

Computer-Related Crime Act

B.E. 2550 (2007)

BHUMIBOL ADULYADEJ, REX.

Given on the 10th of June B.E. 2550;
Being the 62nd Year of the Present Reign.

His Majesty King Bhumibol Adulyadej is graciously pleased to proclaim that:

Whereas it is expedient to have the law on computer related crime;

Be it, therefore, enacted by the King, by and with the advice and consent of the National Legislative Assembly, as follows:

.....
Section 1 This Act shall be called the “Computer-Related Crime Act B.E. 2550”

Section 2 This Act shall come into force after thirty days following the date of its publication in the Government Gazette

Section 3 In this Act:

“**computer system**” means any device or a group of interconnected or related devices, one or more of which pursuant to a program or instruction or anything else, performs automatic processing of data.

“computer data” means information, messages and concepts or instruction, a program or anything else in a form suitable for processing in a computer system and shall include electronic data under the law on electronic transaction.

“traffic data” means any data relating to communication by means of a computer system, indicating the communication’s origin, destination, route, time, date, size, duration, type of underlying service, or other information relating to communication of such a computer system.

ขอขอบคุณ ดร.ดวงทิพย์ สุรินทาธิป และบริษัท ขวลิต แอนด์เอสโซซิเอทส์ จำกัด ที่ได้ช่วยตรวจแก้และปรับปรุงร่างกฎหมายฉบับแปลของสำนักงานเลขาธิการคณะกรรมการคุ้มครองทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติจนแล้วเสร็จ ขณะนี้ร่างกฎหมายฉบับแปลอยู่ระหว่างการตรวจพิจารณาของสำนักงานคณะกรรมการกฤษฎีกา เพื่อให้เป็น Official Translation ต่อไป

“service provider” means:

(1) a person who, either in his own name or in the name or for the benefit of another person, provides to other persons with access to the internet or the ability to communicate by other means through a computer system.

(2) a person who stores computer data for the benefit of other persons.

“user” means a person who uses the service of the service provider with or without pay.

“competent official” means a person appointed by the minister for the execution of this Act.

“Minister” means the Minister having charge and control of this Act.

Section 4 The Minister of the Information and Communication Technology Ministry shall have charge and control of this Act and shall have the power to issue Ministerial Regulations for the execution of this Act.

Such Ministerial Regulations shall come into force upon their publication in the Government Gazette.

Part 1

Computer-Related Offences.

Section 5 Whoever illegally accesses to a computer system that has specific security measures and such security measures are not intended for his use, shall be liable to imprisonment for a term not exceeding six months or to a fine not exceeding ten thousand Baht or to both.

Section 6 Whoever having knowledge of the security measures to access to a computer system created specifically by another person ,discloses, without right, such security measures in a manner that is likely to cause damage to another person, shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding twenty thousand Baht or to both.

Section 7 Whoever illegally accesses to a computer data that has specific security measures which are not intended for his use, shall be liable to imprisonment for a term not exceeding two years or to a fine not exceeding forty thousand Baht or to both.

Section 8 Whoever illegally makes, by any electronic means, an interception of computer data of another person that is being transmitted in a computer system and such computer data is not for the benefit of the public or is not available for other persons to utilize, shall be liable to imprisonment for a term not exceeding three years or to a fine not exceeding sixty thousand Baht or to both.

Section 9 Whoever illegally acts in a manner that causes damage, impairment, deletion, alteration or addition either in whole or in part of computer data of another person, shall be liable to imprisonment for a term not exceeding five years or to a fine not exceeding one hundred thousand Baht or to both.

Section 10 Whoever illegally acts in a manner that causes suspension, deceleration, obstruction or interference of a computer system of another person so that it cannot function normally shall be liable to imprisonment for a term not exceeding five years or a fine not exceeding one hundred thousand Baht or to both.

Section 11 Whoever sends computer data or an electronic mail to another person while hiding or faking its sources, in a manner that interferes with such another person's normal utilization of the computer system, shall be liable to a fine not exceeding one hundred thousand Baht.

Section 12 If the offences under Section 9 or 10

(1) result in damage to the general public, whether the damage takes place immediately or afterwards or simultaneously, the offender shall be liable to imprisonment for a term not exceeding ten years, or to a fine not exceeding two hundred thousand Baht.

(2) are committed in a manner that is likely to cause damage to computer data or computer systems relating to national security, public safety, economic stability or public utilities, or committed against computer data or a computer system that is available for the benefit of the public, the offender shall be liable to imprisonment for a term from three to fifteen years and to a fine from sixty thousand Baht to three hundred thousand Baht.

If the offence under (2) causes death to another person, the offender shall be liable to imprisonment for a term from ten to twenty years.

