THE NATIONAL ASSEMBLY **THE SOCIALIST REPUBLIC OF VIETNAM**
Law No. 51/2005/QH11 **Independence – Freedom - Happiness**

THE NATIONAL ASSEMBLY OF THE SOCIALIST REPUBLIC OF VIETNAM

LEGISLATURE XI, SESSION 8

LAW ON E-TRANSACTIONS

Pursuant to the Constitutions of the Socialist Republic of Vietnam of 1992 as amended by Resolution 51/2001/QH10 of 25/12/2001 of the 10th Legislature, Session No. 10;

This Law provides for e-transactions.

Chapter I

GENERAL PROVISION

Article 1- Governing Scope

This Law provides provisions on e-transactions in operations of State bodies; and in the civil, business and other sectors as provided by the laws.

The provisions of this Law shall not apply to grants of certificates of land use rights, house ownership rights and other immovable properties, writings related to inheritance, marriage certification, divorce decision, birth declaration, death declaration, land and other immovable assets; bills of exchange and other valuable papers

Article 2. Scope of Application

This Law shall apply bodies, organizations, individuals selecting to transact through e-means

Article 3. Application of the Law on E-transactions

In case there is a difference between the provisions of the Law on E-transactions and provisions of other laws concerning one and the same matter on e-transactions, the Law on E-transactions shall apply.

Article 4. Definition

In this Law, the following terms are defined as follows:

1. *An e-certificate* is a data message issued by an e-signature certification service organization in order to verify certified organizations, individuals being the persons who sign e-signatures.

2. *Certification of e-signature* is certification of certified individuals, organizations being the persons who sign e-signatures.

3. *Electronic signing program* is a computer program established to independently operate or through equipment, information system, other computer programs in order to create an identical e-signature for the person who signs data messages.

4. *Database* is a set of data being ordered, established to access, exploit, manage and update through electronic means.

5. *Data* is the information in the form of symbol, writing, number, image, sound or other similar formats.

6. An e- transaction is a transaction that is carried out by electronic means.

7. An automatic e-transaction is an e-transaction that is automatically implemented in part or in whole through information system which has already been established.

8. Information system is a system created for sending, receiving, saving, displaying or implementing other processing with respect to data messages.

9. *An intermediary* is a body, an organization or individual representing other bodies, organizations and individuals to send and receive or store a data message or provide other services relating to such data message.

10. *An electronic means* a means that operates based on electric, electronic, digital, magnetic, wireless, optical, electro-magnetic technologies or similar technologies.

11. A s*ecured examination process* is a process which is used to check sources of data messages, e-signatures; to discover changes or mistakes appearing in the content of a data message during the process of transmission, receipt and storage.

12. *A data message* is information created, transferred, received and stored by electronic means.

13. *An e- signature certification service providing organization* is an organization carrying out e-signature certification activities in accordance with the provisions of the law.

14. *A network service providing organization* is an organization providing infrastructure for transmission lines and other relevant services to carry out e-transactions. Network service providing organizations include organizations providing Internet services and organizations providing network access services.

15. *Electronic data interchange (EDI – electronic data interchange)* is a transfer of information from one computer to another computer by electronic means in accordance with agreed standards on information structure.

Article 5. General Principles in E-Transactions

1. To voluntarily select to use electronic means to carry out transactions.

2. To self agree on selection of type of technology to carry out e-transactions.

3. No technology shall be considered as a sole [technology] in e-transactions

4. To ensure equality and security in e-transactions.

5. To protect lawful rights and interests of organizations, agencies, individuals, interests of the State, public interests.

6. E-transactions of the State bodies shall comply with principles stipulated in Article 40 of this Law.

Article 6. Policies on Development and Application of E-transactions

1. To give priority to develop technology infrastructure and train human resources related to e-transactions.

2. To encourage agencies, organizations, individuals to invest and apply e-transactions in accordance with provisions of this Law.

3. To support with respects to e-transactions in public services.

4. To foster implementation of e-commerce, e-government and computerization of the State bodies' operation.

Article 7. State Management on e-transactions

1. To issue and organize the implementation of strategies, plans and policies for developing and applying e-transactions in social-economic sectors, national defence, security.

