



SUPREME COURT OF THE PHILIPPINES  
PUBLIC INFORMATION OFFICE  
**RECEIVED**  
FEB 21 2014  
BY: HELEN  
TIME: 5:25 PM

Republic of the Philippines  
**Supreme Court**  
Manila

**EN BANC**

**JOSE JESUS M. DISINI, JR., ROWENA  
S. DISINI, LIANNE IVY P. MEDINA,  
JANETTE TORAL and ERNESTO  
SONIDO, JR.,**

Petitioners,

**G.R. No. 203335**

Present:

SERENO, *C.J.*,  
CARPIO,  
VELASCO, JR.,\*  
LEONARDO-DE CASTRO,  
BRION,  
PERALTA,  
BERSAMIN,  
DEL CASTILLO,  
ABAD,  
VILLARAMA, JR.,  
PEREZ,  
MENDOZA,  
REYES,  
PERLAS-BERNABE,\* and  
LEONEN, *JJ.*

- versus -

**THE SECRETARY OF JUSTICE, THE  
SECRETARY OF THE DEPARTMENT OF  
THE INTERIOR AND LOCAL  
GOVERNMENT, THE EXECUTIVE  
DIRECTOR OF THE INFORMATION  
AND COMMUNICATIONS  
TECHNOLOGY OFFICE, THE CHIEF OF  
THE PHILIPPINE NATIONAL POLICE  
and THE DIRECTOR OF THE NATIONAL  
BUREAU OF INVESTIGATION,**

Respondents.

X ----- X

**LOUIS "BAROK" C. BIRAOGO,**  
Petitioner,

**G.R. No. 203299**

- versus -

\* No part.

W

**NATIONAL BUREAU OF INVESTIGATION and PHILIPPINE NATIONAL POLICE,**

Respondents.

X ----- X

**ALAB NG MAMAMAHAYAG (ALAM),  
HUKUMAN NG MAMAMAYAN  
MOVEMENT, INC., JERRY S. YAP,  
BERTENI "TOTO" CAUSING, HERNANI  
Q. CUARE, PERCY LAPID, TRACY  
CABRERA, RONALDO E. RENTA,  
CIRILO P. SABARRE, JR., DERVIN  
CASTRO, ET AL.,**

**G.R. No. 203306**

Petitioners,

- versus -

**OFFICE OF THE PRESIDENT,  
represented by President Benigno Simeon  
Aquino III, SENATE OF THE  
PHILIPPINES, and HOUSE OF  
REPRESENTATIVES,**

Respondents.

X ----- X

**SENATOR TEOFISTO DL GUINGONA III,**  
Petitioner,

**G.R. No. 203359**

- versus -

**EXECUTIVE SECRETARY, THE  
SECRETARY OF JUSTICE, THE  
SECRETARY OF THE DEPARTMENT OF  
INTERIOR AND LOCAL GOVERNMENT,  
THE CHIEF OF THE PHILIPPINE  
NATIONAL POLICE, and DIRECTOR OF  
THE NATIONAL BUREAU OF  
INVESTIGATION,**

Respondents.

X ----- X

**ALEXANDER ADONIS, ELLEN  
TORDESILLAS, MA. GISELA  
ORDENES-CASCOLAN, H. HARRY L.**

**G.R. No. 203378**

**ROQUE, JR., ROMEL R. BAGARES, and  
GILBERT T. ANDRES,**  
Petitioners,

- versus -

**THE EXECUTIVE SECRETARY, THE  
DEPARTMENT OF BUDGET AND  
MANAGEMENT, THE DEPARTMENT  
OF JUSTICE, THE DEPARTMENT OF  
THE INTERIOR AND LOCAL  
GOVERNMENT, THE NATIONAL  
BUREAU OF INVESTIGATION, THE  
PHILIPPINE NATIONAL POLICE, AND  
THE INFORMATION AND  
COMMUNICATIONS TECHNOLOGY  
OFFICE-DEPARTMENT OF SCIENCE  
AND TECHNOLOGY,**  
Respondents.

X ----- X

**HON. RAYMOND V. PALATINO, HON.  
ANTONIO TINIO, VENCER MARI  
CRISOSTOMO OF ANAKBAYAN, MA.  
KATHERINE ELONA OF THE  
PHILIPPINE COLLEGIAN, ISABELLE  
THERESE BAGUISI OF THE NATIONAL  
UNION OF STUDENTS OF THE  
PHILIPPINES, ET AL.,**  
Petitioners,

**G.R. No. 203391**

- versus -

**PAQUITO N. OCHOA, JR., in his capacity  
as Executive Secretary and alter-ego of  
President Benigno Simeon Aquino III,  
LEILA DE LIMA in her capacity as  
Secretary of Justice,**  
Respondents.

X ----- X

**BAGONG ALYANSANG MAKABAYAN  
SECRETARY GENERAL RENATO M.  
REYES, JR., National Artist BIENVENIDO  
L. LUMBERA, Chairperson of Concerned  
Artists of the Philippines, ELMER C.**

**G.R. No. 203407**

**LABOG, Chairperson of Kilusang Mayo Uno, CRISTINA E. PALABAY, Secretary General of Karapatan, FERDINAND R. GAITE, Chairperson of COURAGE, JOEL B. MAGLUNSOD, Vice President of Anakpawis Party-List, LANA R. LINABAN, Secretary General Gabriela Women’s Party, ADOLFO ARES P. GUTIERREZ, and JULIUS GARCIA MATIBAG,**  
 Petitioners,

- versus -

**BENIGNO SIMEON C. AQUINO III, President of the Republic of the Philippines, PAQUITO N. OCHOA, JR., Executive Secretary, SENATE OF THE PHILIPPINES, represented by SENATE PRESIDENT JUAN PONCE ENRILE, HOUSE OF REPRESENTATIVES, represented by SPEAKER FELICIANO BELMONTE, JR., LEILA DE LIMA, Secretary of the Department of Justice, LOUIS NAPOLEON C. CASAMBRE, Executive Director of the Information and Communications Technology Office, NONNATUS CAESAR R. ROJAS, Director of the National Bureau of Investigation, D/GEN. NICANOR A. BARTOLOME, Chief of the Philippine National Police, MANUEL A. ROXAS II, Secretary of the Department of the Interior and Local Government,**  
 Respondents.

X ----- X

**MELENCIO S. STA. MARIA, SEDFREY M. CANDELARIA, AMPARITA STA. MARIA, RAY PAOLO J. SANTIAGO, GILBERT V. SEMBRANO, and RYAN JEREMIAH D. QUAN (all of the Ateneo Human Rights Center),**  
 Petitioners,

**G.R. No. 203440**

- versus -

**HONORABLE PAQUITO OCHOA in his capacity as Executive Secretary,**

**HONORABLE LEILA DE LIMA in her capacity as Secretary of Justice, HONORABLE MANUEL ROXAS in his capacity as Secretary of the Department of Interior and Local Government, The CHIEF of the Philippine National Police, The DIRECTOR of the National Bureau of Investigation (all of the Executive Department of Government),**

Respondents.

X ----- X

**NATIONAL UNION OF JOURNALISTS OF THE PHILIPPINES (NUJP), PHILIPPINE PRESS INSTITUTE (PPI), CENTER FOR MEDIA FREEDOM AND RESPONSIBILITY, ROWENA CARRANZA PARAAN, MELINDA QUINTOS-DE JESUS, JOSEPH ALWYN ALBURO, ARIEL SEBELLINO AND THE PETITIONERS IN THE e-PETITION <http://www.nujp.org/no-to-ra10175/>,**

**G.R. No. 203453**

Petitioners,

- versus -

**THE EXECUTIVE SECRETARY, THE SECRETARY OF JUSTICE, THE SECRETARY OF THE INTERIOR AND LOCAL GOVERNMENT, THE SECRETARY OF BUDGET AND MANAGEMENT, THE DIRECTOR GENERAL OF THE PHILIPPINE NATIONAL POLICE, THE DIRECTOR OF THE NATIONAL BUREAU OF INVESTIGATION, THE CYBERCRIME INVESTIGATION AND COORDINATING CENTER, AND ALL AGENCIES AND INSTRUMENTALITIES OF GOVERNMENT AND ALL PERSONS ACTING UNDER THEIR INSTRUCTIONS, ORDERS, DIRECTION IN RELATION TO THE IMPLEMENTATION OF REPUBLIC ACT NO. 10175,**

Respondents.

