


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

OFFICE OF THE SECRETARY

9 APR 21 P5:46

SENATE

S.B. No. 3177

RECEIVED BY: 

Introduced by Senator JUAN PONCE ENRILE

EXPLANATORY NOTE

Internet use in the Philippines has grown rapidly in the past decade. It has given rise to countless opportunities to a lot of Filipinos in every field imaginable. It has served as venue for growth and development in businesses, trade, engineering, arts and sciences and has sped up the exchange of information about practically all aspects of life. It has since been an integral part of our daily lives.

However, the internet also has its own disadvantages and one of these is cybercrime. Ordinarily, cybercrime is defined as any illegal and criminal activity committed on the internet. These include unlawful acts where information technology is used either a tool or target, or both, in the commission of such unlawful acts. Any criminal activity that employs a computer either as an instrumentality, target or a means for the commission of other illegal acts also goes within the range of cybercrime.

In recent years, we have witnessed how cybercrime has emerged as the latest and most complicated problem in the cyber world. Criminal activities in the cyberspace are on the rise. Computers today are being misused for illegal activities like e-mail espionage, credit card fraud, spams, and software piracy, which not only invade our privacy but also offend our senses. On many instances, the computer have been utilized as an instrument in the following illegal activities: financial crimes, sale of illegal or stolen articles, pornography, online gambling, crimes impinging on intellectual property rights, e-mail spoofing, forgery, cyber defamation, and even cyber stalking.

On the other hand, the computer may has also been the object of other unlawful acts such as, but not limited to, illegal access or hacking, theft of information contained in electronic form, e-mail bombing, virus attacks, internet time thefts and so forth. Examples of these types of conducts include illegal access or access to the whole or any part of a computer system without proper authorization, illegal interception or the interception without right made by technical means, of non-public transmission of computer data to, from or within a computer system, data interference or the damaging, deletion, deterioration, alteration or suppression of computer data without proper authority, system interference or the serious hindering without right of the functioning of a computer

system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data, misuse of devices, forgery and fraud.

Cybercrime is an actual danger to democracy, human rights and the rule of law. It is a dangerous reality which has to be taken seriously at the highest level. Measures to fight and prevent cybercrime must be based on laws that fully respect civil liberties. Thus, it is of utmost importance that an efficient protection and prevention method be developed to combat cybercrime.

In view of the foregoing, the immediate approval of this measure is earnestly sought.

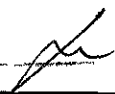


JUAN PONCE ENRILE
Senator

9 APR 21 P5:46

SENATE

S.B. NO. 3177

RECEIVED BY: 

Introduced by Senator Juan Ponce Enrile

AN ACT
DEFINING CYBERCRIME, PROVIDING FOR THE 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 communications 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.

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

3 a) Access - refers to the instruction, communication with, storing data in, retrieving data
4 from, or otherwise making use of any resources of a computer system;

5 b) Alteration – refers to the modification or change, in form or substance, of an existing
6 computer data or program;

7 c) Communication – refers to the transformation of information including voice and
8 non-voice data;

9 d) Computer system – means any device or a group or interconnected or related devices,
10 one or more of which, pursuant to a program, performs automatic processing of data.
11 It covers any type of computer device including devices with data processing
12 capabilities like mobile phones and also computer networks. The device consisting of
13 hardware and software may include input, output and storage facilities which may
14 stand alone or be connected in a network or other similar devices. It also includes
15 computer-data storage devices or medium.

16 e) Computer data – refers to any representation of facts, information, or concepts in a
17 form suitable for processing in a computer system including a program suitable to
18 cause a computer system to perform a function and includes electronic documents
19 electronic data messages;

20 f) Computer Program – refers to a set of instructions executed by the computer to
21 achieve intended results;

22 g) Without Right – refers to either: (1) conduct undertaken without or in excess of
23 authority; or (ii) conduct not covered by established legal defenses, excuses, court
24 orders, justifications, or relevant principles under the law;

25 h) Database – refers to a representation of information, knowledge, facts, concepts, or
26 instructions which are being prepared, processed or stored or have been prepared,

processed or stored in a formalized manner and which are intended for use in a computer system;

i) Interception – refers to listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content of data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring;

j) Service Provider – refers to the provider of:

i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service;

