Electronic Transactions Law in Thailand

Pinai Nanakorn*

The newly enacted Electronic Transactions Act of 2001 emerges as Thailand's first legislation recognising legal effect of the use of electronic records in transactions. The unintelligible phraseology of the Act, based upon blunt translation from the English texts of the international instruments, causes great complexity. This Act also poses a great deal of unresolved uncertainty especially in the electronic contracting context. This paper explores the historical background and discusses fundamental concepts embodied in key provisions of this Law in the light of problematic issues. Legal measures for handling cybercrime and fraud are also discussed succinctly. It is suggested that judges and legal practitioners be ready to tackle the difficulty.

1. Introduction

As information technology is highly advanced, we now have a new law on electronic transactions, officially known as the *"Electronic Transactions Act, B.E. 2544 (2001),"* which has already entered into force as from 4th April 2002.[1] Indeed, this legislation is a long-awaited law amid the exponential growth in electronic transactions, especially, in the e-commerce context. However, since its promulgation, both lawyers and laypersons do not seem to be familiar with this seemingly overexciting Act. The lack of understanding may, for some people, result from the lack of sufficient knowledge in information technology and the Internet, given that many provisions of the Act are intimately IT- and Internet-related. But, it appears that even lawyers well-accustomed to IT, or even IT engineers themselves, find it difficult to grasp provisions of this Act due to

* Faculty of Law, Thammasat University

[1] Published in *Government Gazette*, vol. 118, part 112a, dated 4th December 2001.

their unintelligible phraseology - many provisions of this law are the product of straight translation from the English texts of the Model Law on Electronic Commerce and the Model Law on Electronic Signatures prepared by the United Nations Commission on International Trade Law (UNCITRAL). In fact, such incomprehensible locution can be much avoided if we, rather than bluntly translating the foreign texts into the Thai language, merely couch such foreign concepts in Thai-styled wording.

This paper seeks to explain certain significant concepts reflected in this Act. It will first provide a historical background of the Act, pointing out the work carried out by UNCITRAL and the parallel attempts by the Thai Government in putting forth legislation to accommodate the use of electronic methods of communication in place of paper-based traditional means. The next part will bring out significant contents of the Act, showing, in particular, how the Act eviscerates principal legal obstacles involving the inability to apply legal requirements in existing law to the electronic environment and how the Act formulates new rules applicable to computer-based communications. Finally, this paper attempts discussion on unresolved issues in the context of electronic contracting and points out further steps to be taken in relation to keeping cyberrisks and harm under control.

2. Historical Background

2.1 Pivotal Roles of IT and the Internet

Remarkably rapid advancements of information technology contribute to an extensive array of advantages in the conduct of communications and transactions. The use of electronic methods is universally recognised as yielding swiftness and efficiency; it also reduces transaction costs that would otherwise be incurred in manually manipulated documentation. In effect, traditional means based upon papers or manual documentation are increasingly replaced by electronic methods such as the electronic data interchange (EDI), electronic mail or the Internet. Indeed,

the Internet seems to be the most common medium of global communications. A large number of transactions are carried out over the Internet. We have witnessed a great deal of advertisements on the Word Wide Web (now commonly called "webvertisements") soliciting netusers to acquire a wide range of goods and services, whether in a B2B (business-to-business) or B2C (business-to-consumer) fashion. A potential buyer can make a purchase order simply at a click of a mouse after filling in a digital form provided on a website or by sending in an order via e-mail. Prices can even be paid through various sorts of electronic payment systems including Web-based credit card encryption, electronic funds transfer (EFT) or digital cash. Other electronic means apart from the Internet play similar roles in terms of expediency, efficiency and inordinate swiftness. For instance, with the assistance of the EDI, a purchase order from a department store can automatically be made by the store's computer system to the supplier's as soon as the stock of a particular product is detected as running out; and similarly, an acceptance of such automated order can automatically be transmitted by the supplier's system to the store's-network once the supplier's system detects sufficient availability of the product ordered.

2.2 Introduction of the Global Legal Framework for E-Commerce

2.2.1 Reasons for Enactment

The realization, at a global level, of apparent benefits from electronic methods of communication eventually led to the enactment, in 1996, of the UNCITRAL Model Law on Electronic Commerce with the strong conviction that the establishment of a model law facilitating the use of electronic methods can contribute significantly to the development of harmonious economic relations as well as international trade. In this connection, the compelling reasons for enacting the Model Law are twofold: first, to get rid of legal obstacles to the use of modern means of transactions and, secondly, to lay down legal principles for computer-

based communications.

(a) Removal of Legal Obstacles to Modern Technology: Legal Recognition of "Data Messages"

The benchmark of this Model Law, as primarily embodied in its Article 5,[2] lies in the so-called *"functional equivalent approach"* i.e. recognising that information which is in an electronic form (referred to in the Model Law as a "data message")[3] serves the same function and has the same legal effect, validity or enforceability as that ascribed to a manually made document. *The reason for treating an electronically generated record as an equivalent of a paper-based record is linked to legal barriers or obstacles, found in existing laws, to the development of modern means of communication.* There are, in most legal systems, legal requirements which, although comfortably applicable to manual documents, cannot or may hardly be fulfilled by the use of data messages or computer-based techniques. Amongst others, the principal requirements are those regarding "writing", "signature" and "original." To give an example, section 456 paragraph three of our Civil and Commercial Code requires that an agreement for sale of movable goods worth at least 500 Baht be *evidenced in writing.* Evidently, in the absence of a specific law that treats computer-based documents as being equivalent to paper-based documents, an agreement concluded by e-mail cannot be enforceable simply because an e-mail message evidencing the agreement is not regarded as writing in the eyes of the provisions of section 456 above. Indeed, such an e-mail message is not admissible into evidence, for the Civil Procedure Code allows only original records to be adduced as evidence and in the computer world all computer-generated records can

---

[2] **Article 5**. Legal recognition of data messages

"Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message."

[3] In legislation of some jurisdictions, the term *"electronic record"* is used in preference to the term "data message": see, for example, the Electronic Transactions Act 1998 of the Republic of Singapore and the Electronic Commerce Security Act 1999 of the State of Illinois.

never be original. Similarly, the use of an electronic signature - generally speaking, a signature in the form of a data message - cannot be regarded as a signature within the meaning contemplated by existing law, with a result that the transaction to which an electronic signature is attached may not be enforceable for want of signature where the law requires it to be signed.

Legal recognition of data messages is, under the Model Law, also based upon 'technology-neutrality' (or 'media-neutrality'), that is, data messages are treated as legally effective, valid and enforceable irrespective of technology by which they are generated.[4] However, for data messages to be recognised as functionally equivalent to traditional records, the data messages need to satisfy such minimum criteria as set forth by the Model Law in particular matters as well.[5] For instance, in respect of 'writing', a data message is regarded as satisfying the requirement of writing provided that it is 'accessible so as to be usable for subsequent reference.'[6] As for signatures, an electronic signature enjoys legal recognition as a 'signature' only when it is created by a method that is reliable.[7] With regard to electronic signatures, UNCITRAL has enacted a separate Model Law – **the Model Law on Electronic Signatures** – to elaborate on the Model Law on Electronic Commerce in the particular matter of signatures.[8]

---

[4] See Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996) attached to the text of the Model Law (hereinafter the "Guide to Enactment").

