Unofficial Translation

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 Legislation Assembly, as follows:

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

Section 2[1] This Act shall come into force after thirty days as from 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.

"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.

---

[1] Government Gazette, Volume 124 / Part 27 Gor / Page 4 / 18 June B.E. 2550 (A.D.2007).

"user" means a person who uses the service of the service provider regardless of whether 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 the execution of this Act.

Section 4[2] The Minister of the Ministry of Digital Economy and Society (the "**Minister**") shall have charge and control of the execution of this Act and shall have the authority to appoint the competent officials as well as to issue Ministerial Regulations and Notifications of the Ministry for the purpose of execution of this Act.

Ministerial Regulations and Notifications of the Ministry shall become effective 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/her use, shall be liable to an imprisonment for a term not exceeding six months, ora fine not exceeding TenThousand Baht or both.

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

Section 7 Whoever illegally accesses to a computer data that has specific security measures which are not intended for his/her use, shall be liable to an imprisonment for a term not exceeding two years, or a fine not exceeding Forty Thousand Baht or 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 any other persons to generally utilize, shall be liable to an imprisonment for a term not exceeding three years, or a fine not exceeding Sixty Thousand Baht or 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

[2] Section 4 is repealed and replaced by of the Computer-Related Crime Act No. 2, B.E. 2560.

person, shall be liable to an imprisonment for a term not exceeding five years, or a fine not exceeding One Hundred Thousand Baht or 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 an imprisonment for a term not exceeding five years, or a fine not exceeding One Hundred Thousand Baht or 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.

Whoeversends computer data or electronic mail to another person in a manner that disturbs the recipient, without giving the recipient an easy opportunity to cancel or notify his/her wish to deny receipt of such computer data or electronic mails, shall be liable to a fine not exceeding Two Hundred Thousand Baht.[3]

The Minister shall prescribe and announce the characteristic and method of sending computer data or electronic mail, including the characteristic and size of the computer data or electronic mail which shall not be considered as disturbing the recipient, as well as the manner in which the recipient can easily cancel or notify his/her wish to deny receipt of such computer data or electronic mails.[4]

Section 12[5] In case the perpetration of an offence under Section 5, Section 6, Section 7, Section 8 or Section 11 is associated with computer data or the computer system(s)that relates to the national security and safety, the public security,the economic security of the Kingdom of Thailand, or the basic infrastructure for the public interest, the offender shall be liable to an imprisonment for a term of one year to seven years, or a fine of Twenty Thousand Baht to One Hundred Forty Thousand Baht or both.

In case the perpetration of the offence under Paragraph 1 causes damage to such computer data or computer system, the offender shall be liable to an imprisonment for a term of one year to ten years and a fine of Twenty Thousand Baht to Two Hundred Thousand Baht.

In case the perpetration of the offence under Section 9 or Section 10 is associated with computer data or computer system as specified in Paragraph 1, the offender shall be liable to an imprisonment for a term of three years to fifteen years and a fine of Sixty Thousand Baht to Three Hundred Thousand Baht.

---

3 Section 11, Paragraph 2 is added by the Computer-Related Crime Act (No. 2) B.E. 2560.

4 Section 11, Paragraph 3 is added by the Computer-Related Crime Act (No. 2) B.E. 2560.

5 Section 12 is repealed and replacedby of the Computer-Related Crime Act (No. 2) B.E. 2560.

In case the perpetration of the offence under Paragraph 1 or Paragraph 3 is committed without any intent to kill but has caused the death of another person, the offender shall be liable to an imprisonment for a term of five years to twenty years and a fine of One Hundred Thousand Baht to Four Hundred Thousand Baht.

Section 12/1[6] In case the perpetration of the offence under Section 9 or Section 10 has caused harm to another person or damaged another person's property, the offender shall be liable to an imprisonment for a term not exceeding ten years and a fine not exceeding Two Hundred Thousand Baht.

In case the perpetration of the offence under Section 9 or Section 10 is performed without any intention to kill but has inadvertently caused the death of another person, the offender shall be liable to an imprisonment for a term of five years to twenty years and a fine of One Hundred Thousand Baht to Four Hundred Thousand Baht.

Section 13 Whoever distributes or disseminates a computer program created specifically for the purpose of committingan offence under Section 5, Section 6, Section 7, Section 8, Section 9, Section 10 or Section 11 shall be liable to an imprisonment for a term not exceeding one year, or a fine not exceeding Twenty Thousand Baht or both.

