

DEC -7 P1 27

**SENATE**

S. No. 3553

RECEIVED BY



*Prepared jointly by the Committees on Science and Technology, Constitutional Amendments, Revision of Codes and Laws, Justice and Human Rights, and Finance with Senators Estrada, Legarda, Santiago, Villar, Roxas, Trillanes, Enrile, Lapid, Escudero and Angara as authors.*

**AN ACT DEFINING CYBERCRIME,  
PROVIDING FOR THE PREVENTION, INVESTIGATION 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 communications industries such as content production, 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 databases, 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

1 international levels, and by providing arrangements for fast and reliable  
2 international cooperation.

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

6  
7 a) **Access** – refers to the instruction, communication with, storing data in,  
8 retrieving data from, or otherwise making use of any resources of a  
9 computer system or communication network;

10  
11 b) **Alteration** - refers to the modification or change, in form or substance,  
12 of an existing computer data or program;

13  
14 c) **Communication** - refers to the transmission of information including  
15 voice and non-voice data;

16  
17 d) **Computer system** - means any device or a group of interconnected or  
18 related devices, one or more of which, pursuant to a program, performs  
19 automatic processing of data. It covers any type of computer device  
20 including devices with data processing capabilities like mobile phones  
21 and also computer networks. The device consisting of hardware and  
22 software may include input, output and storage facilities which may  
23 stand alone or be connected in a network or other similar devices. It  
24 also includes computer-data storage devices or medium.

25  
26 e) **Computer Data** - refers to any representation of facts, information, or  
27 concepts in a form suitable for processing in a computer system  
28 including a program suitable to cause a computer system to perform a  
29 function and includes electronic documents and/or electronic data  
30 messages;

31  
32 f) **Computer Program** – refers to a set of instructions executed by the  
33 computer;

34  
35 g) **Without Right** – refers to either: (1) conduct undertaken without or in  
36 excess of authority; or (ii) conduct not covered by established legal

1 defenses, excuses, court orders, justifications, or relevant principles  
2 under the law;

3  
4 h) Database – refers to a representation of information, knowledge, facts,  
5 concepts, or instructions which are being prepared, processed or  
6 stored or have been prepared, processed or stored in a formalized  
7 manner and which are intended for use in a computer system;

8  
9 i) Interception – refers to listening to, recording, monitoring or  
10 surveillance of the content of communications, including procuring of  
11 the content of data, either directly, through access and use of a  
12 computer system or indirectly, through the use of electronic  
13 eavesdropping or tapping devices, at the same time that the  
14 communication is occurring;

15  
16 j) Service Provider – refers to :

- 17  
18 i. any public or private entity that provides to users of its service  
19 the ability to communicate by means of a computer system, and  
20  
21 ii. any other entity that processes or stores computer data on behalf  
22 of such communication service or users of such service;

23  
24 k) Subscriber's Information – refers to any information contained in the  
25 form of computer data or any other form that is held by a service  
26 provider, relating to subscribers of its services other than traffic or  
27 content data and by which can be established;

28  
29 i. The type of communication service used, the technical  
30 provisions taken thereto and the period of service;

31  
32 ii. The subscriber's identity, postal or geographic address,  
33 telephone and other access number, any assigned network  
34 address, billing and payment information, available on the basis  
35 of the service agreement or arrangement;

36

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

4  
5           1) **Traffic Data or Non-Content Data** – refers to any computer data other  
6               than the content of the communication, including but not limited to the  
7               communication’s origin, destination, route, time, date, size, duration, or  
8               type of underlying service.

9  
10  
11                                       **CHAPTER II – PUNISHABLE ACTS**

12  
13           **SEC. 4. Cybercrime Offenses.** -- The following acts constitute the offense  
14               of cybercrime punishable under this Act:

15  
16           **A. Offenses against the confidentiality, integrity and availability of**  
17               **computer data and systems:**

18  
19               1. **Illegal Access** - The intentional access to the whole or any part of a  
20               computer system without right.