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

i. The type of communication service used, the technical provisions taken thereto and the period of service;

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

iii. Any other available information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

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

CHAPTER II – PUNISHABLE ACTS

Sec. 4. *Cybercrime Offenses.* – The following acts constitute the offense of cybercrime punishable under this Act:

- a. Offenses against the confidentiality, integrity and availability of computer data and systems:
 - i. Illegal Access – The intentional access to the whole or any part of a computer system without right.
 - ii. Illegal Interception – The intentional interception made by technical means without right of any non-public transmission of computer data to, from, or within a computer system including electromagnetic emissions from a computer system carrying such computer data: Provided, however, That if shall not be unlawful for an officer, employee, or agent or a service provider, whose facilities are used in the transmission of communications, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity that is necessary to the rendition of his service or to the protection of the rights or property of the service provider, except that the latter shall not utilize service observing or random monitoring except for mechanical or service control quality checks;
 - iii. Data interference – the intentional or reckless alteration of computer data without right.
 - iv. System Interference – the intentional or reckless hindering without right of the functioning of a computer system by inputting, transmitting, deleting, altering or suppressing computer data or program.

v. Misuse of Devices –

a) The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:

i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this Act; or

ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under this Act;

b) The possession of an item referred to in paragraphs 5(a) (i) or (ii) above with intent to use said devices for the purpose of committing any of the offense under this Section.

Provided, That no criminal liability shall attach when the use, production, sale, procurement, importation, distribution, or otherwise making available, or possession of computer devices/data referred to is for the authorized testing of a computer system.

b. Computer-related Offenses:

i. Computer-related Forgery – (a) the intentional input, alteration, or deletion of any computer data without right resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible; (b) the act of knowingly using computer data which is the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design.

ii. Computer-related Fraud – the intentional and unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a

1 computer system, causing damage thereby, with the intent of procuring an
2 economic benefit for oneself or for another person or for the perpetuation of a
3 fraudulent or dishonest activity; Provided, that if no damage has yet been
4 caused, the penalty imposable shall be one degree lower.

5 c. Content-related Offenses:

6 i. Cybersex – any person who establishes, maintains or controls, directly or
7 indirectly, any operation for sexual activity or arousal with the aid of or
8 through the use of a computer system, for a favor or consideration.

9 ii. Child Pornography – any person who engages in the following acts:

10 a) Producing child pornography for the purpose of distribution through
11 a computer system’

12 b) Offering or making available child pornography through a computer
13 system;

14 c) Distribution or transmitting child pornography through a computer
15 system;

16 d) Procuring child pornography through a computer system for oneself
17 or for another person; or

18 e) Possessing child pornography materials in the computer system or on
19 a computer data storage medium.

20 For purposes of this Section, the term “child pornography” shall include
21 pornographic material that visually depicts: (a) a minor engaged in sexually explicit
22 conduct; (b) a person appearing to be a minor engaged in sexually explicit conduct; (c)
23 realistic images representing a minor engaged in sexually explicit conduct.

24 iii. Unsolicited Commercial Communications. – The transmission of commercial
25 electronic communication with the use of computer system which seek to
26 advertise, sell, or offer for sale products and services are prohibited unless:

27 a) There is a prior affirmative consent from the recipient; or

b) The following conditions are present:

- i) The commercial electronic communication contains a simple, valid, and reliable way for the recipient to reject receipt of further commercial electronic messages ('opt-out) from the same source;
- ii) The commercial electronic communication does not purposely disguise the source of the electronic message; and
- iii) The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

SEC. 5. *Other Offenses.*- The following acts shall also constitute an offense:

- a. Aiding or Abetting in the Commission of Cybercrime. – Any person who wilfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable.
- b. Attempt in the Commission of Cybercrime – Any person who wilfully attempts to commit any of offenses enumerated in this Act shall be held liable.

SEC. 6 *Liability under Other Laws.* – A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended or special laws.