[5] As previously pointed out, Article 5 of the Model Law (Legal recognition of data messages) lays down the general principle: 'functional equivalent.' Other Articles elaborate on individual matters: those involving *writing* (Article 6), *signature* (Article 7), *original* (Article 8), *admissibility and evidential weight of data messages* (Article 9), *retention of data messages* (Article 10).

[6] See Article 6 of the UNCITRAL Model Law on Electronic Commerce and Guide to Enactment, paras 47-52.

[7] See Article 7 of the UNCITRAL Model Law on Electronic Commerce.

[8] For example, the UNCITRAL Model Law on Electronic Signatures establishes a presumption of reliability of an electronic signature that is created by a method of such special attributes as described in Article 6 (2), and sets out duties of the signatory, the certification service provider (in case there is certification in support of an electronic signature) and the person who relies on the electronic signature created.

(b) New Principles for Computer-based Communications

There is also a need for formulating certain legal principles for applicability to computerised communications. A striking illustration is a principle for determining the time at which a computer-generated message is regarded as 'dispatched' and 'received'. In effect, in all jurisdictions, the 'dispatch' and 'receipt' rules are found in existing law, especially in the contractual context. For instance, where parties are not in each other's presence, a declaration of will by one party to the other becomes effective, under the Thai Civil and Commercial Code, once it *reaches* that other party (i.e. when that other party receives it) or, in common law jurisdictions, once it is posted (i.e. dispatched). Although, in the traditional means of communication, the moment at which a paper document is dispatched or received can directly be ascertained without significant difficulty, this is not the case in communications of electronic messages. Computer-operated messages are usually transmitted through complicated networks or a communication chain and, in many cases, with the involvement of intermediaries, as envisioned in the prototype case of e-mail transmission. The Model Law thus sets forth objective criteria for determining the time of dispatch and receipt of such electronic messages.[9] Apart from the objective rules as to the time of dispatch and receipt, the Model Law also establishes a rule for ascertaining the place of dispatch and receipt as well.[10]

2.2.2 Scope of Application

The reasons for recognising data messages as functionally equivalent to paper-based records and for setting forth objective criteria applicable to the computer-based environment are valid not only in the context of commerce but also in general contexts. Therefore, although the title of the Model Law refers to 'electronic commerce' (by reason that it

---

[9] Article 15 (1) - (3) of the UNCITRAL Model Law on Electronic Commerce.

[10] Article 15 (4) of the UNCITRAL Model Law on Electronic Commerce.

would mainly serve trade relationships), it leaves with each Enacting State a decision as to the coverage. An Enacting State, in making domestic legislation along the line of the Model Law, may opt to extend the sphere of application of the law to non-commercial activities (even to transactions in the public sector) or to limit the applicability to, for example, international trade. In this regard, a State that enacts a law in line with the Model Law and chooses to have the law applicable to commercial and non-commercial activities alike usually elects to use the term "electronic transactions" as part of the title of the legislation.[11]

3.1 Initiatives by the Thai Government

3.3.1 The IT-2000 Policy and Electronic Transactions Law Drafting

The Government of Thailand, like other countries, has long realised the importance of information technology and paperless methods of transactions. In effect, emphasis of the Government on this matter came about even before the emergence of the UNCITRAL Model Law on Electronic Commerce (1996). In 1992, the "Rule of the Office of the Prime Minister Relating to the Promotion of Information Technology Development, B.E. 2535 (1992)" was issued[12] to accommodate continuous and efficient operation of work towards promoting information technology development of the country. This Rule, now remaining in full force, set up the "National Information Technology Commission" (NITC) to be in charge of, *inter alia*, preparing the National Information Technology Development Plan for submission to the Cabinet for its approval.[13]

---

[11] See, for example, the Electronic Transactions Act 1998 of the Republic of Singapore.

[12] The issuance of this Rule is by virtue of section 11 (8) of the "Organisation of State Administration Act, B.E. 2534 (1991)."

[13] See Clause 7 as last amended by the Rule of the Office of the Prime Minister Relating to the Promotion of Information Technology Development (No. 4), B.E. 2540 (1997). Prior to the amendment, the Commission was called the "National Promotion of Information Technology Development Commission."

In 1996, the Cabinet, by its resolution of 20th February 1996, approved the National Information Technology Policy (the 'IT-2000' Policy) with a view to bringing about social development and building up strength in the spheres of commerce, industry and international trade with the advent of the new millennium. As the Policy included a reform of IT law, the then Ministry of Science, Technology and Environment proposed the IT law development project. Upon its approval by the Cabinet on 15th December 1998, the National Electronics and Computer Technology Center (NECTEC),[14] which serves as the secretariat of the NITC, proceeded to prepare 6 draft laws as follows: the Electronic Transactions Draft; the Electronic Signatures Draft; the Electronic Funds Transfer Draft; the Computer Crime Draft; the Data Protection Draft; and the Information Infrastructure Development (Universal Access) Draft. It is the first two Drafts that, subsequently merged into a single draft, have now become the "Electronic Transactions Act." The first Draft, in the main, contained provisions directly translated from the UNCITRAL Model Law on Electronic Commerce whilst the second Draft was dedicated to elaborating upon electronic signatures, also taking into account the UNCITRAL Model Law on Electronic Signatures.[15]

3.1.2 Draft Law on Electronic Transactions and Draft Law on Electronic Signatures

(a) Draft Law on Electronic Transactions

The Draft Law on Electronic Transactions was, in essence, a blunt translation of the UNCITRAL Model Law on Electronic Commerce.[16]

---

[14] NECTEC is an integral part of the National Science and Technology Development Agency, a special agency established by the National Science and Technology Development Act, B.E. 2534 (1991) and subject to supervision by the Minister of Science.

[15] At the time of drafting, the UNCITRAL Model Law on Electronic Signatures was still a Draft (under the name "Draft Uniform Rules on Electronic Signatures") and was at a rather final stage of consideration by the UNCITRAL Working Group on Electronic Commerce.

[16] See note 5, *supra*, for key provisions of the UNCITRAL Model Law on Electronic Commerce 1996.

However, the scope of the Draft was not limited to commercial activities. The Draft was intended to apply to electronic transactions in general and even to transactions by or with public authorities. It was also felt, during the consideration of the Draft by the Office of the Council of State, that certain provisions of the UNCITRAL Model Law on Electronic Commerce were repetitious, so that there would not be a strong need for the Draft Law on Electronic Transactions to include redundant provisions. In addition, some legal concepts as reflected in certain provisions of the said Model Law could, it was further felt, go without saying, given that the domestic law would already produce the same consequences.[17] Despite such repetitions and redundancy, the Council of State decided to maintain them in the belief that preservation of similarities to the Model Law would better create confidence of the global community, in particular in borderless trade.

