A SHORT HISTORY OF THE DEVELOPMENT OF CYBERCRIME LEGISLATION IN THE PHILIPPINES*

*Geronimo L. Sy***

I. INTRODUCTION

Any discussion of cybercrime in the Philippines starts with reference to the "I Love You" virus unleashed globally in 2000.[1] It placed the country on the global cyber-map and pushed Congress to pass the first 'cybercrime' law, Republic Act No. 8792.[2]

Section 33 of the said E-Commerce Act provides:

> Penalties. - The following Acts, shall be penalized by fine and/or imprisonment, as follows:
>
> (a) Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic documents shall be punished by a minimum fine of One Hundred Thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years.

Hence, the concept of cybercrime which has long been recognized as a scourge in other parts of the world formally became a crime in the country.

---

* *Cite as* Geronimo Sy, *A Short History of the Development of Cybercrime Legislation in the Philippines*, 89 PHIL. L.J. 651, [page cited] (2015).

** Assistant Secretary and Former Head, Office of Cybercrime, Department of Justice, Republic of the Philippines.

[1] *See* David Kleinbard & Richard Richtmayer, *U.S. catches 'Love' virus*, CNN, May 5, 2000, *available at* http://money.cnn.com/2000/05/05/technology/loveyou/; James Meek, *Love bug virus creates worldwide chaos*, The Guardian, May 5, 2000, *available at* http://www.theguardian.com/world/2000/may/05/jamesmeek.

[2] The Electronic Commerce (E-Commerce) Act of 2000.

Not long after, the Department of Justice (DOJ) and the primary law enforcement agencies, the National Bureau of Investigation (NBI) and the Philippine National Police (PNP) Criminal Investigation and Detection Group (CIDG), established the first cybercrime forensic laboratories in 2001 —one for each agency—given the need to build capacity and to spur development of cyber investigations.

The Supreme Court, on the other hand, recognized the emerging crime set and issued the Rules on Electronic Evidence on 17 July 2001. These were initially applicable only to all civil actions and proceedings, as well as quasi-judicial and administrative cases. The Rules were subsequently amended on September 24, 2002 to include criminal cases.[3]

With the budding cybercrime fighting capability, two convictions stemmed out of the several cases investigated by the DOJ under the E-Commerce law.

The first conviction arose in September 2005 when the respondent—an employee of a leading university in the south—pleaded guilty to hacking the governmental portal "gov.ph" and other government websites in Criminal Case No. 419672-CR filed before Branch 14 of the Metropolitan Trial Court of Manila. He was sentenced to serve one to two years of imprisonment and to pay a fine of PHP 100,000.

The second conviction was obtained in May 2006 against a 22-year old former call center agent who broke into the computer system of a credit card company and a client of his multi-national employer in the firm in the Philippines, thereby gaining access to a database maintained by a sister firm in the United States. Using an internal IP address, he proceeded to purchase goods online using various credit cards. He was sentenced by the Quezon City Metropolitan Court to serve a minimum imprisonment term of one to two years plus a fine of PHP 100,000, as provided under Section 33 of the E-Commerce Law.[4]

Meanwhile, in 2008, the DOJ created the Task Force on E-Government, Cyber-security and Cybercrime to address cyber-security issues and to pursue an e-government agenda.[5] The Task Force assessed the state of cybercrime legislation not only in the country but also in the global arena. It was to train law enforcers and prosecutors in dealing with cybercrime and

---

[3] Rules on Electronic Evidence, A.M. No. 01-7-01-SC.

[4] These two convictions were obtained by the author in his capacity as state prosecutor.

[5] DOJ Dep't Order No. 810 (Dec. 9, 2008).

to create e-courts to handle high-tech cases such as hacking and other crimes committed using internet technology.