CHAPTER III – PENALTIES

SEC. 7. *Penalties.* – Any person found guilty of any of the punishable acts enumerated in Sections 4(a) and 4(b) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two Hundred Thousand Pesos (PhP200,000.00) up to a maximum amount commensurate to the damage incurred or both.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(i) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two Hundred Thousand Pesos (PhP200,000.00) but not exceeding One Million Pesos (PhP1,000,000.00) or both.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(ii) of this Act shall be punished with imprisonment of *prision correccional* or a fine of at least One Hundred Thousand Pesos (PhP100,000.00) but not exceeding Five Hundred Thousand Pesos (PhP500,000.00) or both.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(iii) shall be punished with imprisonment of *arresto mayor* or a fine of at least Fifty Thousand Pesos (PhP50,000.00) but not exceeding Two Hundred Fifty Thousand Pesos (PhP250,000.00) or both.

Any person found guilty of any of the punishable acts enumerated in Section 5 shall be punished with imprisonment one degree lower than that of the prescribed penalty for the offense or a fine of at least One Hundred Thousand Pesos (PhP100,000.00) but not exceeding Five Hundred Thousand Pesos (PhP500,000.00) or both.

SEC 8. Corporate Liability – When any of the punishable acts herein defined is knowingly committed on behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person, who has a leading position within in, based on (a) a power of representation of the juridical person, (b) an authority to take decisions on behalf of the juridical person, or (c) an authority to exercise control within the juridical person, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Ten Million Pesos (PhP10,000,000.00).

When the commission of any of the punishable acts herein defined was made possible due to lack of supervision or control by a natural person referred to and described in the preceding paragraph, for the benefit of that juridical person by a natural person acting under its

1 authority, the juridical person shall be held liable for a fine equivalent to at least double the fines
2 imposable in Section 7 up to a maximum of Five Million Pesos (PhP5, 000,000.00).

3 The liability imposed on the juridical person shall be without prejudice to the criminal
4 liability of the natural person who has committed the offense.

6 **CHAPTER IV – ENFORCEMENT AND IMPLEMENTATION**

7 **SEC. 9. *Real-time collection of Computer Data.*** – Law enforcement authorities shall be
8 authorized to collect or record by technical or electronic means, and service providers are
9 required to collect or record by technical or electronic means, and/or to cooperate or assist law
10 enforcement authorities in the collection or recording of, traffic data, in real-time, associated
11 with specified communications transmitted by means of a computer system.

12 **SEC. 10. *Preservation of Computer Data*** – The integrity of traffic data and subscriber
13 information relating to communication services provided by a service provider shall be preserved
14 for a minimum period of six (6) months from the date of the transaction. Content data shall be
15 similarly preserved for six (6) months from the date of receipt of the order from law enforcement
16 authorities requiring its preservation.

17 Law enforcement authorities may order a one-time extension for another six (6) months
18 provided that once computer data preserved, transmitted or stored by a service provider is used
19 as evidence in a case, the mere furnishing to such service provider of the transmittal document to
20 the Office of the Prosecutor shall be deemed a notification to preserve the computer data until
21 termination of the case.

22 The service provider ordered to preserve computer data shall keep confidential the order
23 and its compliance.

24 **SEC. 11. *Disclosure of Computer Data.*** – Law enforcement authorities shall issue an
25 order requiring any person or service provider to disclose or submit subscriber's information,
26 traffic data or relevant data in his/its possession or control within seventy two (72) hours from

1 receipt of the order in relation to a valid complaint officially docketed and assigned for
2 investigation and the disclosure is necessary and relevant for the purpose of investigation.

3 Law enforcement authorities shall submit regular reports to the Department of Justice
4 (DOJ) for monitoring.

5 **SEC.12. Search, Seizure, and Examination of Computer Data** – Where a search and
6 seizure warrant is properly issued, the law enforcement authorities shall likewise have the
7 following powers and duties:

8 Within the time period specified in the warrant, to conduct interception, as defined in this
9 Act, content of communications, procure the content of data either directly, through access and
10 use of computer system, or indirectly, through the use of electronic eavesdropping or tapping
11 devices, *in real time or at the same time that the communication is occurring* and to:

- 12 a. To secure a computer system or a computer data storage medium;
- 13 b. To make and retain a copy of those computer data secured;
- 14 c. To maintain the integrity of the relevant stored computer data;
- 15 d. To conduct examination of the computer data storage medium; and
- 16 e. To render inaccessible or remove those computer data in the accessed computer or
17 computer and communication network.