As some governmental agencies might not be ready to have full use of electronic methods in replacement of, or in addition to, paper-based handling, it would be inapposite for the Draft Law to allow members of the public to, *as of right*, deal with a State agency in an electronic form. To cure this difficulty, the Council of State made an amendment to the "Sphere of Applicability" provision of the Draft by stating clearly that the Draft Law would apply to civil and commercial transactions outright while transactions made with or by a State agency could be made in the form of a data message (i.e. in an electronic form in place of manual documentation) only upon issuance of the Royal Decree prescribing relevant rules and procedures therefor.

---

[17] An illustration is Article 11 (formation and validity of contracts) which reads "In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose". Under the Civil and Commercial Code of Thailand, a manifestation of an intention can already be made by any means.

(b) Draft Law on Electronic Signatures

As is the case of the relationship between the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures, the Draft Law on Electronic Signatures was intended to elaborate upon the "electronic signature" provision of the Draft Law on Electronic Transactions, also taking into account the UNCITRAL Model Law on Electronic Signatures.[18]

Apart from the general principle recognising legal effect of an electronic signature on the condition that it would have to satisfy the "reliability" requirement,[19] the Draft Law on Electronic Signatures introduced the "secure electronic signature" concept, as found in the laws of certain countries. The significance of a secure electronic signature lies in the benefit of the legal presumption. A user of a secure electronic signature would be presumed to be the signatory and, consequently, the information to which such secure electronic signature was affixed would also be presumed to have been unaltered since the specific point in time at which that signature was affixed.

In this connection, as similar to the position taken in the UNCITRAL Model Law on Electronic Signatures, a secure electronic signature under the Draft Law on Electronic Signatures was generally defined as the "electronic signature created *under the sole control of a particular person* at the time of its creation using the method which makes a *unique linkage* of the signatory with such electronic signature." It is generally accepted that, *in most cases*, these "sole control" and "uniqueness" features are, in reality, characteristic of electronic signatures created by the PKI-based method (known as "digital signatures").[20] Thus, as a shortcut, the Draft

---

[18] At the time of drafting, the UNCITRAL Model Law on Electronic Signatures was still a Draft (under the name "Draft Uniform Rules on Electronic Signatures") which was at a rather final stage of consideration by the UNCITRAL Working Group on Electronic Commerce.

[19] See note 8, *supra*.

[20] See page 68, *infra*.

Law regarded a digital signature as being a secure electronic signature provided, however, that certification would be obtained from a licensed certification authority (often called "CA").[21] But, as new technology may emerge from time to time, the "sole control" and "uniqueness" attributes may commonly be found in electronic signatures created by non-PKI methods. Therefore, in an enhanced endeavour to endorse the *media neutrality* conception, the Draft Law has introduced a catch-all provision to the effect that such electronic signatures as prescribed in the Royal Decree would be regarded as secure electronic signatures.

Although legal recognition was intended to be given to all types of electronic signatures meeting the "reliability requirement," a focus of this Draft Law was remarkably placed on digital signatures. Indeed, after having spelled out the general provisions in Chapter I of the Draft, its remaining provisions (sections 8 - 69 in Chapter II and Chapter III) dealt with digital signatures. The Draft introduced the certification regime with regard to digital signatures (no mention was ever made of the possibility of certification in respect of other types of electronic signatures!), and identified rights and duties of the subscriber (holder of a certificate), the certification authority and the relying party (i.e. the person who relies on the information listed in the certificate and on the content of the digitally signed data message). Those wishing to engage in the certification services with regard to digital signatures were required to obtain a licence from the public authority as well. The Draft Law also sought to establish the "Electronic Signatures Commission" as a regulatory body with the powers and duties, *inter alia*, to lay down policies for the promotion and development of the use of electronic signatures as well as prescribe technical and security standards for electronic signatures.

---

[21] The Model Law on Electronic Signatures elects to use the term "certification service provider" (CSP) in place of the term "certification authority" (CA).

3.1.3 The Merger into Single Legislation

The two Drafts were, as suggested by the Office of the Council of State and approved by the Cabinet at its meeting on 25th July 2000, subsequently merged into a single Draft. The rationale for the coalition rested upon the realization that the Draft Law on Electronic Signatures was no more than an elaboration upon the legal recognition of electronic signatures as already provided in the Draft Law on Electronic Transactions, by adding technical details as well as setting out provisions regulating certification services with regard to digital signatures. In view of rapidly advancing technologies, it would be inept to include technical details in the form of an Act. All such details, in order to keep pace with technological changes, should be deleted from the Draft Law and subsequently prescribed by way of a Royal Decree (a form of subordinate legislation). After the evisceration of such technical details (which constituted the large part of the Draft), very few provisions indeed remained and could simply be incorporated into the Draft Law on Electronic Transactions altogether.[22] On this footing, the single Draft - the Electronic Transactions Bill - was presented to the House of Representatives.

It was also felt by the Office of the Council of State that the need for prescribing technical standards or security procedures and the necessity of supervision by the State should not be limited to the context of electronic signatures, as in the Draft Law on Electronic Signatures, but should apply to electronic transactions as a whole. Thus, the Electronic Transactions Bill as presented to the House allowed issuance of Royal Decrees prescribing technical procedures for *any electronic transaction*.[23]

---

[22] In effect, the fact that a significant majority of the provisions of the Draft were devoted merely to digital signatures was also largely criticised as inappropriate.

[23] In this connection, such electronic transaction, where carried out in accordance with the procedures prescribed by a Royal Degree would be presumed to satisfy the requirement of reliability; the relevant provision (then as section 24) read: "The entry of a signature, retention of information in its original form, or *any act in the form of an electronic transaction* shall, if conducted in accordance with the procedure prescribed in the Royal Decree, be presumed to have applied a reliable method and have legal effect." (Emphasis added.)

The Bill also delegated to the Executive the power to issue Royal Decrees regulating the operation of businesses related to *electronic transactions.*[24] Further, the Bill set up the "Electronic Transactions Commission," in place of the Electronic Signatures Commission as appeared in the Electronic Signatures Draft, as a regulating and advisory body for electronic transactions as a whole.

In the House of Representatives, the provisions regarding 'secure electronic signatures' were resurrected.[25] In addition, due to overwhelming fears felt by the business sector of governmental control over electronic transactions on a large scale, regulation of businesses by way of Royal Decree was limited to services of *certification in relation to secure electronic signatures.*[26] The Bill was, with such amendment, approved

---

[24] The regulation was intended to be by way of requiring the businesses concerned to be licensed, registered or notified to the competent official prior to their operation. See *infra.*

[25] The added provisions relating to 'secure electronic signatures' merely stated characteristics of secure electronic signatures as well as legal consequences in terms of the legal presumption. The provisions concerned are herebelow quoted.

Section 33. The following electronic signatures shall be deemed secure electronic signatures:

(1) an electronic signature as prescribed in the Royal Decree under section 24;

(2) where the originator and the addressee so agree, an electronic signature which is created under the sole control of a particular originator at the time of its creation using the creation method which makes a unique linkage of such person with such electronic signature.