21  
22               2. **Illegal Interception** - The intentional interception made by technical  
23               means without right of any non-public transmission of computer data  
24               to, from, or within a computer system including electromagnetic  
25               emissions from a computer system carrying such computer data:  
26               Provided, however, That it shall not be unlawful for an officer,  
27               employee, or agent of a service provider, whose facilities are used  
28               in the transmission of communications, to intercept, disclose, or use  
29               that communication in the normal course of his employment while  
30               engaged in any activity that is necessary to the rendition of his  
31               service or to the protection of the rights or property of the service  
32               provider, except that the latter shall not utilize service observing or  
33               random monitoring except for mechanical or service control quality  
34               checks;

35  
36               3. **Data interference** - the intentional or reckless alteration of computer  
37               data without right.

1  
2 4. System Interference - the intentional or reckless hindering without  
3 right of the functioning of a computer system by inputting,  
4 transmitting, deleting or altering computer data or program.

5  
6 5. Misuse of Devices -

7  
8 a. The use, production, sale, procurement, importation,  
9 distribution, or otherwise making available, without right, of:

10  
11 i. a device, including a computer program, designed or  
12 adapted primarily for the purpose of committing any of the  
13 offenses under this Act; or

14  
15 ii. a computer password, access code, or similar data by which  
16 the whole or any part of a computer system is capable of  
17 being accessed with intent that it be used for the purpose of  
18 committing any of the offenses under this Act;

19  
20 b. The possession of an item referred to in paragraphs 5(a)(i) or (ii)  
21 above with intent to use said devices for the purpose of  
22 committing any of the offenses under this Section.

23  
24 Provided, That no criminal liability shall attach when the use,  
25 production, sale, procurement, importation, distribution, or otherwise  
26 making available, or possession of computer devices/data referred to  
27 is for the authorized testing of a computer system.

28  
29 **B. Computer-related Offenses:**

30  
31 1. Computer-related Forgery - (a) the intentional input, alteration, or  
32 deletion of any computer data without right resulting in inauthentic  
33 data with the intent that it be considered or acted upon for legal  
34 purposes as if it were authentic, regardless whether or not the data  
35 is directly readable and intelligible; (b) the act of knowingly using  
36 computer data which is the product of computer-related forgery as

1 defined herein, for the purpose of perpetuating a fraudulent or  
2 dishonest design.

- 3
- 4 2. Computer-related Fraud – the intentional and unauthorized input,  
5 alteration, or deletion of computer data or program or interference  
6 in the functioning of a computer system, causing damage thereby,  
7 with the intent of procuring an economic benefit for oneself or for  
8 another person or for the perpetuation of a fraudulent or dishonest  
9 activity; Provided, that if no damage has yet been caused, the  
10 penalty imposable shall be one degree lower.

11

12 C. Content-related Offenses:

- 13
- 14 1. Cybersex – any person who establishes, maintains or controls,  
15 directly or indirectly, any operation for sexual activity or arousal  
16 with the aid of or through the use of a computer system, for a favor  
17 or consideration.
- 18
- 19 2. Child Pornography - any person who willfully engages in the  
20 following acts:
- 21
- 22 a. Producing child pornography through a computer system;
- 23 b. Offering or making available child pornography through a  
24 computer system;
- 25 c. Distributing or transmitting child pornography through a  
26 computer system;
- 27 d. Procuring child pornography through a computer system for  
28 oneself or for another person; or
- 29 e. Possessing child pornography materials in the computer system  
30 or on a computer data storage medium.

31

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

1           3. **Unsolicited Commercial Communications.** -- The transmission of  
2 commercial electronic communication with the use of computer  
3 system which seek to advertise, sell, or offer for sale products and  
4 services are prohibited unless:

5  
6           a. There is a prior affirmative consent from the recipient; or

7           b. The following conditions are present:

8                 i. The commercial electronic communication contains a  
9 simple, valid, and reliable way for the recipient to reject  
10 receipt of further commercial electronic messages ('opt-  
11 out') from the same source;

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

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

19  
20           **SEC. 5. *Other Offenses.*** -- The following acts shall also constitute an  
21 offense:

22  
23           1. **Aiding or Abetting in the Commission of Cybercrime.** -- Any  
24 person who willfully abets or aids in the commission of any of the  
25 offenses enumerated in this Act shall be held liable.

26  
27           2. **Attempt in the Commission of Cybercrime** -- Any person who  
28 willfully attempts to commit any of offenses enumerated in this  
29 Act shall be held liable.