2. To promulgate and implement legal documents on e-transactions.

3. To issue and recognize e-transaction standards.

4. To manage service providing organizations related to e-transactions.

5. To manage the development of technological infrastructure for e-transaction activities.

6. To train, manage training activities to develop and build teams of staff and experts in e-transaction sector.

7. To inspect, and supervise the implementation of the laws on e-transactions; to solve complaints and denunciations, to handle acts of breach the laws on e-transactions.

8. To manage and implement international co-operating activities in e-transaction.

Article 8. State responsibilities on e-transactions

1. The Government shall uniformly administer the State administration on e-transactions activities.

2. The Ministry of Post and Telematics shall be responsible before the Government in taking the lead, coordinating with related Ministries, branches on implementation of the State administration on e-transaction activities.

3. Ministries, ministerial-level bodies shall be responsible for carrying out State management on e-transaction activities within the scope of management of their Minister, branch.

4. People's committees of provinces, cities under the Central within their tasks, power shall carry out State management on e-transaction activities in their localities.

Article 9. Prohibited activities in e-transactions

1. Prevent the selection of the use of e-transactions.

2. Illegal prevention or blockage of transmission of, access to and receive data messages.

3. Illegal alteration, deletion, falsification, reproduction, disclosure, display and relocation of part of or the whole data messages.

4. Creation and dissemination of software programs that trouble, change, destroy the operating system or other activities to destroy the technology infrastructure on e-transactions.

5. Creation of data messages in order to carrying out illegal activities.

6. Fraudulent, wrongly identification, appropriation or illegal use of e-signatures of others.

Chapter II

DATA MESSAGE

Section 1

Validity of Data Message

Article 10. Forms showing of data message

Data message is shown in the form of exchanges of electronic data, electronic documents, e-mails, telegram, telegraphy, faxes and other similar forms.

Article 11. Recognition of Validity of Data Message

Information in data message cannot be denied [its] validity for the sole reason that such information is shown in the form of data messages.

Article 12. Data Messages Having the Same Validity as Written Document

Where the law requires information to be in writing, a data message shall be considered as meeting this condition if information containing in the data message is accessible and usable for reference when necessary.

Article 13. Data Message Having Validity as Original Copy

Data messages shall have validity as an original copy when satisfying the following conditions:

1. The contents of the data message are ensured being intact since its first origination in the form of a complete data message.

The content of a data message is considered intact when such contents remain unchanged except changes in its appearance, which arise in the process of sending, storage or display of the data message.

2. The contents of the data message are accessible and usable in its entirety for reference when necessary.

Article 14. Data Message Having Validity as Evidence

1. A data message cannot be denied [its] validity as evidence for the sole reason that it is a data message.

2. The validity as evidence 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 manner to ensure and maintain the integrity of the data message; the manner in which its originator was identified, and on other relevant factors.

Article 15. Storage of Data Message

1. In case where the laws require records, files or information to be stored, such records, files or information can be stored in the form of data messages when the following conditions are satisfied:

a) The information in the data message is accessible for reference 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 contents 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. Contents, time limit of storage of data message shall be carried out in accordance with the law on storage.

Section 2

Dispatch and Receipt of Data Messages

Article 16. Originator of Data Message

1. The originator of data messages shall be the agencies, organization, individual create or send a data message before such data message is stored but not include any intermediary transmitting the data message.

2. In case where parties participating in transactions do not agree otherwise, the determination of the originator of a data message shall be as follow:

a) A data message is considered as that of the originator if such data message is sent by the originator or is sent by an information system established to automatically operate which is designated by the originator;

b) The recipient may consider a data message as being that of the originator if [the recipient] has applied the identifying method, which is approved by the originator and [such method] gives the result that such data message is of the originator.

c) As soon as the recipient is aware of a technical error in the transmission of a data message or has taken appropriate measures to verify the error as accepted by the originator, the provisions of points (a) and (b) of this clause shall not apply.

4. The provisions of items a and b of Clause 2 of this Article shall not apply from the time when the recipient knows that there is a technical error in the transmission of the data message or [the recipient] used errors-verifying methods approved by the originator.

Article 17. Time and Place of Dispatch of Data Messages

Unless otherwise agreed by the parties of the transaction, the time and place of dispatch of a data message is as follows.

1. Time of dispatch of a data message is the point of time when a data message enters information system outside the control of the originator.

2. Place of dispatch of a data message is the place of business of the originator if the originator is an agency, organization or the regular residence of the originator if the originator is an individual. In case the originator has more than one place of business, the place of business is that which has the closest relationship to the transaction.