X ----- X

**PAUL CORNELIUS T. CASTILLO  
& RYAN D. ANDRES,**

**G.R. No. 203454**

Petitioners,

- versus -

**THE HON. SECRETARY OF JUSTICE,  
THE HON. SECRETARY OF  
INTERIOR AND LOCAL  
GOVERNMENT,**

Respondents.

X ----- X

**ANTHONY IAN M. CRUZ; MARCELO R.  
LANDICHO; BENJAMIN NOEL A.  
ESPINA; MARCK RONALD C. RIMORIN;  
JULIUS D. ROCAS; OLIVER RICHARD  
V. ROBILLO; AARON ERICK A.  
LOZADA; GERARD ADRIAN P.  
MAGNAYE; JOSE REGINALD A.  
RAMOS; MA. ROSARIO T. JUAN;  
BRENDALYN P. RAMIREZ; MAUREEN  
A. HERMITANIO; KRISTINE JOY S.  
REMENTILLA; MARICEL O. GRAY;  
JULIUS IVAN F. CABIGON; BENRALPH  
S. YU; CEBU BLOGGERS SOCIETY, INC.  
PRESIDENT RUBEN B. LICERA, JR; and  
PINOY EXPAT/OFW BLOG AWARDS,  
INC. COORDINATOR PEDRO E. RAHON;**

**G.R. No. 203469**

Petitioners,

- versus -

**HIS EXCELLENCY BENIGNO S.  
AQUINO III, in his capacity as President of  
the Republic of the Philippines; SENATE  
OF THE PHILIPPINES, represented by  
HON. JUAN PONCE ENRILE, in his  
capacity as Senate President; HOUSE OF  
REPRESENTATIVES, represented by  
FELICIANO R. BELMONTE, JR., in his  
capacity as Speaker of the House of  
Representatives; HON. PAQUITO N.  
OCHOA, JR., in his capacity as Executive  
Secretary; HON. LEILA M. DE LIMA, in  
her capacity as Secretary of Justice; HON.  
LOUIS NAPOLEON C. CASAMBRE, in his**

**capacity as Executive Director, Information and Communications Technology Office; HON. NONNATUS CAESAR R. ROJAS, in his capacity as Director, National Bureau of Investigation; and P/DGEN. NICANOR A. BARTOLOME, in his capacity as Chief, Philippine National Police,**

Respondents.

X ----- X

**PHILIPPINE BAR ASSOCIATION, INC.,**  
Petitioner,

**G.R. No. 203501**

- versus -

**HIS EXCELLENCY BENIGNO S. AQUINO III, in his official capacity as President of the Republic of the Philippines; HON. PAQUITO N. OCHOA, JR., in his official capacity as Executive Secretary; HON. LEILA M. DE LIMA, in her official capacity as Secretary of Justice; LOUIS NAPOLEON C. CASAMBRE, in his official capacity as Executive Director, Information and Communications Technology Office; NONNATUS CAESAR R. ROJAS, in his official capacity as Director of the National Bureau of Investigation; and DIRECTOR GENERAL NICANOR A. BARTOLOME, in his official capacity as Chief of the Philippine National Police,**

Respondents.

X ----- X

**BAYAN MUNA REPRESENTATIVE NERI J. COLMENARES,**

Petitioner,

**G.R. No. 203509**

- versus -

**THE EXECUTIVE SECRETARY PAQUITO OCHOA, JR.,**

Respondent.

X ----- X

**NATIONAL PRESS CLUB OF THE PHILIPPINES, INC.** represented by **BENNY D. ANTIPORDA** in his capacity as **President and in his personal capacity,**  
Petitioner,

**G.R. No. 203515**

- versus -

**OFFICE OF THE PRESIDENT, PRES. BENIGNO SIMEON AQUINO III, DEPARTMENT OF JUSTICE, DEPARTMENT OF INTERIOR AND LOCAL GOVERNMENT, PHILIPPINE NATIONAL POLICE, NATIONAL BUREAU OF INVESTIGATION, DEPARTMENT OF BUDGET AND MANAGEMENT AND ALL OTHER GOVERNMENT INSTRUMENTALITIES WHO HAVE HANDS IN THE PASSAGE AND/OR IMPLEMENTATION OF REPUBLIC ACT 10175,**  
Respondents.

X ----- X

**PHILIPPINE INTERNET FREEDOM ALLIANCE,** composed of **DAKILA-PHILIPPINE COLLECTIVE FOR MODERN HEROISM,** represented by **Leni Velasco,** **PARTIDO LAKAS NG MASA,** represented by **Cesar S. Melencio,** **FRANCIS EUSTON R. ACERO,** **MARLON ANTHONY ROMASANTA TONSON,** **TEODORO A. CASIÑO,** **NOEMI LARDIZABAL-DADO,** **IMELDA MORALES,** **JAMES MATTHEW B. MIRAFLOR,** **JUAN G.M. RAGRAGIO,** **MARIA FATIMA A. VILLENA,** **MEDARDO M. MANRIQUE, JR.,** **LAUREN DADO,** **MARCO VITTORIA TOBIAS SUMAYAO,** **IRENE CHIA,** **ERASTUS NOEL T. DELIZO,** **CRISTINA SARAH E. OSORIO,** **ROMEO FACTOLERIN,** **NAOMI L. TUPAS,** **KENNETH KENG,** **ANA ALEXANDRA C. CASTRO,**  
Petitioners,

**G.R. No. 203518**



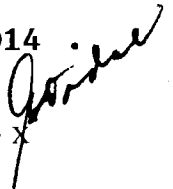
- versus -

**THE EXECUTIVE SECRETARY, THE SECRETARY OF JUSTICE, THE SECRETARY OF INTERIOR AND LOCAL GOVERNMENT, THE SECRETARY OF SCIENCE AND TECHNOLOGY, THE EXECUTIVE DIRECTOR OF THE INFORMATION TECHNOLOGY OFFICE, THE DIRECTOR OF THE NATIONAL BUREAU OF INVESTIGATION, THE CHIEF, PHILIPPINE NATIONAL POLICE, THE HEAD OF THE DOJ OFFICE OF CYBERCRIME, and THE OTHER MEMBERS OF THE CYBERCRIME INVESTIGATION AND COORDINATING CENTER,**

Respondents.

Promulgated:

FEBRUARY 18, 2014



x ----- x

***DECISION***

**ABAD, J.:**

These consolidated petitions seek to declare several provisions of Republic Act (R.A.) 10175, the Cybercrime Prevention Act of 2012, unconstitutional and void.

**The Facts and the Case**

The cybercrime law aims to regulate access to and use of the cyberspace. Using his laptop or computer, a person can connect to the internet, a system that links him to other computers and enable him, among other things, to:

1. Access virtual libraries and encyclopedias for all kinds of information that he needs for research, study, amusement, upliftment, or pure curiosity;
2. Post billboard-like notices or messages, including pictures and videos, for the general public or for special audiences like associates, classmates, or friends and read postings from them;
3. Advertise and promote goods or services and make purchases and payments;



4. Inquire and do business with institutional entities like government agencies, banks, stock exchanges, trade houses, credit card companies, public utilities, hospitals, and schools; and

5. Communicate in writing or by voice with any person through his e-mail address or telephone.

This is cyberspace, a system that accommodates millions and billions of simultaneous and ongoing individual accesses to and uses of the internet. The cyberspace is a boon to the need of the current generation for greater information and facility of communication. But all is not well with the system since it could not filter out a number of persons of ill will who would want to use cyberspace technology for mischiefs and crimes. One of them can, for instance, avail himself of the system to unjustly ruin the reputation of another or bully the latter by posting defamatory statements against him that people can read.

