Computer Crime Act

B.E 2550 (2007)

Bhumibol Adulyadej, Rex.

Given on this 10th day of June B.E. 2550 (2007)
Being the 62nd year if the present reign.

His Majesty King Bhumibol Adulyadej has been pleasantly pleased to proclaim that as it is deemed appropriate to enact a law governing the commission of a computer-related offence.

His Majesty, therefore, granted His Royal assent for the promulgation of the Computer Crime Act in accord with the recommendation and consent of the National Legislative Assembly as follows:

Section 1 This Act shall be called the "Computer Crime Act B.E 2550 (2007)".

Section 2 This Act will come into force 30 days following the date of its publication in the Government Gazette.

Section 3 In this Act,

"Computer System" means a piece of equipment or sets of equipment units, whose function is integrated together, for which sets of instructions and working principles enable it or them to perform the duty of processing data automatically.

"Computer Data" means data, statements, or sets of instructions contained in a computer system, the output of which may be processed by a computer system including electronic data, according to the Law of Electronic Transactions.

"Computer Traffic Data" means data related to computer system-based communications showing sources of origin, starting points, destinations, routes, time, dates, volumes, time periods, types of services or others related to that computer system's communications.

"Service Provider" shall mean:

(1) A person who provides service to the public with respect to access to the Internet or other mutual communication via a computer system, whether on their own behalf, or in the name of, or for the benefit of, another person

(2) A person who provides services with respect to the storage of computer data for the benefit of the other person

"Service User" means a person who uses the services provided by a service provider, with or without fee

"Competent Official" means a person appointed by a Minister to perform duties under this Act.

"Minister" means a Minister who has responsibility and control for the execution of this Act.

Section 4. The Minister of Information and Communications Technology shall have responsibility and control for the execution of this Act and shall have the authority to issue a Ministerial Rule for the purpose of the execution of this Act.

A Ministerial Rule shall be enforceable upon its publication in the Government Gazette.

Chapter 1

Computer-Related Offences

Section 5. Any person illegally accessing a computer system for which a specific access prevention measure that is not intended for their own use is available shall be subject to imprisonment for no longer than six months or a fine of not more than ten thousand baht or both.

Section 6. If any person knowing of a measure to prevent access to a computer system specifically created by a third party illegally discloses that measure in a manner that is likely to cause damage to the third party, then they shall be subject to imprisonment for no longer than one year or a fine of not more than twenty thousand baht or both.

Section 7. If any person illegally accesses computer data, for which there is a specific access prevention measure not intended for their own use available, then he or she shall be subject to imprisonment for no longer than two years or a fine of not more than forty thousand baht or both.

Section 8. Any person who illegally commits any act by electronic means to eavesdrop a third party's computer data in process of being sent in a computer system and not intended for the public interest or general people's use shall be subject to imprisonment for no longer than three years or a fine of not more than sixty thousand baht or both.

Section 9. Any person who illegally damages, destroys, corrects, changes or amends a third party's computer data, either in whole or in part, shall be subject to imprisonment for no longer than five years or a fine of not more than one hundred thousand baht or both.

Section 10. Any person who illegally commits any act that causes the working of a third party's computer system to be suspended, delayed, hindered or disrupted to the extent that the computer system fails to operate normally shall be subject to imprisonment for no longer than five years or a fine of not more than one hundred thousand baht or both.

Section 11 Any person sending computer data or electronic mail to another person and covering up the source of such aforementioned data in a manner that disturbs the other person's normal operation of their computer system shall be subject to a fine of not more than one hundred thousand baht.

Section 12. The perpetration of an offence under Section 9 or Section 10 that:

(1) causes damage, whether it be immediate or subsequent and whether it be synchronous to the public shall be subject to imprisonment for no longer than ten years or a fine of not more than two hundred thousand baht.

(2) is an act that is likely to damage computer data or a computer system related to the country's security, public security and economic security or public services or is an act against computer data or a computer system available for public use shall be subject to imprisonment from three years up to fifteen years and a fine of sixty thousand baht up to three hundred thousand baht.

The commission of an offence under (2) that causes death to another person shall be subject to imprisonment from ten years up to twenty years.

Section 13. Any person who sells or disseminates sets of instructions developed as a tool used in committing an offence under Section 5, Section 6, Section 7, Section 8, Section 9, Section 10 and Section 11 shall be subject to imprisonment for not more than one year or a fine of not more than twenty thousand baht, or both.

Section 14. If any person commits any offence of the following acts shall be subject to imprisonment for not more than five years or a fine of not more than one hundred thousand baht or both:

(1) that involves import to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to that third party or the public;

(2) that involves import to a computer system of false computer data in a manner that is likely to damage the country's security or cause a public panic;

(3) that involves import to a computer system of any computer data related with an offence against the Kingdom's security under the Criminal Code;

(4) that involves import to a computer system of any computer data of a pornographic nature that is publicly accessible;

(5) that involves the dissemination or forwarding of computer data already known to be computer data under (1) (2) (3) or (4);

Section 15. Any service provider intentionally supporting or consenting to an offence under Section 14 within a computer system under their control shall be subject to the same penalty as that imposed upon a person committing an offence under Section 14.