The Task Force began collaborating with the Council of Europe (COE)—the organization which drafted and pushed for the adoption of the first international Convention on Cybercrime (CoC) popularly known as the Budapest Convention.[6]

II. THE CONVENTION ON CYBERCRIME

The Convention on Cybercrime, also known as the Budapest Convention, is an international treaty ratified by 42 states—members and non-members of the COE.[7] It seeks to address computer and internet crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. Specifically, the Convention aims to protect society against cybercrime "by providing for the criminalization of such conduct and the adoption of powers sufficient for effectively combating such criminal offenses, by facilitating their detection, investigation and prosecution at both domestic and international levels and by providing arrangements for fast and reliable international cooperation."

The Convention is divided into three principal parts. The first part identifies the substantive cybercrime offenses which each ratifying State is obliged to adopt in its domestic law. The second part deals with investigative procedures that States must implement. Lastly, the third part relates to mechanisms that will enhance international cooperation.

To monitor the compliance of parties and update observers to the said Convention, the COE conducts a regular conference known as the Octopus Conference which is preceded by the plenary meeting of the Cybercrime Convention Committee ("T-CY").[8]

The author was invited to the annual conference held in Strasbourg, France as an observer, panel speaker, and moderator in 2007 and subsequently thereafter.

---

[6] The Council of Europe is an international organization which promotes co-operation between all countries in Europe in the areas of legal standards, human rights, democratic development, the rule of law and cultural co-operation.

[7] Council of Europe, Convention on Cybercrime, Nov. 23, 2001, *available at* http://www.refworld.org/docid/47fdfb202.html.

[8] "Action against Cybercrime," Council of Europe, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime.

On August 31, 2007, the DOJ through the office of former Undersecretary Ernesto L. Pineda expressed the request of the Government of the Philippines to be invited for accession to the Budapest Convention. In a letter dated June 15, 2011, the COE Secretary General Thorbjørn Jagland formally invited the Philippines to accede to the Budapest Convention.[9]

III. INTRODUCTION TO THE CYBERCRIME PREVENTION ACT OF 2012

The Cybercrime Prevention Act ("CPA") of 2012 is the first piece of legislation comprehensively dealing with cybercrimes. Divided into 31 sections split across eight chapters, the Act criminalizes several types of offenses such as illegal access, data interference, device misuse, cybersquatting, computer fraud, cybersex, among others.[10] It also reaffirms existing laws against child pornography punishable under R.A. No. 9775 (Anti-Child Pornography Act of 2009) and libel punishable under Article 355 of the Revised Penal Code.

While it was R.A. No. 8792 which first penalized "cybercrimes," R.A. No. 8484 (Access Device Regulation Act of 1998) and R.A. No. 4200 (Anti-wiretapping Law) had earlier recognized acts done using information and communication technology ("ICT"). More recently, but prior to the effectivity of the CPA, R.A. No. 10173 or the Data Privacy Act of 2012 was enacted to protect the fundamental human right of privacy and of communication while ensuring free flow of information to promote innovation and growth.

This Essay thus traces the history and development of the CPA—one of the country's most critical and highly debated legislative measures. Through the years, netizens have been victims of numerous cybercrimes committed by criminals with impunity. The CPA's eventual passage into law and the recent 50-page decision[11] of the Supreme Court confirming its constitutionality, save for some provisions, finally opens a new period for law enforcement in cyberspace.

---

[9] Letter of Council of Europe Secretary General Thorbjørn Jagland dated June 15, 2011.

[10] Rep. Act No. 10175 (2012).

[11] Disini v. Secretary of Justice, G.R. No. 203335, 716 SCRA 237, Feb. 18, 2014.

A. The Roots of the CPA

The actual work on the Cybercrime Bill started in 2001 under the Legal and Regulatory Committee of the former Information Technology and e-Commerce Council's ("ITECC") which later became the Commission on Information and Communication Technology ("CICT"). It was headed by former Secretary Virgilio Peña and the Committee was chaired by Atty. Claro Parlade. It was an initiative of the Information Security and Privacy Sub-committee chaired by Albert P. dela Cruz who was the president of Philippine Computer Emergency Response Team, together with then NBI Anti-Computer Crime and Fraud Division Chief, Atty. Elfren Meneses, Jr. The documentation was handled by the Presidential Management Staff ("PMS") acting as the CICT secretariat.

