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

SENATE

S. No. 52

Introduced by SENATOR EDGARDO J. ANGARA

EXPLANATORY NOTE

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

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

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

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

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

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

EDGARDO J. ANGARA

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

OFFICE OF THE SECRETARY

10 JUL -1 A11 09

SENATE

S. No. 52 RECEIVED BY

Introduced by SENATOR EDGARDO J. ANGARA

AN ACT DEFINING CYBERCRIME, PROVIDING FOR 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 2010".

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

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

a) Access – refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer 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 - means any device or a 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. The device 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: (1) 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 of data, either directly, through access and use of a computer system or indirectly,

through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring;

j) Service Provider – refers to :

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

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

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

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

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

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

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

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

A. Offenses against the confidentiality, integrity and availability of computer data and systems:

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 authorized 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 herein, 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 a computer system, for a favor or consideration.

2. Child Pornography - any person who willfully engages in the following acts:

   a. Producing child pornography through a 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 seek 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.

SEC. 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 offenses enumerated in this Act shall be held liable.

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

CHAPTER III - PENALTIES

SEC. 7. ***Penalties.*** -- Any person found guilty of any of the punishable acts enumerated in Sections 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 correcional* 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) shall be punished with imprisonment of *arresto mayor* or a fine of at least Fifty Thousand Pesos (PhP50,000.00) but not exceeding Two Hundred Fifty Thousand Pesos (PhP250,000.00) or both.

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

SEC. 8. ***Corporate Liability.*** -- When any of the punishable acts herein defined 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 offence.

CHAPTER IV – ENFORCEMENT AND IMPLEMENTATION

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

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 data 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 Office of the Prosecutor 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.

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

SEC. 12. ***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 of 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. To secure a computer system or a computer data storage medium;
b. To make and retain a copy of those computer data secured;
c. To maintain the integrity of the relevant stored computer data;
d. To conduct examination of the computer data storage medium; and
e. To render inaccessible or remove those computer data in the accessed computer or computer and communications network.

Pursuant thereof, 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.

SEC. 13. ***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 correctional* 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.

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

CHAPTER V – JURISDICTION

SEC.15. ***Jurisdiction.*** -- The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act including 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

SEC. 16. ***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.

SEC. 17. ***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.

CHAPTER VII – COMPETENT AUTHORITIES

SEC. 18. ***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.

SEC. 19. ***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). In this regard, there is hereby created a CICT National Cyber Security Office to carry out the above responsibilities and all other matters related to cybercrime prevention and suppression, including capacity building.

CHAPTER VIII – CYBERCRIME INVESTIGATION AND COORDINATION CENTER

SEC. 20. ***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, under the control and supervision of the Office of the President, to formulate and implement the national cyber security plan.

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

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

SEC. 22. ***Powers and Functions.*** -- The CICC 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 participating law enforcement and prosecution agencies;
c. To facilitate international cooperation on intelligence, investigations, training and capacity building related to cybercrime prevention, suppression and prosecution;
d. 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;
e. To recommend the enactment of appropriate laws, issuances, measures and policies;
f. To call upon any government agency to render assistance in the accomplishment of the CICC's mandated tasks and functions;
g. To perform such other functions and duties necessary for the proper implementation of this Act.

CHAPTER IX – FINAL PROVISIONS

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

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

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

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

SEC. 27. 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.