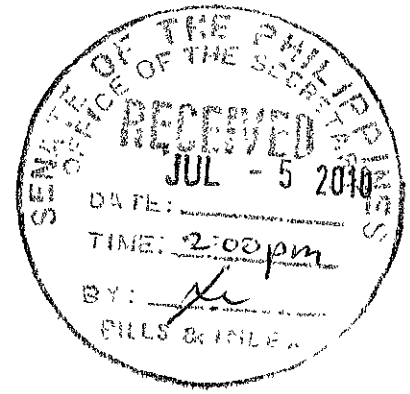


FIFTEENTH CONGRESS OF THE )  
REPUBLIC OF THE PHILIPPINES )  
First Regular Session )



SENATE

S.B. NO. 134

---

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 Filipinos in every field imaginable. It has served as venue for growth and development in business, 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 interest 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 means for the commission of other illegal acts also goes within the range of cybercrime.

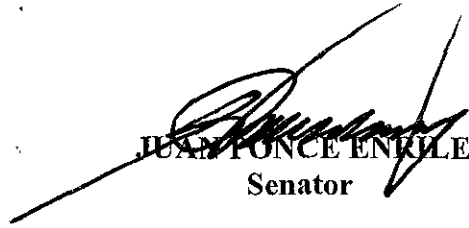
In recent years, we have witnessed how cybercrime has emerged as the latest and most complicated problem in the cyber world. Criminal activities in the cyberspace are on the rise. Computers today are being misused for illegal activities like e-mail espionage, credit card fraud, spams, and software piracy, which not only invade our privacy but also offend our senses. On many instance, 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 object of the other unlawful acts such as, but not limited to, illegal access or hacking, theft of information contained in electronics 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 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, misuses of device, 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 measures is earnestly sought.



**JUAN PONCE ENRILE**  
Senator

FIFTEENTH CONGRESS OF THE )  
REPUBLIC OF THE PHILIPPINES )  
First Regular Session )



SENATE

S.B. NO. 134

---

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

1  
2 SECTION 1. *Title* – This Act shall be known as the “Cybercrime Prevention Act of  
3 2010”.

4 SEC. 2. *Declaration of Policy* – The State recognizes the vital role of information and  
5 content industries, such as telecommunications, broadcasting, electronic commerce, and data  
6 processing, in the nation’s overall social and economic development. The State also recognizes  
7 the importance of providing an environment conducive to the development, acceleration, and  
8 rational application and exploitation of information and communications technology to attain  
9 free, easy, and intelligible access to exchange and/or delivery of information; and the need to  
10 protect and safeguard the integrity of computer, computer and communications systems,  
11 networks, and database, and the confidentiality, integrity, and availability of information and  
12 data stored therein, from all forms of misuse, abuse, and illegal access by making punishable  
13 under the law such conduct or conducts. In this light, the State shall adopt sufficient powers to  
14 effectively prevent and combat such offenses by facilitating their detection, investigation, and  
15 prosecution at both the domestic and international levels, and by providing arrangements for fast  
16 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,

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

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

8 j) Service Provider – refers to the provider of:

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

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

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

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

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

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



1 v. Misuse of Devices –

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

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

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

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

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

18 b. Computer-related Offenses:

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

26 ii. Computer-related Fraud – the intentional and unauthorized input, alteration,  
27 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





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

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

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

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

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

24 When the commission of any of the punishable acts herein defined was made possible  
25 due to lack of supervision or control by a natural person referred to and described in the  
26 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.

5

#### 6 **CHAPTER IV – ENFORCEMENT AND IMPLEMENTATION**

7 **SEC. 9. Expedited Preservation of Stored Computer Data.** – Law enforcement  
8 authorities may issue a preservation order to a service provider to preserve specified computer  
9 data that has been stored by means of a computer system in relation to a valid complaint and/or  
10 pending investigation.

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

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

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

23 **SEC. 11. *Real-time Collection of Traffic Data*.** – Law enforcement authorities shall be  
24 authorized to collect or record by technical or electronic means, and/or to require cooperation  
25 from a service provider in the collection or recording of, traffic data, in real-time, associated with  
26 specified communications transmitted by means of a computer system by issuing a collection  
27 order.

1           **SEC. 12. Interception of Content Data.** – Law enforcement authorities shall be  
2 authorized to collect or record content data upon securing a court order.

3           **SEC. 13. Disclosure of Computer Data.** – Law enforcement authorities shall issue an  
4 order requiring any person or service provider to disclose or submit subscriber’s information,  
5 traffic data or relevant data in his/its possession or control within seventy two (72) hours from  
6 receipt of the order in relation to a valid complaint officially docketed and assigned for  
7 investigation and the disclosure is necessary and relevant for the purpose of investigation.