Whoeverdistributes or disseminates a computer program created specifically for the purpose of committing an offence under Section 12, Paragraph 1 or Paragraph 3, shall be liable to an imprisonment for a term not exceeding two years, or a fine not exceeding Forty Thousand Baht or both.[7]

Whoeverdistributes or disseminates a computer program created specifically for the purpose of committing an offence under Section 5, Section 6, Section 7, Section 8, Section 9, Section 10 or Section 11, if the person who uses such computer program commits an offence under Section 12, Paragraph 1 or Paragraph 3, or is liable to the penalty under Section 12, Paragraph 2 or Paragraph 4 or Section 12/1; such person who distributes or disseminates such computer program shall also be liable to a higher degree of penalty if he/she knew or might have been aware of the consequences that have occurred.[8]

Whoeverdistributes or disseminates a computer program created specifically for use as a tool to commit an offence under Section 12, Paragraph 1 or Paragraph 3 or is liable to the penalty under Section 12, Paragraph 2 or Paragraph 4 or Section 12/1, such person who distributes or disseminates such computer program shall also be liable to a higher degree of penalty.[9]

---

6 Section 12/1 is added by the Computer-Related Crime Act (No. 2) B.E. 2560.

7 Section 13, Paragraph 2 is added by the Computer-Related Crime Act (No. 2), B.E. 2560.

8 Section 13, Paragraph 3 is added by the Computer-Related Crime Act (No. 2), B.E. 2560.

9 Section 13, Paragraph 4 is added by the Computer-Related Crime Act (No. 2), B.E. 2560.

In case the distributor or disseminator is also liable to a penalty under Paragraph 1 or Paragraph 2 and under Paragraph 3 or Paragraph 4, such offender shall be subject to only the highest degree of penalty under one count.[10]

Section 14[11]Whoever commits the following offences shall be liable to an imprisonment for a term not exceeding five years, or a fine not exceeding One Hundred Thousand Baht or both.

(1) Dishonestly or by deception, entering wholly or partially distorted or false computer data into a computer system in a manner likely to cause damage to the general public; which is not a defamation under the Criminal Code;

(2) Entering false computer data into a computer system in a manner which is likely to cause damage to the protection of national security, public safety, economic safety of the Kingdom of Thailand, infrastructures which are for public benefit; or to cause panic to the general public;

(3) Entering into a computer system, any computer data which is an offence related to national security of the Kingdom of Thailand or related to terrorism under the Criminal Code;

(4) Entering any obscene data into a computer system which could be accessed by the general public; or

(5) Disseminating or forwarding computer data despite knowing of the fact that it is computer data under (1), (2), (3), or (4) above.

In case the offence under Paragraph (1) is not committed against the general public but rather against a certain person, the offender, the disseminator or the forwarder of such computer data shall be liable to an imprisonment for a term not exceeding three years, a fine not exceeding Sixty Thousand Baht or both; and such offence shall be deemed a compoundable offence.

Section15[12]A service provider, who cooperates, consents or supports the perpetration of the offences under Section 14 by usinga computer system under his/her control, shall be liable to the same penalty as the offender under Section 14.

The Minister shall issue a Notification specifying the process of warning,as well as blocking the dissemination of such computer data and removal of such computer data from the computer system.

---

[10] Section 13, Paragraph 5 is added by the Computer-Related Crime Act (No. 2), B.E. 2560.

[11] Section 14 is repealed and replaced by the Computer-Related Crime Act (No. 2), B.E. 2560.

[12] Section 15 is repealed and replaced by the Computer-Related Crime Act (No. 2), B.E. 2560.

A service provider who can prove that he/she has complied with the Notification of the Ministry issued under Paragraph 2, shall not be subject to the penalty.

Section 16[13]Whoever enters a picture of another person into computer system where such picture was created, edited, added or amended electronically or by any other means in a manner which is likely to cause such other person to be defamed, denounced, detested or humiliated, shall be liable to an imprisonment for a term not exceeding three years and a fine not exceeding Two Hundred Thousand Baht.

In case the offence under Paragraph 1 is committed against a picture of a deceased person, whereupon such action is likely to cause the parents, spouse, or offspring of such deceased person to be defamed, denounced, detested or humiliated; the offender shall be subject to the penalty as specified in Paragraph 1.

