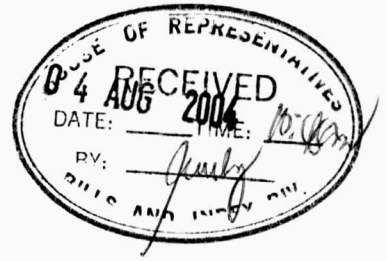


Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

THIRTEENTH CONGRESS

First Regular Session

HOUSE BILL NO. 2093



Introduced by HON. AMADO T. ESPINO, JR.

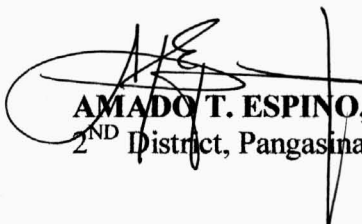
EXPLANATORY NOTE

The rapid growth of technological advancement has brought us immense benefits and convenience in almost all aspects of our lives. The advent of the E-Commerce has greatly changed the procedures and transactions in business, government or other institutions throughout the world. It has bridged the distance of a thousand miles in a matter of seconds.

The value of this high technology, however, is being exploited by criminals in advancing their criminal designs as they ride along the accessibility and convenience of the information highway, the cyber space. Without permission or authority, they access computer files, steal stored data, interfere with the smooth operation of computer systems, corrupt records with computer viruses, and even suppress utilization of much needed information. They intercept messages and send alarming and scandalous correspondence creating fear and panic among the citizenry. They even daringly access state secrets threatening national security and stability. A few years ago, the Philippines was placed in a very embarrassing situation with the introduction of the "Love Bug" virus by a local hacker. The Love Bug virus destroyed an estimated \$30 Billion worth of properties worldwide and this prompted the cyber world to be suspicious of the Philippines and consider it as a haven for cyber-terrorists and unscrupulous computer maniacs.

It is high time that we address this matter with immediate response and coordinated efforts by classifying these acts as offenses under our penal system with effective regulation and severe punishment. It is in this context that we are conforming to the new world order and new policing system.

Due to the immense importance of this measure, immediate passage of this bill is earnestly sought.


AMADO T. ESPINO, JR.
2ND District, Pangasinan

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

THIRTEENTH CONGRESS

First Regular Session

HOUSE BILL NO. 2093

Introduced by HON. AMADO T. ESPINO, JR.

AN ACT
DEFINING DEFINING CYBERCRIME, PROVIDING FOR PREVENTION,
SUPPRESSION AND IMPOSITION OF PENALTIES THEREFOR AND FOR
OTHER PURPOSES

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

Chapter I

Preliminary Provisions

SECTION 1. *Short Title* – This Act shall be known as the “Cybercrime Prevention Act of 2004”

SEC. 2. *Declaration of Basic Policies and Principles* – The State recognizes the vital role information and content industries, such as telecommunications, broadcasting, electronic commerce, and data processing, play 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 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 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 :

a. **“Access”** – refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer, computer system, network, or database.

b. **“Alteration”** – refers to the modification or change, in form or substance, of an existing computer data or program..

c. **“Computer”** – refers to any device or apparatus which, by electronic, electro-mechanical or magnetic impulse, or by other means, is capable or receiving, recording, transmitting, storing, processing, retrieving, or producing information, data, figures, symbols, or other modes of expression according to mathematical and logical rules of performing any one or more of those functions.

d. ***“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.

e. ***“Computer Program”*** – refers to a set of instructions executed by the computer to achieve intended results.

f. ***“Computer System”*** – refers to a group of interconnected or related devices, including, but not limited to, a group of interconnected computers, private branch exchange (PBX), telecommunications switching equipment, one or more of which pursuant to a program, perform automatic processing of data.

g. ***“Cybercrime”*** – refers to any of the offenses punishable by this Act.

h. ***“Damage”*** – in the general sense, refers to damage or injury as defined under the applicable laws, including but not limited to the relevant provisions of the Civil Code of the Philippines. In the limited sense, means any impairment to the integrity or availability of a computer data, program, system, information, or network.

