Feedback Philippine Standard Time: Tuesday, June 8, 2021 9:37:38 AM **About** Official Gazette of the Republic of the Philippines The Official Gazette is the official journal of the Republic of the Philippines. Edited at the Office of the President of the Philippines **Under Commonwealth Act No. 638**

Republic Act No. 10175

(b) Alteration refers to the modification or change, in form or substance, of an existing computer data or program.

(f) Computer program refers to a set of instructions executed by the computer to achieve intended results.

connected in a network or other similar devices. It also includes computer data storage devices or media.

function and includes electronic documents and/or electronic data messages whether stored in local computer systems or online.

(i) Cyber refers to a computer or a computer network, the electronic medium in which online communication takes place.

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

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

(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.

(1) The type of communication service used, the technical provisions taken thereto and the period of service;

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

(i) The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:

(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.

damage has yet been caused, the penalty imposable shall be one (1) degree lower.

Provided, That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

penalty to be imposed shall be (1) one degree higher than that provided for in Republic Act No. 9775.

(bb) The commercial electronic communication does not purposely disguise the source of the electronic message; and

thousand pesos (PhP200,000.00) up to a maximum amount commensurate to the damage incurred or both.

hundred thousand pesos (PhP100,000.00) but not exceeding Five hundred thousand pesos (PhP500,000.00) or both.

(aa) A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this Act; or

(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.

GOVPH

the law.

organization and user's assets.

(n) Service provider refers to:

arrangement; and

type of underlying service.

transmission of viruses.

(5) Misuse of Devices.

offenses under this Act.

(b) Computer-related Offenses:

(1) Computer-related Forgery. —

Provided, That if no

consideration.

prohibited unless:

the future.

(c) Content-related Offenses:

not the data is directly readable and intelligible; or

(i) There is prior affirmative consent from the recipient; or

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

commensurate to the damage incurred or both, shall be imposed.

exceeding Two hundred fifty thousand pesos (PhP250,000.00) or both.

specified communications transmitted by means of a computer system.

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

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

(e) To render inaccessible or remove those computer data in the accessed computer or computer and communications network.

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.

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

(b) To coordinate the preparation of appropriate and effective measures to prevent and suppress cybercrime activities as provided for in this Act;

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

SEC. 27. Appropriations. — The amount of Fifty million pesos (PhP50,000,000.00) shall be appropriated annually for the implementation of this Act.

SEC. 29. Separability Clause — If any provision of this Act is held invalid, the other provisions not affected shall remain in full force and effect.

(d) To facilitate international cooperation on intelligence, investigations, training and capacity building related to cybercrime prevention, suppression and prosecution;

(e) To coordinate the support and participation of the business sector, local government units and nongovernment organizations in cybercrime prevention programs and other

SEC. 31. 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.

This Act which is a consolidation of Senate Bill No. 2796 and House Bill No. 5808 was finally passed by the Senate and the House of Representatives on June 5, 2012 and June 4, 2012, respectively.

(Sgd.) FELICIANO BELMONTE JR.

Speaker of the House of Representatives

(Sgd.) MARILYN B. BARUA-YAP

Secretary General House of Representatives

provide, as is reasonable, the necessary information, to enable the undertaking of the search, seizure and examination.

Within the time period specified in the warrant, to conduct interception, as defined in this Act, and:

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

completely destroy the computer data subject of a preservation and examination.

evidence in electronic form of a criminal, offense shall be given full force and effect.

SEC. 26. *Powers and Functions*. — The CICC shall have the following powers and functions:

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

ninety (90) days from approval of this Act, for its effective implementation.

(c) To monitor cybercrime cases being bandied by participating law enforcement and prosecution agencies;

pesos (PhP5,000,000.00).

available for obtaining such evidence.

is necessary and relevant for the purpose of investigation.

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

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

days from date of approval by the court.

such computer data.

cybersecurity plan.

related projects;

modified accordingly.

Approved: SEP 12 2012

Republic of the Philippines

Feedback Form

About GOVPH

• GOV.PH

Government Links

• The President

• Supreme Court • Court of Appeals • Sandiganbayan

• Office of the President

Office of the Vice President

Senate of the Philippines House of Representatives

• Official Gazette • Open Data Portal

• [PDF] Republic Act No. 10175, September 12, 2012

All content is in the public domain unless otherwise stated.

This entry was posted under Legislature, Republic Acts. Bookmark the permalink.

Learn more about the Philippine government, its structure, how government works and the people behind it.

Managed by EDP/IT Division of the <u>Presidential Communications Operations Office (PCOO)</u>

Resources

Approved,

authorities.

(c) To maintain the integrity of the relevant stored computer data;

(PhP200,000.00) but not exceeding One million pesos (PhP1,000,000.00) or both.

(iii) The following conditions are present:

and which are intended for use in a computer system.

data and by which identity can be established:

computer system carrying such computer data.

<u>September 12, 2012</u> S. No. 2796 H. No. 5808

Republic of the Philippines Congress of the Philippines Metro Manila

Fifteenth Congress Second Regular Session

Begun and held in Metro Manila, on Monday the Twenty-fifth day of July two thousand eleven. [Republic Act No. 10175]

AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE 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 (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, 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.

(c) Communication refers to the transmission of information through ICT media, including voice, video and other forms of data. (d) Computer refers to 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, smart phones, computer networks and other devices connected to the internet.