And because linking with the internet opens up a user to communications from others, the ill-motivated can use the cyberspace for committing theft by hacking into or surreptitiously accessing his bank account or credit card or defrauding him through false representations. The wicked can use the cyberspace, too, for illicit trafficking in sex or for exposing to pornography guileless children who have access to the internet. For this reason, the government has a legitimate right to regulate the use of cyberspace and contain and punish wrongdoings.

Notably, there are also those who would want, like vandals, to wreak or cause havoc to the computer systems and networks of indispensable or highly useful institutions as well as to the laptop or computer programs and memories of innocent individuals. They accomplish this by sending electronic viruses or virtual dynamites that destroy those computer systems, networks, programs, and memories. The government certainly has the duty and the right to prevent these tomfooleries from happening and punish their perpetrators, hence the Cybercrime Prevention Act.

But petitioners claim that the means adopted by the cybercrime law for regulating undesirable cyberspace activities violate certain of their constitutional rights. The government of course asserts that the law merely seeks to reasonably put order into cyberspace activities, punish wrongdoings, and prevent hurtful attacks on the system.

Pending hearing and adjudication of the issues presented in these cases, on February 5, 2013 the Court extended the original 120-day temporary restraining order (TRO) that it earlier issued on October 9, 2012, enjoining respondent government agencies from implementing the cybercrime law until further orders.

## The Issues Presented

Petitioners challenge the constitutionality of the following provisions of the cybercrime law that regard certain acts as crimes and impose penalties for their commission as well as provisions that would enable the government to track down and penalize violators. These provisions are:

- a. Section 4(a)(1) on Illegal Access;
- b. Section 4(a)(3) on Data Interference;
- c. Section 4(a)(6) on Cyber-squatting;
- d. Section 4(b)(3) on Identity Theft;
- e. Section 4(c)(1) on Cybersex;
- f. Section 4(c)(2) on Child Pornography;
- g. Section 4(c)(3) on Unsolicited Commercial Communications;
- h. Section 4(c)(4) on Libel;
- i. Section 5 on Aiding or Abetting and Attempt in the Commission of Cybercrimes;
- j. Section 6 on the Penalty of One Degree Higher;
- k. Section 7 on the Prosecution under both the Revised Penal Code (RPC) and R.A. 10175;
- l. Section 8 on Penalties;
- m. Section 12 on Real-Time Collection of Traffic Data;
- n. Section 13 on Preservation of Computer Data;
- o. Section 14 on Disclosure of Computer Data;
- p. Section 15 on Search, Seizure and Examination of Computer Data;
- q. Section 17 on Destruction of Computer Data;
- r. Section 19 on Restricting or Blocking Access to Computer Data;
- s. Section 20 on Obstruction of Justice;
- t. Section 24 on Cybercrime Investigation and Coordinating Center (CICC); and
- u. Section 26(a) on CICC's Powers and Functions.

Some petitioners also raise the constitutionality of related Articles 353, 354, 361, and 362 of the RPC on the crime of libel.

## The Rulings of the Court

### Section 4(a)(1)

Section 4(a)(1) provides:

Section 4. *Cybercrime Offenses.* – The following acts constitute the offense of cybercrime punishable under this Act:

(a) Offenses against the confidentiality, integrity and availability of computer data and systems:

(1) Illegal Access. – The access to the whole or any part of a computer system without right.

Petitioners contend that Section 4(a)(1) fails to meet the strict scrutiny standard required of laws that interfere with the fundamental rights of the people and should thus be struck down.

The Court has in a way found the strict scrutiny standard, an American constitutional construct,<sup>1</sup> useful in determining the constitutionality of laws that tend to target a class of things or persons. According to this standard, a legislative classification that impermissibly interferes with the exercise of fundamental right or operates to the peculiar class disadvantage of a suspect class is presumed unconstitutional. The burden is on the government to prove that the classification is necessary to achieve a compelling state interest and that it is the least restrictive means to protect such interest.<sup>2</sup> Later, the strict scrutiny standard was used to assess the validity of laws dealing with the regulation of speech, gender, or race as well as other fundamental rights, as expansion from its earlier applications to equal protection.<sup>3</sup>

In the cases before it, the Court finds nothing in Section 4(a)(1) that calls for the application of the strict scrutiny standard since no fundamental freedom, like speech, is involved in punishing what is essentially a condemnable act – accessing the computer system of another without right. It is a universally condemned conduct.<sup>4</sup>

Petitioners of course fear that this section will jeopardize the work of ethical hackers, professionals who employ tools and techniques used by criminal hackers but would neither damage the target systems nor steal information. Ethical hackers evaluate the target system's security and report back to the owners the vulnerabilities they found in it and give instructions for how these can be remedied. Ethical hackers are the equivalent of independent auditors who come into an organization to verify its bookkeeping records.<sup>5</sup>

---

<sup>1</sup> The US Supreme Court first suggested the standard by implication in footnote 4 of *United States v. Carolene Products* (304 U.S. 144, 152 n.4 (1938)). See *Fatal in Theory and Strict in Fact: An Empirical Analysis of Strict Scrutiny in the Federal Courts*, Winkler, A. UCLA School of Law, Public Law & Legal Theory Research Paper Series, Research Paper No. 06-14, <http://ssrn.com/abstract=897360> (last accessed April 10, 2013).

<sup>2</sup> *Serrano v. Gallant Maritime Services, Inc.*, G.R. No. 167614, March 24, 2009, 582 SCRA 254, 278.

<sup>3</sup> *White Light Corporation v. City of Manila*, G.R. No. 122846, January 20, 2009, 576 SCRA 416, 437.

<sup>4</sup> All 50 states of the United States have passed individual state laws criminalizing hacking or unauthorized access, <http://www.ncsl.org/issues-research/telecom/computer-hacking-and-unauthorized-access-laws.aspx> (last accessed May 16, 2013). The United States Congress has also passed the Computer Fraud and Abuse Act 18 U.S.C. § 1030 that penalizes, among others, hacking. The Budapest Convention on Cybercrime considers hacking as an offense against the confidentiality, integrity and availability of computer data and systems and 29 countries have already ratified or acceded, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG> (last accessed May 16, 2013).

<sup>5</sup> *Ethical Hacking*. Palmer, C. IBM Systems Journal, Vol. 40, No. 3, 2001, p. 770, <http://pdf.textfiles.com/security/palmer.pdf> (last accessed April 10, 2013).

Besides, a client's engagement of an ethical hacker requires an agreement between them as to the extent of the search, the methods to be used, and the systems to be tested. This is referred to as the "*get out of jail free card*."<sup>6</sup> Since the ethical hacker does his job with prior permission from the client, such permission would insulate him from the coverage of Section 4(a)(1).

**Section 4(a)(3) of the Cybercrime Law**

Section 4(a)(3) provides:

Section 4. *Cybercrime Offenses*. – The following acts constitute the offense of cybercrime punishable under this Act:

(a) Offenses against the confidentiality, integrity and availability of computer data and systems:

x x x x

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

Petitioners claim that Section 4(a)(3) suffers from overbreadth in that, while it seeks to discourage data interference, it intrudes into the area of protected speech and expression, creating a chilling and deterrent effect on these guaranteed freedoms.

Under the overbreadth doctrine, a proper governmental purpose, constitutionally subject to state regulation, may not be achieved by means that unnecessarily sweep its subject broadly, thereby invading the area of protected freedoms.<sup>7</sup> But Section 4(a)(3) does not encroach on these freedoms at all. It simply punishes what essentially is a form of vandalism,<sup>8</sup> the act of willfully destroying without right the things that belong to others, in this case their computer data, electronic document, or electronic data message. Such act has no connection to guaranteed freedoms. There is no freedom to destroy other people's computer systems and private documents.