With respect to computer data or programs as used in this Act, the words “damaging” and deteriorating” are synonymous.

i. ***“Database”*** – refers to a representation of information, knowledge, facts, concepts, or instructions which are being prepared or processed or have been prepared or processed in a formalized manner and which are intended for use in a computer, computer system, computer server, database, or network.

j. ***“Deletion”*** – refers to the destruction or impairment of information or data contained in a computer system or network by making them unrecognizable or by totally or partially obliterating the information or data from the computer system or network.

k. ***“Distribution”*** – refers to the active dissemination of data, information or material using the computer system or network.

l. ***“Information and Communication System”*** – refers to a system intended for and capable of generating, sending, receiving, storing, or otherwise processing electronic data messages or electronic documents and includes the computer system, network, or other similar device by or in which data is recorded or stored and any procedures related to the recording or storage of electronic data message or electronic document.

m. ***“Interception”*** – refers to listening to, recording, monitoring, or surveillance of the content of communications, procuring of the content of data either directly, through access and use of the computer system or network, or indirectly through the use of electronic eavesdropping or tapping devices in real time or at the same time that the communication is occurring.

n. ***“Making available of”*** – refers to the placing of online devices, including but not limited to, the creation or compilation of hyperlinks in order to facilitate access to such devices, for the use of others.

o. ***“Minor”*** – refers to a person below eighteen (18) years of age or those beyond eighteen (18) years of age but whose mental capacity is that of a person below eighteen (18) years of age.

p. ***“Network”*** – refers to a group of computers, associated devices, and/or its peripherals that are connected either permanently or temporarily by transmission and/or communications facilities which facilitate and/or provide the means of sending, communicating and/or transmitting voice and/or non-voice data and/or information electronically.

q. ***“Non-public transmission”*** – refers to the transmission of information or computer data between computer systems or networks that are not configured so that such electronic communication is readily accessible to the general public.

r. ***“Offering”*** – refers to the act of soliciting others to obtain certain computer data or information for pecuniary or other considerations.

s. ***“Procuring data or material”*** – refers to the act of actively obtaining data, information or material by downloading the same from, or by the use of, a computer system or network.

t. ***“Protected works”*** – refer to works, including but not limited to, computer programs, systems, and design, protected under Philippine laws.

u. ***“Service Provider”*** - refers the provider of:

- (1) Telecommunications and online services or network access, or the operator of communications and network facilities therefore, including entities offering the transmission, routing, or providing of connections for online communications, digital or otherwise, between or among points specified by a user, of electronic documents of the user's choosing; or
- (2) Any other entity that processes or stores information on behalf of such communication service or users of such service.

v. ***“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.

w. ***“Suppression of computer data”*** – refers to any action that prevents or terminates the availability of the data to the person who has access to the computer, computer system or network, or data carrier on which it was stored.

x. ***“By technical means”*** – refers to the use of technical devices which are fixed to transmission lines, as well as devices such as software, passwords, and codes, to collect and/or record wireless communications or those communications passing through, or generated by, computer systems or networks.

y. ***“Traffic data”*** – refers to any computer data relating to a communication by means of, or generated by, a computer system or network that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

z. ***“Without right”*** – refers to either (i) conduct undertaken without or in excess of authority, or (ii) conduct not covered by established legal defenses, excuses, justifications or relevant principles under the law.

Chapter II – PUNISHABLE ACTS

SEC. 4 The following acts shall be punishable under this Act:

4.1. **Illegal Access** - The access to the whole or any part of a computer system or network without right whether for the purpose of obtaining and/or utilizing computer data or program or in the pursuit of a dishonest intent.

4.2. **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 or network, including electromagnetic emissions from a computer system or network carrying such computer data; Provided, however, that it shall not be unlawful for an operator of a switchboard, or an officer, employee, or agent of a service provider, whose facilities are used in the transmission of electronic data, information or communications, to intercept, disclose, or use that data, information or 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.

4.3. **Data Interference** – The intentional damaging, deletion, deterioration, alteration or suppression of computer data, electronic document, or electronic data message, without right, including the introduction of or transmission of viruses.

4.4. **System Interference** – The intentional hindering or interference with the functioning of a computer system or network by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data or program, electronic document, or electronic data message, without right, including the introduction or transmission of viruses.

4.5. *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 Sections 4.1 to 4.4 hereof, or (ii) a computer password, access code, or similar data by which the whole or any part of a computer system or network is capable of being accessed;
- (b) The possession of an item referred to in paragraphs (a) (i) or (ii) above with intent to use said devices for the purpose of committing any of the offenses under Sections 4.1 to 4.4 hereof.

