tampers with, deletes, moves, hides Electronic Information and/or Electronic Records of other Persons or of the public.
(2) Any Person who knowingly and without authority or unlawfully in any manner whatsoever, moves or transfers Electronic Information and/or Electronic Records to Electronic Systems of unauthorized Persons.
(3) Acts as intended by section (1) shall be acts that result in any confidential Electronic Information and/or Electronic Record being compromised such that the data becomes accessible to the public in its entirety in an improper manner.

Article 33

Any Person who knowingly and without authority or unlawfully commits any act resulting in faults on Electronic Systems and/or resulting in Electronic Systems working improperly.

Article 34

(1) Any Person who knowingly and without authority or unlawfully produces, sells, causes to be used, imports, distributes, provides, or owns:
a. Computer hardware or software that is designed or specifically developed to facilitate acts as intended by Article 27 through Article 33;
b. Computer passwords, Access Codes, or the like to make Electronic Systems accessible with the intent to facilitate acts as intended by Article 27 through Article 33;
(2) Acts as intended by section (1) are not criminal acts if aimed at carrying out research activities, testing of Electronic Systems, protection of Electronic Systems themselves in a legal and lawful manner.

Article 35

Any Person who knowingly and without authority or unlawfully manipulates, creates, alters, deletes, tampers with Electronic Information and/or Electronic Records with the intent that such Electronic Information and/or Electronic Records would seem to be authentic data.

Article 36

Any Person who knowingly and without authority or unlawfully commits acts as intended by Article 27 through Article 34 to other Persons' detriment.

Article 37

Any Person who knowingly commits prohibited acts as intended by Article 27 through Article 36 outside the territory of Indonesia towards Electronic Systems residing within jurisdiction of Indonesia.

CHAPTER VIII
DISPUTE RESOLUTION

Article 38

(1) Any Person may institute actions against parties that provide Electronic Systems and/or using Information Technology to his/her detriment.
(2) The public in accordance with provisions of laws and regulations may bring class action lawsuits against parties that provide Electronic Systems and/or using Information Technology to the public detriment.

Article 39

(1) Civil actions shall be instituted in accordance with provisions of laws and regulations.
(2) In addition to resolution by civil actions as intended by section (1) parties may resolve disputes through arbitration or other alternative dispute resolution institutions in accordance with provisions of Laws and Regulations.

CHAPTER IX
ROLE OF THE GOVERNMENT AND ROLE OF THE PUBLIC

Article 40

(1) The Government shall facilitate the Information Technology and Electronic Transaction usage in accordance with provisions of prevailing laws and regulations.

(2) The Government shall protect the public interest from any type of threat as a result of misusing Electronic Information and Electronic Transactions that offends public order, in accordance with provisions of Laws and Regulations.
(3) The Government shall specify agencies or institutions holding strategic electronic data that must be protected.
(4) Agencies or institutions as intended by section (3) must create Electronic Records and the electronic backups thereof, and connect them with specified data centers in the interest of data security.
(5) Other agencies or institutions other than those regulated by section (3) shall create Electronic Records and their electronic backups as necessary to protect data they hold.
(6) Further provisions on role of the Government as intended by section (1), section (2), and section (3) shall be regulated by Regulation of the Government.

Article 41

(1) The public may play role in the improvement of the Information Technology usage through the use and Provision of Electronic Systems and Electronic Transactions in accordance with the provisions of this Law.
(2) Role of the public as intended by section (1) may be played via institutions the public forms.
(3) Institutions as intended by section (2) may have the functions of consultation and mediation.

CHAPTER X
INVESTIGATION

Article 42

Investigation of criminal acts as intended by this Law shall be made under the provisions of the Law of Criminal Procedure and the provisions of this Law.

Article 43

(1) In addition to Investigators of the State Police of the Republic of Indonesia, certain Civil Service Officials within the Government whose scope of duties and responsibilities is in the field of Information Technology and Electronic Transactions shall be granted special authority as investigators as intended by the Law of Criminal Procedure to make investigation of criminal acts of Information Technology and Electronic Transactions.
(2) Investigation of Information Technology and Electronic Transactions as intended by section (1) shall be made with due regard to privacy protection, secrecy, smooth public services, data integrity, or data entirety in accordance with provisions of laws and regulations.
(3) Searches and/or seizures of electronic systems suspiciously involved in criminal acts must be carried out with the permission of the local chief justice of the district court.
(4) In carrying out searches and/or seizures as intended by section (3), investigators are required to maintain the public service interests.
(5) Civil Service Investigators as intended by section (1) shall have the authority:
    a. to receive reports or complaints from Persons of the occurrence of criminal acts under the provisions of this Law;

b. to summons any Person or other party for hearing and/or examination as suspects or witnesses in connection with suspected criminal acts in the field related to the provisions of this Law;
c. to make examination of the truth of reports or inquiries into criminal acts under the provisions of this Law;
d. to make examination of Persons and/or Business Entities that should be suspected of having committed criminal acts under this Law;
e. to make inspection of equipment and/or facilities in connection with the activities of Information Technology suspected of having been used to commit criminal acts under this Law;
f. to search certain places suspected of having been used as the place to commit criminal acts under the provisions of this Law;
g. to seal and seize equipment and/or facilities of Information Technology activities suspected of having been used in a manner departing from provisions of Laws and Regulations;
h. to solicit assistance of experts necessary for investigation of criminal acts under this Law; and/or
i. to cease investigation of criminal acts under this Law in accordance with the provisions of the prevailing law of criminal procedure.

