

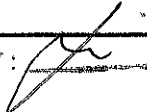
FIFTEENTH CONGRESS OF THE
REPUBLIC OF THE PHILIPPINES)
First Regular Session)

OFFICE OF THE CLERK OF THE SENATE

SENATE
S. B. NO. **2534**

10 SEP 22 06:00

Introduced by **SENATOR FERDINAND R. MARCOS, JR.**

RECEIVED BY: 

EXPLANATORY NOTE

This bill seeks to define cybercrimes, set parameters for its prevention and investigation, and impose penalties for its violation.

High technology has proven to be a useful tool in the world today. Almost every transaction necessitates the use of computer and other related electronic devices. It makes business operations, deals in the government, commercial establishments, academic institutions and other public organization or office much easier and less complicated.

It is however unfortunate that technology is sometimes used to the detriment of the public.

Nowadays, methods of digital attacks, identity theft, and hacking, to mention a few, beleaguer the information technology system. Computers nowadays are used to commit crimes where confidential information is lost or intercepted, or where one's privacy is violated.

This legislative measure enumerates offenses against the confidentiality, integrity and availability of computer data and system, computer-related offenses, and content-related offenses. It provides penalties against individuals violating this proposed law, and enforces corporate liability.

Under this bill, the Regional Trial Court shall have jurisdiction over any violation committed by a Filipino national regardless of the place of commission. Likewise, the Government of the Philippines shall cooperate with, and render assistance to other nations for purposes of detection, investigation, and prosecution of offenses referred to in this proposed Act and in the collection of evidence in electronic form in relation thereto.

Furthermore, there is hereby created a Department of Justice Office of Cybercrime mandated to facilitate or directly carry out the provisions of technical advice, preservation of data, collection of evidence, give legal information and locate suspects and all other cybercrime matters related to investigation and reporting issues. It shall investigate and prosecute the punishable acts defined herein.

The Cybercrime Investigation and Coordinating Center is likewise created, which is tasked, among others, to prepare and implement appropriate and effective measures to prevent and suppress cybercrime activities.

There is a pressing need to address this matter through legislation so that once and for all, cybercrime will no longer plague the society.

In view thereof, the passage of this bill is earnestly requested.


FERDINAND R. MARCOS, JR.

10 SEP 22 10:00

SENATE
S. B. NO. **2534**

Introduced by SENATOR FERDINAND R. MARCOS, JR.

RECEIVED BY

**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 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 2010”.

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

SECTION 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 system or communication network;
- b) Alteration – refers to the modification or change, in form or substance, of an existing computer data or program;
- c) Communication – refers to the transmission of information including voice and non-voice data;
- d) Computer system – refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data. It covers any type of computer device including devices with data processing capabilities like mobile phones and also computer networks consisting of hardware and software may include input, output and storage facilities which may stand alone or be connected in a network or other similar devices. It also includes computer-data storage devices or medium;

- e) Computer data – refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system including a program suitable to cause a computer system to perform a function and includes electronic documents and/or electronic data messages;
- f) Computer program – refers to a set of instructions executed by the computer;
- g) Without right – refers to either: (i) conduct undertaken without or in excess of authority; or (ii) conduct not covered by established legal defenses, excuses, court orders justifications, or relevant principles under the law.
- h) Database – refers to a representation of information, knowledge, facts, concepts, or 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 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:
 - i. Any public or private entity that provides to users of its service the ability to communicate by means of a computer system, or
 - 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 subscriber's 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 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.
- l) 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

SECTION 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:

1. Illegal access – the intentional access to the whole or any part of a computer system without right.

2. 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 it shall not be unlawful for an officer, employee, or agent of 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;

3. Data interference – the intentional or reckless alteration of computer data without right.

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

5. 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 offenses 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 testing of a computer system.

B. Computer-related offenses:

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

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

C. Content-related offenses:

1. Cybersex – any person who establishes, maintains or controls, directly or indirectly, any operation for sexual activity or arousal with the aid of or through the use of computer system, for a favor or consideration.
2. Child pornography – any person who willfully engages in the following acts:
 - a. Producing child pornography through computer system;
 - b. Offering or making available child pornography through a computer system;
 - c. Distributing or transmitting child pornography through a computer system;
 - d. Procuring child pornography through a computer system for oneself or for another person; or
 - e. Possessing child pornography materials in the computer system or on a computer data storage medium.

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

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

- 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.

SECTION 5. Other offenses. – The following acts shall also constitute an offense:

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

SECTION 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 4A and 4B 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 4C(1) 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 4C(2) 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 4C(3) of this Act 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 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.

SECTION 8. Corporate liability. – When any of the punishable acts herein defined are 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).

If the commission of any of the punishable acts herein defined was made possible due to the 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 authority, 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 Five Million Pesos (PhP5,000,000.00).

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

CHAPTER IV – PROCEDURE

SECTION 9. Expedited preservation of stored computer data. – Law enforcement authorities may issue a preservation order to a service provider to preserve specified computer data that has been stored by means of a computer system in relation to a valid complaint and/or pending investigation.

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

Law enforcement authorities may order a one-time extension for another six (6) months provided that once computer data preserved, transmitted or stored by a service provider is used as evidence in a case, the mere furnishing to such service provider of

the transmittal document to the Department of Justice shall be deemed a notification to preserve the computer data until the termination of the case.

