

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City



THIRTEENTH CONGRESS

First Regular Session

HOUSE BILL NO. 3777

Introduced by Rep. Harlin Cast. Abayon and Rep. Simeon L. Kintanar

EXPLANATORY NOTE

Information and communications technologies (ICTs) are revolutionizing our lifestyles. It has changed the way we communicate and do our daily businesses. Most of the world's critical infrastructures now run on networks and, are operated and maintained with the aid of computers and computer systems. These changes come with corresponding drawbacks, especially that aspect which concerns computer-related crimes or cybercrimes.

Cybercrimes have challenged our traditional legal structures, even long-established jurisdictions are blurred by the transnational nature of cybercrimes. It is timely for the Philippines to examine the suitability of its laws in regulating the use of computers, computer systems and networks especially after experiencing several incidents of cybercrimes in the past.

How the Philippines shall deal with cybercrimes is the interest of various stakeholders – end users and civil society, service providers, government, businesses, foreign investors, foreign governments, and multilateral organizations – as policies on cybercrimes shall bear on personal privacy, costs of doing business, national security, opportunities to do business, security and privacy of business-related information that are sent to and processed overseas, prosecution of cybercrimes that impact offshore but which originated in the Philippines, and coordination of cybercrimes with foreign and international entities.

Setting up policies that deal with cybercrimes has become more imperative as the Philippines continues to groom itself to be the most apparent choice for foreign companies to locate their offshore outsourcing businesses.

Cybercrimes fall into one of four (4) categories: computer as targets, computer as instruments in committing a crime, computer as incidental to other crimes, and computer as the direct cause of new forms of crimes. The Philippines has enacted a number of laws that are related to some of these new categories of crimes however, there is a need to determine whether or not there is a pressing need for the enactment of a new law on cybercrimes. If so, another issue needs to be resolved – what form should this legislation take?

The rationale behind cybercrime legislation is that new forms of crimes have developed, and penalties for which have to be explicitly identified in our laws. Cybercrime legislation must be an immediate concern for Congress, for reasons similar to stakeholders' interests identified above, most especially in the aspect of ensuring national security.

Having reviewed existing Philippine laws that are pertinent to cybercrime legislation (i.e. R.A. 8792, R.A. 8293, R.A. 7394, R.A. 7610, R.A. 9208, R.A. 4200, and Act 3815), it was concluded that Philippine laws lack a comprehensive set of regulations on cybercrimes. There is need thus for the Philippine to have a law that will define cybercrimes, identify punishable acts, involving computers with corresponding penalties, determine legal procedures for the investigation and prosecution of cybercrimes, clarify jurisdictions, provide for a clause on mutual assistance and cooperation, and identify a local body that shall be responsible for providing a 24/7 assistance to foreign entities in the resolution of cybercrime cases.

In view of the foregoing, the approval of this bill is earnestly sought.



HARLIN CAST. ABAYON



SIMEON L. KINTANAR

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

THIRTEENTH CONGRESS

First Regular Session

HOUSE BILL NO. 3777

Introduced by Rep. Harlin Cast. Abayon and Rep. Simeon L. Kintanar

AN ACT
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:*

1 CHAPTER I – PRELIMINARY PROVISIONS

2 SECTION 1. *Title.* – This Act shall be known as the “Cybercrime Prevention Act
3 of 2005”.

4 SEC. 2. *Declaration of Policy.* – The State recognizes the vital role of
5 information and content industries, such as telecommunications, broadcasting,
6 electronic commerce, and data processing, play in the nation’s overall social and
7 economic development. The State also recognizes the importance of providing
8 an environment conducive to the development, acceleration, and rational
9 application and exploitation of information and communications technology to
10 attain free, easy, and intelligible access to exchange and/or delivery of
11 information; and the need to protect and safeguard the integrity of computer,
12 computer systems, networks, and database, and the confidentiality, integrity, and
13 availability of information and data stored therein, from all forms of misuse,
14 abuse, and illegal access by making punishable under the law such conduct or
15 conducts. In this light, the State shall adopt sufficient powers to effectively

1 prevent and combat such offenses by facilitating their detection, investigation,
2 and prosecution at both the domestic and international levels and by providing
3 arrangements for fast and reliable international cooperation.

