

CONGRESS OF THE PHILIPPINES
FIFTEENTH CONGRESS
First Regular Session

HOUSE OF REPRESENTATIVES
House Bill No. 383

Introduced by Representatives
GLORIA MACAPAGAL ARROYO and DIOSDADO MACAPAGAL ARROYO

EXPLANATORY NOTE

Modern technology has made the computer and internet access central to commerce, education, entertainment, government and social interaction. Because of these tools, communication and business transactions have become efficient and expedient.

While this breakthrough is undoubtedly beneficial, it cannot be discounted that this has also been used to advance nefarious activities such as committing fraud, child pornography, intellectual property infringement, stealing of identities and privacy violation. These have come to be known as cybercrimes.

The steady growth of crimes committed through the internet has become alarming because of the global reach of internet usage. People from all walks of life may fall prey to fraudsters and other unlawful attacks.

Because of the proliferation and ease of committing cybercrimes, there is a need to ensure the security, integrity, confidentiality and dependability of the country's information and communications structure. A law that will facilitate the detection, investigation and prosecution of the misuse, abuse and illegal access of our information and communication system is therefore imperative.

This measure seeks to protect individuals and institutions from malicious attacks through electronic means.

Immediate approval of this bill is earnestly sought.


GLORIA MACAPAGAL ARROYO
Second District, Pampanga


DIOSDADO MACAPAGAL ARROYO
Second District, Camarines Sur

CONGRESS OF THE PHILIPPINES
FIFTEENTH CONGRESS
First Regular Session

HOUSE OF REPRESENTATIVES
House Bill No. 383

Introduced by Representatives
GLORIA MACAPAGAL ARROYO and DIOSDADO MACAPAGAL ARROYO

**AN ACT DEFINING CYBERCRIME, PROVIDING FOR PREVENTION,
SUPPRESSION 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”.

SEC. 2. *Declaration of Policy.* – The State recognizes the increasingly vital role of information and communications technology (ICT) as an enabler of key industries such as, banking, broadcasting, business process outsourcing, electronic commerce and telecommunications, and as a driving force for the nation's overall social and economic development. The State also recognizes the importance of providing an environment conducive to the development, acceleration and application of ICT 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 and communications systems, networks and database, and the confidentiality, integrity and availability of information and data stored therein, from all forms of misuse, abuse and illegal access by making such conduct punishable under the law. In this light, the State shall adopt sufficient powers to effectively prevent and combat such offences 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, storage of data in, retrieval of data from, or otherwise making use of any resource of a computer system.
- (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 automated processing of data. It covers any type of device with data processing capabilities including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output and storage components which may stand alone or be connected in a network or other similar devices. It also includes computer data storage devices or media.
- (E) *Computer data* refers to any representation of facts, information or concepts in a form suitable for processing in a computer system, including any program capable of causing a computer system to perform a function, as well as electronic documents or electronic data messages.
- (F) *Computer program* refers to a set of instructions executed by the computer to achieve intended results.
- (G) *Conduct without right* refers to either: (1) conduct undertaken without or in excess of authority; or (2) 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 an organized 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 procurement 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) *Phishing* refers to the act of securing personal information such as username, password, bank account numbers and credit card details for the purpose of using it in fraud, or for participating in fraudulent business practices, or for the purpose of identity theft and misrepresentation.
- (K) *Service provider* refers to: (1) any public or private entity that provides to users of its service the ability to communicate by means of a computer

system; or (2) any other entity that processes or stores computer data on behalf of such communication service or users of such service.