Section 34. If a secure electronic signature is used with any data message, it shall be presumed that such data message has not been altered as from the specific point in time at which such secure electronic signature was created and that such person has the intention to treat the said electronic signature as his or her own signature.

[26] "Section 35. A person may operate as a certification service provider [defined as a certification service provider *in relation to secure electronic signatures*] except that in the case where it is necessary for strengthening the reliability and trustworthiness in data message systems or for preventing loss to the public, the Commission may make a recommendation for issuance of a Royal Decree requiring the operation of certification services in any particular case to be subject to prior notification, registration or licence.

In making the determination as to which case shall require a notification, registration or licence under paragraph one, regard shall be had to the appropriateness of the prevention of loss in accordance with the magnitude of severity of impacts likely to occur in consequence of the operation of the certification services.

For this purpose, any particular State agency may be designated by such Royal Decree to be the responsible supervisory agency."

by the House on 27th September 2000. When it went to the Senate, a separate chapter on "Electronic Signatures" was inserted and details regarding duties of the signatory, certification authority (or certification service provider) and relying party were brought back and strictly modelled after the corresponding provisions of the UNCITRAL Model Law on Electronic Signatures (the final draft of which had at that time become final).

3. Significant Contents of the Act

3.1 Legal recognition of Data Messages and Removal of Legal Obstacles

3.1.1 Legal Recognition of Data Messages

The Electronic Transactions Act, B.E. 2544 (2001) adopts the "functional equivalent" approach and eliminates legal obstacles flowing from legal requirements as to writing, signatures, originals and so on, along the line of the UNCITRAL Model Law on Electronic Commerce. In this connection, it is provided: "Information shall not be denied legal effect and enforceability solely on the ground that it is in the form of a data message."[27] This provision is apparently intended to be a general provision treating data messages functionally equivalent to paper documents. An electronically made transaction is, generally, not to be denied legal effect or enforceability by the sole reason that it is not in a paper or manual form.

3.1.2 'Writing', 'Signature' and 'Original'

Overview

Separate provisions are dedicated to how data messages fulfil the legal requirements as to 'writing', 'signature' and 'original', in as much the

[27] Section 7.

same line as Articles 6,[28] 7[29] and 8[30] of the UNCITRAL Model Law on Electronic Commerce. Thus, the use of a data message can now be regarded as satisfying the requirements of writing, signatures and original, provided that minimum criteria set forth in particular provisions are met. For instance, with regard to 'writing', a data message is regarded as being writing or evidenced in writing if, under section 8 of the Act,[31] the information contained in that data message is accessible and usable for subsequent reference, and with respect to 'signature', an electronic signature is regarded as a signature if, under section 9,[32] it is, *inter alia*,

---

[28] Article 6 (1) "Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference."

[29] Article 7 (1) "Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement."

[30] Article 8 (1) "Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented."

[31] Section 8: "Subject to the provisions of section 9, in the case where the law requires that any transaction be made in writing or evidenced by writing or supported by a document which must be produced, if the information is generated in the form of a data message which is accessible and usable for subsequent reference without its meaning being altered, it shall be deemed that such information is already made in writing, evidenced by writing or supported by the produced document."

[32] Section 9: "In the case where a person is to enter a signature in any writing, it shall be deemed that a data message bears a signature if:

(1) a method is used which is capable of identifying the signatory and indicating that the signatory has approved the information contained in the data message as being his own; and

(2) such method is as reliable as was appropriate for the purpose for which the data message was generated or sent, having regard to surrounding circumstances or an agreement between the parties."

created by a reliable method.

Signatures

With respect to signatures, in addition to the principal provision, in section 9, recognising legal effect of all types of electronic signatures (provided that they are created by a reliable method that is capable of identifying the signatory and indicating the signatory's approval of the information to which that electronic signature is affixed[33]), the Electronic Transactions Act even inserts a specific Chapter - Chapter 2 - on 'Electronic signatures.' The very Chapter, in effect, elaborates upon the general rule established by the said section 9 in 2 principal respects - the legal presumption of reliability and duties of parties concerned.

(a) Legal Presumption of Reliability

Chapter 2 of the Act introduces, under section 26, a legal presumption of 'reliability' in favour of an electronic signature created by a special method recognised as reliable. As previously mentioned, under section 9, general electronic signatures need to be created by a method that is *reliable*. In this connection, a person who seeks the benefit from the electronic signature in question will have to prove the reliability. This onus of proof is forsaken in the case of electronic signatures created by special methods as specified in section 26. This section reads:

> *"Section 26. An electronic signature that meets the following features shall be deemed to be a reliable electronic signature:*
>
> *(1) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;*
>
> *(2) the signature creation data were, at the time of creating the electronic signature, under the control of the signatory and of no other person;*
>
> *(3) any alteration to the electronic signature, made as from the time of its creation, is detectable; and*

[33] See note 32, *supra*.

(4) in the case where a purpose of the legal requirement for an electronic signature [sic][34] is to provide assurance as to the integrity of the information, any alteration made to that information as from the time of signing is detectable.

The provision of paragraph one does not imply any limitation that no other method exists for establishing the reliability of an electronic signature or does not limit the adducing of any evidence of the non-reliability of an electronic signature."

Section 26 is, in effect, a replicate of Article 6 (2) of the UNCITRAL Model Law on Electronic Signatures. As evident from the wording of section 26 above, an electronic signature that meets the features set out by the section is deemed to be *reliable.* In other words, the person invoking legal effect of the signature need not prove that it has been created by a reliable method, for the law presumes that it is reliable. The significant features of an electronic signature that triggers the legal presumption of reliability lie in, as in (1) and (2) of section 26 paragraph one, the "uniqueness" and "sole control" elements, that is to say, *the signature creation data (i.e. electronic data, e.g. keys or codes, used to create an electronic signature) are uniquely linked to the signatory and were, at the time of creating the electronic signature, under the sole control of the signatory.* In effect, as far as current technology is concerned, these attributes are generally found in electronic signatures created by the public-key cryptography technology

---

[34] In fact, the correct words are "the legal requirement for *a signature*" (rather than "the legal requirement for *an electronic signature*"), for it is impossible that any law requires an electronic signature. This mistake was occasioned due to carelessness of NECTEC in phrasing this inserted provision when the Bill was considered by the Senate.

(commonly known as the "PKI" method).[35] Indeed, PKI-based electronic signatures, called digital signatures, have long been recognised as very secure (and for this reason the Electronic Transactions Law of some jurisdictions provides that a digital signature is a 'secure electronic signature' and, as a result, is regarded as authentic).

(b) Certification Services and Duties of Parties Concerned

In the context of electronic signatures, there are 3 parties involved, namely, the signatory (the person creating an electronic signature), the certification service provider and the relying party (the third party who relies on an electronic signature created).