Numerous public sector consultations were held. In January 2004, the first local Cybercrime Conference was organized by Atty. Gigo Alampay with representatives from the Department of Justice of both the US and Canada.

These activities were held cognizant of the limited scope of the cybercrime provisions in the E-Commerce Act.

Meanwhile, during the interim years of 2006 and 2007, the prototype Cybercrime Prevention Act was substantially crafted and was later finalized after the first International Cybercrime Conference on October 25-26, 2007, conducted by the DOJ in partnership with the COE. During the first quarter of 2008, legislative strategy on information and communication was created by the government focused mainly in adopting a three-tiered approach in crafting related laws to underline the primacy of three virtual subjects, namely: data privacy, cybercrime, and cybersecurity.

B. Thirteenth Congress (2004-2007)

Initiatives to come up with a law penalizing computer and computer-related crimes originated after the internet was first used in the country. From 2004-2007, several bills were submitted in the Senate. The first two bills were passed by then Senator Luisa "Loi" Ejercito Estrada: "Computer Crimes Act"[12] and the "Anti-Computer Pornography Act."[13]

---

[12] S. No. 151, 13th Cong., 1st Sess. (2004).

[13] S. No. 199, 13th Cong., 1st Sess. (2004).

Senator Sergio Osmeña III also proposed the enactment of the "Computer Abuse Act" through Senate Bill No. 464[14] which was patterned after the United States Computer Fraud and Abuse Act,[15] as amended in 1994 and 1996, as well as Title 18, Section 3933 of the Pennsylvania Consolidated Statutes (Crimes Code). This bill outlaws, among others: (1) illegal access to computers, computer systems, computer networks, computer servers and databases; (2) obtaining information on the financial records of a customer of a financial institution without the proper authorization; (3) obtaining, publishing, and giving out the password to another person's account; and (4) unleashing computer viruses.

Senator Miriam Defensor Santiago proposed the enactment of a Computer Crimes Act consisting of 10 sections. It seeks to prohibit activities such as but not limited to the following, namely (1) use and operation of a computer or computer network primarily to facilitate criminal activity or primarily to commit activities prohibited by the Penal Code and special laws; (2) use of a computer network to transmit a communication intended to conceal or hide the origin of money or other assets, tangible or intangible, that were derived from the commission of a crime; (3) use of a computer or computer network to conceal, obliterate, or hide the identity of persons guilty of committing a crime or an offense; and (4) use of a computer or computer network to conceal or hide commission of a crime or an offense and the evidence thereof. She also proposed the enactment of the "E-mail User Protection Act" which seeks to protect consumers and service providers from the misuse of computer facilities by others sending unsolicited commercial electronic mail over such facilities.[16]

Finally, on 17 September 2004, Senator Ramon Magsaysay, Jr. proposed the enactment of the "Anti-Computer Fraud and Abuse Act of 2004." It defines computer fraud and the offenses covered by the term "computer-related fraudulent activities" and covers such acts as computer fraud, computer forgery, damage to computer data or computer programs, computer sabotage, unauthorized access and unauthorized interception. It imposes both a fine and a penalty of imprisonment for violators. It also accords authority to the National Security Council to conduct investigations on computer related crimes vis-à-vis its effects on national security.[17]

These bills did not make any significant progress.

---

[14] S. No. 464, 13th Cong., 1st Sess. (2004).

[15] 18 U.S.C. § 1030. (Fraud and related activity in connection with computers.)

[16] S. No. 1644, 13th Cong., 1st Sess. (2004).

[17] S. No. 1789, 13th Cong., 1st Sess. (2004).

