

(Draft 5 dated 23-1-2005)

(Documents used for 8th section meeting of the Committee of Science, Technology and Environment)

LAW ON E-TRANSACTIONS

Pursuant to the Constitutions of the Socialist Republic of Vietnam of 1992 as amended by Resolution 51/2001/QH10 of 25/11/2001 of the 10th Legislature, Session No. 10;

This Law provides for e-transactions.

CHAPTER I

GENERAL PROVISION

Article 1- Governing Scope

I. Option 1 of Article 1

1. This Law governs data message; e-signatures; e-certification; e-contracting; e-transactions in Government agencies; confidentiality security and safety in e-transactions; protection of IPR in e-transactions, in respect of trans

8.

3. To develop and issue e-transaction standards.
4. To manage e-certification service providers.
5. To develop communication and information technologies *for* e-transactions.
6. To manage and implement international co-operations on e-transactions.
7. To inspect, check, supervise the implementation of the laws on e-transactions; to deal with breaches of the laws on e-transactions.

Article 9. State responsibilities on e-transactions

1. The Government shall uniformly [perform] the State management on e-transactions activities.
2. The Ministry of Post and Telecom shall be responsible before the Government on implementation of State management on e-transaction activities.
3. The Ministry of Science and Technology, Ministry of Finance, State Bank of Vietnam, Ministry of Police, Ministry of Culture-Information, [other] ministries, ministerial-level bodies within their functions, powers shall co-ordinate with the Ministry of Post and Telecom to implement State management on e-transaction activities.
4. People's Committees within their functions, powers shall implement State management on e-transaction activities in accordance with the de-centralization of the Government.

Article 10. Prohibited activities

1. Unauthorized access to computing resources.
2. Access to computers for the purpose of supporting and preparing illegal activities.
3. Distribution of illegal and false information.
4. Distribution of information that is inconsistent with the good traditional culture, ethics of Vietnamese.
5. Dissemination of information that affects sovereignty, independence and territorial

Chapter II
DATA MESSAGE

Section 1

Validity of Data Message

Article 11. Validity of Data Message

Data message is in accordance with provisions of this Law shall be valid.

Article 12. The Same Validity as Written Document

Where the law requires information to be in writing, a data message shall be the same validity as a written document if the information contained therein is accessible so as to be usable for subsequent reference.

Article 13. Validity of Original Copy

1. Where the law requires information to be presented or retained in its original form, a data message shall be considered as an original copy if:

- a) There is assurance as to the integrity of the information since its first origination;
- b) The contents of the data message are accessible and can be usable in its entirety for reference when necessary.

2. A data message is considered complete and intact when its contents have remain unchanged except changes in its appearance that arise in the normal course of communication, storage and display.

3. Provisions in items 1 and 2 of this Article shall apply in case the law requires that a copy or a notarized copies to be presented or retained.

Article 14. Admissibility as Evidence

1. A data message can be used to be evidence in accordance with this Law and regulations on education.

2. The admissibility of a data message shall be determined based on the reliability of the manner in which the data message was generated, stored or communicated; the reliability of the manner in which the integrity of the information was maintained; the manner in which its originator was identified, and to any other relevant factors.

Article 15. Retention

1. Where the law requires that certain information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

- a) The information in the data message is accessible as and when needed;

b) The data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information of the data message;

c) Such information is retained in a way to enable the identification of the origin and destination of a data message and the date and time when it was sent or received.

2. Clause 1 shall not apply to data that is merely used for sending or receiving another data message.

Section 2

Dispatch and Receipt of Data Messages

Article 16. Dispatch of Data Messages

2. The recipient is entitled to consider each data message as independent and act on it in accordance with this article unless the data are a copy of another data message.

3. Upon receipt of the data message, the recipient has to inform the sender in accordance with the method agreed by the parties according to the following order: .

a) The recipient shall inform, acknowledge the dispatch of the data message to indicate this to the sender.

b) Where the sender has stated before or during the dispatch of data that the data is conditional on receipt of the acknowledgement, the data is treated as though it has never been sent, until the acknowledgement is received by the sender through the report of the recipient acknowledging that [the recipient] has received such data message.

c) In case the sender has not stated of acknowledgement and the acknowledgement has not been received within the time specified or agreed, the sender may give notice to the recipient stating that no acknot

Article 21. Secured Data Messages

1. Secured data messages are the ones that meet the following conditions:
 - a) The contents and format of data messages shall not be changed during transmission, reception or storage since a specific time;
 - b) It is possible to identify the sender of the message.
2. If a data message is verified to meet the conditions specified in Clause 1 of this Article, it is considered a secured message.
3. The parties may agree on procedures for verifying that a data message is secured. If the parties do not have any agreement on procedures for verification, then a reasonable verification method could be used. The reasonableness of procedures for verification is determined based on:

d) Any alteration made to that information after the time of signing is detectable.

2. The Government shall provide for detailed regulations on secured e-signatures.

Article 24. Responsibility of the Signatory

1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall have the following responsibilities:

(a) Have means to avoid unauthorized use of its signature creation data;

(b) Without undue delay, notify any person who rely on the e-signature and Certification Service Providers when the signatory discovers that the signature creation data may not be under the signatory's control;

(c) Where a e-certificate is used, must apply necessary methods to ensure the accuracy and integrity of information included in the e-certificate.

2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of set forth in Clause 1 of this Article.

