

FOURTEENTH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
Second Regular Session)

OFFICE OF THE SECRETARY

9 MAY -6 A.M. :24

SENATE

S. NO. 3213

RECEIVED BY

Introduced by Senator Antonio "Sonny" F. Trillanes IV

EXPLANATORY NOTE

Information and Communications Technologies (ICTs) have revolutionized our lifestyle. Computers have evolved into a versatile instrument in modern society. Computer networks have become essential in maintaining and operating vital infrastructures. The ICT has opened up an endless spectrum of possibilities both in terms of communication and commerce. It has enabled linkages among individuals and organizations in doing business.

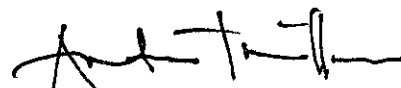
ICT enhances and promotes efficiency in facilitating the exchange and delivery of information. The introduction of computers and computer networks facilitated faster and better data storage, information exchange and communications. Computers also helped improve banking, telecommunications, engineering and data handling.

It is sad to note however, that despite the advances that we were able to achieve in the field of Information and Communications Technology, new breed of deviants, new forms of criminals and criminal activities arose such as unauthorized acquisition of vital and/or confidential information by third parties seeking to profit or benefit from the, utilization of such information.

With the development of new forms of crimes, cybercrime legislation must be an immediate concern of Congress. It is clear however, that even with existing Philippine laws, there still exist a need to provide a comprehensive policy framework that would set regulations on cybercrimes. There is a need for the Philippines to have a law that will define cybercrimes, identify punishable acts involving computers with corresponding penalties, determine legal procedures for the investigation and prosecution of cybercrimes, clarify jurisdictions, provide for a clause on mutual assistance and cooperation, and identify a local body that shall be responsible for providing a 24/7 assistance to foreign entities in the resolution of cybercrime cases.

It is hoped that thru the passage of this bill, cybercriminals will be discouraged from indulging into illegal acts. Moreover, the passage of this bill will send a clear signal to the International community that our country is serious in combating, and does not tolerate, cyber crimes.

In view of the foregoing, immediate passage of this bill is earnestly sought.



ANTONIO "SONNY" F. TRILLANES IV
Senator

9 MAY -6 AIC:24

SENATE

S. NO. 3213

RECEIVED BY



Introduced by Senator Antonio "Sonny" F. Trillanes IV

AN ACT
DEFINING CYBERCRIME, PROVIDING FOR PREVENTION, SUPPRESSION AND
IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES

Be it enacted by the Senate and the House of Representatives of the Philippines in Congress assembled.

CHAPTER I – PRELIMINARY PROVISIONS

SECTION 1. *Title.* – This Act shall be known as the “Cybercrime Prevention Act of 2009”.

SEC. 2. *Declaration of Policy.* – The State recognizes the vital role of information and content industries, such as telecommunications, broadcasting, electronic commerce, and data processing, in the nation’s overall social and economic development. The State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology to attain free, easy, and intelligible access to exchange and/ or delivery of information; and the need to protect and safeguard the integrity of computer, computer and communication systems, networks, and database, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts. In this light, the State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation, and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international cooperation.

SEC. 3. *Definition of Terms.* – For purposes of this Act, the following terms are hereby defined as follows:

- a.) Access – refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer, computer and communications network, or database;

- 1 **b.) Alteration** – refers to the modification or change, in form or substance, of an existing
2 computer data or program;
- 3 **c.) Communication** – refers to the transmission of information, including voice and non-
4 voice data;
- 5 **d.) Computer** – refers to any device or apparatus which by electronic, electro-
6 mechanical, or magnetic impulse, or by other means, is capable of receiving, recording,
7 transmitting, storing, processing, retrieving, or producing information, data, figures,
8 symbols, or other modes of expression according to mathematical and logical rules of
9 performing anyone or more of those functions, including its associated devices and
10 peripherals;
- 11 **e.) Computer Data** – refers to any representation of facts, information, or concepts in a
12 form suitable for processing in a computer system, including a program suitable to cause
13 a computer system to perform a function;
- 14 **f.) Computers and Communications Network or Networks** – refers to:
- 15 *i.* a group of computers, associated devices, and/ or its peripherals that are
16 connected either permanently or temporarily, wired or wireless, by transmission
17 and/ or communications facilities which facilitate and/ or provide the means of
18 sending, communicating, processing and/ or transmitting voice and/ or non-voice
19 data and/ or information electronically ; or
- 20 *ii.* a group of interconnected or related devices, including, but not limited to, a
21 group of interconnected computers, private exchange branch (PBX) wired or
22 wireless, telecommunications switching equipment, one or more of which, pursuant
23 to a program, perform automatic processing of data;
- 24 **g.) Computer Program** – refers to a set of instructions executed by the computer to
25 achieve intended results;
- 26 **h.) Conduct Without Right** – refers to either: (1) conduct undertaken without or in excess
27 of authority; or (2) conduct not covered by established legal defenses, excuses, court
28 orders, justifications, or relevant principles under the law;
- 29 **i.) Cybercrime** – refers to any offense that can be committed by using a computer or
30 communications system or network in a computer or communications system or network
31 against a computer or communications system or network;
- 32 **j.) Cybersex or Virtual Sex** – refers to any form of sexual activity or arousal with the aid
33 of computers or communications network;
- 34 **k.) Damage** – in the general sense, refers to damage or injury as defined under the
35 applicable laws, including but not limited to the relevant provision of the Civil Code of

