CONGRESS OF THE PHILIPPINES
FIFTEENTH CONGRESS
*Second Regular Session*

# S E N A T E

## S. No. 2796

PREPARED AND SUBMITTED JOINTLY BY THE COMMITTEES ON SCIENCE AND TECHNOLOGY; CONSTITUTIONAL AMENDMENTS, REVISION OF CODES AND LAWS; EDUCATION, ARTS AND CULTURE; JUSTICE AND HUMAN RIGHTS; TRADE AND COMMERCE; PUBLIC INFORMATION AND MASS MEDIA AND FINANCE WITH SENATORS TRILLANES, ANGARA, ENRILE, ESTRADA, LAPID, VILLAR, DEFENSOR SANTIAGO, MARCOS, REVILLA JR. AND LEGARDA AS AUTHORS

AN ACT DEFINING CYBERCRIME, PROVIDING FOR 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 2012".

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 – an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device. It covers any type of computer device including devices with data processing capabilities like mobile phones and also computer networks;

e) 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;

f) 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 whether stored in local computer systems or online;

g) Computer Program – refers to a set of instructions executed by the computer;

h) Critical Infrastructure – refers to the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data so vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters;

i) Cybersecurity – refers to the collection of tools, policies, risk management approaches, actions, training, best practices,

assurance and technologies that can be used to protect the cyber environment and organization and user's assets;

j) 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;

k) 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;

l) 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;

m) 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; and

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

n) 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 identity 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 numbers, any assigned network address, billing and payment information, available on the basis of the service agreement or arrangement;

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

o) 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 access to the whole or any part of a computer system without right.

2) Illegal Interception – The 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 deletion, deterioration, alteration of computer data without right.

4) System Interference – The hindering without right of the functioning of a computer system by inputting, transmitting, deleting or altering computer data or program.

5) Cyber-squatting – The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:

i. Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;

ii. Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and

iii. Acquired without right or with intellectual property interests in it.

6) 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 6(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 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 unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent: *Provided,* That if no

damage has yet been caused, the penalty imposable shall be one degree lower.

C. Content-related Offenses:

1) Cybersex – The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.

2) Child Pornography – The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, especially as committed through a computer system.

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.

4) Libel – The unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future.

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 the 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 the punishable act under Section 4A-5 shall be punished with imprisonment of *prision mayor* or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both.

If punishable acts in Section 4A are committed against critical infrastructure, the penalty of *reclusion temporal* or a fine of at least Five hundred thousand pesos (PhP500,000.00) up to 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 the penalties as enumerated in Republic Act No. 9775 or the Anti-Child Pornography Act of 2009.

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.

1 SEC. 8. *Corporate Liability.* – When any of the punishable
2 acts herein defined are knowingly committed on behalf of or for the
3 benefit of a juridical person, by a natural person acting either
4 individually or as part of an organ of the juridical person, who has a
5 leading position within, based on (a) a power of representation of the
6 juridical person, (b) an authority to take decisions on behalf of the
7 juridical person, or (c) an authority to exercise control within the
8 juridical person, the juridical person shall be held liable for a fine
9 equivalent to at least double the fines imposable in Section 7 up to a
10 maximum of Ten million pesos (Php10,000,000.00).

11 If the commission of any of the punishable acts herein defined
12 was made possible due to the lack of supervision or control by a natural
13 person referred to and described in the preceding paragraph, for the
14 benefit of that juridical person by a natural person acting under its
15 authority, the juridical person shall be held liable for a fine equivalent
16 to at least double the fines imposable in Section 7 up to a maximum of
17 Five million pesos (Php5,000,000.00).

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

1 CHAPTER IV – ENFORCEMENT AND IMPLEMENTATION

2 SEC. 9. *Real-Time Collection of Traffic Data.* – Law
3 enforcement authorities, with due cause, shall be authorized to collect
4 or record by technical or electronic means traffic data in real-time
5 associated with specified communications transmitted by means of a
6 computer system.

