

Type: LAW (UU)
By: THE PRESIDENT OF THE REPUBLIC OF INDONESIA
Number: 19 YEAR 2016 (19/2016)
Date: NOVEMBER 25, 2016 (JAKARTA)
Reference: LN 2016/251; TLN NO 5952
Title: AMENDMENT TO LAW NUMBER 11 YEAR 2008 REGARDING
ELECTRONIC INFORMATION AND TRANSACTION

BY THE GRACE OF THE ONE ALMIGHTY GOD

THE PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering:

- a. whereas to guarantee the recognition of as well as homage to the rights and freedom of other persons and to meet fair demands in accordance with the considerations of security and public order in a democratic society, it is necessary to amend Law Number 11 Year 2008 regarding Electronic Information and Transaction so as to realize justice, public order, and legal certainty;
- b. whereas based on the considerations as intended in point a, it is necessary to establish Law regarding Amendment to Law Number 11 Year 2008 regarding Electronic Information and Transaction;

In view of:

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

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

HAS DECIDED:

To Stipulate: LAW REGARDING AMENDMENT TO LAW NUMBER 11 YEAR 2008
REGARDING ELECTRONIC INFORMATION AND TRANSACTION.

Article I

Several provisions in Law Number 11 Year 2008 regarding Electronic Information and Transaction (State Gazette of the Republic of Indonesia Year 2008 Number 58, Supplement to State Gazette of the Republic of Indonesia Number 4843) shall be amended as follows:

1. Between sub-articles 6 and 7 of Article 1 shall be inserted with 1 (one) sub-article, namely sub-article 6a so that Article 1 shall read as follows:

Article 1

In this Law, referred to as:

1. Electronic Information shall be one or a set of electronic data, including but not limited to writing, audio, image, map, design, photo, *electronic data interchange* (EDI), *electronic mail*, telegram, telex, telecopy or the like, characters, signs, numbers, Access Codes, symbols, or perforations which have been processed and have meaning or can be understood by persons who are able to understand them.
2. Electronic Transaction shall be legal actions taken by using a Computer, Computer networks, and/or other electronic media.
3. Information Technology shall be a technique for collecting, preparing, storing, processing, publishing, analyzing, and/or disseminating information.
4. Electronic Document shall be any Electronic Information which is prepared, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical form, or the like, which can be seen, displayed, and/or heard by a Computer or Electronic System, including but not limited to writing, audio, image, map, design, photo or the like, characters, signs, numbers, Access Codes, symbols or perforations which have meaning or significance or can be understood by persons who are able to understand it.
5. Electronic System shall be a set of electronic devices and procedures having the function of preparing, collecting, processing, analyzing, storing, displaying, publishing, sending, and/or disseminating Electronic Information.
6. Electronic System Operation shall be the utilization of Electronic System by state administrators, Persons, Business Entities, and/or community.
- 6a. Electronic System Operator shall be any Person, state administrator, Business Entity, and community who provides, manages, and/or operates an Electronic System, whether individually or jointly to Electronic System users for their own needs and/or for the needs of other parties.
7. Electronic System Networks shall be the connection of two Electronic Systems or more, either closed or open in nature.
8. Electronic Agent shall be an instrument of an Electronic System, which is made for performing an action against a certain Electronic Information automatically, which is operated by Person.

9. Electronic Certificate shall be a certificate which is electronic in nature containing Electronic Signature and identity that indicate the legal subject status of the parties in Electronic Transaction which is issued by an Electronic Certification Operator.
10. Electronic Certification Operator shall be a legal entity having the function as a trusted party which provides and audits Electronic Certificates.
11. Reliability Certification Agency shall be an independent institution established by professional, which is recognized, legalized, and supervised by the Government and has the authorities to audit and issue certificates of reliability in Electronic Transaction.
12. Electronic Signature shall be signature consisting of Electronic Information affixed, associated or related to other Electronic Information, which is used as tool of verification and authentication.
13. Signer shall be a legal subject associated or related to an Electronic Signature.
14. Computer shall be a device for processing electronic, magnetic, optical data, or a system performing logical, arithmetic, and storage functions.
15. Access shall be activity to perform interaction with Electronic System which is stand-alone or in networks.
16. Access Code shall be numbers, letters, symbols, other characters or their combinations, constituting key to be able to access Computer and/or other Electronic Systems.
17. Electronic Contract shall be agreement of parties made into by Electronic System.
18. Sender shall be a legal subject who transmitting Electronic Information and/or Electronic Document.
19. Receiver shall be a legal subject receiving Electronic Information and/or Electronic Document from a Sender.
20. Domain Name shall be internet address of a state administrator, Person, Business Entity, and/or community member, which can be used in communication by internet, in the form of a code or a unique composition of characters to show certain location in internet.
21. Person shall be individual person, whether Indonesian citizen, foreign citizen, or legal entity.
22. Business Entity shall be individual company or partnership company, whether incorporated as a legal entity or not.
23. Government shall be the Minister or other officials appointed by the President.