1 the Philippines. In the limited sense, it means any impairment to the integrity or
2 availability of a computer data, program, system information, or network;

3 With respect to computer data or programs as used in this Act, the words “damaging”
4 and “deteriorating” are synonymous;

5 l.) Database – refers to a representation of information, knowledge, facts, concepts, or
6 instructions which are being prepared or processed or have been prepared or processed in
7 a formalized manner and which are intended for use in a computer, computer and
8 communications network, computer server, or database;

9 m.) Deletion – refers to the destruction or impairment of information or data contained in
10 a computer or computer and communications network by making them unrecognizable or
11 by totally or partially obliterating the information or data from the computer or computer
12 network;

13 n.) Distribution – refers to the active dissemination of data, information or material using
14 the computer and/ or communications computer network;

15 o.) Electronic Data Message – refers to information generated, sent, received, or stored
16 by electronic, optical, or similar means;

17 p.) Electronic Document – refers to the information or the representation of information,
18 data, figures, symbols, or other modes or written expression, described or however,
19 represented, by which a right is established or an obligation extinguished, or by which a
20 fact may be proved and affirmed, which is received, recorded, transmitted, stored,
21 processed, retrieved, or produced in and through computer and/ or computer and
22 communications networks;

23 q.) Interception – refers to listening to, recording, monitoring or surveillance of the
24 content of communications, including producing of the content of data, either directly,
25 through access and use of the computer or computer and communications network or
26 indirectly, through the use of electronic eavesdropping or tapping devices, at the same
27 time that the communication is occurring;

28 r.) Making available – refers to the placing of online devices, including but not limited
29 to, the creation or compilation of hyperlinks in order to facilitate access to such devices,
30 for the use of others;

31 s.) Minor – refers to a person below eighteen (18) years of age or those beyond eighteen
32 (18) years of age but whose mental capacity is that of a person below eighteen (18) years
33 of age;

34 t.) Non-Public Transmission – refers to the transmission of information or computer data
35 between computer or computer and communications networks that are not configured for
36 public access;

1 u.) Procuring Data or Material – refers to the act of actively obtaining data, information
2 or material by downloading the same from a computer or computer and communications
3 network;

4 v.) Protected Computer/s – refers to any computer exclusively for the use of a financial
5 institution or the government, or in the case of a computer not exclusively for use, used
6 by or for a financial institution or the government, and the conduct instituting the
7 offenses affects that use by or for the financial institution or the government;

8 w.) Protected Works – refer to works, including but not limited to computer programs,
9 systems, and design, protected under Philippine laws;

10 x.) Service Provider – refers to the provider of:

11 i. telecommunications and online services or network access, or the operator of
12 communications and network facilities, therefore, including entities offering the
13 transmission, routing, or providing of connections for online communications,
14 digital or otherwise, between or among point specified by a user, of electronic
15 documents of the user's choosing; or

16 ii. any other entity that processes or stores information on behalf of such
17 communication service or users of such service;

18 y.) Subscriber's Information – refers to any information contained in the form of
19 computer data or any other form that is held by a service provider, relating to the
20 subscribers of its services other than traffic or content data and by which can be
21 established:

22 i. the type of communication service used, the technical provisions taken thereto
23 and the period of service.

24 ii. the subscriber's identity, postal or geographic address, telephone and other
25 access number, any assigned network address, billing and payment information,
26 available on the basis of the service agreement or arrangement;

27 z.) Suppression of Computer Data – refers to any action that prevents or terminates the
28 availability of the data to the person who has access to the computer or computer and
29 communications network on which it was stored;

30 aa.) By Technical Means – refers to the use of technical devices which are fixed to
31 transmission lines, as well as devices such as software, passwords, and codes to collect
32 and/ or record wireless communications or those communications passing through, or
33 generated by computer or computer and communications networks;

34 bb.) Traffic Data or Non-Content Data – refers to any other computer data other than the
35 content of the communication, including but not limited to the communication's
36 origin, destination, route, time, date, size, duration, or type of underlying service.