- (L) *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: (1) the type of communication service used, the technical provisions taken thereto and the period of service; (2) 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; or (3) any other available information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.
- (M) *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*. – The following acts constitute 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*, 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 the 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 A, 5(a) (i) or (ii) herein with the 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 Forgery. – (a) The intentional input, alteration or deletion of any computer data, without right resulting in unauthentic 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; or (b) The act of knowingly using a 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 including, but not limited to, phishing, 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. – Engaging in any of the following acts:

- (a) Establishing, maintaining or controlling, 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;
 - (b) Recording private acts including, but not limited to, sexual acts, without the consent of all parties to the said acts or disseminating any such recording by any electronic means with or without the consent of all parties to the said acts;
 - (c) Coercing, intimidating or fraudulently inducing another into doing such indecent acts for exhibition in the internet with the use of computer technologies;
 - (d) Exhibiting live or recorded shows depicting sexual or other obscene or indecent acts;
 - (e) Posting of pictures depicting sexual or other obscene or indecent acts;
 - (f) Establishing, financing, managing, producing or promoting a cybersex operation;
 - (g) Participating, in whatever form, in the cybersex operation; and
 - (h) Coercing, threatening, intimidating or inducing anyone to participate in the cybersex operation.
- (2) Child Pornography. – Engaging in any of the following acts:
- (a) Producing child pornography for the purpose of distribution through a computer system;
 - (b) Offering or making available child pornography through a computer system;
 - (c) Distribution 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 device or medium.

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

- (3) Unsolicited Commercial Communications. – The transmission of commercial electronic communication with the use of a 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 communication from the same source, also referred to as opt-out;
 - (ii) The commercial electronic communication does not purposely disguise the source of the electronic message; and
 - (iii) The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

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

- (A) Aiding or Abetting in the Commission of Cybercrime. – Any person who wilfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable; or
- (B) Attempt to Commit Cybercrime. – Any person who wilfully attempts to commit any of offenses enumerated in this Act shall be held liable.

SEC. 6. *Liability Under Other Laws.* – A prosecution under this Act shall be without prejudice to any liability for violation of any provision of Republic Act No. 3815, as amended, otherwise known as the Revised Penal Code, or any other law.

CHAPTER III PENALTIES

SEC. 7. *Penalties.* – The following penalties shall be imposed on violations under this Act:

- (A) Any person found guilty of any of the punishable acts enumerated in Section 4(A) and 4(B) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos (P200,000.00) up to a maximum amount commensurate to the damage incurred or both;
- (B) Any person found guilty of any of the punishable acts enumerated in Section 4(C)(1) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos (P200,000.00) but not exceeding One million pesos (P1,000,000.00) or both;

- (C) Any person found guilty of any of the punishable acts enumerated in Section 4(C)(2) of this Act shall be punished with imprisonment of *reclusion temporal* or a fine of at least Two hundred fifty thousand pesos (P250,000.00) but not exceeding One million two hundred fifty thousand pesos (P1,250,000.00) or both;
- (D) Any person found guilty of any of the punishable acts enumerated in Section 4(C)(3) shall be punished with imprisonment of *arresto mayor* or a fine of at least Fifty thousand pesos (P50,000.00) but not exceeding Two hundred fifty thousand (P250,000.00) or both; and
- (E) 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 (P100,000.00) but not exceeding Five hundred thousand pesos (P500,000.00) or both.

SEC. 8. *Corporate Liability.* – When any of the punishable acts herein defined is knowingly committed in 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, based on:

- (A) A power representation of the juridical person;
- (B) An authority to take decision 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 (P10,000,000.00).

When 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 (P5,000,000.00).

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 ENFORCEMENT AND IMPLEMENTATION

SEC. 9. *Law Enforcement Agencies.* – The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall designate special investigators to exclusively handle cases involving violations of this Act.

SEC. 10. *Real-time Collection of Computer Data.* – Law enforcement authorities 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 the specified communications transmitted by means of a computer system, subject to existing laws and procedures.

SEC. 11. *Preservation of Computer Data.* – The integrity of traffic data and subscriber information relating to communication services provided by a service provider shall be preserved up to a minimum period of six (6) months from the date of the transaction. Content data shall be preserved for a minimum period of 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 of 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. 12. *Disclosure of Computer Data.* – Law enforcement authorities shall be authorized to 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 investigation purposes.

SEC. 13. *Search, Seizure and Examination of Computer Data.* – Where a search and seizure warrant is properly issued, law enforcement authorities shall, within the time period specified in the warrant, have the following powers and duties:

- (A) To conduct interception, as defined in this Act, of content data;
- (B) To secure a computer system or a computer data storage medium;
- (C) To make and retain a copy of secured computer data;
- (D) To maintain the integrity of the relevant stored computer data;
- (E) To conduct examination of the computer data storage medium; and
- (F) To render inaccessible or remove those computer data in the accessed computer system.