In case the act of entering such picture into a computer system as described in Paragraph 1 or Paragraph 2 is made in good faith, with fair comments given towards any person or thing which is considered to be of a regular manner of the general public, the offender shall not be guilty.

The offences stated under Paragraph 1 and Paragraph 2 are compoundable offences.

In case the injured person under Paragraph 1 or Paragraph 2 has died before filing a complaint with an inquiry official, their parents, spouse or offspring can file a complaint and shall be deemedthe injured person.

Section 16/1[14] In case where the defendant is found guilty of the offence under Section 14 or Section 16, the relevant court may order as follows:

(1) That the data under such Section be destroyed.

(2) That partial or whole judgement be publicised or disseminated via electronic media, radio, television, newspapers or any other media as the relevant court may deem appropriate at the cost and expense of the defendant.

(3) That any other things shall be done as the relevant court deems appropriate in order to minimise the damage incurred from such wrongdoing.

Section 16/2[15]Whoever knows that the computer data which is in his/her possession is the computer data that is subject to be destroyed by the order of the relevant court under Section 16/1, must destroy such computer data; failing which, he/she shall be subject to half of the penalty provided in Section 14 or Section 16, as the case may be.

---

13 Section 16 is repealed and replaced by the Computer-Related Crime Act (No. 2), B.E. 2560.

14 Sections 16/1 is added by the Computer-Related Crime Act (No. 2), B.E. 2560.

15 Sections 16/2 is added by the Computer-Related Crime Act (No. 2), B.E. 2560.

Section 17 Whoever commits an offence pursuant to this Act outside the Kingdom of Thailand, and

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

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

shall be punished in the Kingdom of Thailand.

Section 17/1[16]Commission of the offences stated under Section 5, Section 6, Section 7, Section 11, Section 13 Paragraph 1, Section 16/2, Section 23, Section 24 and Section 27, may cause a fine to be issued by the Fine Committee appointed by the Minister.

The Fine Committee to be appointed by the Minister shall consist of three members, one of whom must be an inquiry official under the Criminal Procedure Code.

Once the Fine Committee gives its order to the offender to pay the fine, and the offender pays the fine within the time limit in compliance with the order imposed by the Fine Committee, the case shall be deemed dissolved under the Criminal Procedure Code.

In the event that the offender fails to pay the fine within the prescribed period of time, the time prescription for filing criminal prosecution shall begin to runas from the expiry date of such time period.

Part 2
Competent Officials

Section 18[17] Subject to Section 19, for the purpose of making inquiries and investigation, in case where there is a reasonable ground to believe that an offence under this Act has been committed or where there is a request under Paragraph 2, the competent official is empowered to do any of the following actions as deemed necessary for the benefit of using it as evidence in order to establish that the offence has been committed, and to find the whereabouts of the offender:

(1) To send a letter or call a person involved in the commission of the offence, in order to make an inquiry about information or submit a written explanation, documents, data or other evidence, in a format which can be clearly understood;

(2) To demand traffic data from the service providers who provide the service of communication via computer systems or from any other related person;

---

16 Section 17/1 is added by the Computer-Related Crime Act (No. 2), B.E. 2560.

17 Section 18 is repealed and replaced by the Computer-Related Crime Act (No. 2), B.E. 2560.

(3) To demand the service provider to submit the data related to its users which must be stored under Section 26, or which is in the possession or control of the service provider, to the competent official, or to keep such data for the time being;

(4) To copy the computer data and traffic data from a computer system in a case where there is a reasonable ground to believe that an offence has been committed, in case such computer system is not already in the possession of the competent official;

(5) To order a person who possesses or controls the computer data or equipment which stores the computer data, to deliver the computer data or such equipment to thecompetent official;

(6) To examine or gain access into the computer system, computer data, traffic data or equipment which stores the computer data of any person, which is evidence or may be used as evidence in relation to the commission of the offence or for the purpose of investigating into who an offender is; and order such person to deliver the relevant computer data and traffic data, as necessary;

(7) To decrypt any person's computer data or order a person related to the encryption of the computer data to decrypt it, or cooperate with the competent official to decrypt it;

(8) To confiscate or attach a computer system as necessary for the purpose of finding out the details of the commission of the offence and the offender.