Article 18. Receipt of Data Messages

1. The recipient of a data message is the person who is designated to receive the data message from the originator of the data message but does not include any intermediary transmitting the data message.

2. Unless otherwise agreed by the parties to the transaction, the receipt of a data messages is provided as follows:

a. The recipient of a data message is deemed to have received the data message when the data message enters into the information system which is designated by him/her and accessible.

b. The recipient is entitled to consider each data message as an independent data message unless such data message is a copy of another data message and the recipient knows or must have known such data message is a copy.

c) Where the originator has required or agreed with the recipient before or during the dispatch of a data message that the recipient must send an acknowledgement when receiving the data message, the recipient must comply with such request or agreement.

dd) In case the orginator has not stated that the recipient must send an acknowledgement and the acknowledgement has not yet received the acknowledgement, the originator may give notice to the recipient stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received. In case the acknowledgement is not received within the time specified, the originator may treat the data message as though it had never been sent.

Article 19. Time and Place of Receipt of Data Messages

Unless otherwise agreed by the parties to the transaction, the time and place of receipt of a data message are provided as follows.

1. In case the recipient has designated an information system for the purpose of receiving data messages, receipt occurs at the time when the data message enters the designated information system. In case the recipient has not designated an information system, the receipt occurs when the data message enters any information system of the recipient.

2. A data message is deemed to be received at the place of business of the recipient if the recipient is an agency, organization or the regular residence of the recipient if the recipient is an individual. In case the recipient has more than one place of business, the place of business is that which has the closest relationship to the transaction.

Article 20. Automatic Dispatch and Receipt of Data Messages

If the orginator or the recipient has designated one or several information systems for the purpose of automatic dispatch or receipt of data messages, the provisions of Articles 16, 17, 18 and 19 of this Law shall apply.

Chapter III

E-SIGNATURES AND CERTIFICATION OF E-SIGNATURES

Section 1

E-signatures

Article 21. E-signature

1, An e-signature is established in the form of words, letters, numbers, symbols, sound or other form by electronic means, logically attached with or associated with a data message, which has an ability to certify the person who signs the data message and to certify the approval of such person to the content of the signed data message.

2. An e-signature shall be deemed as being secured if the e-signature satisfied the conditions stipulated in Article 22.1 of this Law.

3. E-signature may be certied by an e- signature certification service providing organization.

Article 22. Conditions to ensure security of e-signatures

1. An e-signature shall be deemed as being secured if [it] is verified by a security verifying process agreed by transacting parties and satisfied the following conditions:

a) E-signature creation data is attached only to the signatory in the context that such data is used;

b) E-signature creation dat is only under the control of the signatory at the time of signing;

c) All changes to the e-signature after the time of signing are detectable.

d) All changes to the contents of the data message after the time of signing are detectable.

2. E-signatures certified by an e-signature certification service providing organization shall be considered as meeting all the security conditions as set out in clause 1 of this Article.

Article 23. Principles of using e-signatures

1. Unless otherwise provided by the laws, the parties to the transaction have rights to enter into agreement:

a) To use or not to use e-signatures to sign data message in the process of transactions.

b) To use or not to use certified e-signatures.

c) To select an e-signature certification service providing organization in case there is an agreement to use certified e-signatures.

2. E-signatures of the State bodies must becertified by e-signature certification service providing organizations stipulated by the State bodies.

Article 24. Validity of e-signatures

1. Where the law requires a written document to have a signature such requirement with respects to a data message is regarded as being met if the e-signature used to sign such data message satisfies the following conditions:

(a) The method creating the e-signature permit [such method] to identify that person and to indicate that person's approval of the contents of the data message;

(b) Such method is sufficinetly reliable and appropriate for the purpose for which the data message was generated and communicated.

2. Where the law requires a written document to have a seal of the agency or organization, such requirement with respects to a data message is regarded as being met if such date message is signed by the agency or organization that meets all the requirements set out in Article 22.1 of this Law and that e-signature has been certified.

3. The Government shall make specific provisions for the management and use of e-signatures of agencies and organizations.

Article 25. Obligations of the Signatory of an e-signature

1. A signatory of an e-signature or the legal representative of such signatory shall be the person who controls the electronic signing program and uses such equipment to certify his/her intention with respect to the signed data message.