30  
31           **SEC. 6. *Liability under Other Laws.*** -- A prosecution under this Act shall  
32 be without prejudice to any liability for violation of any provision of the  
33 Revised Penal Code, as amended or special laws.

34  
35  
36                                 **CHAPTER III - PENALTIES**

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

6  
7       Any person found guilty of any of the punishable acts enumerated in  
8 Section 4C(1) of this Act shall be punished with imprisonment of *prision mayor*  
9 or a fine of at least Two Hundred Thousand Pesos (PhP200,000.00) but not  
10 exceeding One Million Pesos (PhP1,000,000.00) or both.

11  
12       Any person found guilty of any of the punishable acts enumerated in  
13 Section 4C(2) of this Act shall be punished with imprisonment of *prision*  
14 *correcional* or a fine of at least One Hundred Thousand Pesos (PhP100,000.00)  
15 but not exceeding Five Hundred Thousand Pesos (PhP500,000.00) or both.

16  
17       Any person found guilty of any of the punishable acts enumerated in  
18 Section 4C(3) shall be punished with imprisonment of *arresto mayor* or a fine  
19 of at least Fifty Thousand Pesos (PhP50,000.00) but not exceeding Two  
20 Hundred Fifty Thousand Pesos (PhP250,000.00) or both.

21  
22       Any person found guilty of any of the punishable acts enumerated in  
23 Section 5 shall be punished with imprisonment one degree lower than that of  
24 the prescribed penalty for the offense or a fine of at least One Hundred  
25 Thousand Pesos (PhP100,000.00) but not exceeding Five Hundred Thousand  
26 Pesos (PhP500,000.00) or both.

27  
28       **SEC. 8. Corporate Liability.** -- When any of the punishable acts herein  
29 defined are knowingly committed on behalf of or for the benefit of a juridical  
30 person, by a natural person acting either individually or as part of an organ of  
31 the juridical person, who has a leading position within in, based on (a) a  
32 power of representation of the juridical person, (b) an authority to take  
33 decisions on behalf of the juridical person, or (c) an authority to exercise  
34 control within the juridical person, the juridical person shall be held liable for  
35 a fine equivalent to at least double the fines imposable in Section 7 up to a  
36 maximum of Ten Million Pesos (Php10,000,000.00).

37



1 If the commission of any of the punishable acts herein defined was made  
2 possible due to the lack of supervision or control by a natural person referred  
3 to and described in the preceding paragraph, for the benefit of that juridical  
4 person by a natural person acting under its authority, the juridical person  
5 shall be held liable for a fine equivalent to at least double the fines imposable  
6 in Section 7 up to a maximum of Five Million Pesos (Php5,000,000.00).

7 The liability imposed on the juridical person shall be without prejudice to  
8 the criminal liability of the natural person who has committed the offence.

#### 9 10 11 **CHAPTER IV – ENFORCEMENT AND IMPLEMENTATION**

12  
13 **SEC. 9. *Real-time Collection of Computer Data.*** -- Law enforcement  
14 authorities, with due cause, and upon securing a court warrant, shall be  
15 authorized to collect or record by technical or electronic means, and service  
16 providers are required to collect or record by technical or electronic means,  
17 and/or to cooperate and assist law enforcement authorities in the collection or  
18 recording of, traffic data, in real-time, associated with specified  
19 communications transmitted by means of a computer system.

20  
21 **SEC. 10. *Preservation of Computer Data.*** -- The integrity of traffic data  
22 and subscriber information relating to communication services provided by a  
23 service provider shall be preserved for a minimum period of six (6) months  
24 from the date of the transaction. Content data shall be similarly preserved for  
25 six (6) months from the date of receipt of the order from law enforcement  
26 authorities requiring its preservation.

27  
28 Law enforcement authorities may order a one-time extension for another  
29 six (6) months provided that once computer data preserved, transmitted or  
30 stored by a service provider is used as evidence in a case, the mere  
31 furnishing to such service provider of the transmittal document to the Office of  
32 the Prosecutor shall be deemed a notification to preserve the computer data  
33 until the termination of the case.

34  
35 The service provider ordered to preserve computer data shall keep  
36 confidential the order and its compliance.