Provided that, no criminal liability shall attach when the use, production, sale, procurement, importation, distribution, or otherwise making available of, or possession referred to in paragraph (a) above is for the authorized testing of a computer system, program or network; *provided further that*, no criminal liability shall attach when the production or creation of the items referred to in paragraphs (a) (i) and (ii) above is for purely academic purposes; *provided, however*, that in any event, before such devices are used on a computer system or network, the prior consent of the owner of the computer system or network is obtained.

4.6. **Computer Forgery** – The input, alteration, erasure, or suppression of any computer data, computer program, electronic document, or electronic data message, or interference with the computer system or network, in a manner or under such conditions that would constitute the offense of forgery under the Revised Penal Code. The act of knowingly using computer or electronic data which are the products of computer forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design shall likewise be punishable under this Section.

4.7. **Computer Fraud** - The intentional and unauthorized input, alteration, erasure or suppression of computer data or programs, electronic document, electronic data message, or interference in the functioning of a computer system or network, 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.

4.8. **Unsolicited Commercial Communications** - The transmission of voice or data messages which seek to advertise, sell or offer for sale products and services without the prior consent of the recipient of such messages.

SEC. 5. Offenses Related to Child Pornography. Without prejudice to the prosecution under RA 9208 any person committing any of the following acts is liable under this Act:

- a) Producing child pornography for the purpose of distribution through a computer network;
- b) Offering or making available child pornography through a computer system or network; or
- c) Distributing or transmitting child pornography through a computer system or network.
- d) Remain apolitical and give loyalty and cooperation only to the legitimate leadership;

For purposes of this Section, the term “child pornography” shall include pornographic material that visually depicts (a) a minor engaged in sexually explicit conduct; or (b) a person appearing to be a minor engaged in sexually explicit conduct.

SEC. 6. Infringement of Intellectual Property Rights. – Any person who, without the knowledge and consent of the owner thereof, shall willfully copy, reproduce, disseminate, distribute, or make available online any protected works as defined herein by means of a computer system or network, for his or another person’s benefit provided that the same is inconsistent with fair use as defined in RA 8293 shall, in addition to the penalties provided for under existing laws, be penalized under this Act.

SEC. 7. Violations of the Revised Penal Code, the Consumer Act and Other Relevant Laws – Violations of Act No. 3815, as amended, or the Revised penal Code, Republic Act No. 7394 or the Consumer Act, and other relevant and pertinent laws through the use of, aided by, or involving computer systems or networks or through transactions covered by or using electronic documents or electronic data messages shall likewise be punishable and prosecuted under those laws.

For purposes of this Chapter, “electronic document” refers to information or the representation of information, data, figures, symbols, or other modes or written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved, or produced in and through computer and/or computer systems or networks. “Electronic data message” refers to information generated, sent, received, or stored by electronic, optical, or similar means.

Chapter III – Penalties

SEC. 8. Any person found guilty of any of the punishable acts enumerated in Sections 4 and 6 of this Act shall be punished with imprisonment of *prision correccional* or a fine of at least One Hundred Thousand Pesos (PhP100,000.00) but not exceeding Six Hundred Thousand Pesos (PhP600,000.00) or both fine and imprisonment.

Any person found guilty of any of the punishable acts enumerated in Section 5 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 Eight Hundred Thousand Pesos (PhP800,000.00) or both fine and imprisonment.

In case the offender does not own or possess enough property to satisfy the abovementioned fine, he shall be subjected to a subsidiary penalty of imprisonment in accordance with the rules set forth in Article 39 of Act No. 3185, as amended, or the Revised Penal Code.

SEC. 9. *Corporate Liability* - When any of the punishable acts herein defined is knowingly committed in behalf and for the benefit of a juridical person, the penalties herein provided shall be imposed upon the juridical person’s President, Secretary, members of the Board, or any of its officers and employees who have directly participated in, including those who knowingly authorized, the commission of the said act or acts.

Where the commission of any of the punishable acts herein defined by the juridical person’s employees or agents, acting within the scope of their authority, was made possible due to lack of supervision and control, either willfully or through gross negligence, of the juridical person, which resulted in benefits for said entity, the officers and members of the board of directors above-mentioned are likewise liable.

SEC. 10. *Conspiracy to Commit Cybercrime*. - When two (2) or more persons come to an agreement and decide to commit any of the punishable acts defined in this Act, and one or more of such persons does any act to effect the object of the conspiracy, each of the conspirators shall be punished as if all of the conspirators have done themselves.