Section 13 Whoever sells or disseminates a program specifically designed for the purpose of committing offences under Section 5 to Section 10 or Section 11 shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding twenty thousand Baht or to both.

Section 14 Whoever commits the following acts shall be liable to imprisonment for a term not exceeding five years or to a fine not exceeding one hundred thousand Baht or both:

(1) input into a computer system wholly or partially fake or false computer data that is likely to cause damage to another person or the public;

(2) input into a computer system false computer data in a manner that is likely to undermine national security or to cause public panic;

(3) input into a computer system computer data that is an offence against national security or terrorism according to the Criminal Code.

(4) input into a computer system pornographic computer data that is accessible to the public;

(5) publish or forward any computer data with the full knowledge that such computer data is under paragraph (1), (2) (3) or (4);

Section 15 Any service provider, who intentionally supports or gives consent to the commission of an offence under Section 14 in the computer system in his control, shall be liable to the same penalty as provided in Section 14.

Section 16 Any person inputs into a computer system, that is available to the public, photographs of another person and such photographs are developed, edited, added or altered by electronic or any other means in a manner that is likely to impair the reputation of that other person, to expose that other person to hatred, contempt or humiliation, shall be liable to imprisonment for a term not exceeding three years or to a fine not exceeding sixty thousand Baht or to both.

If any person acts under paragraph one with honest intent, he is not guilty.

The offence under paragraph one is a compoundable offence.

If the aggrieved party dies before lodging a complaint, the parents, spouse or children of the aggrieved party shall be entitled to lodge the complaint and shall be deemed to be an injured party.

Section 17 Whoever commits an offence pursuant to this Act outside the Kingdom , whether

(1) the offender be a Thai person, and there be a request for punishment by the Government of the country where the offence has occurred or by the injured person ; or

(2) the offender be an alien, and the Royal Thai Government or a Thai person be the injured person, and there be a request for punishment by the injured person,

shall be punished in the Kingdom.

Part 2

Competent Officials

Section 18 Subject to Section 19, for the purpose of investigation and interrogation, in case where there is reasonable ground for believing that an offence has been committed under this Act, the competent official shall have the following powers, as deemed necessary for the purpose of providing evidence related to the offence or of the search for the offender :

(1) to notify or summon in writing any person who is involved in the offence prescribed by this Act to give statement or to submit declaration letter, documents, information or other evidence in an understandable form;

(2) to require traffic data from the service provider who is in charge of communications through the computer system or other relevant;

(3) to require the service provider to submit to the competent official user's information that is required to be kept under Section 26 or is in his possession or control;

(4) to copy the computer data and traffic data from the computer system that is suspected of having been used for committing the offence under this Act., in case where the computer system is not in the possession of the competent official;

(5) to require the possessor or controller of the computer data or equipment storing the computer data to deliver to him such computer data or equipment;

(6) to access the computer system, traffic data, or computer data of any person in order to ascertain the offender and in case where it is required, the competent official may also instruct such a person to deliver to him all relevant computer data as deemed necessary;

(7) to decrypt any person's computer data or to require a person who is involved in encryption of computer data to decrypt it or to cooperate with the competent official in carrying out the decryption;

(8) to seize or attach as necessary the computer system for the purpose of identifying details of the offence or the offender under this Act.

Section 19 In exercising his power under Section 18 (4) (5) (6) (7) and (8) the competent official shall submit a request to the competent court for a permission to implement the request. The request should identify reasonable grounds for believing that any person has committed or about to commit an offence under this Act, reasons for exercising this power, the manner of the offence, details of devices used in committing the offence and of the offender to the extent possible. In determining the request, the court shall proceed in a speedy manner.

After the court has granted the permission, the competent official shall, before implementing the court's order, send a copy of a note stating the reasonable grounds for the exercise of his powers under Section 18 (4) (5) (6) (7) and (8) to the owner or possessor of the computer system as evidence. In the absence of the owner or possessor, the competent official shall send a copy of the note to the said owner or possessor promptly.

The competent official who is the chief implementer under Section 18 (4) (5) (6) (7) and (8) shall submit to the competent court a copy of records detailing implementation and its reasons within forty-eight hours as evidence.

A copy of computer data under Section 18 (4) could be made only when there are reasonable grounds to believe that an offence has been committed under this Act. It should not pose unnecessary obstacles to the operations of the owner or possessor of the computer data.

The competent official must send a copy of the seizure or attachment under Section 18 (8), to the owner or the possessor of the computer system as evidence. However, the seizure or attachment shall not last longer than thirty days. If it is necessary to extend the period of seizure or attachment, a request could be submitted to the competent court for such an extension. The court shall allow a maximum period of sixty days extension either for one or several requests put together.