The certification service provider (CSP) is involved because the signatory may, in some cases, wish to have a trusted third party issue a certificate in support of their signature and provide a verification means for such signature so that the recipient of that signature can be assured that the signatory has a real identity and that the signature created as well as the electronically signed record is authentic. In this instance, the signatory will have to subscribe to the certification service offered by a CSP[36] and, after verification of real identity of the signatory, the CSP will issue a certificate to the signatory in support of electronic signatures to be

---

[35] The PKI method involves the use of a key pair - the private key and the public key. These secret keys are assigned by a computer and bear an algorithm association. The message to be digitally signed will be encrypted by the private key to constitute a digital signature, which will then be affixed to the original message. In effect, to generate enhanced security and enable the original message to be smaller in size, a *hash function* may also be employed before the encryption by the private key. The counterpart key - the public key - is to be used in the process of verification of the signature and the digitally signed message (see *infra*). For the association of the PKI method with reliability of electronic signatures, see Guide to Enactment to the UNCITRAL Model Law on Electronic Signatures, *paras*, 32 - 52.

[36] For this reason, the signatory is also called the 'subscriber'. This term can be seen, for example, in the Electronic Transactions Act 1998 of the Republic of Singapore. During the drafting of the UNCITRAL Model Law on Electronic Signatures, the Working Group also considered the following alternative words: 'signatory', 'signature holder', and 'subscriber'. The final draft opted for the term 'signatory'.

created. The certificate will specify the identity of the signatory and the method for creating electronic signatures. When a message affixed with an electronic signature is received by the addressee (the relying party), the addressee can check the signatory's certificate and may have access to the verification system as provided by the CSP to ensure authenticity of the signature and integrity of the message electronically signed. This certification takes place in particular in the case of digital signatures (that are, as earlier mentioned, created by a PKI-based method). In this regard, the public key, a counterpart of the private key used by the signatory to create a digital signature, will also be disclosed to the CSP for the purpose of verification of the signatory's signatures and digitally signed messages.

Given the relationships amongst the three parties as above, Chapter 2 of the Act thus lays down essential duties of these persons. This is, again, in harmony with the UNCITRAL Model Law on Electronic Signatures. For example, the signatory has the duties to exercise reasonable care to avoid unauthorised use of his signature creation data and notify, without delay, a relying party and the CSP in the event the signature creation data are, actually or suspected to be, lost, damaged or compromised.[37] On the CSP's side, the CSP is under obligation to exercise reasonable care to ensure the accuracy and completeness of all material representations listed in the certificate, provide a reasonably accessible means for relying parties to verify the validity and authenticity of the signature creation data used by the signatory, and utilise trustworthy systems, procedures and human resources in performing its services.[38] Likewise, the relying party must take reasonable steps to verify the reliability of an electronic signature, verify the validity, suspension or revocation of the certificate, and observe any limitation with respect to the certificate.[39]

---

[37] See section 27.

[38] See sections 28 - 29

[39] See section 30.

3.1.3 Admissibility into Evidence

In addition, the Act, under section 11,[40] allows admissibility into evidence of data messages to ensure that in legal proceedings electronically generated records can freely be adduced as evidence. However, the evidential weight of a data message is still at the discretion of the Court or the adjudicatory body. Reliability of the data message in question is to be tested by having regard to, for example, the manner or the method of creating that data message and maintaining its integrity.[41] This section is, indeed, a significant revolution of the law of evidence as encapsulated in the Civil Procedure Code and the Criminal Procedure Code. As a result of the promulgation of the Electronic Transactions Act, attempts have also been made to revise the Civil Procedure Code by inserting detailed rules applicable to admissibility in evidence and evidential weight of data messages. (At the time of this article going to press, the revision remains uncompleted.)

3.1.4 Retention of Data Messages

As in the Model Law on Electronic Commerce, the Act makes a provision allowing retention of data messages in place of paper documents where the law requires such documents to be retained. As with other provisions, this provision - section 12 - sets forth minimum rules, with a result that retention in an electronic form is regarded as equivalent

---

[40] Section 11 paragraph one: "The admissibility of a data message in evidence shall not be denied in legal proceedings on the sole ground that it is a data message."

[41] See section 11 paragraph two: "In assessing the evidential weight of a data message so as to conclude whether and to what extent it is reliable, regard shall be had to the reliability of the manner in which or the method by which the data message was generated, stored or communicated, the manner in which or the method by which the integrity of the information was maintained, and the manner in which or the method by which its originator was identified or indicated and also to all relevant circumstances."

to paper-based retention only when these rules are complied with.[42] This provision is of tremendous value to traders who are required by numerous legislation to keep paper records and business accounts. In effect, given that the Electronic Transactions Act also applies to transactions in the public sector, State agencies, that are under legal obligation to keep voluminous official records, will reap great benefit from electronic retention too.

3.1.5 Contract Making

Despite the general rule in section 7 giving legal recognition to data messages, the Act, for added clarity, recognises electronically made contracts. For this purpose, it is provided that an offer and an acceptance, in the conclusion of a contract, may be made in an electronic form and that the contract is not to be denied legal effect on the sole ground that the offer or acceptance was made in the form of a data message.[43] Obviously, this provision results in greater confidence in legal validity and enforceability of "electronic contracting" prevalent especially via the Internet. Offers and acceptances may now be legally made by electronic mail or even by clicking an icon on a webvertisement after filling in a digital order form there. The Act also makes clear that a declaration of will or notice may be made or given in the form of a data message.[44]

3.2 New Rules for Computerised Communications

As previously explained, a need arises for establishing certain legal principles applicable to computerised communications. Without

---

[42] The rules are as follows: (1) the data message [retained in place of paper documents] is accessible and usable for subsequent reference without its meaning being altered; (2) such data message is retained in the format in which it was generated, sent or received or in a format which can display accurately the information generated, sent or received; and (3) the information, if any, which enables the identification of the origin, source and destination of such data message including the date and time when it was sent or received is retained.

[43] Section 13.

[44] Section 14.

these new principles, various rules in existing law cannot be properly employed.[45] The crucial novel rules to be set up are the rules for determining the time of 'dispatch' and 'receipt' of a computer-generated message and the place of its 'dispatch' and 'receipt.' Along the line of the UNCITRAL Model Law on Electronic Commerce, the Electronic Transactions Act sets forth the criteria for determining the moment at which a data message is regarded as 'dispatched' and 'received' and the criteria which determine the place where a data message is taken as dispatched and received.

With regard to the time of dispatch, a data message is taken as dispatched when it *enters an information system outside the control of the person who dispatches it* (so-called "originator").[46] On the other hand, the time of receipt of a data message is determined by reference, generally, to the moment at which the data message *enters an information system of the addressee* or the information system designated by the addressee (if so designated).[47]

The place where a data message is regarded as dispatched is the place of business of the originator; and, similarly, the place of receipt of a data message is the place of business of the addressee, irrespective of the actual place where the originator stays at the particular time or the place where his network is located.[48] Therefore, when A, having a place of business in Bangkok, sends his electronic mail at a hotel in London via his hotmail account, the e-mail is regarded as sent in Bangkok rather than London. Similarly, if A, from the example above, receives an e-mail during his short visit to New York, A is regarded as receiving that e-mail in Bangkok where his place of business is even though at that time he uses the network in America.