SEC. 11. *Aiding or Abetting in the Commission of Cybercrime*. - Any person who willfully abet or aid in the commission of any of the offenses enumerated in Chapter II hereof shall be held liable under this Act.

SEC. 12. *Suppletory Application of the Revised Penal Code*. - The Revised Penal Code shall be made suppletorily applicable, if proper and consistent with the objectives of this Act.

CHAPTER IV

JOINT CYBERCRIME INVESTIGATION UNIT

SEC. 13. *Implementation.* - There is hereby created, within ninety (90) days from the effectivity of this Act, a Joint Cybercrime Investigation Unit (JCIU), principally to combat cybercrimes and computer-related offenses and to investigate, prosecute, and coordinate efforts of all law enforcement agencies in combating the same.

SEC. 14. *Composition.* - The JCIU shall be composed of the Anti-Fraud and Computer Crimes Division of National Bureau of Investigation (NBI), Philippine Center for Transnational Crime (PCTC) and Crimes Investigation and Detection Group (CIDG) of the Philippine National Police (PNP).

The JCIU shall be supervised by an Executive Director to be appointed by heads of the respective member organizations. The Executive Director shall possess adequate training and experience in the field of computer and information technology, communication system, or other related fields. He shall be assisted by a staff that shall from the Secretariat. Selected personnel and representatives from the participating agencies shall be designated or seconded to the JCIU.

The Executive Director may, in accordance with existing laws and rules, call upon any government agency to render assistance in the accomplishment of the JCIU's mandated tasks and functions.

SEC. 15. *Powers and Functions* – The JCIU shall have the following powers and functions:

- a) To prepare and implement appropriate and effective measures to prevent and suppress cybercrimes;
- b) To investigate and/or conduct information gathering activities in order to identify and prosecute persons and entities, including but not limited to private or government-owned corporations, government officials and employees, syndicates and their cohorts engaged in any of the punishable acts enumerated in this Act and other related activities;
- c) To effect searches and seizures in accordance with law, and to cause and/or implement the procedure for the arrest, investigation and prosecution of persons engaged in cybercrimes;
- d) To refer the case(s) prosecuted under this Act, as the JCIU may deem proper and necessary, to the Department of Justice or any other appropriate law enforcement agencies for investigation or prosecution, as the case may be;
- e) To follow up the progress of on-going investigation and prosecution of cases taken cognizance by the JCIU;
- f) To formulate and implement plans and programs for international cooperation on intelligence and investigations relative to cybercrime prevention, suppression and prosecution;
- g) To solicit and coordinate the support and participation of the business sector, local government units, and non-government organizations in cybercrime prevention programs and other related projects of the JCIU;

- h) To recommend the enactment of appropriate laws, issuances, measures, and policies; and
- i) To perform such other functions and duties necessary for the proper implementation of this Act.

Chapter IV – Enforcement And Implementation

SEC. 16. *Collection of Computer Data* – To effectively implement and enforce the provisions of this Act, the JCIU or other law enforcement officer or agencies may, subject to prior application and authority from the courts for a writ or order, require a person or service provider:

- a) To submit specified computer data in his/its possession and control, which is stored in a computer system, network, or a computer-data storage medium;
- b) To submit subscriber information in his/its possession or control;
- c) Within his/its existing technical capability, to collect or record through the application of technical means or to cooperate and assist the JCIU or its deputies or other law enforcement officers or agencies in the collection or recording of traffic data associated with, or content data of, specified communications transmitted within or passing through the territorial jurisdiction of the Philippines by means of computer system or network.

SEC. 17. *Responsibility of Service Provider* – The service provider shall keep confidential the fact of the execution of any power provided under Section 16 and any information relating thereto. The service provider shall likewise take all necessary steps to preserve the records and other evidence in its possession in accordance with the period prescribed under Section 19 hereof, pending the issuance of a court order or other processes.

SEC. 18. *Search And Seizure of Computer Data* – Where a search and seizure warrant has been properly obtained and enforced, the JCIU shall likewise have the power and duty:

- a) Within the time period specified in the warrant, to listen to, record, monitor or conduct surveillance over the content of communications, procure the content of data either directly, through access and use of the computer system or network, or indirectly, through the use of electronic eavesdropping or tapping devices, in real time or at the same time that the communication is occurring;
- b) To secure a computer system or network or part of it or a computer-data storage medium;
- c) To make and retain a copy of those computer data secured;
- d) To maintain the integrity of the relevant stored computer data; and
- e) To render inaccessible or remove those computer data in the accessed computer system or network.