Section 16. Any person, who imports to a computer system that is publicly accessible, computer data where a third party's picture appears either created, edited, added or adapted by electronic means or otherwise in a manner that is likely to impair that third party's reputation or cause that third party to be isolated, disgusted or embarrassed, shall be subject to imprisonment for not longer than three years or a fine of not more than sixty thousand baht, or both.

If the commission under paragraph one is a trustworthy action the perpetrator is not guilty.

An offence under paragraph one shall be a compoundable offence.

If a party injured by an offence under paragraph one has died before filing a complaint, then their parents, spouse or children may file a complaint and shall be deemed to be the injured party.

Section 17. Any person committing an offence against this Act outside the Kingdom and;

(1) the offender is Thai and the government of the country where the offence has occurred or the injured party is required to be punished or;

(2) the offender is a non-citizen and the Thai government or Thai person who is an injured party or the injured party is required to be punished;

shall be penalized within the Kingdom.

Chapter 2
Competent Officials

Section 18. Within the power of Section 19 and for the benefit of an investigation, if there is reasonable cause to believe that there is the perpetration of an offence under this Act, then a relevant competent official shall have any of the following authorities only as necessary to identify a person who has committed an offence in order to:

(1) issue an inquiry letter to any person related to the commission of an offence under this Act or summon them to give statements, forward written explanations or any other documents, data or evidence in an understandable form.

(2) call for computer traffic data related to communications from a service user via a computer system or from other relevant persons.

(3) instruct a service provider to deliver to a relevant competent official service users-related data that must be stored under Section 26 or that is in the possession or under the control of a service provider;

(4) copy computer data, computer traffic data from a computer system, in which there is a reasonable cause to believe that offences under this Act have been committed if that computer is not yet in the possession of the competent official;

(5) instruct a person who possesses or controls computer data or computer data storage equipment to deliver to the relevant competent official the computer data or the equipment pieces;

(6) inspect or access a computer system, computer data, computer traffic data or computer data storage equipment belonging to any person that is evidence of, or may be used as evidence related to, the commission of an offence or used in identifying a person who has committed an offence, and instruct that person to send the relevant computer data to all necessary extent as well;

(7) decode any person's computer data or instruct any person related to the encryption of computer data to decode the computer data or cooperate with a relevant competent official in such decoding;

(8) seize or attach the suspect computer system for the purpose of obtaining details of an offence and the person who has committed an offence under this Act;

Section 19. The power of authority of the relevant competent official under Section 18 (4), (5), (6), (7) and (8), is given when that competent official files a petition to a court with jurisdiction for an instruction to allow the relevant competent official to take action.

However, the petition must identify a reasonable ground to believe that the offender is committing or going to commit an offence under the Act as well as the reason of requesting the authority, including the characteristics of the alleged offense, a description of the equipment used to commit the alleged offensive action and details of the offender, as much as this can be identified. The court should adjudicate urgently such aforementioned petition.

When the court approves permission, and before taking any action according to the court's instruction, the relevant competent official shall submit a copy of the reasonable ground memorandum to show that an authorization under Section 18 (4), (5), (6), (7) and (8), must be employed against the owner or possessor of the computer system, as evidence thereof. If there is no owner of such computer thereby, the relevant competent official should submit a copy of said memorandum as soon as possible.

In order to take action under Section 18 (4), (5), (6), (7) and (8), the senior officer of the relevant competent official shall submit a copy of the memorandum about the description and rationale of the operation to a court with jurisdiction within forty eight (48) hours after the action has been taken as evidence thereof.

When copying computer data under Section 18 (4), and given that it may be done only when there is a reasonable ground to believe that there is an offence against the Act, such action must not excessively interfere or obstruct the business operation of the computer data's owner or possessor.

Regarding seizure or attachment under Section 18 (8), a relevant competent official must issue a letter of seizure or attachment to the person who owns or possesses that computer system as evidence. This is provided, however, that the seizure or attachment shall not last longer than thirty days. If seizure or attachment requires a longer time period, a petition shall be filed at a court with jurisdiction for the extension of the seizure or attachment time period. The court may allow only one or several time extensions, however altogether for no longer than sixty days. When that seizure or attachment is no longer necessary, or upon its expiry date, the competent official must immediately return the computer system that was seized or withdraw the attachment.

The letter of seizure or attachment under paragraph one shall be in accordance with a Ministerial Rule.

Section 20. If an offence under this Act is to disseminate computer data that might have an impact on the Kingdom's security as stipulated in Division 2 type 1 or type 1/1 of the Criminal Code, or that it might be contradictory to the peace and concord or good morals of the people, the competent official appointed by the Minister may file a petition together with the evidence to a court with jurisdiction to restrain the dissemination of such computer data.