---

[45] See page 57, *supra.*

[46] Section 22.

[47] Section 23.

[48] Section 24.

In fact, the determination of the place of dispatch and receipt are intimately linked to the question as to the place where a contract is made, which, in turn, bears direct association with the ascertainment of the applicable law. A contract is usually, in the absence of the parties' choice of applicable law, governed by the law of the place where the contract is concluded (which is, the place where an acceptance takes effect). In Thai law, an acceptance, in non-instantaneous communication, takes effect when it reaches (i.e. received by) the offeror.[49] As the Electronic Transactions Act provides that a person is regarded as receiving a data message at his place of business, it follows that the offeror receives an electronic acceptance at his place of business, with a further result that the contract in question is formed at the offeror's place of business accordingly and is governed by the law of the offeror's place of business.[50]

---

[49] Section 13 paragraph two of the Act on Conflict of Laws also provides this effect: "If the contract is made between persons who are not in each other's presence, the place at which the contract is deemed to have been formed is *the place at which an acceptance has reached the offeror.* If such place cannot be ascertained, the governing law is the law of the place where the contract is to be performed (emphasis added)."

[50] An illustration can be given as follows. A, an American who has a firm in Bangkok but uses the internet service provided from the United States by an American internet service provider, has sent an e-mail to B, a German who runs a Thai restaurant in Germany, offering to buy B's restaurant. B, while on a short vacation in Australia, then sends A an e-mail informing A that B agrees to sell the restaurant to A. In this example, a contract is, under Thai law, formed in Bangkok where A (as the recipient of B's acceptance) has a place of business) although A receives B's message through a server located in America. As a consequence, the contract is governed by Thai law. (This illustration is based upon the assumption that a communication by e-mail is a non-instantaneous communication. For controversy as to whether to perceive e-mail communication as instantaneous or non-instantaneous, see *infra*.)

By way of comparison, in common law jurisdictions, an acceptance, in non-instantaneous communication, takes effect when it is posted (the 'postal rule'). The facts similar to those above will produce different consequences - the contract will be regarded as concluded at the place of B's dispatch. Given that the dispatch is deemed to occur at the place of the dispatcher's place of business, the contract is regarded as formed in Germany albeit B's e-mail is sent while he is in Australia.

3.3 Control of Service Businesses related to Electronic Transactions

The Act delegates to the Executive the power to issue a Royal Decree requiring the operation of a service business related to electronic transactions *in any particular case* to be subject to prior notification, registration or licence *where there would arise necessity in the interest of the public.*[51] It is noteworthy that this provision is not intended to encourage the Government to exercise absolute control over the business sector in respect of electronic transactions. Rather, it aims to provide reasonable safeguards *only in the event of compelling necessity.* Without exigency or pressing need, controlling measures would not be launched at the expense of trade. Besides, the Act makes it compulsory for the Executive to conduct a public hearing before issuance of a Royal Decree to the above-mentioned effect.[52]

3.4 Electronic Transactions in the Public Sector

The Act applies not only to transactions in the private sector but also to transactions made with or by State agencies. According to section 35 of the Act, an application, permission, registration, administrative order, payment, notification or the performance of any act under the law with a State agency or by a State agency may be made in the form of a data message. However, as some State agencies may not be ready to the electronic environment, the Act requires issuance of a Royal Decree for State agencies to use data messages in place of paper-based records.

---

[51] Section 32.

[52] As earlier mentioned, at the stage of the Bill's consideration by the House of Representatives, the control was limited to the *certification service business*, which, when considered in conjunction with the definition "certification service provider" meant merely the business that provided certification services *in relation to secure electronic signatures*. However, at the Senate stage, the control was again extended to general service businesses related to electronic transactions.

3.5 Electronic Transactions Commission

The Act sets up the "Electronic Transactions Commission" as an advisory body in the sphere of electronic transactions. The Commission, *inter alia*, makes recommendations to the Cabinet with regard to the promotion of electronic transactions and the issuance of Royal Decrees under the Act.[53]

4. Unresolved Issues and Further Moves

4.1 Formation of Electronic Contracts

The Electronic Transactions Act is, by no wise, problem-free. Many issues remain uncertain and unresolved, in particular in the context of formation of electronic contracts. A contract is, no doubt, formed when an acceptance becomes effective. In order to conclude the time at which an acceptance takes effect, we need first to determine whether an acceptance is made in an instantaneous or non-instantaneous environment. If the acceptance is communicated in an instantaneous setting, the acceptance will become effective when, under section 168 of the Civil and Commercial Code, it is known to the offeror (Given that the offeror has the knowledge of the acceptance instantly, it follows therefore that the acceptance becomes effective instantly accordingly.) But, if the acceptance is manifested in a non-instantaneous scenario, it takes effect when, under section 169 and section 361 of the Code, it is *received* by the other party (and, in this connection, it is to be recalled that the time of receipt is, according to the rule laid down by the Act, the time *when the data message enters an information system of the addressee*).[54]

---

[53] See sections 36 - 43.

[54] By way of comparison, in common law jurisdictions, an acceptance made in a non-instantaneous context takes effect when *posted* while an acceptance made in an instantaneous setting becomes effective when *received* by the offeror. Thus, the rules as to the time of 'receipt' and 'dispatch' come into play after it is already determined whether the communication in question is instantaneous or non-instantaneous.

Although computer-based communications of certain types (such as a communication over an Internet chatroom or via ICQ) can obviously be envisaged as being of an instantaneous nature, debates are much advanced over the problematic issue as to whether other means of network communication are to be regarded instantaneous as well. Take as an example a communication via electronic mail. Although the message, once transmitted, can travel to the other party, wherever in the world that party is located, in just such a few seconds that we might be led to perceive that the communication is instantaneous, we need to, on the other side of the coin, realise that such other party may not, unlike in a normal telephone conversation, be in a position to have any immediate or continuous feedback, for he may, at that moment, go off-line. There appears to be a time lag between the transmission and the receipt of the e-mail message. As a consequence, an e-mail communication should arguably be regarded as non-instantaneous, which according to the provision of the Civil and Commercial Code above, takes effect when *received* by the other party.[55] However, if an e-mail communication is taken as an instantaneous means, a different conclusion will be arrived at. Thus, where a case involving an electronic mail is brought before the Court, the Court will need to resolve this controversial issue for the sake of clarity and confidence on the part of both traders and consumers.