All penal laws, like the cybercrime law, have of course an inherent chilling effect, an *in terrorem* effect<sup>9</sup> or the fear of possible prosecution that hangs on the heads of citizens who are minded to step beyond the boundaries

<sup>6</sup> Id. at 774.

<sup>7</sup> *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, G.R. Nos. 178552, 178554, 178581, 178890, 179157 & 179461, October 5, 2010, 632 SCRA 146, 185.

<sup>8</sup> The intentional destruction of property is popularly referred to as vandalism. It includes behavior such as breaking windows, slashing tires, spray painting a wall with graffiti, and **destroying a computer system through the use of a computer virus**, <http://legal-dictionary.thefreedictionary.com/Vandalism> (last accessed August 12, 2013).

<sup>9</sup> *Southern Hemisphere Engagement Network, Inc. v. Anti-Terrorism Council*, supra note 7, at 186; *Estrada v. Sandiganbayan*, 421 Phil. 290, 354 (2001).

of what is proper. But to prevent the State from legislating criminal laws because they instill such kind of fear is to render the state powerless in addressing and penalizing socially harmful conduct.<sup>10</sup> Here, the chilling effect that results in paralysis is an illusion since Section 4(a)(3) clearly describes the evil that it seeks to punish and creates no tendency to intimidate the free exercise of one's constitutional rights.

Besides, the overbreadth challenge places on petitioners the heavy burden of proving that under no set of circumstances will Section 4(a)(3) be valid.<sup>11</sup> Petitioner has failed to discharge this burden.

**Section 4(a)(6) of the Cybercrime Law**

Section 4(a)(6) provides:

Section 4. *Cybercrime Offenses.* – The following acts constitute the offense of cybercrime punishable under this Act:

(a) Offenses against the confidentiality, integrity and availability of computer data and systems:

x x x x

(6) Cyber-squatting. – The acquisition of domain name over the internet in bad faith to profit, mislead, destroy the reputation, and deprive others from registering the same, if such a domain name is:

- (i) Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;
- (ii) Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and
- (iii) Acquired without right or with intellectual property interests in it.

Petitioners claim that Section 4(a)(6) or cyber-squatting violates the equal protection clause<sup>12</sup> in that, not being narrowly tailored, it will cause a user using his real name to suffer the same fate as those who use aliases or take the name of another in satire, parody, or any other literary device. For example, supposing there exists a well known billionaire-philanthropist named “Julio Gandolfo,” the law would punish for cyber-squatting both the person who registers such name because he claims it to be his pseudo-name and another who registers the name because it happens to be his real name. Petitioners claim that, considering the substantial distinction between the two, the law should recognize the difference.

<sup>10</sup> Id.

<sup>11</sup> Id., citing the Opinion of Justice Vicente V. Mendoza in *Estrada v. Sandiganbayan*.

<sup>12</sup> 1987 CONSTITUTION, Article III, Section 1.

But there is no real difference whether he uses “Julio Gandolfo” which happens to be his real name or use it as a pseudo-name for it is the evil purpose for which he uses the name that the law condemns. The law is reasonable in penalizing him for acquiring the domain name in bad faith to profit, mislead, destroy reputation, or deprive others who are not ill-motivated of the rightful opportunity of registering the same. The challenge to the constitutionality of Section 4(a)(6) on ground of denial of equal protection is baseless.

**Section 4(b)(3) of the Cybercrime Law**

Section 4(b)(3) provides:

Section 4. *Cybercrime Offenses.* – The following acts constitute the offense of cybercrime punishable under this Act:

x x x x

b) Computer-related Offenses:

x x x x

(3) Computer-related Identity Theft. – The intentional acquisition, use, misuse, transfer, possession, alteration, or deletion of identifying information belonging to another, whether natural or juridical, without right: *Provided:* that if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

Petitioners claim that Section 4(b)(3) violates the constitutional rights to due process and to privacy and correspondence, and transgresses the freedom of the press.

The right to privacy, or the right to be let alone, was institutionalized in the 1987 Constitution as a facet of the right protected by the guarantee against unreasonable searches and seizures.<sup>13</sup> But the Court acknowledged its existence as early as 1968 in *Morfe v. Mutuc*,<sup>14</sup> it ruled that the right to privacy exists independently of its identification with liberty; it is in itself fully deserving of constitutional protection.

Relevant to any discussion of the right to privacy is the concept known as the “Zones of Privacy.” The Court explained in “*In the Matter of the Petition for Issuance of Writ of Habeas Corpus of Sabio v. Senator Gordon*”<sup>15</sup> the relevance of these zones to the right to privacy:

Zones of privacy are recognized and protected in our laws. Within these zones, any form of intrusion is impermissible unless excused by law

<sup>13</sup> *Pollo v. Constantino-David*, G.R. No. 181881, October 18, 2011, 659 SCRA 189, 204-205.

<sup>14</sup> 130 Phil. 415 (1968)

<sup>15</sup> 535 Phil. 687, 714-715 (2006).

and in accordance with customary legal process. The meticulous regard we accord to these zones arises not only from our conviction that the right to privacy is a “constitutional right” and “the right most valued by civilized men,” but also from our adherence to the Universal Declaration of Human Rights which mandates that, “no one shall be subjected to arbitrary interference with his privacy” and “everyone has the right to the protection of the law against such interference or attacks.”

Two constitutional guarantees create these zones of privacy: (a) the right against unreasonable searches<sup>16</sup> and seizures, which is the basis of the right to be let alone, and (b) the right to privacy of communication and correspondence.<sup>17</sup>

In assessing the challenge that the State has impermissibly intruded into these zones of privacy, a court must determine whether a person has exhibited a reasonable expectation of privacy and, if so, whether that expectation has been violated by unreasonable government intrusion.<sup>18</sup>

The usual identifying information regarding a person includes his name, his citizenship, his residence address, his contact number, his place and date of birth, the name of his spouse if any, his occupation, and similar data.<sup>19</sup> The law punishes those who acquire or use such identifying information without right, implicitly to cause damage. Petitioners simply fail to show how government effort to curb computer-related identity theft violates the right to privacy and correspondence as well as the right to due process of law.

Also, the charge of invalidity of this section based on the overbreadth doctrine will not hold water since the specific conducts proscribed do not intrude into guaranteed freedoms like speech. Clearly, what this section regulates are specific actions: the acquisition, use, misuse or deletion of personal identifying data of another. There is no fundamental right to acquire another’s personal data.

Further, petitioners fear that Section 4(b)(3) violates the freedom of the press in that journalists would be hindered from accessing the unrestricted user account of a person in the news to secure information about him that could be published. But this is not the essence of identity theft that the law seeks to prohibit and punish. Evidently, the theft of identity information must be intended for an illegitimate purpose. Moreover, acquiring and disseminating information made public by the user himself cannot be regarded as a form of theft.

---

<sup>16</sup> Supra note 12, Article II, Section 2.

<sup>17</sup> Supra note 12, Article III, Section 3.

<sup>18</sup> *In the Matter of the Petition for Issuance of Writ of Habeas Corpus of Sabio v. Senator Gordon*, supra note 15.

<sup>19</sup> Section 3(g) of Republic Act 10173 or the Data Privacy Act of 2012 defines personal information as “any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.”



The Court has defined intent to gain as an internal act which can be established through the overt acts of the offender, and it may be presumed from the furtive taking of useful property pertaining to another, unless special circumstances reveal a different intent on the part of the perpetrator.<sup>20</sup> As such, the press, whether in quest of news reporting or social investigation, has nothing to fear since a special circumstance is present to negate intent to gain which is required by this Section.

**Section 4(c)(1) of the Cybercrime Law**

Section 4(c)(1) provides:

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

x x x x

(c) Content-related Offenses:

(1) Cybersex.— The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.