2. The provisions of Article 5 shall remain unamended with amendment to the elucidation on paragraphs (1) and (2) so that the elucidation on Article 5 shall become as stipulated in elucidation on article by article of this Law.
3. The provisions of Article 26 shall be added with 3 (three) paragraphs, namely paragraphs (3), (4), and (5) so that Article 26 shall read as follows:

Article 26

- (1) Except provided otherwise by laws and regulations, the use of any information by electronic media related to personal data of someone must be performed upon approval of the Person concerned.
 - (2) Anyone whose rights as intended in paragraph (1) are infringed may file lawsuit for the losses caused based on this Law.
 - (3) Every Electronic System Operator must delete irrelevant Electronic Information and/or Electronic Document under its control at the request of the Person concerned based on a court stipulation.
 - (4) Every Electronic System Operator must provide a mechanism for the deletion of irrelevant Electronic Information and/or Electronic Document in accordance with the provisions of laws and regulations.
 - (5) The provisions on the procedures for deletion of Electronic Information and/or Electronic Document as intended in paragraphs (3) and (4) shall be stipulated in a government regulation.
4. The provisions of Article 27 shall remain unamended with amendment to the elucidation on paragraphs (1), (3), and (4) so that the elucidation on Article 27 shall become as stipulated in the elucidation on article by article of this Law.
 5. The provisions of paragraphs (3) and (4) of Article 31 shall be amended so that Article 31 shall read as follows:

Article 31

- (1) Any person who intentionally and unrightfully or against the law performs interception of Electronic Information and/or Electronic Document in a Computer and/or in certain Electronic System owned by other Persons.
- (2) Anyone who intentionally and unrightfully or against the law performs interception of transmission of Electronic Information and/or Electronic Document that are/is not public from, to, and in a Computer and/or in certain Electronic System owned by other Persons, whether such action causes no change or causes any change, removal, and/or discontinuation of Electronic Information and/or Electronic Document being transmitted.
- (3) The provisions as intended in paragraphs (1) and (2) shall not be applicable to interception which is performed in the context of law enforcement at request of police, public prosecutor's office, or other institutions the authorities of which are stipulated by law.

- (4) Further provisions on the procedures for interception as intended in paragraph (3) shall be stipulated in a law.
6. Between paragraphs (2) and (3) of Article 40 shall be inserted with 2 (two) paragraphs, namely paragraphs (2a) and (2b); the provisions of paragraph (6) of Article 40 shall be amended; as well as elucidation on paragraph (1) of Article 40 shall be amended so that Article 40 shall read as follows:

Article 40

- (1) The Government shall facilitate the utilization of Information Technology and Electronic Transaction in accordance with the provisions of laws and regulations.
- (2) The Government shall protect public interests from all types of disturbances caused by misuse of Electronic Information and Electronic Transaction which disturbs public order, in accordance with the provisions of laws and regulations.
- (2a) The Government must prevent the dissemination and use of Electronic Information and/or Electronic Document having prohibited content in accordance with the provisions of laws and regulations.
- (2b) In conducting the prevention as intended in paragraph (2a), the Government shall be authorized to perform disconnection of access and/or to order Electronic System Operator to perform disconnection of access to Electronic Information and/or Electronic Document having unlawful contents.
- (3) The Government shall designate agencies or institutions having strategic electronic data that must be protected.
- (4) Agencies or institutions as intended in paragraph (3) must prepare Electronic Documents and electronic backup as well as must connect it to a certain data center for the purpose of maintaining data security.
- (5) Agencies or institutions other than those set out in paragraph (3) shall prepare Electronic Documents and electronic backup in accordance with the need for the protection of their data.
- (6) Further provisions on the Government's role as intended in paragraphs (1), (2), (2a), (2b), and (3) shall be stipulated in a government regulation.
7. The provisions of paragraphs (2), (3), (5), (6), (7), and (8) of Article 43 shall be amended; between paragraphs (7) and (8) of Article 43 shall be inserted with 1 (one) paragraph, namely paragraph (7a); as well as elucidation on paragraph (1) of Article 43 shall be amended so that Article 43 shall read as follows:

Article 43

- (1) In addition to Investigators of the National Police of the Republic of Indonesia, certain Civil Servant Investigators within the Government whose scope of duties and responsibilities covers the field of Information Technology and Electronic Transaction shall be granted special authorities to act as investigators as intended in Law regarding Criminal

Procedure Law to perform investigation on criminal acts in the field of Information Technology and Electronic Transaction.

- (2) Investigation in the field of Information Technology and Electronic Transaction as intended in paragraph (1) shall be performed with due observance of the protection of privacy, confidentiality, smooth provision of public services, as well as integrity or wholeness of data in accordance with the provisions of laws and regulations.
- (3) Search and/or confiscation of Electronic System relating to alleged criminal acts in the field of Information Technology and Electronic Transaction shall be performed in accordance with the provisions of the criminal procedure law.
- (4) In conducting a search and/or confiscation as intended in paragraph (3), investigators must maintain the interests of public services.
- (5) Civil Servant Investigators as intended in paragraph (1) shall be authorized to:
 - a. receive report or complaints from any person regarding criminal acts in the field of Information Technology and Electronic Transaction;
 - b. invite any Person or other parties to be heard and interrogated as suspect or witness in connection with alleged criminal acts in the field of Information Technology and Electronic Transaction;
 - c. examine the accuracy of report or information with regard to criminal acts in the field of Information Technology and Electronic Transaction;
 - d. conduct interrogation of Persons and/or Business Entities which are reasonably alleged to have committed criminal acts in the field of Information Technology and Electronic Transaction;
 - e. examine tools and/or facilities relating to activities of Information Technology which are alleged to be used for committing criminal acts in the field of Information Technology and Electronic Transaction;
 - f. conduct a search of certain places which are alleged to be used as places for committing criminal acts in the field of Information Technology and Electronic Transaction;
 - g. seal and confiscate tools and/or facilities of activities of Information Technology which are alleged to be used in violation of the provisions of laws and regulations;
 - h. make data and/or Electronic System relating to criminal acts in the field of Information Technology and Electronic Transaction inaccessible;
 - i. ask for information existing in Electronic System or information generated by Electronic System to Electronic System Operator

relating to criminal acts in the field of Information Technology and Electronic Transaction;

- j. ask for necessary assistance of experts in the investigation of criminal acts in the field of Information Technology and Electronic Transaction; and/or
 - k. discontinue investigation on criminal acts in the field of Information Technology and Electronic Transaction in accordance with the provisions of criminal procedure law.
- (6) Arrest and detention of perpetrator of criminal acts in the field of Information Technology and Electronic Transaction shall be performed in accordance with the provisions of criminal procedure law.
- (7) Civil Servant Investigator as intended in paragraph (1) in carrying out his/her duties shall notify start of investigation to Public Prosecutor through Investigator of National Police of the Republic of Indonesia.
- (7a) As investigation is finished, Civil Servant Investigator as intended in paragraph (1) shall convey his/her investigation result to Public Prosecutor through Investigator of National Police of the Republic of Indonesia.
- (8) In the context of disclosing criminal acts of Electronic Information and Electronic Transaction, investigator can cooperate with investigator of other country to share information and evidences in accordance with the provisions of laws and regulations.
8. The provisions of Article 45 shall be amended as well as between Articles 45 and 46 shall be inserted with 2 (two) articles, namely Articles 45A and 45B so as to read as follows:

Article 45

- (1) Anyone who intentionally and unrightfully distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Document the content of which infringes decency as intended in Article 27 paragraph (1) shall be subject to a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp1,000,000,000.00 (one billion rupiah).
- (2) Anyone who intentionally and unrightfully distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Document having content of gambling as intended in Article 27 paragraph (2) shall be subject to a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp 1,000,000,000.00 (one billion rupiah).
- (3) Anyone who intentionally and unrightfully distributes and/or transmits and/or makes accessibility of Electronic Information and/or Electronic Document having content of insult and/or defamation as intended in Article 27 paragraph (3) shall be subject to a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp750,000,000.00 (seven hundred fifty million rupiah).

