BILL OF THE REPUBLIC OF INDONESIA
NUMBER ... OF ...
CONCERNING
THE SECOND AMENDMENT TO LAW NUMBER 11 OF 2008
CONCERNING ELECTRONIC INFORMATION AND TRANSACTIONS

BY THE GRACE OF GOD ALMIGHTY

PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering

a. Whereas in order to maintain Indonesia's digital space which is clean, healthy, ethical, productive and fair, it is necessary to regulate the use of Information Technology and Electronic Transactions which provides a legal certainty, justice, and protects the public interests from all kinds of disturbances as a result of misuse of an Electronic Information, Electronic Documents, Information Technology, and/or Electronic Transactions that disrupt public order;
b. Whereas several provisions in Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 0f 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, in its implementation, it still give rise to multiple interpretations and controversy in society and therefore changes need to be made to create a sense of social justice and legal certainty;
c. Whereas based on the considerations as intended in letter a and b, it is necessary to establish a Law concerning the Second Amendment to Law Number 11 of 2018 concerning Information and Electronic Transactions;

In the view of

1. Article 5 Paragraph (1), Article 20, Article 28D Paragraph (1), Article 28E, Article 28F, Article 28G Paragraph (1), Article 28I, and Article 28J of the Constitution of 1945 of the Republic of Indonesia;
2. Law Number 11 of 2008 concerning Electronic Transactions Information (State Gazette of the Republic of 2008 Number 58, Supplement to State Gazette of the Republic of Indonesia Number 4843) as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008

concerning Information and Electronic Transactions (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952).

With The Approval Of:
THE HOUSE OF REPRESENTATIVES OF THE REPUBLIC OF INDONESIA
And
THE PRESIDENT OF THE REPUBLIC OF INDONESIA

DECIDES:

To Enact : LAW CONCERNING THE SECOND AMENDMENT TO LAW NUMBER 11 OF 2008 CONCERNING INFORMATION AND ELECTRONIC TRANSACTIONS.

Article 1

Several provisions in Law Number 11 of 2008 concerning Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843) as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952) is amended as follows.

1. The provisions on Paragraph (4) of Article 2 as well as the explanation on Paragraph (1) and Paragraph (4) of Article 5 are amended therefore Article 5 reads as follows:

Article 5

(1) Electronic Information and/or Electronic Documents and/or printouts are a valid legal evidences.
(2) Electronic Information and/or Electronic Documents and/or printouts as intended in Paragraph (1) are an extension of legal evidence in accordance with the Procedural Laws in force in Indonesia.
(3) Electronic Information and/or Electronic Documents are declared valid if the Electronic System used is in accordance with the provisions regulated in this Law.

(4) Provisions regarding Electronic Information and/or Electronic Documents as intended in Paragraph (1) does not apply if regulated by the Law otherwise.

2. The provisions of Paragraph (3), Paragraph (4), Paragraph (5), and Paragraph (6) of Article 13 as well as the explanation of Paragraph (5) of Article 13 are amended therefore Article 13 reads as follows:

Article 13

(1) Every person has the right to use the services of an Electronic Certification Provider to create an Electronic Signature.
(2) Electronic Certificate Operators must ensure that an Electronic Signature is linked to its owner.
(3) Electronic Certification Providers operating in Indonesia must be Indonesian legal entities and domiciled in Indonesia.
(4) The provisions as intended in Paragraph (3) are excluded if the provision of services which use an Electronic Certification is not yet available in Indonesia.
(5) The provisions as intended in Paragraph (3) are excluded if the provision of services using Electronic Certification is not yet available in Indonesia.
(6) Further provisions regarding Electronic Certification Providers as referred to in Paragraph (3), Paragraph (4), and Paragraph (5) are regulated in the Government Regulations.

3. Between Article 13 and Article 14, 1 (one) article is inserted, namely Article 13A therefore it is read as follows:

Article 13A

(1) Implementation of an Electronic Certification can provide services in the form of:
    a. Electronic Signature;
    b. Electronic seal;
    c. Electronic time stamp;
    d. Electronic time stamp;
    e. Website authentication;
    f. Preservation of electronic signatures and/or electronic seals;
    g. Digital identity; and/or
    h. Other services that use Electronic Certification.
(2) Further provisions regarding the implementation of services as intended in Paragraph (1) are regulated in Government Regulations.