Petitioners claim that the above violates the freedom of expression clause of the Constitution.<sup>21</sup> They express fear that private communications of sexual character between husband and wife or consenting adults, which are not regarded as crimes under the penal code, would now be regarded as crimes when done “for favor” in cyberspace. In common usage, the term “favor” includes “gracious kindness,” “a special privilege or right granted or conceded,” or “a token of love (as a ribbon) usually worn conspicuously.”<sup>22</sup> This meaning given to the term “favor” embraces socially tolerated trysts. The law as written would invite law enforcement agencies into the bedrooms of married couples or consenting individuals.

But the deliberations of the Bicameral Committee of Congress on this section of the Cybercrime Prevention Act give a proper perspective on the issue. These deliberations show a lack of intent to penalize a “private showing x x x between and among two private persons x x x although that may be a form of obscenity to some.”<sup>23</sup> The understanding of those who drew up the cybercrime law is that the element of “engaging in a business” is necessary to constitute the illegal cybersex.<sup>24</sup> The Act actually seeks to punish cyber prostitution, white slave trade, and pornography for favor and

<sup>20</sup> *People v. Uy*, G.R. No. 174660, May 30, 2011, 649 SCRA 236.

<sup>21</sup> *Supra* note 17 (G.R. No. 203359 [*Guingona*]; G.R. No. 203518 [*PIFA*]).

<sup>22</sup> Merriam-Webster, <http://www.merriam-webster.com/dictionary/favor> (last accessed May 30, 2013).

<sup>23</sup> Bicameral Conference Committee, pp. 5-6.

<sup>24</sup> *Id.*

consideration. This includes interactive prostitution and pornography, *i.e.*, by webcam.<sup>25</sup>

The subject of Section 4(c)(1)—lascivious exhibition of sexual organs or sexual activity—is not novel. Article 201 of the RPC punishes “obscene publications and exhibitions and indecent shows.” The Anti-Trafficking in Persons Act of 2003 penalizes those who “maintain or hire a person to engage in prostitution or pornography.”<sup>26</sup> The law defines prostitution as any act, transaction, scheme, or design involving the use of a person by another, for sexual intercourse or lascivious conduct in exchange for money, profit, or any other consideration.<sup>27</sup>

The case of *Nogales v. People*<sup>28</sup> shows the extent to which the State can regulate materials that serve no other purpose than satisfy the market for violence, lust, or pornography.<sup>29</sup> The Court weighed the property rights of individuals against the public welfare. Private property, if containing pornographic materials, may be forfeited and destroyed. Likewise, engaging in sexual acts privately through internet connection, perceived by some as a right, has to be balanced with the mandate of the State to eradicate white slavery and the exploitation of women.

In any event, consenting adults are protected by the wealth of jurisprudence delineating the bounds of obscenity.<sup>30</sup> The Court will not declare Section 4(c)(1) unconstitutional where it stands a construction that makes it apply only to persons engaged in the business of maintaining, controlling, or operating, directly or indirectly, the lascivious exhibition of sexual organs or sexual activity with the aid of a computer system as Congress has intended.

### **Section 4(c)(2) of the Cybercrime Law**

Section 4(c)(2) provides:

Sec. 4. *Cybercrime Offenses.* – The following acts constitute the offense of cybercrime punishable under this Act:

x x x x

(c) Content-related Offenses:

x x x x

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

<sup>25</sup> Office of the Solicitor General, COMMENT, p. 71.

<sup>26</sup> REPUBLIC ACT 9208, Section 4(e).

<sup>27</sup> *Id.*, Section 3(c).

<sup>28</sup> G.R. No. 191080, November 21, 2011, 660 SCRA 475.

<sup>29</sup> REVISED PENAL CODE, Article 201 (2)(b)(2), as amended by Presidential Decree 969.

<sup>30</sup> *Pita v. Court of Appeals*, 258-A Phil. 134 (1989).

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

It seems that the above merely expands the scope of the Anti-Child Pornography Act of 2009<sup>31</sup> (ACPA) to cover identical activities in cyberspace. In theory, nothing prevents the government from invoking the ACPA when prosecuting persons who commit child pornography using a computer system. Actually, ACPA's definition of child pornography already embraces the use of "electronic, mechanical, digital, optical, magnetic or any other means." Notably, no one has questioned this ACPA provision.

Of course, the law makes the penalty higher by one degree when the crime is committed in cyberspace. But no one can complain since the intensity or duration of penalty is a legislative prerogative and there is rational basis for such higher penalty.<sup>32</sup> The potential for uncontrolled proliferation of a particular piece of child pornography when uploaded in the cyberspace is incalculable.

Petitioners point out that the provision of ACPA that makes it unlawful for any person to "produce, direct, manufacture or create any form of child pornography"<sup>33</sup> clearly relates to the prosecution of persons who aid and abet the core offenses that ACPA seeks to punish.<sup>34</sup> Petitioners are wary that a person who merely doodles on paper and imagines a sexual abuse of a 16-year-old is not criminally liable for producing child pornography but one who formulates the idea on his laptop would be. Further, if the author bounces off his ideas on Twitter, anyone who replies to the tweet could be considered aiding and abetting a cybercrime.

The question of aiding and abetting the offense by simply commenting on it will be discussed elsewhere below. For now the Court must hold that the constitutionality of Section 4(c)(2) is not successfully challenged.

### **Section 4(c)(3) of the Cybercrime Law**

Section 4(c)(3) provides:

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

X X X X

---

<sup>31</sup> REPUBLIC ACT 9775 entitled AN ACT DEFINING THE CRIME OF CHILD PORNOGRAPHY, PRESCRIBING PENALTIES THEREFOR AND FOR OTHER PURPOSES.

<sup>32</sup> *Sto. Tomas v. Salac*, G.R. No. 152642, November 13, 2012, 685 SCRA 245, citing *People v. Ventura*, 114 Phil. 162, 167 (1962).

<sup>33</sup> *Supra* note 31, Section 4(b).

<sup>34</sup> G.R. No. 203407 (*Bagong Alyansang Makabayan*), MEMORANDUM, pp. 34-37.

## (c) Content-related Offenses:

x x x x

(3) *Unsolicited Commercial Communications.* – The transmission of commercial electronic communication with the use of computer system which seeks to advertise, sell, or offer for sale products and services are prohibited unless:

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

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

(iii) The following conditions are present:

(aa) The commercial electronic communication contains a simple, valid, and reliable way for the recipient to reject receipt of further commercial electronic messages (opt-out) from the same source;

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

(cc) The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

The above penalizes the transmission of unsolicited commercial communications, also known as “spam.” The term “spam” surfaced in early internet chat rooms and interactive fantasy games. One who repeats the same sentence or comment was said to be making a “spam.” The term referred to a Monty Python’s Flying Circus scene in which actors would keep saying “Spam, Spam, Spam, and Spam” when reading options from a menu.<sup>35</sup>

The Government, represented by the Solicitor General, points out that unsolicited commercial communications or spams are a nuisance that wastes the storage and network capacities of internet service providers, reduces the efficiency of commerce and technology, and interferes with the owner’s peaceful enjoyment of his property. Transmitting spams amounts to trespass to one’s privacy since the person sending out spams enters the recipient’s domain without prior permission. The OSG contends that commercial speech enjoys less protection in law.

But, firstly, the government presents no basis for holding that unsolicited electronic ads reduce the “efficiency of computers.” Secondly, people, before the arrival of the age of computers, have already been receiving such unsolicited ads by mail. These have never been outlawed as

---

<sup>35</sup> *White Buffalo Ventures, LLC v. Univ. of Tex. at Austin*, 2004 U.S. Dist. LEXIS 19152 (W.D. Tex. Mar. 22, 2004).

nuisance since people might have interest in such ads. What matters is that the recipient has the option of not opening or reading these mail ads. That is true with spams. Their recipients always have the option to delete or not to read them.