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

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

SECTION 12 Interception of content data. – Law enforcement authorities shall be authorized to collect or record content data upon securing a court order.

SECTION 13. Disclosure of subscriber's information, traffic data or relevant data. – Law enforcement authorities may issue a disclosure order requiring a service provider to disclose or submit subscriber's information, traffic data or relevant data in its possession or control within seventy two (72) hours from receipt of the order in relation to a valid complaint and/or pending investigation.

SECTION 14. Search, seizure, and examination of computer data. –Where a search and seizure warrant is properly issued, the law enforcement authorities shall likewise have the following powers and duties:

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

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

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

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

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

CHAPTER V – JURISDICTION

SECTION 16. Jurisdiction. – The Regional Trial Court shall have jurisdiction over any violation committed by a Filipino national regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed within the Philippines or committed with the use of any computer system wholly or partly situated

in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

CHAPTER VI – INTERNATIONAL COOPERATION

SECTION 17. Mutual Assistance and Cooperation. – The Government of the Philippines shall cooperate with, and render assistance to other nations for purposes of detection, investigation, and prosecution of offenses referred to in this Act and in the collection of evidence in electronic form in relation thereto. The principles contained in Presidential Decree No. 1069, otherwise known as the Philippine Extradition Law and other pertinent laws shall apply.

In this regard, the Government of the Philippines shall:

1. Provide assistance to a requesting nation in the real-time collection of traffic data associated with specified communications in the Philippine territory transmitted by means of a computer system, with respect to criminal offenses defined in this law for which real-time collection of traffic data would be available;
2. Provide assistance to a requesting nation in the real-time collection, recording or interception of content data of specified communications transmitted by means of a computer system;
3. Allow another state, without its authorization to:
 - a. access publicly available stored computer data, located in the territory, or elsewhere; or
 - b. access or receive, through a computer system located in the territory, stored computer data located in another country, if the nation obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the nation through that computer system;
4. Entertain a request of another nation for it to order or obtain the expeditious preservation of data stored by means of a computer system, located within the territory, relative to which the requesting nation intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.
 - a. A request for preservation of data under this Section shall specify:
 - i. the authority seeking the preservation;
 - ii. the offense that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
 - iii. the stored computer data to be preserved and its relationship to the offense;
 - iv. the necessity of the preservation; and
 - v. that the requesting nation intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.
 - b. Upon receiving the request from another nation, the Government of the Philippines shall take all appropriate measures to preserve expeditiously the specified data in accordance with this law and other pertinent laws. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.
 - c. A request for preservation may only be refused if:

- i. the request concerns an offense which the Government of the Philippines considers as a political offense or an offense connected with a political offense; or
 - ii. the Government of the Philippines considers the execution of the request will prejudice its sovereignty, security, public order or other national interest.
- d. Where the Government of the Philippines believes that preservation will not ensure the future availability of the data, or will threaten the confidentiality of, or otherwise prejudice the requesting nation's investigation, it shall promptly so inform the requesting nation. The requesting nation will determine whether its request should be executed.
- e. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting nation to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request the data shall continue to be preserved pending a decision on that request.

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

- a. The request shall be responded to on an expedited basis where:
 - i. there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
 - ii. the instruments, arrangements and laws referred to in number 2 of this Section otherwise provide for expedited co-operation.
- b. The requesting nation must maintain the confidentiality of the fact or the subject of request for assistance and cooperation. It may only use the request information subject to the conditions specified in the grant.

SECTION 18. General principles relating to international cooperation. – All relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense shall be given full force and effect.

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

SECTION 20. Cooperation based on reciprocity. – In the absence of a treaty or agreement, mutual assistance and cooperation under the preceding sections in this Chapter shall be based on the principle of reciprocity.

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

CHAPTER VII – COMPETENT AUTHORITIES

SECTION 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.

SECTION 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

SECTION 24. Cybercrime Investigation and Coordinating Center; Powers and Functions. – 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. To prepare and implement appropriate and effective measures to prevent and suppress cybercrime activities as provided in this Act;
- b. To monitor cybercrime cases being handled by law enforcement authorities and prosecution agencies and require the submission of timely reports;
- c. To facilitate international cooperation on intelligence, investigations, training and capacity building related to cybercrime prevention, suppression and prosecution;
- d. To designate a point of contact available on a twenty-four hour, seven-day-a-week basis;
- e. To coordinate the support and participation of the business sector, local government units, and non-government organizations in cybercrime prevention programs and other related projects;
- f. To recommend the enactment of appropriate laws, issuances, measures and policies;
- g. To call upon any government agency to render assistance in the accomplishment of the CICC's mandated tasks and functions;
- h. To perform such other functions and duties necessary for the proper implementation of this Act.

SECTION 25. Composition. – The CICC shall be chaired by the Secretary of Justice or his representative with the following agencies as members: Chairperson of the Commission on Information and Communications Technology (CICT); the Director of the NBI; Chief of the PNP; Head of the National Computer Center (NCC), or their representatives as members.

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

CHAPTER IX – FINAL PROVISIONS

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

SECTION 27. Implementing Rules and Regulations. – The Department of Justice (DOJ) in consultation with the agencies mentioned in the creation of the Cybercrime Investigation and Coordinating Center shall formulate the necessary rules and regulations for the effective implementation of this Act to include the establishment of the relevant computer emergency response team and/or 24/7 network.

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

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

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

Approved.