1 **CHAPTER II – PUNISHABLE ACTS**

2
3 **SEC. 4.** - The following acts constitute the offense of cybercrime punishable under this
4 Act:

5 **A.** Computer Crime – any act committed by means of electronic operations that targets the
6 security of computer or communications systems or network and the data processed by
7 them such as but not limited to:

8 1. *Illegal Access* – The access to the whole or any part of a computer or communications
9 system or computer or communications network without right.

10 2. *Illegal Interception* – The interception made by technical means without right of any
11 non-public transmission of computer or communication data to, from, or within a
12 computer or communication network, including electromagnetic emissions from a
13 computer or communication network carrying such computer data: *Provided,*
14 *however,* That it shall not be unlawful for an officer, employee, or agent of a service
15 provider, whose facilities are used in the transmission of communications, to
16 intercept, disclose, or use that communication in the normal course of his
17 employment while engaged in any activity that is necessary to the rendition of his
18 service or to the protection of the rights or property of the service provider, except
19 that the latter shall not utilize service observing or random monitoring except for
20 mechanical or service control quality checks: *Provided, further,* That it shall not be
21 unlawful for a person to intercept or record a communication where there is no
22 reasonable expectation of privacy.

23 3. *Misuse of Devices* –

24 **a.** The use, production, sale, procurement, importation, distribution, or otherwise
25 making available, without right, of: (1) a device, including a computer program,
26 designed or adapted primarily for the purpose of committing any of the offenses
27 under Section 4.1 to .4 hereof; or (2) a computer password, access code, or
28 similar data by which the whole or any part of a computer or computer network
29 is capable of being accessed;

30 **b.** The possession of an item referred to in paragraphs (a) (1) or (2) above with
31 intent to use said devices for the purpose of committing any of the offenses
32 under Section 4.1 to 4.4 hereof. *Provided,* That no criminal liability shall attach
33 when the use, production, sale, procurement, importation, distribution, or
34 otherwise making available, or possession of computer devices/ data referred to
35 in paragraph 3(a) herein is for: (1) the authorized testing of a computer,
36 computer network, or computer program; or (2) purely academic purposes:

1 *Provided, however,* That in any event, before such devices are used on a
2 computer or computer network, the prior consent of the owner of the computer
3 or computer network is obtained.

4 **4. *Unsolicited Commercial Communications*** – The transmission of electronic messages
5 with the use of computers, computer networks, or other communication devices
6 which seek to advertise, sell, or offer for sale products and services are prohibited
7 unless:

8 **a.** There is prior affirmative consent from the recipient; or

9 **b.** The following conditions are present:

10 **i.** The commercial electronic communication contains a simple, valid, and
11 reliable way for the recipient to reject receipt of further commercial
12 electronic messages (also known as “opt-out”) from the same source;

13 **ii.** The commercial electronic communication does not purposely disguise the
14 source of the electronic message; and

15 **iii.** The commercial electronic communication does not purposely include
16 misleading information in any part of the message in order to induce the
17 recipients to read message.

18 **B. Computer Sabotage** – the input, alteration, erasure or suppression of computer or
19 communication data or computer or communication programs, or interference with
20 computer and communication system or network, with the intent to hinder the
21 functioning of a computer or communication system or network such as but not limited
22 to:

23 **1. *Data Interference*** – the intentional or reckless damaging, deletion, deterioration,
24 alteration or suppression of computer data, electronic document, or electronic data
25 message, without right, including the introduction or transmission of viruses.

26 **2. *System Interference*** – the alteration, or reckless hindering or interference with the
27 functioning of a computer or computer network by inputting, transmitting, damaging,
28 deleting, deteriorating, altering, or suppressing computer data or program, electronic
29 document, or electronic data message, without right, including the introduction or
30 transmission of viruses.

31 **3. *Computer Fraud*** – the intentional and unauthorized input, alteration, erasure or
32 suppression of computer data or program, electronic document, or electronic data
33 message, or interference in the functioning of a computer or computer network,
34 causing damage thereby, with the intent of procuring an economic benefit for oneself
35 or for another person or for the perpetuation of a fraudulent or dishonest activity.