To prohibit the transmission of unsolicited ads would deny a person the right to read his emails, even unsolicited commercial ads addressed to him. Commercial speech is a separate category of speech which is not accorded the same level of protection as that given to other constitutionally guaranteed forms of expression but is nonetheless entitled to protection.<sup>36</sup> The State cannot rob him of this right without violating the constitutionally guaranteed freedom of expression. Unsolicited advertisements are legitimate forms of expression.

**Articles 353, 354, and 355 of the Penal Code**  
**Section 4(c)(4) of the Cyber Crime Law**

Petitioners dispute the constitutionality of both the penal code provisions on libel as well as Section 4(c)(4) of the Cybercrime Prevention Act on cyberlibel.

The RPC provisions on libel read:

Art. 353. *Definition of libel.* — A libel is public and malicious imputation of a crime, or of a vice or defect, real or imaginary, or any act, omission, condition, status, or circumstance tending to cause the dishonor, discredit, or contempt of a natural or juridical person, or to blacken the memory of one who is dead.

Art. 354. *Requirement for publicity.* — Every defamatory imputation is presumed to be malicious, even if it be true, if no good intention and justifiable motive for making it is shown, except in the following cases:

1. A private communication made by any person to another in the performance of any legal, moral or social duty; and
2. A fair and true report, made in good faith, without any comments or remarks, of any judicial, legislative or other official proceedings which are not of confidential nature, or of any statement, report or speech delivered in said proceedings, or of any other act performed by public officers in the exercise of their functions.

Art. 355. *Libel means by writings or similar means.* — A libel committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means, shall be punished by *prision correccional* in its minimum and medium periods or a fine ranging from 200 to 6,000 pesos,

---

<sup>36</sup> Concurring Opinion of Chief Justice Reynato S. Puno in *Pharmaceutical and Health Care Association of the Philippines v. Duque III*, 561 Phil. 387, 449 (2007).

or both, in addition to the civil action which may be brought by the offended party.

The libel provision of the cybercrime law, on the other hand, merely incorporates to form part of it the provisions of the RPC on libel. Thus Section 4(c)(4) reads:

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

x x x x

(c) Content-related Offenses:

x x x x

(4) *Libel.* — The unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future.

Petitioners lament that libel provisions of the penal code<sup>37</sup> and, in effect, the libel provisions of the cybercrime law carry with them the requirement of “presumed malice” even when the latest jurisprudence already replaces it with the higher standard of “actual malice” as a basis for conviction.<sup>38</sup> Petitioners argue that inferring “presumed malice” from the accused’s defamatory statement by virtue of Article 354 of the penal code infringes on his constitutionally guaranteed freedom of expression.

Petitioners would go further. They contend that the laws on libel should be stricken down as unconstitutional for otherwise good jurisprudence requiring “actual malice” could easily be overturned as the Court has done in *Fermin v. People*<sup>39</sup> even where the offended parties happened to be public figures.

The elements of libel are: (a) the allegation of a discreditable act or condition concerning another; (b) publication of the charge; (c) identity of the person defamed; and (d) existence of malice.<sup>40</sup>

There is “actual malice” or malice in fact<sup>41</sup> when the offender makes the defamatory statement with the knowledge that it is false or with reckless disregard of whether it was false or not.<sup>42</sup> The reckless disregard standard used here requires a high degree of awareness of probable falsity. There must be sufficient evidence to permit the conclusion that the accused in fact

<sup>37</sup> Supra note 29, Article 362.

<sup>38</sup> *Borjal v. Court of Appeals*, 361 Phil. 1 (1999); *Vasquez v. Court of Appeals*, 373 Phil. 238 (1999).

<sup>39</sup> 573 Phil. 278 (2008).

<sup>40</sup> *Vasquez v. Court of Appeals*, supra note 38.

<sup>41</sup> L. BOADO, COMPACT REVIEWER IN CRIMINAL LAW 403-404 (2d ed. 2007).

<sup>42</sup> *Vasquez v. Court of Appeals*, supra note 38, citing *New York Times v. Sullivan*, 376 U.S. 254, 11 L.Ed.2d 686 (1964).

entertained serious doubts as to the truth of the statement he published. Gross or even extreme negligence is not sufficient to establish actual malice.<sup>43</sup>

The prosecution bears the burden of proving the presence of actual malice in instances where such element is required to establish guilt. The defense of absence of actual malice, even when the statement turns out to be false, is available where the offended party is a public official or a public figure, as in the cases of *Vasquez* (a *barangay* official) and *Borjal* (the Executive Director, First National Conference on Land Transportation). Since the penal code and implicitly, the cybercrime law, mainly target libel against private persons, the Court recognizes that these laws imply a stricter standard of “malice” to convict the author of a defamatory statement where the offended party is a public figure. Society’s interest and the maintenance of good government demand a full discussion of public affairs.<sup>44</sup>

Parenthetically, the Court cannot accept the proposition that its ruling in *Fermin* disregarded the higher standard of actual malice or malice in fact when it found Cristinelli Fermin guilty of committing libel against complainants who were public figures. Actually, the Court found the presence of malice in fact in that case. Thus:

It can be gleaned from her testimony that petitioner had the motive to make defamatory imputations against complainants. Thus, petitioner cannot, by simply making a general denial, convince us that there was no malice on her part. Verily, **not only was there malice in law**, the article being malicious in itself, **but there was also malice in fact**, as there was motive to talk ill against complainants during the electoral campaign. (Emphasis ours)

Indeed, the Court took into account the relatively wide leeway given to utterances against public figures in the above case, cinema and television personalities, when it modified the penalty of imprisonment to just a fine of ₱6,000.00.

But, where the offended party is a private individual, the prosecution need not prove the presence of malice. The law explicitly presumes its existence (malice in law) from the defamatory character of the assailed statement.<sup>45</sup> For his defense, the accused must show that he has a justifiable reason for the defamatory statement even if it was in fact true.<sup>46</sup>

Petitioners peddle the view that both the penal code and the Cybercrime Prevention Act violate the country’s obligations under the International Covenant of Civil and Political Rights (ICCPR). They point out that in *Adonis v. Republic of the Philippines*,<sup>47</sup> the United Nations

<sup>43</sup> *Annette F. v. Sharon S.*, 119 Cal. App. 4th 1146, 1151 (Cal. App. 4th Dist. 2004).

<sup>44</sup> *Borjal v. Court of Appeals*, supra note 38, citing *United States v. Bustos*, 37 Phil. 731 (1918).

<sup>45</sup> Supra note 41, at 403.

<sup>46</sup> Supra note 29, Article 354.

<sup>47</sup> Communication 1815/2008.

Human Rights Committee (UNHRC) cited its General Comment 34 to the effect that penal defamation laws should include the defense of truth.

But General Comment 34 does not say that the truth of the defamatory statement should constitute an all-encompassing defense. As it happens, Article 361 recognizes truth as a defense but under the condition that the accused has been prompted in making the statement by good motives and for justifiable ends. Thus:

Art. 361. Proof of the truth. — In every criminal prosecution for libel, the truth may be given in evidence to the court and if it appears that the matter charged as libelous is true, and, moreover, that it was published with good motives and for justifiable ends, the defendants shall be acquitted.

Proof of the truth of an imputation of an act or omission not constituting a crime shall not be admitted, unless the imputation shall have been made against Government employees with respect to facts related to the discharge of their official duties.

In such cases if the defendant proves the truth of the imputation made by him, he shall be acquitted.

Besides, the UNHRC did not actually enjoin the Philippines, as petitioners urge, to decriminalize libel. It simply suggested that defamation laws be crafted with care to ensure that they do not stifle freedom of expression.<sup>48</sup> Indeed, the ICCPR states that although everyone should enjoy freedom of expression, its exercise carries with it special duties and responsibilities. Free speech is not absolute. It is subject to certain restrictions, as may be necessary and as may be provided by law.<sup>49</sup>

The Court agrees with the Solicitor General that libel is not a constitutionally protected speech and that the government has an obligation to protect private individuals from defamation. Indeed, cyberlibel is actually not a new crime since Article 353, in relation to Article 355 of the penal code, already punishes it. In effect, Section 4(c)(4) above merely affirms that online defamation constitutes “similar means” for committing libel.