Pursuant thereof, the JCIU may order any person who has knowledge about the functioning of the computer system or network 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 and seizure measure referred to in Section 15 (c).

SEC. 19. *Preservation And Disclosure of Computer Data and Traffic Record* – The integrity of a computer data and traffic record stored by means of a computer system connected to a network, where the public at large is involved, shall be preserved up to a maximum period of six (6) months from the date of the transaction. The said period may be extended by order of the JCIU upon a reasonable belief that the computer data may have been used for or in connection with, or the traffic record may contain information as regards, any violation of this Act.

In the event that such a reasonable ground exists in connection with a violation of this Act, the JCIU or its deputized officer may, after a hearing to determine probable cause, by virtue of a writ or order issued by the courts of competent jurisdiction, require the expeditious production or disclosure of traffic data to identify the service providers and the path through which the communication was transmitted.

SEC. 20. *Cost Incidental to Preservation and Collection of Data* –The cost incidental to the preservation beyond the period prescribed under the first paragraph of the preceding section, or to the expeditious production or disclosure of a sufficient amount under the second paragraph thereof, of computer data or traffic record, shall be shouldered by the person or persons who caused the preservation, production, or disclosure of the said computer data or traffic record beyond the prescribed period.

Chapter VI - Jurisdiction

SEC. 21. *Jurisdiction* – The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act committed within the territory of the Philippines. In case any of the offenses herein defined is committed outside the territorial limits of the Philippines, and by such commission any damage is caused to a computer system or network situated in the Philippines, or to a natural or juridical person who , at the time the offense was committed, is in the Philippines, the proper Regional Trial Court in the Philippines shall have jurisdiction.

Chapter VII – International Cooperation

SEC. 22. *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 punished under this Act and in the collection of evidence in electronic form in relation thereto.

SEC. 23. *Limitations on Cooperation* – No mutual assistance or cooperation shall be acted upon by the Government of the Philippines unless such request is formally made by the duly authorized representative of the foreign government concerned pursuant to or by virtue of a treaty or agreement.

The requesting party must maintain the confidentiality of the fact or the subject of the request. It may only use the requested information subject to the conditions specified in the grant.

SEC. 24. *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. 25. ***Cooperation Based on Reciprocity*** – In the absence of a treaty or agreement, mutual assistance and cooperation under the preceding sections under this Chapter shall be based on the principle of reciprocity.

SEC. 26. ***Communications Center*** – The JCIU shall be responsible for sending and answering requests for mutual assistance as well as the execution of such requests or their transmission to the proper authorities for implementation and execution.

Chapter VIII – Other Provisions

SEC. 27. ***Liability Under the Revised Penal Code and Other Laws*** – A prosecution under this Act shall be without prejudice to any liability for violation of any provision of Act. No. 3185, as amended, or the Revised Penal Code or any other law.

SEC. 28. ***Other Remedies*** – Any person who suffers damage or loss by reason of a violation of this Act may maintain a separate and independent civil action against the violator to obtain compensatory damages, injunctive and/or other equitable relief.

SEC. 29. ***Training*** – The JCIU is mandated to design a special training course in computer technology specifically focusing on cybercrime prevention and control and offer the same to qualified members of the Philippine National Police (PNP) and the National Bureau of Investigation (NBI).

Chapter IX – Final Provisions

SEC. 30. ***Appropriations*** – The amount necessary for the implementation of this Act shall be charged against the appropriations of the NBI and the PNP.

SEC. 31. ***Implementing Rules and Regulations*** – The JCIU shall formulate the necessary rules and regulations for the effective implementation of this Act.

SEC. 32. ***Public Information Campaign*** – The Office of the President, Department of Education, Department of Justice, Department of Trade and Industry, Department of Transportation and Communications, and the National Computer Center shall, in accordance with the Philippine Information Agency, undertake a public information campaign to educate the general public on the salient provisions and implication of this Act.

SEC. 33. ***Separability Clause*** – If any provision of this Act is held invalid, the other provisions not affected shall remain in full force and effect.

SEC. 34. ***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. 35. ***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) national newspapers of general circulation, whichever comes earlier.

Approved,