4. The explanation of Paragraph (1) and Paragraph (2) of Article 15 is amended as stated in the explanation.
5. Between Article 16 and Article 17, 2 (two) articles are inserted, namely Article 16A and Article 16B therefore they are read as follows:

Article 16A

(1) Electronic System Operators are obliged to provide protection for children who use or access the Electronic System.
(2) The protection as intended in Paragraph (1) includes the protection of children's rights as intended in the laws and regulations regarding the use of products, services and features developed and operated by Electronic System Operators.
(3) In providing products, services and features for children, Electronic System Operators are required to implement a technology and an operational technical measures to provide protection as intended in Paragraph (1) from the development stage to the Electronic System implementation stage.
(4) In providing protection as intended in Paragraph (1), Electronic System Operators are required to provide:
    a. Information regarding the minimum age limit for children who can use the product or service;
    b. Child user verification mechanism; and
    c. Mechanisms for reporting abuse of products, services and features that violate or have the potential to violate children's rights.
(5) Further provisions regarding the protection as intended in Paragraph (1) to Paragraph (4) are regulated in the Government Regulations.

Article 16B

(1) Violations of the provisions as intended in Article 16A are subject to administrative sanctions.
(2) Administrative sanctions as intended in paragraph (1) can be in the form of:
    a. Written warning
    b. Administrative fines;
    c. Temporary suspension; and/or
    d. Termination of access.
(3) Further provisions regarding the imposition of administrative sanctions as intended in Paragraph (1) and Paragraph (2) are regulated in the Government Regulations.

6. The provisions of Paragraph (1) of Article 17 are amended, and between Paragraph (2) and Paragraph (3) of Article 17, 1 (one) paragraph is

inserted, namely Paragraph (2a), and the provisions of Paragraph (3) of Article 17 are amended therefore Article 17 reads as following:

Article 17

(1) Electronic Transactions can be carried out in the public or private sphere.

(2) The parties carrying out Electronic Transactions as intended in paragraph (1) are required to act in good faith in interacting and/or exchanging Electronic Information and/or Electronic Documents during the transaction.

(2a) Electronic Transactions that have a high risk for the parties using electronic signatures are secured by Electronic Certificates.

(3) Further provisions regarding the implementation of Electronic Transactions as referred to in Paragraph (1), Paragraph (2), and Paragraph (2a) are regulated in the Government Regulations.

7. Between Article 18 and Article 19, 1 (one) Article is inserted, namely Article 18 A therefore it reads as follows:

Article 18A

(1) International Electronic Contracts that uses standard clauses made by Electronic System Operators are regulated by Indonesian law in the terms of:

a. The Users of Electronic System Operator services as one of the parties to Electronic Transactions originates from Indonesia and provide their consent from or within the jurisdiction of Indonesia;
b. The place of contract's implementation is in the territory of Indonesia; and/or
c. Electronic System Operators have a place of business or conduct business activities in the territory of Indonesia.

(2) Electronic Contracts as intended in Paragraph (1) uses a simple, clear and easy way to understand a language, and uphold the principles of good faith and transparency.

8. The provisions of Article 27 are amended therefore it is read as follows

Article 27

(1) Every person who intentionally and without any rights broadcasts, displays, distributes, transmits and/or makes Electronic Information and/or Electronic Documents accessible that have any content which violates the decency for public knowledge.

(2) Every person who intentionally and without any rights distributes, transmits and/or makes Electronic Information and/or Electronic Documents accessible which contains gambling content.

9. Between Article 27 and Article 28, 2 (two) articles are inserted, namely Article 27A and Article 27B therefore they are read as follows:

Article 27A

Every person who intentionally attacks the honor or the good name of another person by accusing someone of something with the intention of making the matter known to the public in the form of Electronic Information and/or Electronic Documents carried out through an Electronic System.

Article 27B

(1) Every person who intentionally and without any right distributes and/or transmits Electronic Information and/or Electronic Documents, with the intention of unlawfully benefiting himself or another person, forcing someone with threats of violence to:
    a. Giving an item, which partly or wholly belongs to that person or to another person; or
    b. Giving debt, making an acknowledgment of debt, or writing off receivables.
(2) Every person who intentionally and without any right distributes and/or transmits Electronic Information and/or Electronic Documents, with the intention of benefiting himself or another person unlawfully, with the threat of contamination or with the threat of disclosing secrets, forcing someone to:
    a. Giving an item that is partly or wholly owned by that person or someone else; or
    b. Giving debt, making an acknowledgment of debt, or writing off receivables.