But the Court’s acquiescence goes only insofar as the cybercrime law penalizes the author of the libelous statement or article. Cyberlibel brings with it certain intricacies, unheard of when the penal code provisions on libel were enacted. The culture associated with internet media is distinct from that of print.

The internet is characterized as encouraging a freewheeling, anything-goes writing style.<sup>50</sup> In a sense, they are a world apart in terms of quickness of the reader’s reaction to defamatory statements posted in cyberspace,

---

<sup>48</sup> General Comment 34, ICCPR, par. 47.

<sup>49</sup> ICCPR, Article 19(2) and (3).

<sup>50</sup> *Sandals Resorts Int’l. Ltd. v. Google, Inc.*, 86 A.D.3d 32 (N.Y. App. Div. 1st Dep’t 2011).



facilitated by one-click reply options offered by the networking site as well as by the speed with which such reactions are disseminated down the line to other internet users. Whether these reactions to defamatory statement posted on the internet constitute aiding and abetting libel, acts that Section 5 of the cybercrime law punishes, is another matter that the Court will deal with next in relation to Section 5 of the law.

### **Section 5 of the Cybercrime Law**

Section 5 provides:

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

(a) *Aiding or Abetting in the Commission of Cybercrime.* — Any person who willfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable.

(b) *Attempt in the Commission of Cybercrime.* — Any person who willfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

Petitioners assail the constitutionality of Section 5 that renders criminally liable any person who willfully abets or aids in the commission or attempts to commit any of the offenses enumerated as cybercrimes. It suffers from overbreadth, creating a chilling and deterrent effect on protected expression.

The Solicitor General contends, however, that the current body of jurisprudence and laws on aiding and abetting sufficiently protects the freedom of expression of “netizens,” the multitude that avail themselves of the services of the internet. He points out that existing laws and jurisprudence sufficiently delineate the meaning of “aiding or abetting” a crime as to protect the innocent. The Solicitor General argues that plain, ordinary, and common usage is at times sufficient to guide law enforcement agencies in enforcing the law.<sup>51</sup> The legislature is not required to define every single word contained in the laws they craft.

Aiding or abetting has of course well-defined meaning and application in existing laws. When a person aids or abets another in destroying a forest,<sup>52</sup> smuggling merchandise into the country,<sup>53</sup> or interfering in the peaceful picketing of laborers,<sup>54</sup> his action is essentially physical and so is susceptible to easy assessment as criminal in character. These forms of aiding or abetting lend themselves to the tests of common sense and human experience.

---

<sup>51</sup> Office of the Solicitor General, MEMORANDUM, pp. 69-70.

<sup>52</sup> REPUBLIC ACT 3701, Section 1.

<sup>53</sup> REPUBLIC ACT 4712, Section 5.

<sup>54</sup> LABOR CODE, Article 264.

But, when it comes to certain cybercrimes, the waters are muddier and the line of sight is somewhat blurred. The idea of “aiding or abetting” wrongdoings online threatens the heretofore popular and unchallenged dogmas of cyberspace use.

According to the 2011 Southeast Asia Digital Consumer Report, 33% of Filipinos have accessed the internet within a year, translating to about 31 million users.<sup>55</sup> Based on a recent survey, the Philippines ranks 6<sup>th</sup> in the top 10 most engaged countries for social networking.<sup>56</sup> Social networking sites build social relations among people who, for example, share interests, activities, backgrounds, or real-life connections.<sup>57</sup>

Two of the most popular of these sites are Facebook and Twitter. As of late 2012, 1.2 billion people with shared interests use Facebook to get in touch.<sup>58</sup> Users register at this site, create a personal profile or an open book of who they are, add other users as friends, and exchange messages, including automatic notifications when they update their profile.<sup>59</sup> A user can post a statement, a photo, or a video on Facebook, which can be made visible to anyone, depending on the user’s privacy settings.

If the post is made available to the public, meaning to everyone and not only to his friends, anyone on Facebook can react to the posting, clicking any of several buttons of preferences on the program’s screen such as “Like,” “Comment,” or “Share.” “Like” signifies that the reader likes the posting while “Comment” enables him to post online his feelings or views about the same, such as “This is great!” When a Facebook user “Shares” a posting, the original “posting” will appear on his own Facebook profile, consequently making it visible to his down-line Facebook Friends.

Twitter, on the other hand, is an internet social networking and microblogging service that enables its users to send and read short text-based messages of up to 140 characters. These are known as “Tweets.” Microblogging is the practice of posting small pieces of digital content—which could be in the form of text, pictures, links, short videos, or other media—on the internet. Instead of friends, a Twitter user has “Followers,” those who subscribe to this particular user’s posts, enabling them to read the same, and “Following,” those whom this particular user is subscribed to, enabling him to read their posts. Like Facebook, a Twitter user can make his tweets available only to his Followers, or to the general public. If a post is available to the public, any Twitter user can “Retweet” a given posting. Retweeting is just reposting or republishing another person’s tweet without the need of copying and pasting it.

---

<sup>55</sup> G.R. No. 203440 (*Sta. Maria*), PETITION, p. 2.

<sup>56</sup> <http://www.statisticbrain.com/social-networking-statistics/> (last accessed January 14, 2013).

<sup>57</sup> [http://en.wikipedia.org/wiki/Social\\_networking\\_service](http://en.wikipedia.org/wiki/Social_networking_service) (last accessed January 14, 2013).

<sup>58</sup> <http://www.statisticbrain.com/social-networking-statistics/> (last accessed January 14, 2013).

<sup>59</sup> <http://en.wikipedia.org/wiki/Facebook> (last accessed January 14, 2013).

In the cyberworld, there are many actors: a) the blogger who originates the assailed statement; b) the blog service provider like Yahoo; c) the internet service provider like PLDT, Smart, Globe, or Sun; d) the internet café that may have provided the computer used for posting the blog; e) the person who makes a favorable comment on the blog; and f) the person who posts a link to the blog site.<sup>60</sup> Now, suppose Maria (a blogger) maintains a blog on WordPress.com (blog service provider). She needs the internet to access her blog so she subscribes to Sun Broadband (Internet Service Provider).

One day, Maria posts on her internet account the statement that a certain married public official has an illicit affair with a movie star. Linda, one of Maria's friends who sees this post, comments online, "Yes, this is so true! They are so immoral." Maria's original post is then multiplied by her friends and the latter's friends, and down the line to friends of friends almost *ad infinitum*. Nena, who is a stranger to both Maria and Linda, comes across this blog, finds it interesting and so shares the link to this apparently defamatory blog on her Twitter account. Nena's "Followers" then "Retweet" the link to that blog site.

Pamela, a Twitter user, stumbles upon a random person's "Retweet" of Nena's original tweet and posts this on her Facebook account. Immediately, Pamela's Facebook Friends start Liking and making Comments on the assailed posting. A lot of them even press the Share button, resulting in the further spread of the original posting into tens, hundreds, thousands, and greater postings.

The question is: are online postings such as "Liking" an openly defamatory statement, "Commenting" on it, or "Sharing" it with others, to be regarded as "aiding or abetting?" In libel in the physical world, if Nestor places on the office bulletin board a small poster that says, "Armand is a thief!," he could certainly be charged with libel. If Roger, seeing the poster, writes on it, "I like this!," that could not be libel since he did not author the poster. If Arthur, passing by and noticing the poster, writes on it, "Correct!," would that be libel? No, for he merely expresses agreement with the statement on the poster. He still is not its author. Besides, it is not clear if aiding or abetting libel in the physical world is a crime.