2. A signatory of an e-signature shall have the following obligations:

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

(b) Without undue delay, using appropriate methods to notify any person who rely on the e-signature and the e-signature certification service providing organization in case the e-signature is certified, when the signatory discovers that the e-signature may not be under the signatory's control;

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

3. A signatory of an e-signature shall be liable before the law for all consequences of its failure to comply with the provisions of Clause 2 of this Article.

Article 26. Obligations of the Party accepting e-signatures

1. A party accepting e-signatures is the organization, individual who acts based on the reliance of e-certificates or e-signature of senders.

2. A party accepting e-signatures shall have the responsibilities:

a. To take necessary steps to verify the reliability of an e-signature before accepting such e-signature;

b. To take necessary steps to verify the validity of the e-certificate and any limitation with respect to the e-certificate in case the e-certificate is used to certify the e-signature.

3. The party accepting e-signature shall be liable before the law for its failure to comply with the provisions stipulated in Clause 2 of this Article.

Article 27. Recognition of foreign e-certificates and e-signatures

1. The Government recognizes the validity of foreign e-certificates and e-signatures if such e-signatures or e-certificate have the reliable level equivalent to the reliability of e-signatures and e-certificate in accordance with the provisions of laws. The determination of the reliability of foreign e-signatures and e-certificates shall be based on internationally accepted standards, international treaties of which the Socialist Republic of Vietnam is a party and other relevant factors.

2. The Government provides for detailed regulations on foreign e-signatures and e-certificates.

Section 2

E-signature certification Services

Article 28. Activities of E-certification Services

1. Issuance, renewal, suspension, restoration, revocation of e-certificates.

2. Providing necessary information to assist the certification of ane-signature of a person who sign a data message.

3. Providing other services related to e-signatures and e-signature certificates in accordance with the law.

Article 29. Contents of E-certificates

1. Information about e-signature certification service providing organizations.

2. Information about agencies, organizations, individuals to whom e-certificates are provided.

3. Number of e-certificate.

4. Effective term of e-certificate.

5. E-signature inspection data of the person who holds e-certificate.

6. E-signature of e-signature certification service providing organizations.

7. Limitation on the purpose or use of the certificate.

8. Limitation on the legal liabilities of the e-signature certification service providing organization.

9. Other contents in accordance with the regulation of the Government.

Article 30. E-signature certification service providing organizations

1. An e-signature certification service providing organization include a public e-signature certification service providing organization and a specialized e-signature certification service providing organization licensed to carry out e-signature certification activities in accordance with the law.

2. A public e-signature certification service providing organization is an organization providing e-signature certification services to agencies, organizations, individuals for use in public activities. Activities to provide pulbic e-signature certification services are business activities which are subject to conditions in accordance with the provisions of the laws.

3. A specialized e-signature certification service providing organization is an organization providing e-signature certification services to agencies, organizations, individuals for use in specialized activities or sectors. Activities to provide specialized e-certification services shall be subject to registration with the State management bodies on e-signature certification services.

4. The Government provides in detail on establishment, organization, business registration, operation and mutual-recognition of e-signature certification service providing organizations stipulated in Clauses 2 and 3 of this Article.

Article 31. Rights and Obligations of e-signature certification service providing organizations

1. E-signature certification service providing organizations shall have the following rights and obligations:

a) Carry out e-signature certification service activities specified in Article 28 of this Law;

b) Comply with legislation on e-signature certification service providing organizations;

c) Use reliable technical equipment, procedures and resources in conducting their business;

d) Assurance of the accuracy and integrity of basic data in their e-certificates;

dd) Make public information related to e-certificates already issued, renewed, suspended, restored or revoked;

e) Provide appropriate facilities to enable those who accept e-signatures and State competent authorities to rely on the e-certificate to ascertain the origin of a data message and e-signature;

g) Notify relevant parties in case where problems happen, which affect e-certification.

h) Make public and notify those who have been issued with e-certifications, relevant management agencies within 90 days prior to the suspension or termination of operation.

i) Restore information related to e-certificate which are issued by themselves for at least 5 years as from the date the e-certificate is out of valid.

k) Have other rights and obligations as provided by law.

2. The Government shall provide for detailed regulations on rights and obligations of e-signature certification service providing organizations stipulated the provisions of Clause 1 of this Article.