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

10           **SEC. 14. Search, Seizure, and Examination of Computer Data** – Where a search and  
11 seizure warrant is properly issued, the law enforcement authorities shall likewise have the  
12 following powers and duties:

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

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

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

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

4 **SEC. 15. *Non-compliance.*** – Failure to comply with the provisions of Chapter IV hereof  
5 specifically the orders from law enforcement authorities shall be punished as a violation of P.D.  
6 No. 1829 with imprisonment of *prision correccional* in its maximum period or a fine of One  
7 Hundred Thousand Pesos (PhP100,000.00) or both, for each and every non-compliance with an  
8 order issued by law enforcement authorities.

#### 10 **CHAPTER V – JURISDICTION**

11 **SEC. 16. *Jurisdiction*** – The Regional Trial Court shall have jurisdiction over any  
12 violation of the provisions of this Act including any violation committed by a Filipino national  
13 regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed  
14 within the Philippines or committed with the use of any computer system wholly or partly  
15 situated in the country, or when by such commission any damage is caused to a natural or  
16 juridical person who, at the time the offense was committed, was in the Philippines.

#### 18 **CHAPTER VI – INTERNATIONAL COOPERATION**

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

25 **SEC. 18. *Applicability of the Convention on Cybercrime.*** – The provisions of Chapter  
26 III of the Convention on Cybercrime shall be directly applicable in the implementation of this

1 Act as it relates to international cooperation taking into account the procedural laws obtaining in  
2 the jurisdiction.

3 **SEC. 19. *Mutual Assistance and Cooperation.*** – The Government of the Philippines  
4 shall cooperate with, and render assistance to other nations for purposes of detection,  
5 investigation, and prosecution of offenses referred to in this Act and in the collection of evidence  
6 in electronic form in relation thereto. The principles contained in Presidential Decree No. 1069,  
7 otherwise known as the Philippine Extradition Law and other pertinent laws shall apply.

8 In this regard, the Government of the Philippines shall:

- 9 a) Provide assistance to a requesting nation in the real-time collection of traffic data  
10 *associated with specified communications in the Philippine territory transmitted by*  
11 *means of a computer system, with respect to criminal offenses defined in this law for*  
12 *which real-time collection of traffic data would be available;*
- 13 b) Provide assistance to a requesting nation in the real-time collection, recording or  
14 interception of content data of specified communications transmitted by means of a  
15 computer system;
- 16 c) Allow another state, without its authorization to:
- 17 i. access publicly available stored computer data, located in the territory, or  
18 elsewhere; or
- 19 ii. access or receive, through a computer system located in the territory, stored  
20 computer data located in another country, if the nation obtains the lawful and  
21 voluntary consent of the person who has the lawful authority to disclose the data  
22 to the nation through that computer system;
- 23 d) Entertain a request of another nation for it to order or obtain the expeditious  
24 preservation of data stored by means of a computer system, located within the  
25 territory, relative to which the requesting nation intends to submit a request for  
26 mutual assistance for the search or similar access, seizure or similar securing, or  
27 disclosure of the stored computer data.

- 1           i. A request for preservation of data under this Section shall specify:
- 2           a. the authority seeking the preservation;
- 3           b. the offense that is the subject of a criminal investigation or proceedings
- 4           and a brief summary of the related facts;
- 5           c. the stored computer data to be preserved and its relationship to the
- 6           offense;
- 7           d. the necessity of the preservation; and
- 8           e. that the requesting nation intends to submit a request for mutual assistance
- 9           for the search or similar access, seizure or similar securing, or disclosure
- 10          of the stored computer data.
- 11         ii. Upon receiving the request from another nation, the Government of the
- 12          Philippines shall take all appropriate measures to preserve expeditiously the
- 13          specified data in accordance with this law and other pertinent laws. For the
- 14          purposes of responding to a request, dual criminality shall not be required as a
- 15          condition to providing such preservation.
- 16         iii. A request for preservation may only be refused if:
- 17           a. the request concerns an offense which the Government of the Philippines
- 18           considers as a political offense or an offense connected with a political
- 19           offense; or
- 20           b. the Government of the Philippines considers the execution of the request
- 21           will prejudice its sovereignty, security, public order or other national
- 22           interest.
- 23         iv. Where the Government of the Philippines believes that preservation will not
- 24          ensure the future availability of the data, or will threaten the confidentiality of,
- 25          or otherwise prejudice the requesting nation's investigation, it shall promptly
- 26          so inform the requesting nation. The requesting nation will determine whether
- 27          its request should be executed.

1 v. Any preservation effected in response to the request referred to in Section 19,  
2 paragraph (a) shall be for a period not less than sixty days, in order to enable  
3 the requesting nation to submit a request for the search or similar access,  
4 seizure or similar securing, or disclosure of the data. Following the receipt of  
5 such a request the data shall continue to be preserved pending a decision on  
6 that request.

7 e) Accommodate request from another nation to search, access, seize, secure, or disclose  
8 data stored by means of a computer system located within Philippine territory,  
9 including data that has been preserved under the previous subsection. The  
10 Government of the Philippines shall respond to the request through the proper  
11 application of international instruments, arrangements and laws.

12 a. The request shall be responded to on an expedited basis where:

13 i. there are grounds to believe that relevant data is particularly vulnerable to  
14 loss or modification; or

15 ii. the instruments, arrangements and laws referred to in number 2 of this  
16 Section otherwise provide for expedited co-operation.