Article 25: Responsibilities of the Party relying on e-signatures

A party relying on e-signatures shall have the responsibilities:

1. To take necessary steps to verify the reliability of an electronic signature;

1. E- certification service providers shall have the following rights and obligations:
 - a) Carry out the tasks specified in Article 27 of this Law;
 - b) Comply with legislation on the establishment, organization and operations of this type of services;
 - c) Use reliable equipment, procedures and resources in conducting their business;
 - d) Assurance of the accuracy and integrity of basic data in the e-certificates issued by themselves;
 - dd) Publishing information related to e-certificates issued, renewed, suspended, restored or revoked;
 - e) Providing appropriate facilities to enable those who rely on an e-signature and competent

Article 31: State management of E-certification Services

1. Promulgation legal documents on e-certification services;
2. Promulgation regulations on e-certification services; monitoring, inspection of implementation of such regulations;
3. Promulgation and monitoring the compliance of technical standards of e-signatures, e-certificates and e-certification activities;
4. Issuance, renewal, suspension, restoration and revocation of licenses for e-certification activities of e-certification service providers in Vietnam.

a.) Formats, forms of data messages;

b) In case e-transactions require e-signatures, descriptions of types of e-signatures and e-certification;

c) Procedures to ensure the integrity, security and confidentiality of e-transactions;

2. A State agency can provide public services in electronic forms based on regulations of such agency. Such regulations shall not be contrary to provisions of the current laws and this Law.

Article 36. Security, confidentiality and storage of electronic information in State agencies

1. State agencies shall ensure confidentiality, security and storage of information in conducting e-transactions in accordance with the provisions of this Law and related legislation.

2. Organizations and individuals conducting e-transactions must take necessary measures to ensure smooth operations of the information system under their control used in e-transactions. If technical errors of the information systems cause damage to other organizations and individuals, [the organizations and individuals] shall have to pay compensation in accordance with laws.

d. Presentation of or providing information related to the user of the services when the organizations and individuals being requested are computing service providers controlling this information.

dd. Other responsibilities provided by law.

2. Competent bodies and persons shall be responsible before the laws for their requests.

Article 45. Authority of State agencies

The recipient of a data message shall be all legal responsibilities for any consequence of its action of receiving the data message that gives rise to IP relations, including copying of work whose copyright is protected by printing from the computer network data messages containing this work.

Article 49 – Responsibilities of the Intermediary

1. Unless otherwise agreed by the originator and the intermediary, the intermediary when sending, receiving and storing a data message or providing a service related to the data message shall take reasonable and necessary measures to ensure the contents of the data message which has trade secret are not accessible by nor easily disclosed to people other than the recipient designated in the data message.

2. If the failure of the intermediary to comply or fully fulfill the provisions of Clause 1 of this Article leads to the disclosure of a trade secret, this shall be deemed as the action of disclosing a trade secret.

3. The intermediary shall not bear any legal responsibility for materials of a third party in the form of electronic record to which it only provides access to the materials, provided that the responsibility arises from the intermediary's actions:

2a) Creations of data messages containing trade secrets which are not accessible by nor easily disclosed to people other than the recipient designated in the data message.

Article 51. Responsibility of Network Service Providers in Respect of IP

1. Network service providers shall be responsible for taking necessary confidential protection measures to ensure trade secrets of the network users who want to keep confidential when uploading [these] on the network which shall not be accessible by or easily disclosed to others.

2. Network service providers shall not bear any legal responsibility for any material of a third party in the form of electronic records which they only provide access to the data, if the responsibility arises from:

a) Creation, publication and dissemination of materials;

b) Infringement of any right of the materials or related materials.

3. The provisions of Clauses 1 and 2 of this Article shall not affect:

a) any obligation of a network service provider arising out of a contract or law;

b) Any obligations of a network service provider as provided by law or valid verdicts and decision of the courts in respect of deletion, prevention or refusal of access to the materials.

CHAPTER VIII INSPECTION, DISPUTE SETTLEMENT AND HANDLING BREACHES

Article 52. Inspection of E-transactions

1. Inspection of e-transactions shall have the responsibilities for inspecting the implementation of e-transactions regulations; discovering, preventing and handling within its authorities ; ; recommending measures to enforce the regulations one-transactions.

2. Organization, duties and authority of e-transaction inspectors shall follow the provision of the regulations on Inspection.

3. The Government shall provide for organization, duties, authority and delegation of inspection in e-transactions in each area to officials of branches, localities.

Article 53. Handling of Deputes in E-transactions

Disputes in e-transactions shall be handled in accordance with law.

Article 54. Principles of handling IP disputes in e-transactions

1. The right to request, authority, order, procedures of handling breaches, disputes on IP stipulated in this Law shall be implemented in accordance with the laws on handling breaches, resolving disputes on IP.

2. Regarding breaches stipulated in provisions of Articles 55. 56 and 57 of this Law, the disputes on domain names shall be proceeded as following:

a) Regarding high-level domain names [being] national codes of Vietnam, disputes on domain names shall be handled in accordance with Vietnamese regulations on resolving disputes on domain names;

b) Regarding common high-level domain names, disputes on domain names shall be handled in accordance with regulations on resolving disputes on domain names of The Organization

Article 55. Responsibility for Violation of Laws in E-transactions

1. Organizations, individuals that violate laws in e-transactions, depending on the nature and seriousness of the violation, shall be subject to discipline, administrative fines and criminal

Article 59. Effectiveness

This Law shall take effect on,2006.

Article 60. Implementing Regulations

The Government shall provide for detail regulations and implementation guidelines of this Law.

This Law is passed by XI National Assembly, section no. ... dated....

Chairman of the National Assembly

Nguyen Van An