Section 3

Administration of E-signature certification Services

Article 32: Conditions for Providing E-signature certification Services

1. E-signature certification service providing organizations shall meet the following conditions:

a) Having sufficient professional technical and administrative staff to provide e-signature certification services.

b) Having sufficient technical means and equipment, which are suitable with security, national safety standards;

c) Registering with the State management bodies on providign e-signature certification services.

2. The Government shall provide for detailed regulations on the following:

a) Order, procedures for registration of e-signature certification service providing activities.

b) Technical standards, procedures, human resources and other conditions necessary for e-signature certification service providing activities.

c) Contents and form of e-certificates.

d) Procedures on issuance, renewal, suspension, restoration and revocation of e-certificates.

dd) Storage and publication of information related to e-certificates issued by e-signature certification service providing organization.

e) Conditions and procedures for foreign e-signature certification service providing organizations to provide e-signature certification services in Vietnam.

g) Other contents necessary to e-signature certification services providing activities.

Chapter IV

ENTERING INTO AND EXECUTION OF E-CONTRACTS

Article 33. E-contracts

E-contracts are contracts established in the form of data messages in accordance with the provisions of this Law.

Article 34. Recognition of validity of e-contracts

Validity of an e-contract shall not be denied for the sole reason that such contract is in the form of a data message.

Article 35. Principles of entering into, execution of e-contracts

1. Parties have rights to agree on use electronic means in the process of entering into, execution of contracts.

2. The entering into, execution of an e-contract shall comply with the provisions of this Law and laws on contracts.

3. When entering into, executing e-contracts, the parties shall have right to agree on technical requirements, certification, conditions ensuring the integrity, confidentiality related to such e-contracts.

Article 36. Entering into e-contracts

1. Entering into e-contracts shall be the use of data messages in order to carry out parts of or the whole transaction during the process of entering into contracts.

2. During the process of entering into contracts, unless otherwise agreed by the parties, an offer to entering into contracts and acceptance of the offer to entering into contracts may be carried out through data messages.

Article 37. Receipt, Dispatch, Time, location of dispatch, receipt of data messages in entering into and execution of e-contracts

The receipt, dispatch, time, location of dispatch, receipt of data messages in entering into and execution of e-contracts shall be implemented in accordance with Articles 17, 18, 19 and 20 of this Law.

Article 38. Validity of a Notice in E-contracts

In the process of entering into, execution of an e-contract, a notice in the form of a data message shall be legally valid as a notice in other traditional form.

Chapter V

E-TRANSACTIONS IN STATE AGENCIES

Article 39. Types of E-transactions in State Agencies

1. E-transactions within an agency;

2. E-transactions among different State agencies;

3. E-transactions between State agencies with agencies, organizations and individuals.

Article 40. Principles for Conducting E-transactions in State agencies

1. Principles shall be stipulated in Clauses 3, 4 and 5 of Article 5 of this Law.

2. E-transactions between State bodies must be in accordance with the provisions of this Law and other provisions of related laws.

3. A State body within their tasks, powers shall hold initiate in carrying out a part or all of transactions in its internal body or with other State bodies by electronic means.

4. Based on socio-economic development conditions and their specific situations, State bodies determine a reasonable roadmap for using electronic means in the types of transactions stipulated in Article 39 of this Law.

5. Agencies, organizations, individuals have rights to select transactional means with State bodies with such State bodies agree to accept transactions in traditional forms as well as transactions in electronic means, unless the law provides otherwise.

6. When conducting e-transaction, State agencies shall determine the following:

a.) Formats, forms of data messages;

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

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

7. 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 this Law and other provisions of related laws.

Article 41. Security, confidentiality and storage of electronic information in State agencies

1). Periodic review and ensuring security of their electronic data system in conducting e-transactions.

2). Ensuring confidentiality of information related to e-transactions; not to use the information for other purposes in contrary to the provisions on the use of such information; not to disclose the information to a third party in accordance with the law.

3). Ensuring the integrity of data messages in e-transactions; ensuring safety in operating their computer network;

4). Creating database of corresponding transactions, ensuring information security and having standby system to recover information in case of errors of the electronic information system.

5) Ensuring security, confidentiality and storage of information in accordance with the provisions of this Law and other provisions of related laws.

Article 42. Responsibilities of State Agencies in case of Errors of E-information System

1. In case e-information system of a State agency has errors, which do not ensure the safety of data messages, such agency shall be responsible for informing users immediately of the errors and taking all necessary steps to correct the errors.

2. The State Agencies shall be responsible before the law if not complying with the provisions of Clause 1 of this Article.