1 4. *Computer Forgery* – the input, alteration, erasure, or suppression of any computer or
2 communication data, computer or communication program, electronic document, or
3 electronic data message, or interference with the computer and communication
4 system or network, in a manner or under such conditions that would constitute the
5 offense of forgery under Act No. 3815 as amended, otherwise known as the Revised
6 Penal Code or special laws; the act of knowingly using a computer and
7 communication data which are the products of computer or communication forgery as
8 defined herein, for the purpose of perpetuating a fraudulent or dishonest design.

9 C. *Computer Facilitated Crime* – an act where the computer or communication system or
10 network is used as a tool or instrument or is illegally accessed to facilitate the
11 commission of crimes and offenses, to include, but not limited to the following:

12 I. *Offenses Related to Cybersex* – Without prejudice to the prosecution under Republic
13 Act No. 9208, otherwise known as the Anti-Trafficking Act and Republic Act No.
14 7610, otherwise known as the Child Protection Act, any person who in any manner
15 advertises, promotes, or facilitates the commission of cybersex through the use of
16 information and communications technology such as but not limited to computers,
17 computer networks, television, satellite, mobile telephone, or any person committing
18 any of the following acts is liable under this Act:

- 19 a. Producing child pornography for the purpose of distribution through a computer
20 or computer network;
- 21 b. Offering or making available child pornography through a computer or computer
22 network; or
- 23 c. Distribution or transmitting child pornography through a computer or computer
24 network;
- 25 d. Possessing child pornography materials in the computer/ communications system
26 or network or on a computer data storage medium;
- 27 e. Prostitution or solicitation of any form of cybersex for any favor or monetary
28 consideration;
- 29 f. Operation of internet café or any type of establishment which engages in any form
30 of cybersex for any favor or monetary consideration; and
- 31 g. Promotion and advertisement of any form of cybersex.

32 For purposes of this Section, the term “child pornography” shall include pornographic
33 material that visually depicts: (a) a minor engaged in sexually explicit conduct; or (b) a person
34 appearing to be a minor engaged in sexually explicit conduct. The term “prostitution” shall refer
35 to any act, transaction, scheme or design involving the use of a person by another, for sexual
36 intercourse or lascivious conduct in exchange for money, profit or any other consideration.

1 **SEC. 6. Corporate Liability.** – When any of the punishable acts herein defined is
2 knowingly committed in behalf and for the benefit of a juridical person, the penalties herein
3 provided shall be imposed upon the juridical person’s President, Secretary, members of the
4 Board of Directors, or any of its officers and employees who have directly participated in,
5 including those who knowingly authorized, the commission of the said act or acts.

6 Where the commission of any of the punishable acts herein defined by the juridical
7 person’s employees or agents, acting within the scope of their authority, was made possible due
8 to the lack of supervision and control of the juridical person, which resulted in benefits for the
9 said entity, the officers and members of the Board of Directors above-mentioned are likewise
10 liable.

11 **SEC. 7. Conspiracy to Commit Cybercrime.** – When two (2) or more persons come to an
12 agreement and decide to commit any of the punishable acts defined in this Act, and one or more
13 of such persons does any act to effect the object of the conspiracy, each of the conspirators shall
14 be punished as if all of the conspirators have done the act themselves.

15 **SEC. 8. Aiding or Abetting in the Commission of Cybercrime.** – Any person who
16 willfully abet or aid in the commission of any of the offenses enumerated in Chapter II hereof
17 shall be held liable under this Act.

18

19 **CHAPTER IV- COMPUTER EMERGENCY RESPONSE COUNCIL**

20

21 **SEC. 9. Computer Emergency Response Council.** – There is hereby created, thirty (30)
22 days from the effectivity of this Act, a Computer Emergency Response Council, hereinafter
23 referred to as CERC, under the control and supervision of the Office of the President principally
24 to formulate and implement a national plan of action to address and combat cyber-crime.

25 **SEC. 10. Composition.** – The CERC shall be headed by the Chairman of the
26 Commission on Information and Communications Technology (CICT) as Chairman; the Director
27 of the National Bureau of Investigation (NBI) as Vice-Chairman and the following as members:
28 Director-General of the Philippine National Police (PNP), the Chief of the National Prosecution
29 Service (NPS), the Head of the National Computer Center (NCC), the head of the Philippine
30 Center for Transnational Crime (PCTC), the head of the Anti-fraud and Computer Crimes
31 Division (AFCCD) of the NBI and the head of the Criminal Investigation and Detection Group
32 (CIDG) of the PNP and three (3) representatives from the private sector involved in information
33 security to be appointed by the President of the Philippines.