10. The provisions of Article 28 are amended to read as follows:

Article 28

(1) Any Person who intentionally distributes and/or transmits Electronic Information and/or Electronic Documents containing false notices or misleading information which results in material losses for consumers in Electronic Transactions.
(2) Any Person who intentionally and without any right distributes and/or transmits Electronic Information and/or Electronic Documents that are inciting, inviting, or influencing other people to give rise to the feelings

of hatred or hostility towards certain individuals and/or community groups based on race, nationality, ethnicity, color. skin, religion, belief, gender, mental disability, or physical disability.

(3) Every person deliberately distributes Electronic Information and/or Electronic Documents which of the person are aware that it contain false notifications that cause unrest in the society.

11. The provisions of Article 29 are amended to read as follows:

Article 29

Any Person intentionally and without authorization sends Electronic Information and/or Electronic Documents directly to a victim that contains threats of a violence and/or an intimidation.

12. The provisions of Article 36 are amended to read as follows:

Article 36

Every person intentionally and without right commits an act as intended in Article 30 to Article 34 which results in material loss to another person.

13. Between Paragraph (2b) and Paragraph (3) of Article 40, 2 (two) paragraphs are inserted, namely Paragraph (2c) and Paragraph 2d), the provisions of Paragraph (5) of Article 40 were amended, and the explanation of Paragraph (2b) of Article 40 was amended therefore Article 40 are read as follows:

Article 40

(1) The Government facilitates the use of Information Technology and Electronic Transactions in accordance with the provisions of laws and regulations.

(2) The Government protects the public interest from all types of disturbances as a result of misuse of an Electronic Information and Electronic Transactions which disrupt the public order, in accordance with statutory provisions.

(2a) The government is obliged to prevent the dissemination and use of an Electronic Information and/or Electronic Documents which contains a prohibited content in accordance with the provisions of statutory regulations.

(2b) In carrying out prevention as intended in Paragraph (2a), the Government has the authority to terminate access and/or order Electronic System Operators to terminate access to Electronic Information and/or Electronic Documents that contain unlawful content.

(2c) Orders to Electronic System Operators as intended in Paragraph (2b) in the form of terminating access and/or independent content moderation of Electronic Information and/or Electronic Documents which contains pornography, gambling or any other content as intended in the provisions of statutory regulations as long as technologically possible.

(2d) In carrying out prevention as intended in Paragraph (2a), the Government has the authority to order Electronic System Operators to moderate the content of Electronic Information and/or Electronic Documents which have any content that is dangerous for the safety of life or health of individuals or the public.

(3) The government determines agencies or institutions that have strategic electronic data that must be protected.

(4) The agency or institution as intended in Paragraph (3) must create Electronic Documents and electronic backup records and connect them to a certain data center for data security purposes.

(5) Agencies or institutions other than those regulated in Paragraph (3) creates Electronic Documents and electronic backup records in accordance with their data protection requirements.

(6) Further provisions regarding the role of the Government as intended in Paragraph (1), Paragraph (2), Paragraph (2a), Paragraph (2b), Paragraph (2c), Paragraph (2d), and Paragraph (3) are regulated in Government Regulations.

14. Between Article 40 and Article 41, 1 (one) article is inserted, namely Article 40A therefore it reads as follows:

Article 40A

(1) The government is responsible for encouraging the creation of a digital ecosystem that is fair, accountable, safe and innovative.

(2) In order to carry out the responsibilities as intended in Paragraph (1), the Government has the authority to order Electronic System Operators to make adjustments to the Electronic System and/or take certain actions.

(3) Electronic System Operators are obliged to carry out orders as intended in Paragraph (2).

(4) In the event that the Electronic System Operator violates the obligations as intended in Paragraph (3), the Electronic System Operator will be subject to administrative sanctions.

(5) Administrative sanctions as intended in Paragraph (4) can be in the form of:

a. Written warning;

b. Administrative fines;

c. Temporary suspension; and/or
d. Termination of access.

(6) Further provisions regarding responsibility as intended in Paragraph (1), Government authority as intended in Paragraph (2); Electronic System Operator obligations as intended in Paragraph (3). And the imposition of administrative sanctions as intended in Paragraph (4) and Paragraph (5) is regulated in Government Regulations.