(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

(g) 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

(h) 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

(j) 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

(k) 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

(1) 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

(m) 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

(o) 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

(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

(p) 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

CHAPTER II **PUNISHABLE ACTS**

(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

(3) Data Interference. — The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or

(4) System Interference. — The intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating,

(bb) 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

(i) 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

(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:

(3) Computer-related Identity Theft. – The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right:

(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

(2) Child Pornography. — The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system: Provided, That the

(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

(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

SEC. 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by

CHAPTER III **PENALTIES**

SEC. 8. Penalties. — Any person found guilty of any of the punishable acts enumerated in Sections 4(a) and 4(b) of this Act shall be punished with imprisonment of prision mayor or a fine of at least Two hundred

If punishable acts in Section 4(a) 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

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

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(2) of this Act shall be punished with the penalties as enumerated in Republic Act No. 9775 or the "Anti-Child Pornography Act of

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 (PhP50,000.00) but not

Any person found guilty of any of the punishable acts enumerated in Section 5 shall be punished with imprisonment one (1) degree lower than that of the prescribed penalty for the offense or a fine of at least One

SEC. 9. 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, based on: (a) a power of representation of the juridical person provided the act committed falls within the scope of such authority; (b) an authority to take decisions on behalf of the juridical person: Provided, That the act committed falls within the scope of such authority; or (c) an authority to exercise control within the juridical person, the juridical

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

> CHAPTER IV ENFORCEMENT AND IMPLEMENTATION

SEC. 10. Law Enforcement Authorities. — 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

SEC. 11. 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,

SEC. 12. Real-Time Collection of Traffic Data. — Law enforcement authorities, with due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with

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

SEC. 13. 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

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

SEC. 14. 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

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

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)

SEC. 16. Custody of Computer Data. — All computer data, including content and traffic data, examined under a proper warrant shall, within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package, and shall be accompanied by an affidavit of the law enforcement authority executing it stating the dates and times covered by the examination, and the law enforcement authority who may access the deposit, among other relevant data. The law enforcement authority shall also certify that no duplicates or copies of the whole or any part thereof have been made, or if made, that all such duplicates or copies are included in the package deposited with the court. The package so deposited shall not be opened, or the recordings replayed, or used in evidence, or then contents revealed, except upon

SEC. 17. Destruction of Computer Data. — Upon expiration of the periods as provided in Sections 13 and 15, service providers and law enforcement authorities, as the case may be, shall immediately and

SEC. 19. 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

SEC. 20. Noncompliance. — Failure to comply with the provisions of Chapter IV hereof specifically the orders from law enforcement authorities shall be punished as a violation of Presidential Decree 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

> CHAPTER V **JURISDICTION**

SEC. 21. 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

> CHAPTER VI INTERNATIONAL COOPERATION

Sec. 22. 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

> CHAPTER VII COMPETENT AUTHORITIES

SEC 23. 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. 24. Cybercrime Investigation and Coordinating Center. — There is hereby created, within thirty (30) days from the effectivity of this Act, an inter-agency body to be known as the Cybercrime Investigation and Coordinating Center (CICC), under the administrative supervision of the Office of the President, for policy coordination among concerned agencies and for the formulation and enforcement of the national

SEC. 25. Composition. — The CICC shall be headed by the Executive Director of the Information and Communications Technology Office under the Department of Science and Technology (ICTO-DOST) as Chairperson with the Director of the NBI as Vice Chairperson; the Chief of the PNP; Head of the DOJ Office of Cybercrime; and one (1) representative from the private sector and academe, as members. The CICC

(a) To formulate a national cybersecurity plan and extend immediate assistance for the suppression of real-time commission of cybercrime offenses through a computer emergency response team (CERT);

(h) To perform all other matters related to cybercrime prevention and suppression, including capacity building and such other functions and duties as may be necessary for the proper implementation of this Act.

CHAPTER VIII FINAL PROVISIONS

SEC. 28. Implementing Rules and Regulations. — The ICTO-DOST, the DOJ and the Department of the Interior and Local Government (DILG) shall jointly formulate the necessary rules and regulations within

SEC. 30. 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

(Sgd.) BENIGNO S. AQUINO III President of the Philippines

(Sgd.) JUAN PONCE ENRILE President of the Senate

(Sgd.) EMMA LIRIO-REYES

Secretary of the Senate

order of the court, which shall not be granted except upon motion, with due notice and opportunity to be heard to the person or persons whose conversation or communications have been recorded.

SEC. 18. Exclusionary Rule. — Any evidence procured without a valid warrant or beyond the authority of the same shall be inadmissible for any proceeding before any court or tribunal.

SEC. 15. 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.

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.

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.

Any person found guilty of the punishable act under Section 4(a)(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.

the relevant provisions of this Act: *Provided*, That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

SEC. 7. 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.

(aa) 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;

(cc) 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.

(a) 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.

altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses.

(ii) The possession of an item referred to in paragraphs 5(i)(aa) or (bb) above with intent to use said devices for the purpose of committing any of the offenses under this section.

(ii) 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.

(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) The primary intent of the communication is for service and/or administrative announcements from the sender to its existing users, subscribers or customers; or

(b) 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.

2009": Provided, That the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775, if committed through a computer system.

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).

of this Act. The NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations of this Act.

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

post-operation and investigation results and such other documents as may be required to the Department of Justice (DOJ) for review and monitoring.

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

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

(6) 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:

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.