34 **SEC. 11. CERC Secretariat.** – The CERC shall be manned by a Secretariat, the
35 personnel of which shall come from the CICT and selected personnel and representatives who

1 shall be detailed from the participating agencies. An Executive Director shall be appointed by the
2 Chairman of the CICT to head the secretariat.

3 **SEC. 12. Powers and Functions.** – The CERC shall have the following powers and
4 functions:

5 *a.)* To prepare and implement appropriate and effective measures to prevent and suppress
6 computer fraud, abuses and other cyber-related fraudulent activities as provided in this Act;

7 *b.)* To monitor the investigation of cybercrime cases being handled by participating law
8 enforcement and prosecution agencies initiate international cooperation on intelligence,
9 investigations, training and capacity building relative to cybercrime prevention, suppression, and
10 prosecution;

11 *c.)* To recommend the attendance of qualified personnel in trainings, conferences and other
12 fora on information security and cybercrime prevention, investigation and suppression;

13 *d.)* To coordinate the support and participation of the business sector, local government units,
14 and non-governmental organizations in cybercrime prevention programs and other related
15 projects;

16 *e.)* To recommend the enactment of appropriate laws, issuances, measures and policies;

17 *f.)* To call upon any government agency to render assistance in the accomplishment of the
18 CERC's mandated tasks and functions; and

19 *g.)* To perform such other functions and duties necessary for the proper implementation of this
20 Act.

21

22 **CHAPTER V- ENFORCEMENT AND IMPLEMENTATION**

23

24 **SEC. 13. Collection of Computer Data.** – To effectively implement and enforce the
25 provisions of this Act, the National Bureau of Investigation (NBI) and the CIDG of the
26 Philippine National Police (PNP), subject to existing laws and procedures, shall require a person
27 or service provider:

28 *a.)* To submit specified computer data and other relevant data in his/ its possession and control,
29 which is stored in a computer, computer and communications network, or a computer-data
30 storage medium;

31 *b.)* To submit subscriber information in his/ its possession or control;

32 *c.)* Within his/ its existing technical capability, to collect or record through the application of
33 technical means or to cooperate and assist the proper law enforcement officers or agencies in the
34 collection or recording of traffic data and interception of specified communications transmitted
35 within or passing through the territorial jurisdiction of the Philippines by means of a computer
36 and communications network; and

1 *d.)* To require the expeditious production or disclosure of traffic data to identify the service
2 providers and the path through which the communication was transmitted.

3 **SEC. 14. *Search and Seizure of Computer Data.*** – Where a search and seizure warrant
4 is properly issued, the NBI and the PNP shall likewise have the following powers and duties:

5 *a.)* Within the time period specified in the warrant, to conduct interception, as defined in this
6 Act, content of communications, procure the content of data either directly, through access and
7 use of the computer or computer and communications network, or indirectly, through the use of
8 electronic eavesdropping or tapping devices, in real time or at the same time that the
9 communication is occurring;

10 *b.)* To secure a computer or computer and communications network or parts of it or a
11 computer-data storage medium;

12 *c.)* To make and retain a copy of those computer data secured;

13 *d.)* To maintain the integrity of the relevant stored computer data; and

14 *e.)* To render inaccessible, or remove those computer data in the accessed computer or
15 computer and communications network.

16 Pursuant thereof, the NBI and CIDG of the PNP may order any person who has
17 knowledge about the functioning of the computer or computer and communications network and
18 the measures to protect and preserve the computer data therein to provide, as is reasonable, the
19 necessary information, to enable the undertaking of the search and seizure measure referred to in
20 paragraph (c) of Section 17 hereof.

21 **SEC. 15. *Preservation and Disclosure of Computer Data and Traffic Record.*** – The
22 integrity of traffic data and subscriber information relating to communication services provided
23 by a service provider shall be preserved up to a minimum period of six (6) months from the date
24 of the transaction. Said period may be extended by order of the NBI or PNP upon a reasonable
25 belief that the computer data may have been used for in connection with, or the traffic record
26 may contain information as regards any violation of this Act.

27

28

CHAPTER VI – JURISDICTION

29

30 **SEC. 16. *Jurisdiction.*** – The Regional Trial Court shall have jurisdiction over any
31 violation of the provisions of this Act committed within the territory of the Philippines or by any
32 of its nationals regardless of the place of commission. In case any of the offenses herein defined
33 is committed outside the territorial limits of the Philippines, and by such commission any
34 damage is caused to a computer or computer and communications network situated in the
35 Philippines, or to a natural or juridical person who, at the time the offense was committed, is in
36 the Philippines, the proper Regional Trial Court in the Philippines shall have jurisdiction.