For the purpose of the inquiry and investigation of an inquiry official under the Criminal Procedure Code, in relation to criminal offences in violation of any other laws committed against any persons by using a computer system, computer data or equipment storing computer data, which is a composition or part of the commission of the offence or has computer data relating to a commission of any offence under another law, such inquiry official may request the competent official under Paragraph 1 to take actions under Paragraph 1 or if such fact appears to the competent official in the performance of his/her duties under this Act, the competent official shall expeditiously collect the facts and evidence, and inform the relevant officer to proceed further.

A person who has been requested by the competent official under Paragraph 1 (1), (2) and (3) shall act in compliance with such request without delay, which shall not be later than seven days from the date on which the request is received or shall be within the time specified by the competent official, which must not be less than seven days but shall not exceed fifteen days; unless there is a reasonable cause, for which a permission must be obtained from the competent official. The Minister may issue aNotification prescribing a reasonable time period within which a person must act in compliance with a request and the type of service provider.

Section 19[18]In exercising the authority of a competent official under Section 18(4), (5), (6), (7) and (8), the competent official shall file a petition with the court having jurisdiction requesting for an order to permit such competent official to act in accordance with the petition. The petition must specify a reasonable ground to believe that a person commits or is going to commit any act which is an offence, a reason to exercise his/her power, the manner of commission of the offence, details relating to the equipment used in committing the offence and the offender, in so far that is known and can be specified as part of the petition. In considering such petition, the court shall consider such petition expeditiously.

After the relevant court has granted such order, prior to exercising his/her authority in accord with the court's order, the competent official shall deliver to the owner or possessor of the computer system for keeping as an evidence, a copy of the note stating the reasonable ground(s) to believe and that such authority under Section 18(4), (5), (6), (7) and (8) must be exercised. In the event that no owner or possessor of the computer hardware (or system) is present there, the competent official shall later deliver a copy of such note to the owner or possessor of the computer hardware (or system) as soon as practicable.

The competent official who leads the exercise of authority under Section 18(4), (5), (6), (7) and (8) must submit a copy of the report, describing the details of the exercise and reasons for such exercise to the court having jurisdiction within 48 hours from the time of the exercise, as evidence.

Making a copy or copies of computer data under Section 18(4) may be done only if there is a reasonable ground to believe that the offence has been committed and in doing so is notcaused any obstruction to the operation of the owner or possessor of computer data in excess of necessity.

In confiscating or attaching the computer system under Section 18(8), in addition to the provision of a copy of the document showing the confiscation or attachment to the owner or possessor of the computer system as evidence, the competent official shall not confiscate or attach such computer system for a period exceeding thirty days. In case of a necessity which requires the confiscation or attachment in excess of thirty days, the competent official shall file a petition with the court having jurisdiction requesting for an extension of time for such confiscation or attachment. The relevant court may order one or more extensions of time totalling not exceedingsixty days. Once there is no longer the necessity to confiscate or attach the computer system or the allowed period of confiscation or attachment has expired, the competent official shall instantly return the confiscated computer system to the owner or the possessor of the computer system or revoke the attachment.

[18] Section 19 is repealed and replaced by the Computer-Related Crime Act (No. 2), B.E. 2560.

The document showing the confiscation or attachment referred to in Paragraph 5 above shall be in accordance with the relevant Ministerial Regulation.

Section 20[19]In case of dissemination of computer data in the following manner, the competent official may, with the approval of the Minister, file a petition together with evidence with the court having jurisdiction requesting for an order to block the dissemination, or delete the computer data from the computer system

(1) Computer data which constitutes an offence under this Act.

(2) Computer data which may adversely affect the security of the Kingdom of Thailand as prescribed in Book II, Title 1 or Title 1/1 of the Criminal Code.

(3) Computer data that constitutes a criminal offence under the law relating to intellectual property or any other laws under which such computer data in its character contrary to public order or good morals of the people of Thailand; and of which the officer under such law or the inquiry official under the Criminal Procedure Code has requested.

In the case of dissemination of computer data in the manner which is contrary to public order or good morals, the Minister, with an approval of the Computer Data Review Committee, may entrust a competent official to file a petition together with evidence with the court having jurisdiction requesting for an order to block the dissemination or to delete such computer data from the computer system. For such purpose, the provisions relating to theComputer Data Review Committee, which isempowered to proceed with the administrative procedures under the law on administrative procedure shall by implication apply to the meeting of the Computer Data Review Committee.