7 Traffic data refer only to the communication's origin,
8 destination, route, time, date, size, duration, or type of underlying
9 service, but not content, nor identities.

10 All other data to be collected or seized or disclosed will require
11 a court warrant.

12 Service providers are required to cooperate and assist law
13 enforcement authorities in the collection or recording of the above-
14 stated information.

15 The court warrant required under this section shall only be
16 issued or granted upon written application and the examination under
17 oath or affirmation of the applicant and the witnesses he may produce
18 and the showing: (1) that there are reasonable grounds to believe that
19 any of the crimes enumerated hereinabove has been committed, or is
20 being committed or is about to be committed; (2) that there are

reasonable grounds to believe that evidence will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and (3) that there are no other means readily available for obtaining such evidence.

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 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, and:

1) To secure a computer system or a computer data storage medium;

2) To make and retain a copy of those computer data secured;

3) To maintain the integrity of the relevant stored computer data;

4) To conduct forensic analysis or examination of the computer data storage medium; and

5) 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. *Restricting or Blocking Access to Computer Data.* – When a computer data is *prima facie* found to be in violation of the provisions of this Act, the DOJ shall issue an order to restrict or block access to such computer data.

SEC. 14. *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 noncompliance with an order issued by law enforcement authorities.

SEC. 15. *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.16. *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.

There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.

## CHAPTER VI – INTERNATIONAL COOPERATION

SEC. 17. *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.

## CHAPTER VII – COMPETENT AUTHORITIES

SEC. 18. *Department of Justice (DOJ).* – There is hereby created an Office of Cybercrime within the DOJ designated as the central authority in all matters related to international mutual assistance and extradition.

SEC. 19. *Department of Science and Technology–Information and Communications Technology Office (DOST-ICTO).* – There is hereby created a National Cyber Security Center (NCSC) within the DOST-ICTO designated to formulate and implement a national

cybersecurity plan, and extend technical assistance for the suppression of real-time commission of cybercrime offenses through a Computer Emergency Response Team (CERT).

## CHAPTER VIII – NATIONAL CYBERSECURITY COORDINATING COUNCIL

SEC. 20. *National Cybersecurity Coordinating Council (NCCC).* – There is hereby created, within thirty (30) days from the effectivity of this Act, A National Cybersecurity Coordinating Council hereinafter referred to as NCCC, under the control and supervision of the Office of the President, to formulate and implement the national cybersecurity plan.

SEC. 21. *Composition.* – The NCCC shall be headed by the Executive Director of the DOST-ICTO as Chairman; with the Director of the NBI; Chief of the PNP; Head of the DOJ Office of Cybercrime, as members; and representatives from the private sector and academe.

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

SEC. 22. *Powers and Functions*. – The NCCC shall have the following powers and functions:

a) To prepare and implement appropriate and effective measures related to cybersecurity as provided in this Act;

b) To monitor cybercrime cases being handled by participating law enforcement and prosecution agencies;

c) To coordinate the support and participation of the business sector, local government units, and nongovernment organizations in cybersecurity programs and other related projects;

d) To recommend the enactment of appropriate laws, issuances, measures and policies;

e) To call upon any government agency to render assistance in the accomplishment of the NCCC's mandated tasks and functions;

f) To perform such other functions and duties as necessary.

## CHAPTER IX – FINAL PROVISIONS

SEC. 23. *Appropriations*. – The amount of Fifty million pesos (PhP50,000,000.00) shall be appropriated annually for the implementation of this Act.

SEC. 24. *Implementing Rules and Regulations*. – The Department of Justice in consultation with the Department of Science

and Technology and the Department of the Interior and Local Government, within ninety (90) days from the effectivity of this Act, shall formulate the necessary rules and regulations for the effective implementation of this Act including the creation and establishment of a national cyber security center 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-A 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,