Indeed, the disputable issue surrounding whether to classify an e-mail communication as instantaneous or non-instantaneous - the issue intimately connected to the formation of an electronic contract - is globally felt. For instance, in the United Kingdom, some commentators advocate that an e-mail communication is non-instantaneous, with a result that a postal rule applies to e-mails as well, while other scholars articulate a

---

[55] See, for a comparison purpose, the common law position, *supra*.

contrary view.[56] Notably, the UNCITRAL Working Group on Electronic Commerce appears to be aware of the difficulty involving the contract formation phase in an electronic setting. This has led to the Working Group's attempt to draw up the "preliminary draft convention on contracts concluded or evidenced by data messages."[57] Under this draft convention, an offer and an acceptance becomes effective when *received* by the other party (that is, the draft convention eliminates the problematic instantaneous/non-instantaneous distinction in an electronic contract).[58]

In effect, even if we adopt the "receipt" rule, we will have yet to encounter a further interpretation difficulty. As already explained, the time of receipt of a data message is the time at which the data message 'enters an information system' of the other party (the addressee). The crucial question that arises is whether A's e-mail message is considered as received by B as soon as it arrives at B's mailbox on a server of an ISP to which B subscribes although at that instant B is not connected to the Internet. Some may hold that in order for A's e-mail to be regarded as 'entering B's information system' B has to be on-line at that time. An alternative argument may be advanced that B receives A's e-mail message only after A's e-mail is downloaded off the server onto B's computer. Amid this uncertainty, the Courts will have to move forward to set clear precedents over this kind of subtle issue. In the absence of clearcut judicial positions, merchants are advised to avoid uncertainty through the use of

---

[56] See, for example, Michael Chisick *et al*, Electronic Commerce: Law and Practice, 2nd edn., London: Sweet & Maxwell, 2000, pp. 80 - 82; David Johnston *et al*, Cyber Law, Selangor: Pelanduk Publications, 1998, pp. 179 - 185; David I Bainbridge, Introduction to Computer Law, 4th edn., Pearson on Education, 2000, pp. 266 - 268.

[57] See UNCITRAL Working Group on Electronic Commerce, A/CN.9/WG.IV/WP.95 (Legal aspects of electronic commerce, Electronic contracting: provisions for a draft convention, Note by the Secretariat, thirty-ninth session, New York, 11 - 15 March 2002, and see also A/CN.9/527 (Report of the Working Group IV (Electronic Commerce) on the work of its fortieth session, Vienna, 18 - 14 October 2002), available at the UNCITRAL website (http://www.uncitral.org).

[58] See Draft Article 8 of the Draft Convention.

disclaimers clearly specifying the exact time at which their acceptances are regarded as effective.

4.2 Consumer Protection

4.2.1 Common Predicament

Despite meritorious values of electronic transactions, cyberspace poses an extensive array of risks at the expense of consumers. We have, as a matter of fact, witnessed a great deal of fraudulent and unethical conduct committed by e-merchants towards consumers. In effect, the 'anonymity' feature inherent in cyberspace constitutes a major driving force for the commission of fraud and inequitable conduct, which actually turns the virtual world into a largely insecure business forum.

Take as an example the instance of misleading and false information. A great deal of information contained in webvertisements is misleading or inaccurate. Although this phenomenon is not specific to e-businesses (for it is apparent in all forms of trade alike), the convenience and cost-effectiveness offered by the electronic world contribute to a higher incidence of informational confusion and falsity than in a traditional mode of trade. A list of misleading or misrepresented information in cyberspace can only be non-exhaustive. A graphical illustration, amongst others, is an indication of a price with hidden costs. Consumers, in many cases, find it blissful to be offered a discount package but subsequently become unfairly surprised at a series of hidden charges. This is particularly true of web-based click-wrap contracts. E-merchants usually hold consumers who have clicked at a designed "submission" button on the web ("I accept" or "Submit") bound by terms and conditions wrapped by their webpage even if those terms and conditions are placed in a rather unnoticeable location.

Cyberfraud may be of a criminal nature. The most common incidence is perhaps an unauthorised use of credits card numbers to make payment over the Internet. A rogue can take advantage of the

faceless nature of E-Commerce to enter credit card numbers of third persons. With advanced technologies nowadays, intangible goods such as computer programmes or music can be instantaneously downloaded from the supplier's server upon web-based credit card payment. The rogue may simply abscond in a few seconds when the download is complete. The fact that in the new trading environment netusers can easily access the Internet from public places (usually at internet cafés) where identification of users is not strictly needed renders tracing the rogue immensely difficult. Further, a diversity of methods are used in an attempt to obtain credit card numbers and pertinent information from card holders. In the easiest case, a shopkeeper might use the data derived from the customer's credit card payment slip. A case of sophistication can be illustrated by the "Microsoft" saga as to which an e-mail was, in 1997, deceitfully sent to Microsoft's customers informing the customers that Microsoft's computer system encountered a serious problem which caused a loss of certain data related to the billing record. In this connection, the email-approached customers were requested to forward their credit card numbers, bank names, addresses and other confidential data to the "MSN Credit Department" and were, as an encouragement, offered a 50 percent discount on the next monthly bill. It can be imagined how much personal information could be obtained by this crafty e-mail sender.

In addition, consumers in electronic transactions are, more often than not, irritated by privacy issues.[59] A number of webvertisements require potential customers to make an entry of such personal data as address, telephone number, profession, annual income, marital status, personal interests, hobbies, etc. The incidence of E-merchants disclosing customers' personal data to third parties for commercial purposes without customers' consent is not uncommon. On many occasions, consumers are

---

[59] For useful general discussion, see Gerald R. Ferrera *et al*, Cyber Law: Text and Cases, West Thomson Learning, 2001, pp.188 - 220; David Johnston *et al, op. cit.*, note 36 *supra*, pp.66-87.

exasperated at junk e-mail messages or postings in violation of privacy.[60] Some traders post advertisements that are specifically aimed at children and are intended to collect from children a wide reach of personal information ranging from residential addresses to parents' credit card numbers.

4.2.2 Policing Measures

All kinds of consumer risks emerging in the era of the information superhighway must be kept under immediate control and, importantly, consumers have to be made aware of these risks. Working measures, legal and extra-legal, must be at hand for preventive and remedial purposes. In this connection, the newly enacted Electronic Transactions Act does not directly deal with consumer protection. Rather, it leaves the issues to particular legislation.[61] In the contractual context, the Consumer Protection Act, B.E. 2522 (1979) provides a wide preventive net in favour of consumers. Although the Act was drafted before the advent of the digital age, it has equal application to the E-Commerce era.

To begin with, the Consumer Protection Board is equipped with the power to notify or publish information on goods or services likely to cause loss of, or prejudice to, rights of consumers. In such notification or publication, the Board may also identify the goods or services or business operators concerned.[62] The exercise of this power is evidently an efficient way to educate consumers on risks involved. Thus, a package prejudicial to consumers, as in the case of a pyramid selling scheme advertised across the Internet, also falls within the reach of this statutory arm.

---

[60] In some countries, advertising by e-mail without the consent of the recipient (the so-called *'spamming'*) is prohibited: see, for example, section 101 subpara 3 of the Telecommunications Act of Austria. For decided cases regarding spamming elsewhere, see *Cyber Promotion, Inc. v. American Online, Inc.* 948 F. Supp. 436 (E.D. Pa. 1996); *Compuserve Inc. v. Cyber Promotions* 962 F. Supp. 1015 (S.D. Ohio 1997).