The Minister shall appoint one or more Computer Data Review Committees under Paragraph 2, each of which shall consist of nine members, and three persons out of said nine members shall be appointed from the representatives of the private sector with experience in human rights, public communication, information technology or any other related field. Such Computer Data Review Committee members shall be entitled to receive remuneration in accordance with the criteria prescribed by the Minister, which have been approved by the Ministry of Finance.

The Criminal Procedure Code shall by implication apply to the proceedings of the court under Paragraphs 1 and 2. In case where the relevant court orders a block of the dissemination or deletion of the computer data under Paragraph 1 or Paragraph 2, the competent official may either block the dissemination or delete the computer data by himself/herself, or order the service provider to block the dissemination or delete such computer data. For such purpose, the Minister shall issue a Notification prescribing the criteria, period of time and method of blocking the dissemination or deletion of the

[19] Section 20 is repealed and replaced by the Computer-Related Crime Act (No. 2), B.E. 2560.

computer data by the competent official or the service provider which is appropriate and relevant with the current development of technology, unless the court orders otherwise.

In case of urgency and necessity, the competent official may file a petition under Paragraph 1 before he/she receives an approval of the Minister or the competent official may file a petition under Paragraph 2 with an approval of the Computer Data Review Committee, before he/she is entrusted to do so by the Minister. In any case, the competent official must expeditiously report such filing of petition to the Minister.

Section 21 In case where the competent official finds that any computer data comprises undesirable programs, the competent official may file a petition with the court having jurisdiction requesting for an order to prohibit the distribution or dissemination or to instruct the owner or the possessor of such computer data to cease using, to destroy or to correct such computer data or may specify conditions of use, possession, or dissemination of such undesirable programs.

An undesirable program under Paragraph 1 means any program that adversely affects computer data, computer system or other programs by causing damage, destruction, alteration, interruption or deviation from the determined command; or causing any other impact as prescribed by the Ministerial Regulation, except for the undesirable program which is designed to protect or modify the aforesaid program. The Minister may announce and publish in the Government Gazette the names, characteristics or details of any program which is designed to protect or modify an undesirable program. [20]

Section 22[21] The competent official and the inquiry official in the case pursuant to Section 18, Paragraph 2 shall not disclose nor deliver computer data, traffic data or user's dataobtained under Section 18 to any person.

The provisions in Paragraph 1 shall not apply to any execution for the purpose of taking legal actions against the offender under this Act or the offender under any other acts in accordance with Section 18, Paragraph 2; any execution for the purpose of taking legal actions against the competent official or inquiry official who has abused his/her powers in accordance with Section 18, Paragraph 2; or the commission of any act in accordance with the order or permission of the relevant court.

Any competent official or inquiry official who violates the provisions of Paragraph 1 shall be liable to an imprisonment for a term not exceeding three years, or a fine not exceeding Sixty Thousand Baht or both.

Section 23[22] Any competent official or inquiry official in the case pursuant to Section 18, Paragraph 2 who acts negligently, thus causing any other person to know of

---

20 Section 21,Paragraph 2 is repealed and replaced by the Computer-Related Crime Act (No. 2), B.E. 2560.

21 Section 22 is repealed and replaced by the Computer-Related Crime Act (No. 2), B.E. 2560.

22 Section 23is repealed and replaced by the Computer-Related Crime Act (No. 2), B.E. 2560.

computer data, computer traffic data or user's dataobtained under Section 18; shall be liable to an imprisonment for a term not exceeding one year, or a fine not exceeding Twenty Thousand Baht or both.

Section 24[23] Whoever comes to know of computer data, traffic data or user's dataobtained by the competent official or inquiry official under Section 18, and discloses such data to any person, shall be liable to an imprisonment for a term not exceeding two years, or a fine of not exceeding Forty Thousand Baht or both.

Section 25[24] Any data, computer data or traffic data obtained by the competent official under Section 18, Paragraph 2 shall be referred to and admissible as evidence in accordance with the provisions of the Criminal Procedure Code or other laws in relation to evidence, but not including those obtained through any inducement, promise, threat, deceit or other unlawful means.

Section 26 A service provider shall maintain traffic data for a period not less than ninety days as from the date on which such data was entered into the computer system. If necessary, the competent official may, on case by case basis for particular cases and certain situations, order any service provider to maintain computer traffic data for a period longer than ninety days but not exceeding two years.[25]

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's data for a period not less than ninety days from its expiry date.