C. Fourteenth Congress (2007-2010)

Initiatives to come up with a law penalizing computer crimes continued in 2007 during the 14th Congress. In the Senate, Senate Bill No. 653 entitled "The Computer Crimes Act" was submitted on July 3, 2007 by Senator Jinggoy Ejercito Estrada with the aim of penalizing the use of computers and computer networks in the commission of a crime.[18]

With only nine sections, the bill defines what a computer is and makes it unlawful for any person to use and operate a computer or computer network to perform any of the following acts, namely (a) to facilitate criminal activity or commit any of the crimes enumerated in the Revised Penal Code, (b) to transmit communication intended to conceal or hide the origin of money or other assets, tangible or intangible, which were derived from the commission of a crime, (c) to conceal, obliterate, or hide the identity of persons guilty of committing a crime or an offense, or (d) to conceal or hide the commission of a crime or an offense and the evidence thereof. The commission of any of the abovementioned acts subjects the offender to 10 to 15 years of imprisonment and a fine between PHP 20,000 and PHP 50,000.

Within the same month, Senator Loren Legarda introduced Senate Bill No. 1377, "The Anti-Computer Fraud and Abuses Act of 2007." The proposed law seeks to penalize several defined crimes or offenses such as computer fraud, computer forgery, damage to computer data or computer programs, computer sabotage, unauthorized access, and unauthorized interception. The bill likewise prescribes a higher penalty: imprisonment of not more than 20 years and a fine not more than PHP 100,000.

Senator Miriam Defensor-Santiago, on the other hand, introduced four separate bills on computer and internet usage, namely: (1) Senate Bill No. 1626, "Anti-Phishing Act of 2007"; (2) Senate Bill No. 1844, "Email User Protection Act of 2007"; (3) Senate Bill No. 2053, "Anti-Spyware Act of 2008"; and (4) Senate Bill No. 2176, "Consumer Protection Against Computer Grayware Act of 2008."

Senator Santiago's version of the anti-phishing law was met with a slightly different version in the form of Senator Manny Villar's Senate Bill No. 2405, which penalizes the act of phishing in the internet or instant messaging. Phishing or the act of securing or getting of sensitive personal information for the purpose of using it in fraud, or for participating in fraudulent business practices, or for the purpose of identity theft and misrepresentation, was

[18] S. No. 653, 14th Cong., 1st Sess. (2007).

proposed to be penalized by imprisonment for at least two years but not more than 10 years or payment of a fine of not less than PHP 50,000 but not more than PHP 500,000 or both at the discretion of the court.

By the middle of 2008, Senator Mar Roxas introduced Senate Bill No. 2412, the "Computer Abuse Act of 2008." The bill was patterned after the United States Computer Fraud and Abuse Act[19] as well as Title 18, Section 3933 of the Pennsylvania Consolidated Statutes (Crimes Code). It outlaws: (1) illegal access to computers, computer systems, computer networks, computer servers, and database; (2) obtaining information relative to the financial records of a customer of a financial institution without the proper authorization; (3) obtaining, publishing, and giving out the password to another person's account; and (4) unleashing computer viruses.

Not long after, Senator Roxas introduced Senate Bill No. 2480 or the "Anti-Cybersquatting Act of 2008." It declares as unlawful the acquisition of a domain name over the internet if there is bad faith, intent to profit, mislead, destroy reputation, and deprive others from registering, and such domain name is: (a) similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration; (b) identical or in any way similar with the name of a person other than the registrant, in case of a personal name; or (c) acquired with no right or intellectual property interests in it.

The successive introduction of bills aimed at criminalizing detrimental acts with the use of a computer or through the use of the internet resulted in the first draft of a Senate bill dubbed as a Cybercrime Prevention Act.

Introduced by Senator Juan Ponce Enrile on April 21, 2009, Senate Bill No. 3177 entitled the "Cybercrime Prevention Act of 2009," was divided into seven chapters.[20] Chapter 1 defines significant terms such as computer system, computer data, computer program, database, service provider, traffic data, among others. Chapter 2 enumerates acts punishable under the proposed law which were categorized into (a) offenses against the confidentiality, integrity and availability of computer data and systems, such as illegal access, illegal interception, data interference, and system interference; (b) computer-related offenses such as computer-related forgery and computer-related fraud; (c) content-related offenses such as cybersex, child pornography, and unsolicited commercial communications. Chapter 3 prescribes the penalties imposable for each violation. The same chapter introduces corporate liability, that is, the

---

[19] 18 U.S.C. § 1030.