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 expiration of the warrant.

CHAPTER V JURISDICTION

SEC. 14. *Jurisdiction.* – The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act committed within the territory of the Philippines, including Philippine ships or airships, or by a Filipino national regardless of the place of commission. Jurisdiction shall also cover any of the elements 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.

The Department of Justice (DOJ) shall designate special prosecutors to exclusively handle cases involving violations of this Act.

CHAPTER VI INTERNATIONAL COOPERATION

SEC. 15. *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:

- (A) 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 Act for which real-time collection of traffic data would be available;
- (B) 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 to the extent permitted under Republic Act No. 4200, otherwise known as the "Anti-Wiretapping Act", Republic Act No. 9372, otherwise known as the "Human Security Act of 2007", and other related and pertinent laws;

(C) Allow another nation, without its authorization to:

- (1) Access publicly available stored computer data, located in Philippine territory, or elsewhere; or
- (2) Access or receive, through a computer system located in Philippine 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;

(D) 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 Philippine 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:

(1) A request for preservation of data under this section shall specify:

- (a) The authority seeking the preservation;
- (b) The offense that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
- (c) The stored computer data to be preserved and its relationship to the offense;
- (d) The necessity of the preservation; and
- (e) 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.

(2) 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 Act 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;

(3) A request for preservation may only be refused if:

- (a) 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
- (b) The government of the Philippines considers the execution of the request will prejudice its sovereignty, security, public order or other national interest.

- (4) 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; and
 - (5) Any preservation effected in response to the request referred to in paragraph (a) shall be for a period not less than sixty (60) 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.
- (E) 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:
- (1) The request shall be responded to on an expedited basis where:
 - (a) There are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
 - (b) The instruments, arrangements and laws referred to in paragraph (B) of this section otherwise provide for expedited cooperation.
 - (2) The requesting nation must maintain the confidentiality of the fact or the subject of request for assistance and cooperation. It may only use the requested information subject to the conditions specified in the grant.

SEC. 16. *Grounds for Refusal to Cooperate.* – The government of the Philippines shall have the right to refuse cooperation under any of the following grounds:

- (A) The offense is punishable under Philippine laws and the Philippine courts have acquired jurisdiction over the person of the accused;
- (B) The information requested is privileged, protected under Philippine laws, or that which affects national security;
- (C) If, for any reason, the production of the information is unreasonable;
- (D) The foreign government requesting for assistance has previously refused without justifiable reason, a similar request by the government of the Philippines; and

- (E) The foreign government requesting for assistance has previously breached an agreement to keep the fact or subject of request confidential, or has previously violated any condition of the grant.

SEC. 17. *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.

CHAPTER VII

CYBERCRIME INVESTIGATION AND COORDINATING CENTER

SEC. 18. *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 the CICC, under the control and supervision of the Office of the President, to formulate and implement the national cyber security plan.

SEC. 19. *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; the Chief of the PNP, the 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. 20. *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 for 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 nongovernment 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; and

- (G) To perform such other functions and duties necessary for the proper implementation of this Act.

CHAPTER VIII FINAL PROVISIONS

SEC. 21. *Appropriations.* – The amount necessary to implement the provisions of this Act shall be included in the annual General Appropriations Act.

SEC. 22. *Implementing Rules and Regulations.* – The CICT and the DOJ shall jointly formulate the necessary rules and regulations for the effective implementation of this Act.

SEC. 23. *Separability Clause.* – If any provision of this Act is held invalid, the other provisions not affected shall remain in full force and effect.

SEC. 24. *Repealing Clause.* – All laws, decrees or rules inconsistent with this Act are hereby repealed or modified accordingly. Specifically, Section 33 of Republic Act No. 8792 or the Electronic Commerce Act is hereby modified accordingly.

SEC. 25. *Effectivity.* – This Act shall take effect fifteen (15) days after its publication in the *Official Gazette* or in at least two (2) newspapers of general circulation.

Approved,