The Minister shall prescribe the type of service providers, how and when the provisions ofParagraph 1 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's 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 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.

---

[23] Section 24is repealed and replaced by the Computer-Related Crime Act (No. 2), B.E. 2560.

[24] Section 25is repealed and replaced by the Computer-Related Crime Act (No. 2), B.E. 2560.

[25] Section 26, Paragraph 1 is repealed and replaced by the Computer-Related Crime Act (No. 2), B.E. 2560.

Whoever has been appointed as a competent official may receive special remuneration as stipulated by the Minister with an approval of the Ministry of Finance.[26]

In determining the special remuneration, consideration must be given to the responsibility, knowledge and specialisation, a lack of personnel to undertake the duty, high rate of turnover due to resignation of personnel from governmental organisations, quality of work and maintenance of conduct for justice, by comparing with the remuneration of another officers in the judicial process.[27]

Section 29 In performing his/her duties under this Act, the competent official 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 the offences under this Act.

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

The Prime Minister whose mandate is to control and supervise the Royal Thai Police, together with the Minister, shall jointly empower to stipulate the rulesprescribing the guidelines and procedural methods for the execution under Paragraph 2.

Section 30 In carrying out his/her 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 prescribed by the Minister and published in the Government Gazette.

Section 31[28] The expenditures relating to the following matters, including thedisbursement procedure shall be in accordance with the rules prescribed by the Minister with an approval of the Ministry of Finance:

(1) Investigation, acquiring information and gathering of evidences of the offences under this Act;

(2) Executing actions under Section 18, Paragraph (4), (5), (6), (7) and (8), and Section 20; and

---

26 Section 28, Paragraph 2 is added by the Computer-Related Crime Act (No. 2), B.E. 2560.

27 Section 28, Paragraph 3 is added by the Computer-Related Crime Act (No. 2), B.E. 2560.

28 Section 31 is added by the Computer-Related Crime Act (No. 2), B.E. 2560.

(3) Executing any other necessary actions for the prevention and suppressionof the offences under this Act.

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 malfunctions, or failing to perform as instructed, or illegally accesses, alters or destroys data belonging to another person in the computer system, or uses the computer system for dissemination or pornographic, such acts will cause damages and impact society, economy and national security including public peace and good morals. It is therefore expedient to impose measures to prevent and suppress of such by promulgation of this Act.

Computer-Related Crime Act (No. 2), B.E. 2560 (A.D. 2017)[29]

Section 2. This Act shall come into force after the expiration of one hundred and twenty days as from the date of its publication in the Government Gazette.

Section 20. All Rules or Notificationsissued under the Computer-Related Crime Act B.E. 2550, which were in force before the dateon which this Act comes into force shall remain in force to the extent that they are notcontrary to or inconsistent with the provisions of the Computer-Related Crime Act B.E. 2550 as amended by this Act until the Rules or Notifications issued under the Computer-Related Crime Act B.E. 2550 as amended by this Act are came into force.

The issuance of Rules or Notificationsunder Paragraph 1 must be completed within sixty days from the date on which this Act comes into force. In case it is not capable to do so within the time period specified, the Minister of the Ministry of Digital Economy and Society shall report to the Cabinet of the reasons for not being able to do so.

Section 21. The Minister of the Ministry of Digital Economy and Society shall have charge and control of the execution of this Act.

Rationale: The reason for promulgating the Act is due to some provisions of the Computer-Related Crime Act B.E. 2550 (A.D. 2007) are not appropriate for the prevention and suppression of the computer related crime nowadays as the method of the crime has become more complicated following rapid changes and development in technology. Further, the Ministry of Digital Economy and Society has been established and entrusted with the responsibility to prescribe the standards and measures for cyber security, including surveillance and keeping up-to-date with the security of information technology and telecommunications of the Kingdom of Thailand. Therefore, it is necessary to amend the provisions regarding the organisation which is having charge and control of the law, as well as to prescribe new offences and amendments of the existing offences, including the provisions on penalty for such offences, amendments to the processes and rules relating to dissemination or deletion of computer data, as well as the appointment of a Fine Committee which is empowered to impose fines on the offender who commits an offence under this Act; and amendment of the provisions relating to the power of the competent official to be more suitable.

[29] Government Gazette, Volume 134 / Part 10 Gor / Page 24 / 24 January 2560 (A.D. 2017).