[61] It is specified in section 3 paragraph two of the Act that the applicability of the Act does not prejudice any law or by-law enacted for consumer protection.

[62] Section 10 (3).

Indeed, with respect to advertisements, the Act prohibits the use of a statement that is "unfair to consumers or likely to have adverse effects on the public."[63] A statement of such an attribute, according to the elaboration under the Act itself,[64] includes a false or distorted statement, a statement threatening to cause substantial misunderstanding of the goods or services and *other statements prescribed in the Ministerial Regulation*.[65] Obviously, the catch-all expression (as italicised above) brings a variety of fraudulently crafted advertisements under the safe-guard umbrella of the Act. Moreover, an advertisement that may cause disturbance to consumers is also not allowed, as will be prescribed in the Ministerial Regulation.[66] As a result, the random transmission of junk e-mails to introduce goods or services without the consent of the recipients can be embraced by the Act as well. Violation of such statutory prohibition amounts to a criminal offence provided in the Act[67] and is also subject to the Board's order that the advertisement in question be, *inter alia*, modified.[68]

The Consumer Protection Act also attempts to ensure that only fair terms and conditions are circulated in the market place. In this connection, the Act empowers the so-called "Sub-committee on Contracts" to, by way of Notification, set out requirements for policing fairness of contract terms either through imposition of compulsory terms or through outright prohibition of certain terms.[69]

Despite a wide array of protective measures introduced by the Consumer Protection Act, it seems that provisions of the Act are not

---

[63] Section 22.

[64] Section 22, paragraph two.

[65] Section 22, paragraph two (5)

[66] Section 23.

[67] Section 48.

[68] Section 27.

[69] See the Notification of the Sub-committee on Contract Terms Designating the Credit Card Business as the Business for the Purpose of Contractual Scrutiny, B.E. 2542 (1999).

effectively enforced in the cyberspace context. At least, we have still witnessed voluminous misleading and fraudulent conduct on the Internet without consumers being adequately educated on cyberrisks. It is questionable whether officials in charge are well-trained to cope with cyberspace and information technology. It is indeed felt that the Office of the Consumer Protection Board, the Secretariat of the Board, by and large, waits for consumers' complaints rather than taking active roles in protecting them.

In addition to the Consumer Protection Act, new legislation - the Direct Selling and Direct Marketing Act, B.E. 2545 (2002) - is enacted. It is the 'direct marketing' part of the Act that bears evident relevance to electronic commerce. The Act defines "direct marketing" as "the marketing of goods or services by way of communicating information, for the purpose of making an offer to sell goods or services, directly to distant consumers, with an intention that each consumer will reply for purchasing goods or services from that direct marketing operator." Apparently, webvertisements fall within the purview of this Act, whether intentionally or inadvertently.[70] The Act, in the first place, requires those engaging in direct marketing to register with the competent officials; violation of this requirement is subject to criminal liability (imprisonment for a term not exceeding one year, or a fine not exceeding 100,000 Baht, or both, and a daily fine not exceeding 10,000 Baht throughout the violation). Secondly, the Act controls the contents of statements communicated to consumers by requiring them to comply with Ministerial Regulations. In addition, documents used in direct marketing must be furnished to consumers and must be in Thai and plain language. The Direct Selling and Direct Marketing Board, set up by the Act, is empowered to specify details of documents used by direct marketing merchants.[71] Further, the Act offers

[70] Doubt is cast on whether at the time of drafting this Act the drafters had E-Commerce in mind.

[71] Sections 28, 30 and 31.

consumers a seven-day 'cooling-off' period within which to terminate a contract.[72] Pyramid selling is outright prohibited.[73] All these mechanisms are intended to supplement the Consumer Protection Act. However, as with the experience surrounding the enforcement of the Consumer Protection Act, doubt can be cast whether this new legislation presents just added written provisions without them being put into real effect. Cardinal importance must thus be attached to real and effective enforcement of law. (In effect, the new Act does not seem to be well-crafted to suit the Internet environment. For instance, it is questionable how the registration requirement can be enforced *vis-à-vis* millions of merchants offering goods and services through the Internet websites.)

Another necessary move appears to be towards the introduction of legislation dealing with computer crime so that severe unethical conduct in cyberspace, such as unauthorised interception of data, invasion of personal data or forgery of computer data, can be punished. This endeavour has been initiated by the Government. But the process seems to drag on; no further delay is desirable.

5. Conclusion

The Electronic Transactions Act will, no doubt, contribute to a great deal of advancements both in commerce and the Government sector. Data messages are now recognised as functionally equivalent to paper documentation, so that computer-based transactions can be legally valid and enforceable. However, the Act, at this stage, appears to be a subject of complexity for both lawyers and laypersons. In order to keep pace with global development and reap full benefits flowing from the promulgation of this hi-tech legislation, we need to build up acquaintance with this masterpiece law. Indeed, despite cherished provisions of the Act, several

---

[72] Sections 33 - 36

[73] Section 19.

issues remain controversial, including, in particular, issues related to electronic contracting. Courts and adjudicating bodies will certainly have to attempt answers to these unresolved questions in order to build up greater confidence on the part of both traders and consumers. In addition, authorities concerned need to move forward towards effective measures preventing risks and harm posed by cyberspace.

References

Bainbridge D. (2000) *Introduction to computer law*, 4th edition, Pearson on Education.

Brinson D. *et al.* (2000) *Internet Law and business handbook*, Ladera Press.

Chisick M. *et al.* (2000) *Electronic commerce: law and practice,* 2nd edition, London: Sweet & Maxwell.

Edwards L. *et al.* (2000), *Law and the internet: a framework for electronic commerce*, 2nd edition, Hart Publishing, Oxford.

Johnston D. *et al.* (1998) *Cyber law*, Selangor, Pelanduk Publications.

National Electronics and Computer Technology Center, (2001), *Compilation of draft information technology laws*, Guest Design And Print, Bangkok.

Nanakorn, P. (2000) Law on electronic commerce and electronic signatures. *Thai Bar Association Law Journal*, 56(2), pp.1-42.

Nanakorn, P. (2000) Consumer protection in e-commerce and direct sales in Thailand. *Proceedings for the Workshop on "Law on Consumer Protection" organised by the Faculty of Law, Thammasat University in association with the Ministry of International Trade and Industry of Japan and the Institute of Developing Economies of Japan,* 19-20 December 2000.

UNCITRAL (1996) *Guide to Enactment of the Model Law on Electronic Commerce.*

UNCITRAL (2001) *Guide to Enactment to the Model Law on Electronic Signatures.*

UNCITRAL (2002) Working Group on Electronic Commerce, A/CN.9/WG.IV/WP.95 (Legal aspects of electronic commerce, Electronic contracting: provisions for a draft convention, Note by the Secretariat, thirty-ninth session, New York, 11-15 March 2002.

UNCITRAL (2002) A/CN.9/527 (Report of the Working Group IV (Electronic Commerce) on the work of its fortieth session, Vienna, 18-14 October 2002.