When it is no longer necessary to seize or to attach or upon the expiry of such period, the competent official must proceed to return the computer system promptly

Summons of seizure or attachment under paragraph five shall be in accordance with the rules and procedures prescribed in the Ministerial Regulations.

Section 20 In the case where an offence committed under this Act involves disseminating computer data that could undermine national security as prescribed in the Criminal Code, or is against the public peace or good morals, the competent official, with the Minister's approval, may submit a request with evidence to the competent court for an order to suspend/block the dissemination of such computer data.

Section 21 In case where the competent official finds that any computer data comprises undesirable programs, the competent official has the power to prohibit its sale or dissemination or to instruct the owner or the possessor of the computer data to cease using, to destroy or to alter such computer data or may specify conditions of use, possession, or dissemination of such undesirable programs.

An undesirable program in paragraph one shall mean any program which causes damage to computer data, computer systems, or other computer programs by destroying, altering, changing or corrupting them, and rendering them unable to function as instructed or being in conditions as specified by the Ministerial Regulations. However, exception is made for a program which aims at protecting or modifying such undesirable programs as stipulated by the Minister in the Government Gazette.

Section 22 The competent official is prohibited from disclosing or delivering computer data, traffic data or user's data that have been obtained under Section 18 to any person.

Paragraph one shall not apply to the acts carried out for the benefit of legal actions against the offender under this Act or for the benefit of legal actions against the competent official on the ground of wrongful exercise of his power or the act done in accordance with the court's order.

The competent official who is in breach of paragraph two shall be liable to imprisonment for a term not exceeding three years or to a fine not exceeding sixty thousand Baht or to both.

Section 23 Any competent official commits an act by negligence and thereby causing another person to gain a knowledge of computer data, traffic data or user's information obtained by means provided in Section 18, shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding twenty thousand Baht or to both.

Section 24 Whoever having gained a knowledge of the computer data, traffic data or user's information which the competent official has obtained according to Section 18, discloses the same to a third party, shall be liable to imprisonment for a term not exceeding two years or to a fine not exceeding forty thousand Baht or to both.

Section 25 Data, computer data, traffic data or user's information, obtained by the competent official under this Act, shall be used and admissible as evidence according to the provision of the Criminal Procedure Code or other laws that have relevant provision on taking evidence except that such evidence must not be obtained by means of persuasion, promises, threat, swindling or other illegal actions.

Section 26 A service provider shall keep traffic data for not less than ninety days from the day when such data has been entered into a computer system. If necessary, the competent official shall, as a particular case and time, instruct any service provider to keep traffic data for over ninety days but not exceeding one year.

A service provider shall keep user's data as necessary for the purpose of identifying the user from the first day of such a service and store such user data for not less than ninety days from its expiry date.

The Minister shall prescribe the type of service providers, how and when the provisions in paragraph one shall apply by promulgation in the Government Gazette,

Any service provider, who fails to comply with this Section, shall be liable to a fine not exceeding five hundred thousand Baht.

Section 27 Whoever fails to comply with an order of the court or the competent official pursuant to Section 18 or Section 20 or fails to comply with the court order pursuant to Section 21, shall be liable to a fine not exceeding two hundred thousand Baht and a daily fine not exceeding five thousand Baht until the order or condition is properly complied with.

Section 28 Under this Act, the Minister shall appoint the competent officials who have knowledge and expertise in computer systems and other qualifications as determined by the Minister.

Section 29 In performing his duties under this Act, the competent official designated by the Minister shall be deemed to be a senior administrative officer or a senior police officer under the Criminal Procedure Code having the authority to receive complaint or accusation, and to investigate and interrogate only of offences under this Act.

In arresting, confining, searching, investigating and instituting criminal prosecution against the offender under this Act within the authorities prescribed by the Criminal Procedure Code of a senior administrative officer or a senior police officer or an investigating officer, the competent official shall coordinate with the investigating officer who will proceed further within his authority.

The Prime Minister whose mandate is to control and supervise the National Police Bureau, together with the Minister, shall jointly stipulate those regulations relating to the guidelines and procedural methods for the action described in paragraph two.

Section 30 In carrying out his duties under this Act, the competent official shall present his identity card to the person involved.

The identity card under paragraph one shall be in the form as prescribed by the Minister by promulgation in the Government Gazette.

Countersigned by

General Surayud Chulanont

Prime Minister

Rationale: Nowadays computer systems play a significant role in business operations and people's lifestyle. If a person commits any act in a manner that causes computer malfunctioning as programmed or failing to perform as instructed or illegally accesses, compromises , alters or destroys data belonging to another person in the computer system or uses the computer system for dissemination of false or pornographic computer data, it will cause damage and adverse effects to the society, economy and national security including public peace and good morals. It is therefore expedient to impose measures for prevention and suppression of such acts, and to promulgate this Act.