[20] The author was tasked by Senator Enrile to submit a single, comprehensive draft.

imposition of a fine amounting to a maximum of 10 million pesos if the crime is committed on behalf of or for the benefit of a juridical person, by a natural person who has a leading position within said juridical person. Chapter 4, on the other hand, gives law-enforcement authorities power to collect and preserve computer data. Chapter 5 defines the jurisdiction of the Regional Trial Courts and empowers them to hear and decide cases involving violations of the proposed law if committed within the territory of the Philippines or by a Filipino national regardless of the place of commission. Chapters 6 and 7 contain provisions on international cooperation and final provisions such as appropriations, implementing rules and regulations, among others.

Less than a month later, Senator Antonio Trillanes IV came up with his own version of the CPA and introduced Senate Bill No. 3213 on May 6, 2009. The proposed bill contained almost similar provisions as the earlier version except that Senate Bill No. 3213 sought the creation of a Computer Emergency Response Council under the control and supervision of the Office of the President. It is primarily tasked to formulate and implement a national plan of action to address and combat cybercrime. It is envisioned to be composed of the Chairman of the Commission on Information and Communications Technology ("CICT") as Chairman; the Director of NBI as Vice-Chairman, and other officials of the government as members including the Directorate-General of PNP, the Chief of the National Prosecution Service, the Head of the National Computer Center (NCC), the head of the Philippine Center for Transnational Crime (PCTC), three representatives from the private sector, among others.

These two versions of the CPA were later merged forming Senate Bill No. 3553 which was prepared jointly by the Committees on Science and Technology, Constitutional Amendments, Revision of Codes and Laws, Justice and Human Rights, and Finance. Senate Bill No. 3553 maintained most of the provisions contained in Senator Enrile's version of the CPA such as the categorization of the punishable acts and the law enforcement authorities' power to collect and preserve computer data. It incorporated Senator Trillanes' proposal to create a body tasked to formulate and implement the national cyber security plan, however, this time, it was referred to as the Cybercrime Investigation and Coordinating Center composed of a smaller number of people, namely: (a) the Chairman of the Commission on Information and Communications Technology as the Chairman with (b) the Director of the NBI as Vice-Chairman, (c) the Chief of the PNP, (d) the Chief of the National Prosecution Service and (e) the Head of the National Computer Center as members. More importantly, Senate Bill No. 3553 proposed the creation of the Office of Cybercrime ("OOC") in the Department of Justice, which would be responsible for extending immediate assistance in the

investigation and prosecution of criminal offenses related to computer systems and data, and ensure that the provisions of the proposed law are duly complied with.

In the meantime, House Bill No. 6794, which is the counterpart bill of Senate Bill No. 3553 in the House of Representatives, was approved on third reading on January 18, 2010. This was transmitted to and received by the Senate on January 20, 2010.[21]

The CPA of 2009 was not enacted into law at this stage.

D. Fifteenth Congress (2010-2013)

House Bill No. 5808 was principally authored by Representative Susan A. Yap and 34 co-author House Members. It was substituted for the consolidated ten bills previously filed in the House of Representatives with Representative Sigfrido R. Tinga as sponsor.[22]

Senate Bill No. 2796, on the other hand, was principally sponsored by Senator Edgardo J. Angara. The bill was jointly submitted by the Committees on Science and Technology; Constitutional Amendments; Revisions of Codes and Laws; Education, Arts and Culture; Justice and Human Rights; Trade and Commerce; Public Information and Mass Media; and Finance on 3 May 2011. Except for Sec. 7 par. 3, Chapter III which cites R.A. No. 9775 or the Anti-Child Pornography Act of 2009, Senate Bill No. 2796 contained provisions identical to Senate Bill No. 3553 or the earlier proposed CPA of 2009.