- (4) Anyone who intentionally and unrightfully distributes and/or transmits and/or makes accessibility of Electronic Information and/or Electronic Document having content of extortion and/or threatening as intended in Article 27 paragraph (4) shall be subject to a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp 1,000,000,000.00 (one billion rupiah).
- (5) The provisions as intended in paragraph (3) shall constitute offenses subject to complaint.

Article 45A

- (1) Anyone who intentionally and unrightfully disseminates hoax and misleading news inflicting losses to consumers in Electronic Transactions as intended in Article 28 paragraph (1) shall be subject to a maximum imprisonment of 6 (six) years and/or a maximum fines of Rp1,000,000,000.00 (one billion rupiah).
- (2) Anyone who intentionally and unrightfully disseminates information which is intended to cause hatred or hostility against certain individual and/or group of people based on ethnicity, religion, race and societal group (SARA) as intended in Article 28 paragraph (2) shall be subject to a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp1,000,000,000.00 (one billion rupiah).

Article 45B

Anyone who intentionally and unrightfully transmits Electronic Information and/or Electronic Document containing threats of violence or intimidation which is directed personally as intended in Article 29 shall be subject to a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp750,000,000.00 (seven hundred fifty million rupiah).

Article II

This Law shall come into effect on the date of its promulgation.

For public cognizance, this Law shall be promulgated by placing it in State Gazette of the Republic of Indonesia.

Ratified in Jakarta
on November 25, 2016

THE PRESIDENT OF THE REPUBLIC OF INDONESIA,

signed
JOKO WIDODO

Promulgated in Jakarta
on November 25, 2016

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

signed
YASONNA H. LAOLY

STATE GAZETTE OF THE REPUBLIC OF INDONESIA YEAR 2016 NUMBER 251

Issued as true copy
THE STATE SECRETARIAT MINISTRY OF THE REPUBLIC OF INDONESIA
Assistant Deputy for Economy,
Deputy for Laws and Regulations,

signed and stamped
Lydia Silvanna Djaman

ELUCIDATION ON
LAW OF THE REPUBLIC OF INDONESIA
NUMBER 19 YEAR 2016
REGARDING
AMENDMENT TO LAW NUMBER 11 YEAR 2008 REGARDING INFORMATION AND
ELECTRONIC TRANSACTION

I. GENERAL

Whereas freedom of expression and freedom of speech as well as rights to obtain information by the use and utilization of Information Technology and communication are aimed at improving public welfare, and enhancing the intellectual life of the nation as well as providing sense of security, equality, and legal certainty to users and operators of Electronic Systems.

In the life as a society, nation, and state, the aforementioned rights and freedom for the use and utilization of Information Technology must be performed by taking into account the limitations set out laws for the mere purpose of guaranteeing the recognition as well as honor of the rights and freedom of others and meeting fair demands in accordance with the considerations of morality, religious values, security, and public order in a democratic society.

Law Number 11 Year 2008 regarding Electronic Information and Transaction (ITE Law) is the first law in the field of Information Technology and Electronic Transaction as a highly needed product of legislation and it has become a pioneer by setting out the basis for regulations in the field of the utilization of Information Technology and Electronic Transactions. However, in the actual implementation of the ITE Law, many problems have been encountered.

First, several petitions for judicial review have been filed against this Law to the Constitutional Court resulting in Decisions of the Constitutional Court Number 50/PUU-VI/2008, Number 2/PUU-VII/2009, Number 5/PUU-VIII/2010, and Number 20/PUU-XIV/2016.

Pursuant to Decisions of the Constitutional Court Number 50/PUU-VI/2008 and Number 2/PUU-VII/2009, criminal act of blasphemy and defamation in the field of Electronic Information and Electronic Transaction is not merely a general criminal act, but its is rather an offense based on complaint. Confirmation of it is being an offense based on complaint is intended to make it in line with the principles of legal certainty and sense of equity of the society.