4 SEC. 3. *Definition of Terms.* – For purposes of this Act, the following
5 terms are hereby defined as follows:

- 6 a. Access – refers to the instruction, communication with, storing data in,
7 retrieving data from, or otherwise making use of any resources of a
8 computer, computer network, or database.
- 9 b. Alteration - refers to the modification or change, in form or substance, of
10 an existing computer data or program.
- 11 c. Communication - refers to the transmission of information, including
12 voice and non-voice data.
- 13 d. Computer - refers to any device or apparatus which, by electronic,
14 electro-mechanical, or magnetic impulse, or by other means, is capable
15 of receiving, recording, transmitting, storing, processing, retrieving, or
16 producing information, data, figures, symbols, or other modes of
17 expression according to mathematical and logical rules of performing any
18 one or more of those functions, including its associated devices and
19 peripherals.
- 20 e. Computer Data - refers to any representation of facts, information, or
21 concepts in a form suitable for processing in a computer system,
22 including a program suitable to cause a computer system to perform a
23 function.
- 24 f. Computer Network or Networks - refers to:
 - 25 i. a group of computers, associated devices, and/or its
26 peripherals that are connected either permanently or temporarily
27 by transmission and/or communications facilities which facilitate
28 and/or provide the means of sending, communicating, and/or
29 transmitting voice and/or non-voice data and/or information
30 electronically; or

1 ii. a group of interconnected or related devices, including, but not
2 limited to, a group of interconn4ected computers, private
3 exchange branch (PBX), telecommunications switching
4 equipment, one or more of which, pursuant to a program,
5 perform automatic processing of data.

6 g. Computer Program – refers to a set of instructions executed by the
7 computer to achieve intended results.

8 h. Cybercrime – refers to any of the offenses punishable by this Act.

9 i. Damage – in the general sense, refers to damage or injury as defined
10 under the applicable laws, including but not limited to the relevant
11 provision of the Civil Code of the Philippines. In the limited sense, means
12 any impairment to the integrity or availability of a computer data,
13 program, system information, or network.

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

16 j. Database – refers to a representation of information, knowledge, facts,
17 concepts, or instructions which are being prepared or processed or have
18 been prepared or processed in a formalized manner and which are
19 intended for use in a computer, computer network, computer server, or
20 database.

21 k. Deletion – refers to the destruction or impairment of information or data
22 contained in a computer or computer network by making them
23 unrecognizable or by totally or partially obliterating the information or data
24 from the computer or computer network.

25 l. Distribution – refers to the active dissemination of data, information or
26 material using the computer or computer network.

27 m. Electronic Data Message – refers to information generated, sent,
28 received, or stored by electronic, optical, or similar means.

29 n. Electronic Document – refers to information or the representation of
30 information, data, figures, symbols, or other modes or written expression,
31 described or however, represented, by which a right is established or an

- 1 obligation extinguished, or by which a fact may be proved and affirmed,
2 which is received, recorded, transmitted, stored, processed, retrieved, or
3 produced in and through computer and/or computer networks.
- 4 o. **Information and Communication System** – refers to a system intended for
5 and capable of generating, sending, receiving, storing, or otherwise
6 processing electronic data messages or electronic documents and
7 includes the computer network or other similar device by or in which data
8 is recorded or stored and any procedures related to the recording or
9 storage of electronic data message or electronic document.
- 10 p. **Interception** – refers to listening to, recording, monitoring or surveillance
11 of the content of communications, including procuring of the content of
12 data, either directly, through access and use of the computer or computer
13 network or indirectly, through the use of electronic eavesdropping or
14 tapping devices, at the same time that the communication is occurring.
- 15 q. **Making Available of** – refers to the placing of online devices, including ubt
16 not limited to, the creation or compilation of hyperlinks in order ot
17 facilitate access to such devices, for the use of others.
- 18 r. **Minor** – refers to a person below eighteen (18) years of age or those
19 beyond eighteen (18) years of age but whose mental capacity is that of a
20 person below eighteen (18) years of age.
- 21 s. **Non-Public Transmission** – refers to the transmission of information or
22 computer data between computer or computer networks that are not
23 configures so that such electronic communication is readily accessible to
24 the general public.
- 25 t. **Procuring Data or Material** – refers to the act of actively obtaining data,
26 information or material by downloading the same from a computer or
27 computer network.
- 28 u. **Protected Works** – refer to works, including but not limited to computer
29 programs, systems, and design, protected under Philippine laws.
- 30 v. **Service Provider** – refers to the provider of:

- 1 i. Telecommunications and online services or network access, or
2 the operator of communications and network facilities, therefore,
3 including entities offering the transmission, routing, or providing
4 of connections for online communications, digital or otherwise,
5 between or among point specified by a user, of electronic
6 documents of the user's choosing; or
7 ii. Any other entity that processes or stores information on behalf
8 of such communication service or users of such service.
- 9 w. Subscriber's Information – refers to any information contained in the form
10 of computer data or any other form that is held by a service provider,
11 relating to subscribers of its services other than traffic or content data and
12 by which can be established:
- 13 i. The type of communication service used, the technical
14 provisions taken thereto and the period of service.
- 15 ii. The subscriber's identity, postal or geographic address,
16 telephone and other access number, any assigned network
17 address, billing and payment information, available on the basis
18 of the service agreement or arrangement.
- 19 x. Suppression of Computer Data – refers to any action that prevents or
20 terminates the availability of the data to the person who has access to the
21 computer or computer network on which it was stored.
- 22 y. By Technical Means – refers to the use of technical devices which are
23 fixed to transmission lines, as well as devices such as software,
24 passwords, and codes to collect and /or record wireless communications
25 or those communications passing through, or generated by computer or
26 computer networks.
- 27 z. Traffic Data or Non-Content Data – refers to any computer data other
28 than the content of the communication, including but not limited to the
29 communication's origin, destination, route, time, date, size, duration, or
30 type of underlying service.

1 aa. Without Right – refers to either: (1) conduct undertaken without or in
2 excess of authority; or (ii) conduct not covered by established legal
3 defenses, excuses, court orders, justifications, or relevant principles
4 under the law.

5 CHAPTER II – PUNISHABLE ACTS

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

- 7 1. *Illegal Access.* - The access to the whole or any part of a computer or
8 computer network without right.
- 9 2. *Illegal Interception.* - The interception made by technical means without
10 right of any non-public transmission of computer data to, from, or within a
11 computer or computer network, including electromagnetic emissions from
12 a computer or computer network carrying such computer data; Provided,
13 however, that it shall not be unlawful for an officer, employee, or agent of
14 a service provider, whose facilities are used in the transmission of
15 communications, to intercept, disclose, or use that communication in the
16 normal course of his employment while engaged in any activity that is
17 necessary to the rendition of his service or to the protection of the rights
18 or property of the service provider, except that the latter shall not utilize
19 service observing or random monitoring except for mechanical or service
20 control quality checks; Provided, finally, that it shall not be unlawful for a
21 person to intercept or record a communications where there is no
22 reasonable expectation of privacy.
- 23 3. *Data interference.* - The intentional or reckless damaging, deletion,
24 deterioration, alteration or suppression of computer data, electronic
25 document, or electronic data message, without right, including the
26 introduction or transmission of viruses.
- 27 4. *System Interference.* - The Alteration, or reckless hindering or
28 interference with the functioning of a computer or computer network by
29 inputting, transmitting, damaging, deleting, deteriorating, altering, or
30 suppressing computer data or program, electronic document, or

1 electronic data message, without right, including the introduction or
2 transmission of viruses.