(6) To make arrest and detention, investigators through public prosecutors are required to seek order of the local chief justice of the district court within a period of twenty-four hours.
(7) Civil Service Investigators as intended by section (1) shall coordinate with Investigators of the State Police of the Republic of Indonesia to notify the commencement of investigation and deliver the results thereof to public prosecutors.
(8) To uncover criminal acts of Electronic Information and Electronic Transactions, investigators may cooperate with investigators of other countries to share information and means of proof.

Article 44

Means of proof on the investigation, prosecution and examination at court under the provisions of this Law shall be as follows:
a. means of proof as intended by provisions of laws and regulations; and
b. other means of proof in the form of Electronic Information and/or Electronic Records as intended by Article 1 point 1 and point 4 as well as Article 5 section (1), section (2), and section (3).

CHAPTER XI
PENAL PROVISIONS

Article 45

(1) Any Person who satisfies the elements as intended by Article 27 section (1), section (2), section (3), or section (4) shall be sentenced to imprisonment not exceeding 6 (six) years and/or a fine not exceeding Rp1,000,000,000 (one billion rupiah).

(2) Any Person who satisfies the elements as intended by Article 28 section (1) or section (2) shall be sentenced to imprisonment not exceeding 6 (six) years and/or a fine not exceeding Rp1,000,000,000,- (one billion rupiah).
(3) Any Person who satisfies the elements as intended by Article 29 shall be sentenced to imprisonment not exceeding 12 (twelve) years and/or a fine not exceeding Rp2,000,000,000 (two billion rupiah).

Article 46

(1) Any Person who satisfies the elements as intended by Article 30 section (1) shall be sentenced to imprisonment not exceeding 6 (six) years and/or a fine not exceeding Rp600,000,000 (six hundred million rupiah).
(2) Any Person who satisfies the elements as intended by Article 30 section (2) shall be sentenced to imprisonment not exceeding 7 (seven) years and/or a fine not exceeding Rp700,000,000 (seven hundred million rupiah).
(3) Any Person who satisfies the elements as intended by Article 30 section (3) shall be sentenced to imprisonment not exceeding 8 (eight) years and/or a fine not exceeding Rp800,000,000 (eight hundred million rupiah).

Article 47

Any Person who satisfies the elements as intended by Article 31 section (1) or section (2) shall be sentenced to imprisonment not exceeding 10 (ten) years and/or a fine not exceeding Rp800,000,000 (eight hundred million rupiah).

Article 48

(1) Any Person who satisfies the elements as intended by Article 32 section (1) shall be sentenced to imprisonment not exceeding 8 (eight) years and/or a fine not exceeding Rp2,000,000,000 (two billion rupiah).
(2) Any Person who satisfies the elements as intended by Article 32 section (2) shall be sentenced to imprisonment not exceeding 9 (nine) years and/or a fine not exceeding Rp3,000,000,000 (three billion rupiah).
(3) Any Person who satisfies the elements as intended by Article 32 section (3) shall be sentenced to imprisonment not exceeding 10 (ten) years and/or a fine not exceeding Rp5,000,000,000 (five billion rupiah).

Article 49

Any Person who satisfies the elements as intended by Article 33 shall be sentenced to imprisonment not exceeding 10 (ten) years and/or a fine not exceeding Rp10,000,000,000 (ten billion rupiah).

Article 50

Any Person who satisfies the elements as intended by Article 34 section (1) shall be sentenced to imprisonment not exceeding 10 (ten) years and/or a fine not exceeding Rp10,000,000,000 (ten billion rupiah).

Article 51

(1) Any Person who satisfies the elements as intended by Article 35 shall be sentenced to imprisonment not exceeding 12 (twelve) years and/or a fine not exceeding Rp12,000,000,000 (twelve billion rupiah).
(2) Any Person who satisfies the elements as intended by Article 36 shall be sentenced to imprisonment not exceeding 12 (twelve) years and/or a fine not exceeding Rp12,000,000,000 (twelve billion rupiah).

Article 52

(1) Criminal acts as intended by Article 27 section (1) involving propriety or sexual exploitation of children shall be subject to an increase in the sentence by one third of the basic sentence.
(2) Criminal acts as intended by Article 30 through Article 37 aimed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Records of the Government and/or used for public services shall be sentenced to the basic sentence plus one third.
(3) Criminal acts as intended by Article 30 through Article 37 aimed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Records of the Government and/or strategic bodies including and not limited to defense institutions, the central bank, banking, finance, international institutions, aviation authority shall be subject to a sentence of maximally the basic sentence for the respective Articles plus two-thirds.
(4) Criminal acts as intended by Article 27 through Article 37 committed by corporations shall be sentenced to the basic sentence plus two-thirds.

CHAPTER XII
TRANSITIONAL PROVISIONS

Article 53

Upon effectiveness of this Law, all Laws and Regulations and institutions in connection with Information Technology usage that are not against this Law are declared to remain valid.

CHAPTER XIII
CONCLUDING PROVISIONS

Article 54

(1) This law shall take effect from the date it is promulgated.
(2) Government Regulations must have been enacted not longer than 2 (two) years upon promulgation of this Law. In order that any person may know of it, the promulgation of this Law is ordered by placement in the State Gazette of the Republic of Indonesia.

Ratified in Jakarta
on April 21, 2008

PRESIDENT OF THE REPUBLIC OF INDONESIA
sgd. DR. H. SUSILO BAMBANG YUDHOYONO

Promulgated in Jakarta
on April 21, 2008

MINISTER OF LAW AND HUMAN RIGHTS OF THE REPUBLIC OF INDONESIA,
sgd ANDI MATTALATTA

STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER 58 OF 2008
SUPPLEMENT TO STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER 4843

***