Pursuant to Decision of the Constitutional Court Number 5/PUU-VIII/2010, the Constitutional Court is of opinion that activities and authorities related to interception are very sensitive because on the one hand they pose limitation on human rights, but on the other hand they have aspect of legal interests. Therefore, regulation on the legality of interception must be accurately established and formulated in accordance with the 1945 Constitution of the State of the Republic of Indonesia. Moreover, the Court is of opinion that as interception is an infringement of human rights as confirmed by Article 28J paragraph (2) of the 1945 Constitution of the State of the Republic of Indonesia, it is very appropriate and reasonable that if the state intends to infringe the privacy rights of the citizens, the state must do so in the form of law instead of government regulation.

Furthermore, pursuant to Decision of the Constitutional Court Number 20/PUU-XIV/2016, the Constitutional Court is of opinion that to prevent different interpretation of Article 5 paragraphs (1) and (2) of the ITE Law, the Court confirms that every interception must be performed lawfully, especially in the context of law enforcement. Therefore, the Court in its decision adds word or phrase "especially" to the phrase "Electronic Information and/or Electronic Document". To prevent any interpretation that the court decision will narrow the meaning of Article 5 paragraphs (1) and (2) of the ITE Law, it is necessary to re-confirm it in the Elucidation on Article 5 of the ITE Law in order to provide legal certainty to the existence of Electronic Information and/or Electronic Document as instruments of evidence.

Second, the provisions on search, confiscation, arrest, and detention set out in the ITE Law have caused problems to investigators because criminal acts in the field of Information Technology and Electronic Transaction are so fast and the perpetrators can easily obscure acts or evidences of their crime.

Third, the virtuality characteristic of cyber space enables illegal contents, such as Electronic Information and/or Documents containing infringement of decency, gambling, blasphemy or defamation, extortion and/or intimidation, dissemination of hoax and misleading news inflicting losses to consumers in Electronic Transactions, as well as acts to disseminate hatred or hostility based on ethnicity, religion, race, and societal group, and conveyance of threats of violence or intimidation which are directed personally can be accessed, distributed, transmitted, copied, stored to be re-disseminated from anywhere and at anytime. In the context of protecting the public interests from all types of disturbances caused by misuse of Electronic Information and Electronic Transaction, it is necessary to provide confirmation of the Government role in the prevention of the dissemination of illegal contents by taking measures for the disconnection of access to Electronic Information and/or Electronic Document having unlawful contents that cannot be accessed from Indonesian jurisdiction, as well as it is necessary for investigators to have the authority to ask for information held by Electronic System Operators for purpose of law enforcement on criminal acts in the field of Information Technology and Electronic Transaction.

Fourth, the use of any information by electronic media or Electronic System which is related to a person's personal data must be performed upon the approval of the Person concerned. Therefore, guarantee for the fulfillment of individual protection is required by obliging every Electronic System Operator to delete irrelevant Electronic Information and/or Electronic Document under its control at the request of the Person concerned based on stipulation of court.

Based on the aforementioned considerations, it is necessary to establish a Law regarding Amendment to Law Number 11 Year 2008 regarding Electronic Information and Transaction by re-confirming the provisions on the existence of Electronic Information and/or Electronic Document in Elucidation on Article 5, adding provisions on mandatory deletion of irrelevant Electronic Information and/or Electronic Document in Article 26, amending the provisions of Article 31 paragraph (4) regarding the delegation of the duty for drafting procedures for interception, adding the Government role in the prevention of the dissemination and use of Electronic Information and/or Electronic Document having prohibited contents as intended in Article 40, amending several provisions on investigation of alleged criminal acts in the field of Information Technology and Electronic Transaction in Article 43, and adding elucidation on Article 27 paragraphs (1), (3), and (4) to make them in line with the material criminal law system applicable in Indonesia.

II. ARTICLE BY ARTICLE

Article I

Sub-article 1

Article 1

Self-explanatory.

Sub-article 2

Article 5

Paragraph (1)

Whereas the existence of Electronic Information and/or Electronic Document is binding in nature and is recognized as admissible evidence in order to provide legal certainty with regard to the Administration of Electronic Systems and Electronic Transactions, especially in substantiation and matters relating to legal actions taken by using Electronic Systems.