15. The provisions of Paragraph (2) and Paragraph (8) of Article 43 are amended, the provisions of Paragraph (5) of Article 43 are added by 1 (one) letter, namely letter I, and the explanation of Paragraph (5) letter j of Article 43 is amended therefore Article 43 are read as follows:

Article 43

(1) Apart from the Investigators from the State Police of the Republic of Indonesia, certain Civil Servant Officials within the Government whose scope of duties and responsibilities are in the field of Information Technology and Electronic Transactions, are given special authority as investigators as intended in the Law on Criminal Procedure Law to carry out investigations of criminal acts in in the field of Information Technology and Electronic Transactions.
(2) Investigations in the field of Information Technology and Electronic Transactions as referred to in Paragraph (1) are carried out by paying attention to the protection of privacy, confidentiality, the smooth running of public services, and the integrity of data in accordance with the provisions of statutory regulations.
(3) Search and/or confiscation of Electronic Systems related to alleged criminal acts in the fields of Technology and Information and Electronic Transactions is carried out in accordance with the provisions of the criminal procedural law.
(4) In carrying out searches and/or confiscations as intended in Paragraph (3), investigators are obliged to safeguard the interests of public services.
(5) Civil Servant Investigators as intended in Paragraph (1) have the authority to:
    a. Receive reports or complaints from someone regarding criminal acts in the field of Information Technology and Electronic Transactions;
    b. Summon every person or other party to be heard and examined as a suspect or witness in connection with an alleged criminal act in the field of Information Technology and Electronic Transactions;

c. Carrying out checks on the veracity of reports or information relating to criminal acts in the field of Information Technology and Electronic Transactions;
d. Carrying out examinations of Persons and/or Business Entities who are reasonably suspected of committing criminal acts in the field of Information Technology and Electronic Transactions;
e. Carrying out inspections of tools and/or facilities related to Information Technology activities that are suspected of being used to commit criminal acts in the field of Information Technology and Electronic Transactions;
f. Conduct searches of certain places suspected of being used as places to commit criminal acts in the field of Information Technology and Electronic Transactions;
g. Sealing and confiscating tools and/or means of Information Technology activities that are suspected of being used in deviation from the provisions of laws and regulations;
h. Make data and/or Electronic Systems related to criminal acts in the field of Information Technology and Electronic Transactions so that they cannot be accessed;
i. Requests information contained in the Electronic System or information produced by the Electronic System from the Electronic System Operator which is related to criminal acts in the field of Information Technology and Electronic Transactions.
j. Requests expert assistance as needed in investigating criminal acts in the field of Information Technology and Electronic Transactions
k. To terminate investigations into criminal acts in the field of Information Technology and Electronic Transactions in accordance with the provisions of the criminal procedural law; and/or
l. Order Electronic System Operators to temporarily terminate access to social media accounts, bank accounts, electronic money and/or digital assets.

(6) Arrest and detention of the perpetrators of criminal acts in the field of Information Technology and Electronic Transactions are carried out in accordance with the provisions of the criminal procedural law.

(7) Civil State Official Investigators as referred to in Paragraph (1) in carrying out their duties to notify the Public Prosecutor of the commencement on the investigation through the State Police Investigator of the Republic of Indonesia.

(7a) In the event that the investigation has been completed, the Civil Servant Official Investigator as referred to in Paragraph (1) shall

submit the results of their investigation to the Public Prosecutor through the State Police Investigator of the Republic of Indonesia.

(8) In order to uncover the criminal acts of an Electronic Information and Electronic Transactions, investigators can collaborate with investigators from other countries to share information and evidence in accordance with statutory provisions.

16. The provisions of Article 45 are amended to read as follows:

Article 45

(1) Every person who deliberately and without any rights that broadcasts, displays, distributes, transmits, and/or makes an Electronic Information and/or Electronic Documents accessible, which contains a content that violates the decency for a public knowledge as intended in Article 27 Paragraph (1) shall be punished with a criminal offense, imprisonment for a maximum of 6 (six) years and/or a fine of a maximum of IDR 1,000,000,000.00 (one billion rupiah):

(2) The actions as intended in Paragraph (1) will not be criminalized in the event that:
   a. It is carried out in the public interest;
   b. It is done for self-defense; or
   c. The Electronic Information and/or Electronic Documents are works of art, culture, sports, health and/or science.

(3) Every person who intentionally and without authorization distributes, transmits and/or makes accessible an Electronic Information and/or Electronic Documents containing a gambling content as intended in Article 27 Paragraph (2) shall be punished with a maximum imprisonment of 10 (ten) years and/or a maximum fine of IDR 10,000,000,000.00 (ten billion rupiah).