Article 43. Responsibilities of Agencies, Organizations and Individuals in E-transactions with State Agencies

Agencies, organizations and individuals in their e-transactions with State agencies shall comply with the provisions of this Law, the regulations on e-transactions issued by the competent authority and other related laws.

Chapter VI

CONFIDENTIALITY, SECURITY AND SAFETY IN E-TRANSACTIONS

Article 44. Ensuring Security and Safety in E-transactions

1. Agencies, organizations and individuals have rights to select measures to ensure security, safety in accordance with the law when conducting e-transactions.

2. Agencies, 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; where any technical errors occur in the information systems which cause damage to other agencies, organizations and individuals, [the organizations and individuals] shall have to pay compensation in accordance with laws.

3. Agencies, organizations and individuals are prohibited from taking any action that prevent or cause damage to the assurance of security, safety in e-transactions.

Article 45. Protection of Data Messages

Agencies, organizations, individuals are not allowed to take any action that affects the integrity of data messages of other agencies, organizations and individuals.

Article 46. Information Confidentiality in E-transactions

1. Agencies, organizations, individuals shall have rights to select security measures in accordance with the provisions of the law when conducting e-transactions.

2. Agencies, organizations, individuals are not allowed to use, provide or disclose part or all of information related to private and personal affairs or information of other agencies, organizations, individuals which is accessible by or under the control [of the first-mentioned agencies, organizations and individuals] in e-transactions without prior agreement [of the other agencies, organizations and individuals] unless the law provides otherwise.

Article 47. Responsibility of Network Service Providing Organizations

1. Network service providing organizations shall be responsible for co-coordinating with relevant agencies to establish the management mechanism and technical measures to prevent the use of [their] network services to disseminate data messages which are against the traditional culture, national ethics, [and] cause harm to the national security, social safety and security or [are] breaches of other laws and regulations .

2. A Network service providing organization shall be responsible before the laws for its failure to promptly remove any data messages referred to in clause 1 of this Article although it has been notified thereof by the State competent agency.

Article 48. Responsibilities of agencies, organizations, individuals upon requests of competent State agencies

1. Upon requests of competent State agencies, agencies, organizations and individuals shall have the following responsibilities:

a. Storage of a particular data message including the transfer of the data to another computer system or other storage place;

b. Maintenance of the integrity of a particular data messages;

c. Presentation of or providing a particular data messages they have or under their control including password and other encryption methods;

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

dd. Other responsibilities provided by law.

2. Competent State agencies shall be responsible before the laws for their requests.

Article 49. Rights and responsibilities of State competent agencies

1. Competent State agencies shall have the following rights:

a. Search or otherwise access part or all of the computer system and data messages in such system;

b. Seize part or all of the computer system;

c. Copy and store copies of data messages;

d. Prevent access to a computer system;

dd. Other rights provided by law.

2. When exercising the rights stipulated in Clause 1 of this Article, competent State agencies shall be responsible before the laws for their decisions.

Chapter VII

DISPUTE SETTLEMENT AND HANDLING BREACHES

Article 50. Dealing with breaches of laws in e-transactions

1. Any person violating the law in e-transactions shall be subject to disciplines, administrative sactions or criminal liabilities depending on the nature, level of violation, if causing damage, a compensation must be paid in accordance with the law.

2. Agencies or organizations violating laws in e-transactions must be subject to administrative sanctions, suspension depending on the nature, level of violation, if causing damage, compensation must be paid in accordance with the law.

Article 51. Disputes in E-transactions

Disputes in e-transactions are disputes arising during transactions by electronic means.

Article 52. Dealing with disputes in e-transactions

1. The State encourages parties to a dispute in e-transactions to solve disputes by themselves through concilliation.

2. In case where the parties cannot resolve their disputes or cannot reach agreement, the power, procedures and order for resolving disputes on e-transactions must be carried out in accordance with the laws.

Chapter VIII

IMPLEMENTING PROVISIONS

Article 53. Effectiveness

This Law shall take effect on 1 March, 2006.

Article 54. Implementing Regulations

The Government shall make detailed provisions and provide guidelines for implementing this Law.

This Law has been ratified by the Legislature XI of the National Assembly of the Socialist Republic of Vietnam in its 8th session on November 29, 2005.

THE CHAIRMAN OF THE NATIONAL ASSEMBLY

NGUYEN VAN AN