Senator Angara and Representative Tinga co-chaired the Bicameral Conference Committee where House Bill No. 5808 and Senate Bill No. 2796 were discussed. The Bicameral Conference Committee decided to generally adopt the Senate version of the bill to be used as the working draft with insertions coming from the House version, including the title of the proposed Act.[23] A new section not found in both versions was likewise inserted.[24]

---

[21] See legislative history of House Bill No. 6795 at http://www.congress.gov.ph/legis/search/hist_show.php?congress=14&save=1&journal=&switch=0&bill_no=HB06794.

[22] H. Nos. 85, 167, 364, 383, 511, 1444, 2279, 3376, 4031, & 4162.

[23] An Act Defining Cybercrime, Providing For The Prevention, Investigation, Suppression And The Imposition Of Penalties Therefor And For Other Purposes.

[24] "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 the relevant provisions of this Act. Provided, That the penalty to be imposed shall be one degree higher than that provided for by the revised Penal Code and special laws."

The Bicameral Conference Committee Report was transmitted to President Benigno S. Aquino III on August 15, 2012. Not long after, the CPA of 2012 was signed into law on September 12, 2012 and came into force on October 3, 2012.

Before the approval and the official recording of the Cybercrime Prevention Act, the DOJ conducted several seminars with the active participation of prosecutors nationwide. A Technical Working Group ("TWG") on Cybercrime and Cybersecurity consisting of representatives from national government agencies, including those engaged in law enforcement like the PNP and the NBI, as well as private companies and the academia. These stakeholders came together to address issues relating to cybersecurity and cybercrime in the Philippines.

One of the aims of the TWG was to consolidate and concretize the government's efforts on cybersecurity and successfully implement measures to fight cybercrime. The Cybercrime seminars entitled "Investigating Cybercrime: A Global Training Program for Prosecutors" were held on separate dates in various cities in the country, *viz*: September 19-20, 2011 in Manila; October 20-21, 2011 in Cebu City; January 26-27, 2012 in Davao City; February 22-23, 2012 in Tuguegarao City; April 19-22, 2012 in Laoag City; May 22-25, 2012 in Legazpi City, and July 19-20, 2012 in Iloilo City. Comments were considered and the draft cybercrime bill was continuously revised and endorsed to both houses of Congress.

After the CPA of 2012 was signed into law, the DOJ in partnership with the Department of Science and Technology Information and Communications Technology Office ("DOST-ICTO") hosted a multi-sectoral forum on October 9, 2012 to ensure proper dissemination of information about the new law. Key provisions of the CPA were presented and inputs and insights for the law's implementing rules and regulations were solicited.[25] Unfortunately, it was on that same day when the Supreme Court issued a temporary restraining order suspending the application of the legislative measure in view of numerous petitions filed by concerned groups, mostly from the media, academe and legal community, assailing the CPA's constitutionality.[26]

---

[25] DOJ-DOST-ICTO Forum on Cybercrime Program, Oct. 9, 2012.

[26] Consolidated cases of Disini v. Sec. of Justice, G.R. No. 203335; Biraogo v. NBI, G.R. No. 203299; Alab ng Mamamahayag v. Office of the President, G.R. No. 203306; Guingona III v. Executive Secretary, G.R. No. 203359; Adonis v. Executive Secretary, G.R. No. 203378; Palatino v. Ochoa, G.R. No. 203391; Reyes v. Aquino, G.R. No. 203407; Sta. Maria v. Ochoa, G.R. No. 203440, National Union of Journalists of the Philippines v. Executive Secretary, G.R. No. 203453; Cruz v. Aquino, G.R. No. 203469; Philippine Bar

The original 120-day temporary restraining order issued on 9 October 2012 was extended on February 5, 2013 pending hearing and adjudication of the issues.[27]

Given the close cooperation with the COE, the DOJ organized on May 23-24, 2013 the Regional Workshop on the protection of children against online sexual violence in Southeast Asia to enhance law enforcement cooperation and criminal law benchmarks of the Budapest and Lanzarote Conventions.[28]

The conference was attended by Ministries of Justice and other institutions responsible for law drafting, prosecution service, and law enforcement in child protection, or cybercrime units of the participating countries in Southeast Asia. It seeks to promote the implementation of the criminal law benchmarks of the Budapest and Lanzarote Conventions as a basis for enhanced law enforcement cooperation to protect children against sexual violence.