(4) Every person who deliberately attacks the honor or good name of another person by accusing them of something, with the intention of making the matter known to the public in the form of Electronic Information and/or Electronic Documents carried out through the Electronic System as intended in Article 27A, shall be punished with a criminal offense. imprisonment for a maximum of 2 (two) years and/or a fine of a maximum of IDR 400,000,000.00 (four hundred million rupiah).

(5) The provisions as intended in Paragraph (4) constitutes a complaint crime which can only be prosecuted based on a complaint by the victim or person affected by the crime and not by a legal entity.

(6) In the event that the act as referred to in Paragraph (4) could not be proven and is contrary to what is known even though the opportunity has been given to prove it, the person shall be punished for slander with

a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp. 750.000.000.00 (seven hundred and fifty million rupiah).

(7) Actions as intended in Paragraph (4) are not criminalized in the event that:
   a. It is carried out in the public interest; or
   b. It is done because they were forced to defend themselves.

(8) Any person who deliberately and without authority distributes and/or transmits Electronic Information and/or Electronic Documents, with the intention of unlawfully benefiting himself or another person, forcing the person with the threat of violence to:
   a. give an item, which is partly or wholly owned by that person or someone else; or
   b. give a debt, making a confession of a debt, or writing off a receivable, as intended in Article 27B Paragraph (1) is punishable by imprisonment for a maximum of 6 (six) years and/or a fine of a maximum of IDR 1,000,000,000.00 (one billion rupiah).

(9) In the event that the act as intended in Paragraph (8) is committed within the family environment, criminal prosecution can only be carried out based on a complaint.

(10) Any person who intentionally and without authorization distributes and/or transmits Electronic Information and/or Documents Electronically, with the intention of unlawfully benefiting oneself or another person, with the threat of contamination or with the threat of disclosing secrets, forcing people to:
   a. give an item which partly or wholly belongs to that person or to another person; or
   b. give a debt, making a confession of a debt, or writing off a receivable as intended in Article 27B Paragraph (2) shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah).

(11) Criminal acts as intended in Paragraph (10) can only be prosecuted based on the complaints from the victims of criminal acts.

17. The provisions of Article 45A are amended to read as follows:

Article 45A

(1) Every person who deliberately distributes and/or transmits Electronic Information and/or Electronic Documents containing false notifications or misleading information which results in material losses for consumers in Electronic Transactions as intended in Article 28 Paragraph (1) shall be punished by a maximum imprisonment of 6 (six)

years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah).

(2) Any person who intentionally and without any rights distributes and/or transmits Electronic Information and/or Electronic Documents that are inciting, inviting, or influencing other people in order to create a feelings of hatred or enmity towards certain individuals and/or community groups based on race, nationality, ethnicity, skin color, religion, creed, gender, mental disability, or physical disability as intended in Article 28 Paragraph (2) shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah).

(3) Every person who deliberately distributes an Electronic Information and/or Electronic Documents which they knows contains a false notifications which cause an unrest in society as intended in Article 28 Paragraph (3) shall be punished with imprisonment for a maximum of 6 (six) years and/or a fine. a maximum of IDR 1,000,000,000.00 (one billion rupiah).

18. The provisions of Article 45B are amended to read as follows:

Article 45B

Any person who intentionally and without authorization sends an Electronic Information and/or Electronic Documents directly to a victim containing threats of violence and/or intimidation as intended in Article 29 shall be punished by imprisonment for a maximum of 4 (four) years and/or a fine. a maximum of IDR 750,000,000.00 (seven hundred and fifty million rupiah).

Article II

1. When this Law comes into force, the provisions in Article 27 Paragraph (1), Article 27A, Article 28 Paragraph (2), Article 28 Paragraph (3), Article 36, Article 45 paragraph (1), Article 45 Paragraph (2), Article 45 Paragraph (4), Article 45 Paragraph (5), Article 45 Paragraph (6), Article 45 Paragraph (7), Article 45A Paragraph (2), and Article 45A Paragraph (3) are valid until the enactment Law Number 1 of 2023 concerning the Criminal Code (State Gazette of the Republic of Indonesia of 2023 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 6842).
2. This Law comes into force on the date of promulgation.

In order for everyone to be aware, this Law is ordered to be promulgated by placing it in the State Gazette of the Republic of Indonesia.

Enacted in Jakarta

On

PRESIDENT OF THE REPUBLIC OF INDONESIA,

JOKO WIDODO

Promulgated in Jakarta
On

MINISTER SECRETARY OF STATE
REPUBLIC OF INDONESIA,

PRATIKNO

STATE GAZETTE OF THE REPUBLIC OF INDONESIA YEAR... NUMBER...