Paragraph (2)

Especially for Electronic Information and/or Electronic Document in the form of the results of interception or recording constituting part of interception, such action must be taken in the context of law enforcement upon request of the police, public prosecutor's office, and/or other institutions the authorities of which are stipulated based on law.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Sub-paragraph a

Letters which according to the law must be prepared in writing shall include but not limited to commercial papers, valuable letters, and letters which are used in civil,

criminal, and state administrative procedure laws.

Sub-paragraph b
Self-explanatory.

Sub-article 3

Article 26

Paragraph (1)

In the utilization of Information Technology, protection of personal data is an aspect of *privacy rights*. Privacy rights have the following definitions:

- a. Privacy rights are rights to enjoy personal life and free from all kinds of disturbance.
- b. Privacy rights are rights to communicate with Others without act of spying.
- c. Privacy rights are rights to supervise access to a person's information on personal life and data.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Sub-article 4

Article 27

Paragraph (1)

Referred to as "distributes" shall be sending and/or disseminating Electronic Information and/or Electronic Document to a lot of People or various parties by Electronic System.

Referred to as "transmits" shall be sending Electronic Information and/or Electronic Document which is addressed to one other party with an Electronic System.

Referred to as "making accessible" shall be all other actions other than distribution and transmission by Electronic System which make Electronic Information and/or Electronic Document be known by other parties or public.

Paragraph (2)

Self-explanatory.

Paragraph (3)

The provisions in this paragraph refer to the provisions on defamation and/or slander set out in the Indonesian Criminal Code (KUHP).

Paragraph (4)

The provisions in this paragraph refer to the provisions on extortion and/or intimidation set out in the Indonesian Criminal Code (KUHP).

Sub-article 5

Article 31

Paragraph (1)

Referred to as "interception " shall be activities to hear, record, redirect, change, inhibit, and/or record the transmission of non-public Electronic Information and/or Electronic Document, either by using communication cable networks or wireless networks, such as electromagnetic transmission or radio frequency.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Sub-article 6

Article 40

Paragraph (1)

Facilitation for the utilization of Information Technology, includes safe, ethical, smart, creative, productive, and innovative governance of Information Technology and Electronic Transaction. The provisions include the facilitation for the general public, government agencies, and business actors in developing products and services of Information Technology and communication.

Paragraph (2)

Self-explanatory.

Paragraph (2a)

Self-explanatory.

Paragraph (2b)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)
Self-explanatory.

Paragraph (5)
Self-explanatory.

Paragraph (6)
Self-explanatory.

Sub-article 7
Article 43

Paragraph (1)
Referred to as "certain Civil Servant Investigators" shall be Civil Servant Investigators at the ministry who are in charge of government affairs in the field of communication and information technology meeting the requirements based on the provisions of laws and regulations.

Paragraph (2)
Self-explanatory.

Paragraph (3)
Self-explanatory.

Paragraph (4)
Self-explanatory.

Paragraph (5)
Sub-paragraph a
Self-explanatory.

Sub-paragraph b
Self-explanatory.

Sub-paragraph c
Self-explanatory.

Sub-paragraph d
Self-explanatory.

Sub-paragraph e
Self-explanatory.

Sub-paragraph f
Self-explanatory.

Sub-paragraph g
Self-explanatory.

Sub-paragraph h
Self-explanatory.

Sub-paragraph i

Self-explanatory.

Sub-paragraph j

Referred to as "expert" shall be someone having special skills in the field of Information Technology whose knowledge can be accounted for academically or practically.

Sub-paragraph k

Self-explanatory.

Paragraph (6)

Self-explanatory.

Paragraph (7)

Self-explanatory.

Paragraph (7a)

Self-explanatory.

Paragraph (8)

Self-explanatory.

Sub-article 8

Article 45

Self-explanatory.

Article 45A

Self-explanatory.

Article 45B

The provisions in this Article shall also cover *cyber bullying* which contains the elements of threats of violence or intimidation and which causes physical, psychological violence, and/or material losses.

SUPPLEMENT TO STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER
5952

NOTE

Source: LOOSE LEAF STATE SECRETARIAT YEAR 2016