1       **SEC. 11. Disclosure of Computer Data.** -- Law enforcement authorities,  
2 upon securing a court warrant, shall issue an order requiring any person or  
3 service provider to disclose or submit subscriber's information, traffic data or  
4 relevant data in his/its possession or control within seventy two (72) hours  
5 from receipt of the order in relation to a valid complaint officially docketed  
6 and assigned for investigation and the disclosure is necessary and relevant  
7 for the purpose of investigation.

8  
9       **SEC.12. Search, Seizure, and Examination of Computer Data.** -- Where a  
10 search and seizure warrant is properly issued, the law enforcement  
11 authorities shall likewise have the following powers and duties:

12  
13       Within the time period specified in the warrant, to conduct interception, as  
14 defined in this Act, content of communications, procure the content of data  
15 either directly, through access and use of computer system, or indirectly,  
16 through the use of electronic eavesdropping or tapping devices, in real time  
17 or at the same time that the communication is occurring and to:

- 18  
19       a. To secure a computer system or a computer data storage medium;  
20       b. To make and retain a copy of those computer data secured;  
21       c. To maintain the integrity of the relevant stored computer data;  
22       d. To conduct examination of the computer data storage medium; and  
23       e. To render inaccessible or remove those computer data in the  
24       accessed computer or computer and communications network.

25  
26       Pursuant thereof, the law enforcement authorities may order any person  
27 who has knowledge about the functioning of the computer system and the  
28 measures to protect and preserve the computer data therein to provide, as is  
29 reasonable, the necessary information, to enable the undertaking of the  
30 search, seizure and examination.

31  
32       Law enforcement authorities may request for an extension of time to  
33 complete the examination of the computer data storage medium and to make  
34 a return thereon but in no case for a period longer than thirty (30) days from  
35 date of approval by the court.

1       **SEC. 13. Non-compliance.** -- Failure to comply with the provisions of  
2 Chapter IV hereof specifically the orders from law enforcement authorities  
3 shall be punished as a violation of P.D. No. 1829 with imprisonment of *prision*  
4 *correctional* in its maximum period or a fine of One Hundred Thousand Pesos  
5 (Php100,000.00) or both, for each and every non-compliance with an order  
6 issued by law enforcement authorities.

7  
8       **SEC. 14. Duties of Law Enforcement Authorities.** -- To ensure that the  
9 technical nature of cybercrime and its prevention is given focus and  
10 considering the procedures involved for international cooperation, law  
11 enforcement authorities specifically the computer or technology crime  
12 divisions or units responsible for the investigation of cybercrimes are  
13 required to submit timely and regular reports including pre-operation, post-  
14 operation and investigation results and such other documents as may be  
15 required to the Department of Justice (DOJ) for review and monitoring.

16  
17                                   **CHAPTER V – JURISDICTION**  
18

19       **SEC.15. Jurisdiction.** -- The Regional Trial Court shall have jurisdiction  
20 over any violation of the provisions of this Act including any violation  
21 committed by a Filipino national regardless of the place of commission.  
22 Jurisdiction shall lie if any of the elements was committed within the  
23 Philippines or committed with the use of any computer system wholly or  
24 partly situated in the country, or when by such commission any damage is  
25 caused to a natural or juridical person who, at the time the offense was  
26 committed, was in the Philippines.

27  
28                                   **CHAPTER VI – INTERNATIONAL COOPERATION**  
29

30       **SEC. 16. General principles relating to international cooperation.** -- All  
31 relevant international instruments on international cooperation in criminal  
32 matters, arrangements agreed on the basis of uniform or reciprocal  
33 legislation, and domestic laws, to the widest extent possible for the purposes  
34 of investigations or proceedings concerning criminal offenses related to  
35 computer systems and data, or for the collection of evidence in electronic  
36 form of a criminal offense shall be given full force and effect.

1  
2       **SEC. 17. *Applicability of the Convention on Cybercrime.*** -- The  
3 provisions of Chapter III of the Convention on Cybercrime shall be directly  
4 applicable in the implementation of this Act as it relates to international  
5 cooperation taking into account the procedural laws obtaining in the  
6 jurisdiction.