3 5. *Misuse of Devices* –

4 a. The use, production, sale, procurement, importation, distribution, or
5 otherwise making available, without right, of: (1) a device, including
6 a computer program, designed or adapted primarily for the purpose
7 of committing any of the offenses under Section 4.1 to 4.4 hereof;
8 or (ii) a computer password, access code, or similar data by which
9 the whole or any part of a computer or computer network is
10 capable of being accessed;

11 b. The possession of an item referred to in paragraphs (a) (i) or(ii)
12 above with intent to use said devices for the purpose of committing
13 any of the offenses under Section 4.1 to 4.4 hereof.

14 *Provided*, That no criminal liability shall attach when the use,
15 production, sale, procurement, importation, distribution, or
16 otherwise making available of, or possession referred to in
17 paragraph (a) above is for : (i) the authorized testing of a computer,
18 computer network, or computer program; or (ii) purely academic
19 purposes; *Provided*, However, that in any event, before such
20 devices are used on a computer or computer network, the prior
21 consent of the owner of the computer or computer network is
22 obtained.

23 6. *Computer Fraud*. – The intentional and unauthorized input, alteration,
24 erasure or suppression of computer data or program, electronic
25 document, or electronic data message, or interference in the functioning
26 of a computer or computer network, causing damage thereby, with the
27 intent of procuring an economic benefit for oneself or for another person
28 or for the perpetuation of a fraudulent or dishonest activity.

29 7. *Unsolicited Commercial Communications*. — The transmission of
30 electronic messages with the use of computers, computer networks, or

1 other communication devices which seek to advertise, sell, or offer for
2 sale products and services are prohibited unless:

- 3 a. There is a prior affirmative consent from the recipient; or
- 4 b. The following conditions are present:
 - 5 i. The commercial electronic communication contains a simple,
6 valid, and reliable way for the recipient to reject receipt of further
7 commercial electronic messages (also known as 'opt-out') from
8 the same source;
 - 9 ii. The commercial electronic communication does not
10 purposely disguise the source of the electronic message;
11 and
 - 12 iii. The commercial electronic communication does not
13 purposely include misleading information in any part of the
14 message in order to induce the recipients to read the
15 message.

16 SEC. 5. *Offenses Related to Prostitution & Child Pornography.* - Without
17 prejudice to the prosecution under Republic Act No. 9208 and Republic Act No.
18 7610, any person who in any manner advertises, promotes, or facilitates the
19 commission of prostitution through the use of information and communications
20 technology such as but not limited to computers, computer networks, television,
21 satellite, mobile telephone, or any person committing any of the following acts is
22 liable under this Act::

- 23 a. Producing child pornography for the purpose of distribution
24 through a computer or computer network;
- 25 b. Offering or making available child pornography through a
26 computer or computer network; or
- 27 c. Distribution or transmitting child pornography through a
28 computer or computer network.

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

1 explicit conduct and the term "prostitution" shall refer to any act, transaction,
2 scheme or design involving the use of a person by another, for sexual
3 intercourse or lascivious conduct in exchange for money, profit or any other
4 consideration.

5 SEC. 6. *Violations of the Revised Penal Code, the Intellectual Property*
6 *Code, the Consumer Act and Other Relevant Laws.* -- Violations of Act No.
7 3815, as amended, or the Revised Penal Code, Republic Act No. 8293 or the
8 Intellectual Property Code, Republic Act No. 7394 or the Consumer Act, and
9 other relevant and pertinent laws through the use of, aided by, involving
10 computers or computer networks or through transactions covered by or using
11 electronic documents or electronic data messages shall likewise be punishable
12 and prosecuted under those laws.

13 CHAPTER III - PENALTIES

14 SEC. 7. *Penalties.* -- Any person found guilty of any of the punishable
15 acts enumerated in Section 4.1 to 4.5 of this Act shall be punished with a fine of
16 at least One Hundred Thousand Pesos (PhP 100,000.00) and a maximum
17 commensurate to the damage incurred and a mandatory imprisonment of *prision*
18 *mayor*.