17 b. The requesting nation must maintain the confidentiality of the fact or the  
18 subject of request for assistance and cooperation. It may only use the request  
19 information subject to the conditions specified in the grant.

20 **SEC. 20. Cooperation Based on Reciprocity.** – In the absence of a treaty or agreement,  
21 mutual assistance and cooperation under Chapter VI, Section 19 of this Act shall be based on the  
22 principle of reciprocity.

23 **SEC. 21. Spontaneous Information.** – Information obtained within the framework of  
24 investigation and enforcement may be forwarded to another nation without prior request when  
25 the disclosure of such information might assist in initiating or carrying out investigations or  
26 proceedings concerning criminal offenses punishable in the Convention on Cybercrime or might  
27 lead to a request for cooperation.



**CHAPTER VII – COMPETENT AUTHORITIES**

**SEC. 22. *Department of Justice.*** – The Department of Justice (DOJ) shall be responsible for extending immediate assistance for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of electronic evidence of a criminal offense and to otherwise ensure that the provisions of this law are complied. In this regard, there is hereby created a DOJ Office of Cybercrime for facilitating or directly carrying out the provisions of technical advice, preservation of data, collection of evidence, giving legal information and locating suspects and all other cybercrime matters related to investigation and reporting issues. It shall investigate and prosecute the punishable acts defined in this Act.

Law enforcement authorities specifically the computer or technology crime divisions or units responsible for the investigation of cybercrimes are deputized under the Department of Justice Office of Cybercrime created in this Act to ensure the proper and effective implementation of this Act.

**SEC. 23. *Commission on Information and Communications Technology.*** – The Commission on Information and Communications Technology (CICT) shall be responsible for formulating and implementing a national cyber security plan and extending immediate assistance for the suppression of real-time commission of cybercrime offenses through a computer emergency response team (CERT).

**CHAPTER VIII– CYBERCRIME INVESTIGATION AND COORDINATING CENTER**

**SEC. 24. *Creation of the Cybercrime Investigation and Coordinating Center.*** – There is hereby created, within thirty (30) days from the effectivity of this Act, a Cybercrime Investigation and Coordinating Center, hereinafter referred to as CICC, which shall have the following powers and functions:

- a. Prepare and implement appropriate and effective measures to prevent and suppress cybercrime activities as provided in this Act;

- 1 b. Monitor cybercrime cases being handled by law enforcement authorities and  
2 prosecution agencies and require the submission of timely reports;
- 3 c. Facilitate international cooperation on intelligence, investigations, training and  
4 capacity building related to cybercrime prevention, suppression and prosecution;
- 5 d. Designate a point of contact available on a twenty-four hour, seven-day-a-week basis;
- 6 e. Coordinate the support and participation of the business sector, local government  
7 units, and non-government organizations in cybercrime prevention programs and  
8 other related projects;
- 9 f. Recommend the enactment of appropriate laws, issuances, measures and policies;
- 10 g. Call upon any government agency to render assistance in the accomplishment of the  
11 CICC's mandated tasks and functions;
- 12 h. Perform such other functions and duties necessary for the proper implementation of  
13 this Act.

14 **SEC. 25. *Composition Cybercrime Investigation and Coordinating Center.*** – The CICC  
15 shall be chaired by the Secretary of Justice or his representative with the following agencies as  
16 members:

- 17 a. Chairperson of the Commission on Information and Communications Technology  
18 (CICT);
- 19 b. Director of the National Bureau of Investigation (NBI);
- 20 c. Chief of the Philippine National Police (PNP); and
- 21 d. Head of the National Computer Center (NCC), or their representatives as  
22 members.

23 The CICC shall be manned by a secretariat of selected personnel and representatives  
24 from the different participating agencies.

25  
26 **CHAPTER IX – FINAL PROVISIONS**

1           **SEC. 26. Appropriations.** – The amount of Ten Million Pesos (PhP10,000,000.00) shall  
2 be appropriated annually for the implementation of this Act.

3           **SEC. 27. Implementing Rules and Regulations.** – The Department of Justice (DOJ), in  
4 consultation with the agencies mentioned in the creation of the Cybercrime Investigation and  
5 Coordinating Center, shall formulate the necessary rules and regulations for the effective  
6 implementation of this Act including the establishment of a national cyber security plan and the  
7 relevant computer emergency response team.

8           **SEC. 28. Separability Clause.** — If any provision of this Act is held invalid, the other  
9 provisions not affected shall remain in full force and effect.

10           **SEC. 29. Repealing Clause.** – All laws, decrees, or rules inconsistent with this Act are  
11 hereby repealed or modified accordingly. The provisions of Presidential Decree No. 1829,  
12 Republic Act Nos. 4200, 8792 and 9372 are hereby modified accordingly.

13           **SEC. 30. Effectivity.** – This Act shall take effect fifteen (15) days after the completion of  
14 its publication in the Official Gazette or in at least two (2) newspapers of general circulation.