7  
8  
9                   **CHAPTER VII – COMPETENT AUTHORITIES**  
10

11       **SEC. 18. *Department of Justice.*** – The Department of Justice (DOJ) shall  
12 be responsible for extending immediate assistance for the purpose of  
13 investigations or proceedings concerning criminal offenses related to  
14 computer systems and data, or for the collection of electronic evidence of a  
15 criminal offense and to otherwise ensure that the provisions of this law are  
16 complied. In this regard, there is hereby created a DOJ Office of Cybercrime  
17 for facilitating or directly carrying out the provisions of technical advice,  
18 preservation of data, collection of evidence, giving legal information and  
19 locating suspects and all other cybercrime matters related to investigation  
20 and reporting issues.

21  
22       **SEC. 19. *Commission on Information and Communications***  
23 ***Technology.*** – The Commission on Information and Communications  
24 Technology (CICT) shall be responsible for formulating and implementing a  
25 national cyber security plan and extending immediate assistance for the  
26 suppression of real-time commission of cybercrime offenses through a  
27 computer emergency response team (CERT). In this regard, there is hereby  
28 created a CICT National Cyber Security Office to carry out the above  
29 responsibilities and all other matters related to cybercrime prevention and  
30 suppression, including capacity building.

31  
32  
33                   **CHAPTER VIII – CYBERCRIME INVESTIGATION AND**  
34                   **COORDINATION CENTER**  
35

36       **SEC. 20. *Cybercrime Investigation and Coordinating Center.*** -- There is  
37 hereby created, within thirty (30) days from the effectivity of this Act, a

1 Cybercrime Investigation and Coordinating Center, hereinafter referred to as  
2 CICC, under the control and supervision of the Office of the President, to  
3 formulate and implement the national cyber security plan.

4  
5 **SEC. 21. Composition.** -- The CICC shall be headed by the Chairman of  
6 the Commission on Information and Communications Technology as  
7 Chairman; with the Director of the NBI as Vice-Chairman; Chief of the PNP;  
8 Chief of the National Prosecution Service (NPS); and the Head of the National  
9 Computer Center (NCC) as members.

10  
11 The CICC shall be manned by a secretariat of selected personnel and  
12 representatives from the different participating agencies.

13  
14 **SEC. 22. Powers and Functions.** -- The CICC shall have the following  
15 powers and functions:

- 16 a. To prepare and implement appropriate and effective measures to  
17 prevent and suppress cybercrime activities as provided in this Act;
- 18 b. To monitor cybercrime cases being handled by participating law  
19 enforcement and prosecution agencies;
- 20 c. To facilitate international cooperation on intelligence,  
21 investigations, training and capacity building related to cybercrime  
22 prevention, suppression and prosecution;
- 23 d. To coordinate the support and participation of the business sector,  
24 local government units, and non-government organizations in  
25 cybercrime prevention programs and other related projects;
- 26 e. To recommend the enactment of appropriate laws, issuances,  
27 measures and policies;
- 28 f. To call upon any government agency to render assistance in the  
29 accomplishment of the CICC's mandated tasks and functions;
- 30 g. To perform such other functions and duties necessary for the proper  
31 implementation of this Act.

32  
33  
34 **CHAPTER IX – FINAL PROVISIONS**  
35

1       **SEC. 23. Appropriations.** -- The amount of ten million pesos  
2 (Php10,000,000.00) shall be appropriated annually for the implementation of  
3 this Act.

4  
5       **SEC. 24. Implementing Rules and Regulations.** - The Department of  
6 Justice in consultation with the Commission on Information and  
7 Communication Technology shall formulate the necessary rules and  
8 regulations for the effective implementation of this Act including the creation  
9 and establishment of a national cyber security office with the relevant  
10 computer emergency response council or team.

11  
12       **SEC. 25. Separability Clause.** -- If any provision of this Act is held  
13 invalid, the other provisions not affected shall remain in full force and effect.

14  
15       **SEC. 26. Repealing Clause.** --. All laws, decrees, or rules inconsistent  
16 with this Act are hereby repealed or modified accordingly. Section 33 of  
17 Republic Act No. 8792 or the Electronic Commerce Act is hereby modified  
18 accordingly.

19  
20       **SEC. 27. Effectivity.** -- This Act shall take effect fifteen (15) days after  
21 the completion of its publication in the Official Gazette or in at least two (2)  
22 newspapers of general circulation.

23  
24       **Approved.**  
25