18 Pursuant thereof, the law enforcement authorities may order any person who has
19 knowledge of the functioning of the computer system and the measures to protect and preserve
20 the computer data therein to provide, as is reasonable, the necessary information, to enable the
21 undertaking of the search, seizure and examination.

22 Law enforcement authorities may request for an extension of time to complete the
23 examination of the computer data storage medium and to make a return thereon but in no case
24 for a period longer than thirty (30) days from the date of approval by the court.

25 **SEC.13. Non-compliance.** – Failure to comply with the provisions of Chapter IV hereof
26 specifically the orders from law enforcement authorities shall be punished as a violation of P.D.
27 No. 1829 with imprisonment of *prision correccional* in its maximum period or a fine of One

1 Hundred Thousand Pesos (PhP100,000.00) or both, for each and every non-compliance with an
2 order issued by law enforcement authorities.

4 CHAPTER V – JURISDICTION

5 **SEC.14. *Jurisdiction*** – The Regional Trial Court shall have jurisdiction over any
6 violation of the provisions of this Act including any violation committed by a Filipino national
7 regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed
8 within the Philippines or committed with the use of any computer system wholly or partly
9 situated in the country, or when by such commission any damage is caused to a natural or
10 juridical person who, at the time the offense was committed, was in the Philippines.

12 CHAPTER VI – INTERNATIONAL COOPERATION

13 **SEC. 15. *General principle relating to international cooperation.*** – All relevant
14 international instruments on international cooperation in criminal matters, arrangement agreed on
15 the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for
16 the purpose of investigations or proceedings concerning criminal offenses related to computer
17 systems and data, or for the collection of evidence in electronic form of a criminal offense shall
18 be given full force and effect.

19 **SEC. 16. *Applicability of the Convention on Cybercrime.*** – The provisions of Chapter
20 III of the Convention on Cybercrime shall be directly applicable in the implementation of this
21 Act as it relates to international cooperation taking into account the procedural laws obtaining in
22 the jurisdiction.

24 **SEC. 17. *Competent Authority and 24/7 Point of Contact.*** – The Department of Justice
25 (DOJ) shall be responsible to ensure the provision of immediate assistance for the purpose of
26 investigations or proceedings concerning the criminal offenses related to computer system and
27 data, or for the collection of electronic evidence of a criminal offense. In this regard, there is

1 hereby created a DOJ Office of Cybercrime for facilitating or directly carrying out the provisions
2 of technical advice, preservation of data, collection of evidence, giving legal information and
3 locating suspects. The DOJ, in execution of requests for international cooperation, shall carry out
4 communications with the concerned agencies or offices specifically the national cyber security
5 office under the Commission on Information and Communication Technology (CICT) outlined
6 in Section 20 of this Act on an expedited basis which is hereby designated and shall serve as the
7 24/7 point of contact.

9 CHAPTER VII – FINAL PROVISIONS

10 **SEC. 18. Appropriations.** – The amount of Ten Million Pesos (PhP10, 000,000.00) shall
11 be appropriated annually for the implementation of this Act.

12 **SEC. 19. Implementing Rules and Regulation.** – The Department of Justice in
13 consultation with the Commission on Information and Communication Technology shall
14 formulate the necessary rules and regulations for the effective implementation of this Act
15 including the creation and establishment of a national cyber security office with the relevant
16 computer emergency response council or team.

17 **SEC.20. Separability Clause.** – If any provision of this Act is held invalid, the other
18 provisions not affected shall remain in full force and effect.

19 **SEC.21. Repealing Clause.** – All laws, decrees, or rules inconsistent with this Act are
20 hereby repealed or modified accordingly. Section 33 of Republic Act No.8792 or the Electronic
21 Commerce Act is hereby modified accordingly.

22 **SEC.22. Effectivity.** – This Act shall take effect fifteen (15) days after the completion of
23 its publication in the Official Gazette or in at least two (2) newspapers of general circulation.

24 *Approved.*

25