19 Any person found guilty of any of the punishable acts enumerated in
20 Section 4.6 and 4.7 of this Act shall be punished with imprisonment of *prision*
21 *correccional* or a fine of at least one hundred thousand pesos (PhP 100,000.00)
22 but not exceeding six hundred thousand pesos (PhP 600,000.00) or both fine
23 and imprisonment.

24 Any person found guilty of any of the punishable acts enumerated in
25 Section 5 of this Act shall be punished with a fine of at least Two Hundred
26 Thousand Pesos (PhP 200,000.00) but not exceeding eight Hundred Thousand
27 Pesos (PhP 800,000.00) and a mandatory imprisonment of *prision mayor*.

28 For punishable acts under this Act, the maximum penalty shall be imposed
29 for offenses --

1 a) whereby information that has been determined by the Philippine
2 government pursuant to law, executive order, or other issuance to be
3 confidential is communicated, delivered or transmitted to any person not
4 authorized to receive it; and

5 b) whereby the offender, without authorization to access any non-public
6 computer of a department or agency of the Philippines, accesses such a
7 computer of the department or agency of the Philippines.

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

12 SEC. 8. *Corporate Liability.* – When any of the punishable acts herein
13 defined is knowingly committed in behalf and for the benefit of a juridical person,
14 the penalties herein provided shall be imposed upon the juridical person's
15 president, secretary, members of the board of directors, or any of its officers and
16 employees who have directly participated in, including those who knowingly
17 authorized, the commission of the said act or acts.

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

23 SEC.9. *Conspiracy to Commit Cybercrime.* -- When two (2) or more
24 persons come to an agreement and decide to commit any of the punishable acts
25 defined in this Act, and one or more of such persons does any act to effect the
26 object of the conspiracy, each of the conspirators shall be punished as if all of the
27 conspirators have done the act themselves.

28 SEC. 10. *Aiding or Abetting in the Commission of Cybercrime.* -- Any
29 person who willfully abet or aid in the commission of any of the offenses
30 enumerated in Chapter II hereof shall be held liable under this Act.

1 CHAPTER IV – CYBER-CRIME INVESTIGATION AND COORDINATION

2 SEC. 11. *Cyber-Crime Investigation and Coordination Center.* - There is
3 hereby created, thirty (30) days from the effectivity of this Act, a Cyber-Crime
4 Investigation and Coordination Center, hereinafter referred to s CICC, under the
5 control and supervision of the Office of the President principally to combat cyber-
6 crime related fraudulent activities and to investigate, coordinate, collate and
7 synergize efforts of all law enforcement agencies in combating cyber crimes.

8 SEC. 12. *Composition* – The CICC shall be headed by the Secretary of
9 the Department of Transportation and Communications (DOTC) as Chairman;
10 with the Director of the National Bureau of Investigation (NBI) as Vice-Chairman.
11 The Director-General of the Philippine National Police (PNP), the Chief of the
12 National Prosecution Service (NPS), the Head of the National Computer Center
13 (NCC), the head of the Philippine Center for Transnational Crime (PCTC), the
14 head of the Anti-Fraud and Computer Crimes Division (AFCCD) of the NBI and
15 the head of the Crimes Investigation and Detection Group (CIDG).

16 SEC. 13. *CICC Secretariat* - The CICC shall be manned by a Secretariat
17 headed by an Executive Director to be appointed by the Chairman. The
18 Executive Director shall possess adequate training and experience in the field of
19 computer technology, or in information and communications systems, or other
20 related fields. He shall be assisted by a Secretariat staff composed of selected
21 personnel and representatives who shall be seconded from the participating
22 agencies.

23 The Chairman of the CICC may call upon any government agency to
24 render assistance in the accomplishment of the CICC's mandated tasks and
25 functions.