The DOJ, through the author, presented its efforts to come up with a second version of a cybercrime law amending the CPA of 2012, as a response to the clamor of netizens on cybercrimes, both domestic and international, taking into account the constitutional and statutory rights guaranteed under the present Charter. The second version of the law sought to set aside cyber-squatting as an offense as well as content-related offenses of cybersex, child-pornography, and libel. It deleted the imposition of penalty one degree higher for crimes penalized by the Revised Penal Code and special laws if committed with the use of information and communication technology; the provision on liabilities under other laws; the provision on restricting or blocking access to computer data; and the provision on qualified crimes. This second version was duly endorsed to both Houses through letter by the Secretary of Justice dated August 28, 2013.

Association, Inc. v. Aquino, G.R. No. 203501; Colmenares v. Executive Secretary, G.R. No. 203509; National Press Club of the Philippines, Inc. v. Office of the President, G.R. No. 203515; Philippine Internet Freedom Alliance v. Executive Secretary, G.R. No. 203518.

[27] *Id.*

[28] The COE Convention on the Protection of Children against sexual exploitation and sexual abuse, or the Lanzarote Convention, aims to prevent and combat sexual exploitation and sexual abuse of children; protect the rights of child victims of this kind of exploitation and abuse; and promote national and international cooperation against these misdeeds against children. http://www.coe.int/t/dg3/children/1in5/Source/Lanzarote Convention_EN.pdf.

E. Sixteenth Congress (2013-2016)

Similar efforts to address controversial provisions of the CPA were made by legislators such as the amendments proposed by Senators Ferdinand Marcos, Jr., Francis Escudero, Pia Cayetano, and Alan Peter Cayetano to delete Sections 4(c)(2), 4(c)(4), 6, 7, 12 and 19 as well as to revisit Section 21 of the Act.[29] On the other hand, Senators Miriam Defensor Santiago and Paolo Benigno Aquino IV aim to establish a Magna Carta for Philippine Internet Freedom.[30]

Pending the approval of these bills, the Supreme Court confirmed the constitutionality of the CPA on 18 February 2014. In its 50-page decision, the Supreme Court declared valid and constitutional the following provisions:

(1) Section 4(a)(1), which penalizes accessing a computer system;
(2) Section 4(a)(3), which penalizes data interference, including transmission of viruses;
(3) Section 4(a)(6), which penalizes cyber-squatting or acquiring domain name over the internet in bad faith to the prejudice of others;
(4) Section 4(b)(3), which penalizes identity theft or the use or misuse of identifying information belonging to another;
(5) Section 4(c)(1), which penalizes cybersex or the lascivious exhibition of sexual organs or sexual activity for favor or consideration;
(6) Section 4(c)(2), which penalizes the production of child pornography;
(7) Section 6, which imposes penalties one degree higher when crimes defined under the Revised Penal Code are committed with the use of information and communications technologies;
(8) Section 8, which prescribes the penalties for cybercrimes;
(9) Section 13, which permits law enforcement authorities to require service providers to preserve traffic data and subscriber information as well as specified content data for six months;
(10) Section 14, which authorizes the disclosure of computer data under a court-issued warrant;

---

[29] *See* S. Nos. 11, 126, 154, 248, & 249, 16th Cong.
[30] *See* S. Nos. 53 & 1091, 16th Cong.

(11) Section 15, which authorizes the search, seizure, and examination of computer data under a court-issued warrant;
(12) Section 17, which authorizes the destruction of previously preserved computer data after the expiration of the prescribed holding periods;
(13) Section 20, which penalizes obstruction of justice in relation to cybercrime investigations;
(14) Section 24, which establishes a Cybercrime Investigation and Coordinating Center (CICC); and
(15) Section 26(a), which defines the CICC's powers and functions.