If the court gives an instruction to restrain the dissemination of computer data according to paragraph one, the relevant competent official shall conduct the restraint either

by himself or instruct the Service Provider to restrain the dissemination of such computer data.

Section 21. If a relevant competent official found that any computer data contains undesirable sets of instructions, a relevant competent official with the authority to prohibit the sale or dissemination of such, may instruct the person who owns or possesses the computer data to suspend the use of, destroy or correct the computer data therein, or to impose a condition with respect to the use, possession or dissemination of the undesirable sets of instructions.

The undesirable sets of instructions under paragraph one shall mean to include sets of instructions that cause computer data, a computer system or other instruction sets to be damaged, destroyed, corrected, changed, added, interrupted or, fail to perform according to pre-determined instructions or otherwise as required by a relevant Ministerial Rule, with the exception of sets of instructions aimed at preventing or correcting the foregoing sets of instructions as required by a Minister and published in the Government Gazette.

Section 22. A relevant competent official shall not disclose or deliver computer data, computer traffic data or service users' data acquired under Section 18 to any person.

The provisions under paragraph one shall not apply to any actions performed for the benefit of lodging a lawsuit against a person who has committed an offence under this Act or for the benefit of lodging a lawsuit against a relevant competent official on the grounds of their abuse of authority or for action taken according to a court's instruction or permission.

Any competent official who violates paragraph one must be subject to imprisonment for no longer than three years or a fine of not more than sixty thousand baht, or both.

Section 23. Any competent official who commits an act of negligence that causes a third party to know of computer data, computer traffic data or a service user's data acquired under Section 18 must be subject to imprisonment for no more than one year or a fine of not more than twenty thousand baht, or both.

Section 24. Any person knowing of computer data, computer traffic data or a service user's data acquired by a relevant competent official under Section 18 and disclosing it to any person shall be subject to imprisonment for no longer than two years or a fine of not more than forty thousand baht, or both.

Section 25. Data, computer data or computer traffic data that the competent official acquired under this Act shall be admissible as evidence under the provision of the Criminal

Procedure Code or other relevant law related to the investigation, however, it must not be in the way of influencing, promising, deceiving or other wrongful ways.

Section 26. A service provider must store computer traffic data for at least ninety days from the date on which the data is input into a computer system. However, if necessary, a relevant competent official may instruct a service provider to store data for a period of longer than ninety days but not exceeding one year on a special case by case basis or on a temporary basis.

The service provider must keep the necessary information of the service user in order to be able to identify the service user from the beginning of the service provision, and such information must be kept for a further period not exceeding ninety days after the service agreement has been terminated.

The types of service provider to whom the provisions under paragraph one shall apply and the timing of this application shall be established by a Minister and published in the Government Gazette.

A service provider who fails to comply with this Section must be subject to a fine of not more than five hundred thousand baht.

Section 27. If any person fails to comply with the instructions of court or relevant competent official under Section 18 or Section 20 or fails to comply with the court's instruction under Section 21 shall be subject to a fine of not more than two hundred thousand baht and a further daily fine of not more than five thousand baht until the relevant corrective action has been taken.

Section 28. Regarding the appointment of a competent official under this Act, the Minister shall appoint persons with knowledge of, and expertise in, computer systems and having the qualifications as required by the Minister.

Section 29. In performance of the duties under this Act, the competent official appointed by the Minister shall be an administrative officer or a senior police officer under the Criminal Procedure Code competent to receive a petition or accusation and be authorized to investigate only on an offence under this Act.

In arresting, controlling, searching, investigating, and filing a lawsuit against a person who commits an offence under this Act, and for what is within the authority of an administrative officer or a senior police officer, such competent officer shall coordinate with the relevant investigating officer in charge to take action within their authorized duties.

The Prime Minister is in charge of the Royal Thai Police Headquarters and with a Minister shall have a joint authority to establish a regulation with respect to the means and action-related procedures under paragraph two.

Section 30. In the performance of duties, a relevant competent official must produce an identity card to a relevant person.

The identity card shall be as per the form required by a Minister and published in the Government Gazette.

Countersigned

General Surayud Chulanont

Prime Minister

Remark:- The rationale for the issue of this Act as of today is that a computer system is essential to business operations and the human way of life, as such, if any person commits an act that disables the working of a computer system according to the pre-determined instructions or that causes a working error – a deviation from that required by the pre-determined instructions or that resorts to any means to illegally know of, correct or destroy a third party's data contained in a computer system or that uses a computer system to disseminate false or pornographic computer data, then that act will damage and affect the country's economy, society and security including people's peace and good morals. Therefore, it is deemed appropriate to stipulate measures aimed at preventing and suppressing such acts. Hence the enactment of this Act.