26 SEC. 14. *Powers and Functions* - The CICC shall have the following
27 powers and functions:

- 1 a) To prepare and implement appropriate and effective measures to prevent and
2 suppress computer fraud, abuses and other cyber-related fraudulent activities
3 as provided in this Act;
- 4 b) To investigate and/or conduct information gathering activities in order to
5 identify and prosecute persons and entities, including but not limited to private
6 or government-owned corporations, government officials and employees,
7 syndicates and their cohorts engaged in any of the punishable acts
8 enumerated in this Act;
- 9 c) To effect searches and seizures in accordance with law, and to cause and / or
10 implement the procedure for the arrest, investigation and prosecution of
11 persons engaged in cybercrimes;
- 12 d) To refer the case(s) prosecuted under this Act, as the CICC may deem proper
13 and necessary, to the Department of Justice, or any other appropriate law
14 enforcement agencies for investigation or prosecution, as the case may be;
- 15 e) To follow-up on the progress of on-going investigation and prosecution of
16 cases taken cognizance of by the CICC;
- 17 f) To formulate and implement plans and programs for international cooperation
18 on intelligence and investigations relative to cybercrime prevention,
19 suppression, and prosecution;
- 20 g) To coordinate the support and participation of the business sector, local
21 government units, and non-government organizations in cybercrime
22 prevention programs and other related projects;
- 23 h) To recommend the enactment of appropriate laws, issuances, measures and
24 policies, and
- 25 i) To perform such other functions and duties necessary for the proper
26 implementation of this Act.

27 CHAPTER V – ENFORCEMENT AND IMPLEMENTATION

28 SEC. 15. *Collection of Computer Data.* - To effectively implement and
29 enforce the provisions of this Act, the National Bureau of Investigation (NBI) and

1 the Philippine National Police (PNP), subject to existing laws and procedures,
2 require a person or service provider:

- 3 a) To submit specified computer data and other relevant data in his/its
4 possession and control, which is stored in a computer, computer network,
5 or a computer-data storage medium;
- 6 b) To submit subscriber information in his/its possession or control;
- 7 c) Within his /its existing technical capability, to collect or record through the
8 application of technical means or to cooperate and assist the proper law
9 enforcement officers or agencies in the collection or recording of traffic
10 data and interception of specified communications transmitted within or
11 passing through the territorial jurisdiction of the Philippines by means of a
12 computer network; and
- 13 d) To require the expeditious production or disclosure of traffic data to
14 identify the service providers and the path through which the
15 communication was transmitted.

16 SEC. 16. *Responsibility of Service Provider.* -- Any person or service
17 provider shall keep confidential the facts of cases under investigation as provided
18 under this Act. Such person or service provider shall likewise take all necessary
19 steps to preserve the records and other evidence in its possession.

20 SEC. 17. *Search and Seizure of Computer Data.* -- Where a search and
21 seizure warrant is proper, the NBI and the PNP shall likewise have the power
22 and duty:

- 23 a) Within the time period specified in the warrant, to conduct interception,
24 as defined in this Act, content of communications, procure the content
25 of data either directly, through access and use of the computer or
26 computer network, or indirectly, through the use of electronic
27 eavesdropping or tapping devices, in real time or at the same time that
28 the communication is occurring;
- 29 b) To secure a computer or computer network or parts of it or a computer-
30 data storage medium;
- 31 c) To make and retain a copy of those computer data secured;

- 1 d) To maintain the integrity of the relevant stored computer data; and
2 e) To render inaccessible or remove those computer data in the accessed
3 computer or computer network.

4 Pursuant thereof, the NBI and PNP may order any person who has
5 knowledge about the functioning of the computer or computer network and the
6 measures to protect and preserve the computer data therein to provide, as is
7 reasonable, the necessary information, to enable the undertaking of the search
8 and seizure measure referred to in Section 16 (c).

9 SEC. 18 *Preservation and Disclosure of Computer Data and Traffic*
10 *Record.* -- The integrity of traffic data and subscriber information relating to
11 communication services provided by a service provider shall be preserved up to
12 a minimum period of six (6) months from the date of the transaction. Said period
13 may be extended by order of the NBI or PNP upon a reasonable belief that the
14 computer data may have been used for or in connection with, or the traffic record
15 may contain information as regards, any violation of this Act.

