

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

19TH CONGRESS
Third Regular Session

HOUSE BILL NO. **10647**



Introduced by Representative Michael L. Romero

EXPLANATORY NOTE

The **1987 Constitution** mandates the state to prevent, investigate and punish **cybercrime offenses** through appropriate technology and research, adequate financial services and other related services.

For purposes of this Act, the terms enumerated 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 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 function and includes electronic documents and/or electronic data messages whether stored in local computer systems or online.

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

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

(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 the law.

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

(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 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.

(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 organization and user's assets.

(l) *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.

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

(n) *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.

(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 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; and

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

(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 type of underlying service.

This House Bill seeks to achieve and attain a higher degree of awareness in the acts and violations of **cybercrime** with the end view that harmony and order shall be maintained more effectively, and the laws enforced with more impartiality.

Thus, the early passage of this bill is earnestly requested.

A handwritten signature in black ink, appearing to read 'Michael L. Romero', with a long horizontal stroke extending to the right.

MICHAEL L. ROMERO Ph.D.

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

19TH CONGRESS
Third Regular Session

HOUSE BILL NO. **10647**

Introduced by Representative Michael L. Romero

AN ACT

AMENDING **REPUBLIC ACT NO. 10175, “CYBERCRIME PREVENTION ACT OF 2012”**, TO EFFECTIVELY SUPPRESS AND COMBAT SUCH VIOLATIONS, PROVIDING FOR STIFFER PENALTIES AND SANCTIONS AND FOR OTHER PURPOSES

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

SECTION 1. 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.

It is a declared policy of the state in conformity with the mandate of the Constitution, to promote and Filipino dignity and privacy. The State also hereby recognizes the complementary roles of public and private institutions in the invaluable contributions they have made and will make to the state.

For these purposes, the state shall provide the mechanisms to prevent and punish **cybercrime offenses** by maximizing the use of existing resources of the state, recognizing in the process the government's responsibility as having priority over its other functions.

SECTION 2. section 8 chapter III of RA10175 is hereby amended to read as follows:

CHAPTER III PENALTIES

Section 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 five hundred thousand pesos **(PhP500,000.00)** up to a maximum amount commensurate to the damage incurred or both.

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 **less than** five hundred thousand pesos **(PhP500,000.00)** or both.

If punishable acts in Section 4(a) are committed against critical infrastructure, the penalty of *reclusion temporal* or a fine of at least One million pesos **(PhP1,000,000.00)** up to maximum amount commensurate to the damage incurred or both, shall be imposed.

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 five hundred thousand pesos **(PhP500,000.00)** 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 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 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.

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 three hundred thousand pesos **(PhP300,000.00)** 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 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 three hundred thousand pesos **(PhP300,000.00)** but not exceeding one million pesos **(PhP1,000,000.00)** or both.

SECTION 3. section 9 chapter III of RA10175 is hereby amended to read as follows:

Section 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 person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 of **RA10175** up to a maximum of Fifteen million pesos **(PhP15,000,000.00)**.

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 of **RA10175** up to a maximum of Ten million pesos **(PhP10,000,000.00)**.

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

SECTION 4. section 27 chapter VIII of RA10175 is hereby amended to read as follows:

CHAPTER VIII FINAL PROVISIONS

Section 27. Appropriations. — The amount of Five hundred million pesos **(PhP500,000,000_00)** shall be appropriated annually for the implementation of this Act.

The amount necessary for the initial implementation to fund this act shall be charged under the Department of Information and Communications Technology **(DICT)**.

The amount of Five hundred Million Pesos **(Php 500,000,000.00)** for the operation and administration of this act shall be chargeable against funds for

the purpose and other sources recommended by the **Department of Budget and Management (DBM)**.

Thereafter, such amounts necessary for the implementation of this act shall be included in the annual **General Appropriations Act (GAA)**.

The agencies concerned shall provide for the continued maintenance, operation, and management of all the facilities and equipment's.

Thereafter, appropriations for the **(DICT)**, shall be included in the budget proposals under the annual **General Appropriations Act (GAA)**

The Department of Budget and Management **(DBM)** shall rationalize the existing organizational structure and staffing pattern of the **(DICT)** in accordance with the prevailing provisions and relevant compensation and position classification laws, rules and regulations.

SECTION 5. INADMISSIBILITY OF EVIDENCE. - Any record, photo or video, or copy thereof, obtained or secured by any person in violation of **RA9775 and RA 10175** shall not be admissible in evidence in any judicial, quasi-judicial, legislative or administrative hearing or investigation.

SECTION 6. PRESCRIPTION OF CRIMES. - The crime punishable under this act shall be prescribed in twenty **(20)** years.

SECTION 7. TRANSITORY PROVISION - Existing industries, businesses and offices affected by the implementation of this Act shall be given six **(6)** months transitory period from the effectivity of the IRR or such other period as may be determined, to comply with the requirements of this Act.

SECTION 8. IMPLEMENTING RULES AND REGULATIONS. – The departments and agencies charged with carrying out the provisions of this Act shall, within sixty **(60)** days after the effectivity of this Act, formulate the necessary rules and regulations for its effective implementation.

in accordance with **Republic Act No. 9775**, and **RA10175** subject to compliance with the requirements prescribed by the state.

The **DICT**, the **DOJ** and the Department of the Interior and Local Government (**DILG**) shall jointly formulate the necessary rules and regulations within ninety **(90)** days from approval of this Act, for its effective implementation.

SECTION 9. OTHER CRIMES - 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 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.

SECTION 10. 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.

SECTION 11. 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 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.

SECTION 12. OBLIGATIONS 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.

SECTION 13. 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 specified communications transmitted by means of a computer system.

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.

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

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

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 available for obtaining such evidence.

SECTION 14. 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.

SECTION 15. 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.

SECTION 16. SEARCH, SEIZURE AND EXAMINATION OF COMPUTER DATA. — Where a search and seizure warrant are properly issued, the law enforcement authorities shall likewise have the following powers and duties.

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.

SECTION 17. 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 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.

SECTION 18. 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 completely destroy the computer data subject of a preservation and examination.

SECTION 19. 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.

SECTION 20. 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.

SECTION 21. 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 Presidential Decree No. 1829 with imprisonment or prison correctional in its maximum period or a fine of Three hundred thousand pesos (**Php300,00.00**) or both, for each and every noncompliance with an order issued by law enforcement authorities.

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

SECTION 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.

Section 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 cybersecurity plan.

SECTION 25. REPEALING CLAUSE. – All laws, decrees, executive orders, rules and regulations, or parts thereof inconsistent with the provisions of 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.

SECTION 26. SEPARABILITY CLAUSE. – If, for any reason, any section or provision of this Act is held unconstitutional or invalid, the other sections or provisions hereof shall not be affected thereby.

SECTION 27. EFFECTIVITY CLAUSE. – This Act shall take effect after fifteen (15) days from its publication in the Official Gazette or in at least two (2) national newspapers of general circulation, whichever comes earlier.

Approved,