The Supreme Court likewise declared as constitutional Section 4(c)(4), which penalizes online libel with respect to the original author of the post but declared unconstitutional with respect to others who simply receive the post and react to it; and Section 5, which penalizes aiding or abetting and attempt in the commission of cybercrimes only in relation to Section 4(a)1 on Illegal Access, Section 4(a)(2) on Illegal Interception, Section 4(a)(3) on Data Interference, Section 4(a)(4) on System Interference, Section 4(a)(5) on Misuse of Devices, Section 4(a)(6) on Cyber-squatting, Section 4(b)(1) on Computer-related Forgery, Section 4(b)(2) on Computer-related Fraud, Section 4(b)(3) on Computer-related Identity Theft, and Section 4(c)(1) on Cybersex, but void with respect to Sections 4(c)(2) on Child Pornography, 4(c)(3) on Unsolicited Commercial Communications, and 4(c)(4) on Online Libel.

On the other hand, Sections 4(c)(3) which penalizes posting of unsolicited commercial communications, Section 12 which authorizes the collection or recording of traffic data in real-time, and Section 19 which authorizes the DOJ to restrict or block access to suspected Computer Data were however declared void for being violative of the Constitution. Similarly, the Supreme Court declared that charging an offender for online libel under both Section 4(c)(4) of the CPA and Article 353 of the Revised Penal Code, or for child pornography committed online under both Section 4(c)(2) of the CPA and the Anti-Child Pornography Act of 2009 violates the Constitutional proscription against double jeopardy.

Immediately, petitioners and respondents filed separate motions for reconsideration before the Supreme Court asking for the latter to reexamine its decision. These were denied on April 22, 2014 declaring with finality that the CPA, except for the stated provisions, is valid and enforceable.

IV. CONCLUSION

The development, passage, and enactment of cybercrime legislation in the Philippines have been long and tedious. The technical issues coupled with the strong resolve of several groups of people, especially bloggers and internet users, to safeguard their freedom of speech and expression has resulted in public debates and court litigation. Indeed, the State, as *parens patriae,* has the obligation to protect the Filipino people against cyberbullies but it must strike the balance between penalizing what are considered as cybercrimes and respecting the people's fundamental rights. With the final resolution on the validity and constitutionality of the CPA, coupled with the active enforcement of its provisions and related laws by the OOC, NBI, and PNP, the security of the public in cyberspace is now greatly assured.

The implementing rules and regulations (IRR) of the CPA were drafted by the DOJ jointly with the Information and Communications Technology Office of the Department of Science and Technology, and the Department of Interior and Local Government pursuant to Section 28 of the CPA, with the cooperation of the NBI and PNP. Consultations with members of the academe, government and private sectors were also conducted. The IRR, which is intended to be straightforward and comprehensive, seeks to harmonize provisions of the CPA with other laws such as the Access Devices Regulation Act of 1998, E-Commerce Act of 2000, Anti-Child Pornography Act of 2009, and Anti-Photo and Voyeurism Act of 2009, as well as fill in the gaps in law enforcement procedures on cybercrimes.

The consultation process consisted of practical, technical and legal review and application of the CPA, engaging various public and private sectors. In particular, the TWG convened to draft the IRR on March 10, 17, and 26, August 20 and 26, and September 5, 2014. Also, stakeholders from the business sector, the academe and non-governmental organizations were consulted on April 8, 2014; national government agencies and organizations in the legal profession on April 15, 2014; media, ICT groups and internet service providers (ISPs) on April 29 and May 16, 2014.

On August 12, 2015, after a final round of legal scrubbing by the three Departments, the IRR of the Cybercrime Prevention Act of 2012 was finally signed at a ceremony held in was held in Manila City, Philippines, which was attended by a number of stakeholders from different sectors of the society. It was published in the Official Gazette Online on August 28, 2015, in *The Manila Times* and *The Standard* on September 24, 2015, and to take effect 15 days after the completion of its publication.