16 CHAPTER VI – JURISDICTION

17 SEC. 19. *Jurisdiction.* – The Regional Trial Court shall have jurisdiction
18 over any violation of the provisions of this Act committed within the territory of the
19 Philippines or by any of its nationals regardless of the place of commission. In
20 case any of the offenses herein defined is committed outside the territorial limits
21 of the Philippines, and by such commission any damage is caused to a computer
22 or computer network situated in the Philippines, or to a natural or juridical person
23 who, at the time the offense was committed, is in the Philippines, the proper
24 Regional Trial Court in the Philippines shall have jurisdiction.

25 CHAPTER VII – INTERNATIONAL COOPERATION

26 SEC. 20. *Mutual Assistance and Cooperation.* – The Government of the
27 Philippines shall cooperate with, and render assistance to other nations for

1 purposes of detection, investigation, and prosecution of offenses referred to in
2 Sections 7 and 22 of this Act and in the collection of evidence in electronic form
3 in relation thereto.

4 The requesting nation must maintain the confidentiality of the fact or the
5 subject of request for assistance and cooperation. It may only use the requested
6 information subject to the conditions specified in the grant.

7 SEC. 21. *Grounds for Refusal to Cooperate.* – The Government of the
8 Philippines shall have the right to refuse cooperation under any of the following
9 grounds:

- 10 a) The offense is punishable under Philippine laws and the Philippine courts
11 have acquired jurisdiction over the person of the accused;
- 12 b) The information requested is privileged, protected under Philippine laws,
13 or that which affects national security;
- 14 c) If, for any reason, the production of the information is unreasonable,
- 15 d) the foreign government requesting for assistance has previously refused
16 without justifiable reason, a similar request by the Government of the
17 Philippines; and
- 18 e) The foreign government requesting for assistance has previously
19 breached an agreement to keep the fact or subject of request confidential,
20 or has previously violated any condition of the grant.

21 SEC. 22. *Cooperation Based on Reciprocity.* – In the absence of a
22 treaty or agreement, mutual assistance and cooperation under the preceding
23 sections under this Chapter shall be based on the principle of reciprocity.

24 SEC. 23. *Communications Center.* -- The National Computer Center
25 (NCC) shall be responsible for sending and answering requests for mutual
26 assistance as well as the execution of such requests or their transmission to the
27 proper authorities for implementation and enforcement.

1

CHAPTER VIII – OTHER PROVISIONS

2

3

4

5

6

7

8

9

10

CHAPTER IX – FINAL PROVISIONS

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

SEC. 24. *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 3185, as amended, or the Revised Penal Code or any other law.

SEC. 25. *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. 26. *Appropriations.* -- The amount necessary for the implementation of this Act shall be charged against the appropriations of the NBI, PNP and the NCC.

SEC. 27. *Implementing Rules and Regulations.* – The Department of Justice and the Department of Interior and Local Governments shall jointly formulate the necessary rules and regulations for the effective implementation of this Act.

SEC. 28. *Public Information Campaign.* -- The Office of the President, National Computer Center, Department of Education, Department of Justice, Department of Trade and Industry, Department of Transportation and Communications, and the National Computer Center shall, in coordination 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. 29. *Suppletory Application.* -- This Act shall have suppletory application to the provisions of the Revised Penal Code, RA 7610 and RA 9208 or the Anti-Trafficking in Persons Act.

SEC. 30. *Separability Clause.* -- If any provision of this Act is held invalid, the other provisions not affected shall remain in full force and effect.

1 SEC. 31. *Repealing Clause.* -- All laws, decrees, or rules inconsistent
2 with this Act are hereby repealed or modified accordingly. Specifically, Section
3 33 of Republic Act No. 8792 or the Electronic Commerce Act is hereby modified
4 accordingly.

5 SEC. 32. *Effectivity.* -- This Act shall take effect fifteen (15) days after the
6 completion of its publication in the Official Gazette or in at least two (2)
7 newspapers of general circulation,

8 Approved,