But suppose Nestor posts the blog, "Armand is a thief!" on a social networking site. Would a reader and his Friends or Followers, availing themselves of any of the "Like," "Comment," and "Share" reactions, be guilty of aiding or abetting libel? And, in the complex world of cyberspace expressions of thoughts, when will one be liable for aiding or abetting cybercrimes? Where is the venue of the crime?

---

<sup>60</sup> G.R. No. 203378 (*Adonis*) and G.R. No. 203391 (*Palatino*), CONSOLIDATED MEMORANDUM, p. 34.

Except for the original author of the assailed statement, the rest (those who pressed Like, Comment and Share) are essentially knee-jerk sentiments of readers who may think little or haphazardly of their response to the original posting. Will they be liable for aiding or abetting? And, considering the inherent impossibility of joining hundreds or thousands of responding “Friends” or “Followers” in the criminal charge to be filed in court, who will make a choice as to who should go to jail for the outbreak of the challenged posting?

The old parameters for enforcing the traditional form of libel would be a square peg in a round hole when applied to cyberspace libel. Unless the legislature crafts a cyber libel law that takes into account its unique circumstances and culture, such law will tend to create a chilling effect on the millions that use this new medium of communication in violation of their constitutionally-guaranteed right to freedom of expression.

The United States Supreme Court faced the same issue in *Reno v. American Civil Liberties Union*,<sup>61</sup> a case involving the constitutionality of the Communications Decency Act of 1996. The law prohibited (1) the knowing transmission, by means of a telecommunications device, of “obscene or indecent” communications to any recipient under 18 years of age; and (2) the knowing use of an interactive computer service to send to a specific person or persons under 18 years of age or to display in a manner available to a person under 18 years of age communications that, in context, depict or describe, in terms “patently offensive” as measured by contemporary community standards, sexual or excretory activities or organs.

Those who challenged the Act claim that the law violated the First Amendment’s guarantee of freedom of speech for being overbroad. The U.S. Supreme Court agreed and ruled:

The vagueness of the Communications Decency Act of 1996 (CDA), 47 U.S.C.S. §223, is a matter of special concern for two reasons. First, the CDA is a content-based regulation of speech. The **vagueness of such a regulation** raises special U.S. Const. amend. I concerns because of its **obvious chilling effect on free speech**. Second, the CDA is a criminal statute. In addition to the opprobrium and stigma of a criminal conviction, the CDA threatens violators with penalties including up to two years in prison for each act of violation. **The severity of criminal sanctions may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images.** As a practical matter, this increased deterrent effect, coupled with the risk of discriminatory enforcement of vague regulations, poses greater U.S. Const. amend. I concerns than those implicated by certain civil regulations.

X X X X

The Communications Decency Act of 1996 (CDA), 47 U.S.C.S. § 223, **presents a great threat of censoring speech that, in fact, falls**

---

<sup>61</sup> 521 U.S. 844 (1997).

**outside the statute's scope. Given the vague contours of the coverage of the statute, it unquestionably silences some speakers whose messages would be entitled to constitutional protection.** That danger provides further reason for insisting that the statute not be overly broad. **The CDA's burden on protected speech cannot be justified if it could be avoided by a more carefully drafted statute.** (Emphasis ours)

Libel in the cyberspace can of course stain a person's image with just one click of the mouse. Scurrilous statements can spread and travel fast across the globe like bad news. Moreover, cyberlibel often goes hand in hand with cyberbullying that oppresses the victim, his relatives, and friends, evoking from mild to disastrous reactions. Still, a governmental purpose, which seeks to regulate the use of this cyberspace communication technology to protect a person's reputation and peace of mind, cannot adopt means that will unnecessarily and broadly sweep, invading the area of protected freedoms.<sup>62</sup>

If such means are adopted, self-inhibition borne of fear of what sinister predicaments await internet users will suppress otherwise robust discussion of public issues. Democracy will be threatened and with it, all liberties. Penal laws should provide reasonably clear guidelines for law enforcement officials and triers of facts to prevent arbitrary and discriminatory enforcement.<sup>63</sup> The terms "aiding or abetting" constitute broad sweep that generates chilling effect on those who express themselves through cyberspace posts, comments, and other messages.<sup>64</sup> Hence, Section 5 of the cybercrime law that punishes "aiding or abetting" libel on the cyberspace is a nullity.

When a penal statute encroaches upon the freedom of speech, a facial challenge grounded on the void-for-vagueness doctrine is acceptable. The inapplicability of the doctrine must be carefully delineated. As Justice Antonio T. Carpio explained in his dissent in *Romualdez v. Commission on Elections*,<sup>65</sup> "we must view these statements of the Court on the inapplicability of the overbreadth and vagueness doctrines to penal statutes as appropriate only insofar as these doctrines are used to mount 'facial' challenges to penal statutes not involving free speech."

In an "as applied" challenge, the petitioner who claims a violation of his constitutional right can raise any constitutional ground – absence of due process, lack of fair notice, lack of ascertainable standards, overbreadth, or vagueness. Here, one can challenge the constitutionality of a statute only if he asserts a violation of his own rights. It prohibits one from assailing the constitutionality of the statute based solely on the violation of the rights of

---

<sup>62</sup> *Griswold v. Connecticut*, 381 U.S. 479 (1965).

<sup>63</sup> G.R. No. 203378 (*Adonis*), First AMENDED PETITION, pp. 35-36.

<sup>64</sup> *Supra* note 55, at 33.

<sup>65</sup> 576 Phil. 357 (2008).

third persons not before the court. This rule is also known as the prohibition against third-party standing.<sup>66</sup>

But this rule admits of exceptions. A petitioner may for instance mount a “facial” challenge to the constitutionality of a statute even if he claims no violation of his own rights under the assailed statute where it involves free speech on grounds of overbreadth or vagueness of the statute. The rationale for this exception is to counter the “chilling effect” on protected speech that comes from statutes violating free speech. A person who does not know whether his speech constitutes a crime under an overbroad or vague law may simply restrain himself from speaking in order to avoid being charged of a crime. The overbroad or vague law thus chills him into silence.<sup>67</sup>

As already stated, the cyberspace is an incomparable, pervasive medium of communication. It is inevitable that any government threat of punishment regarding certain uses of the medium creates a chilling effect on the constitutionally-protected freedom of expression of the great masses that use it. In this case, the particularly complex web of interaction on social media websites would give law enforcers such latitude that they could arbitrarily or selectively enforce the law.

Who is to decide when to prosecute persons who boost the visibility of a posting on the internet by liking it? Netizens are not given “fair notice” or warning as to what is criminal conduct and what is lawful conduct. When a case is filed, how will the court ascertain whether or not one netizen’s comment aided and abetted a cybercrime while another comment did not?

Of course, if the “Comment” does not merely react to the original posting but creates an altogether new defamatory story against Armand like “He beats his wife and children,” then that should be considered an original posting published on the internet. Both the penal code and the cybercrime law clearly punish authors of defamatory publications. Make no mistake, libel destroys reputations that society values. Allowed to cascade in the internet, it will destroy relationships and, under certain circumstances, will generate enmity and tension between social or economic groups, races, or religions, exacerbating existing tension in their relationships.

In regard to the crime that targets child pornography, when “Google procures, stores, and indexes child pornography and facilitates the completion of transactions involving the dissemination of child pornography,” does this make Google and its users aiders and abettors in the commission of child pornography crimes?<sup>68</sup> Byars highlights a feature in

---

<sup>66</sup> Id.

<sup>67</sup> Id.

<sup>68</sup> A contention found in Bruce Byars, Timothy O’Keefe, and Thomas Clement “Google, Inc.: Procurer, Possessor, Distributor, Aider and Abettor in Child Pornography,” <http://forumonpublicpolicy.com/archivespring08/byars.pdf> (last accessed May 25, 2013).

the American law on child pornography that the Cybercrimes law lacks—the exemption of a provider or notably a plain user of interactive computer service from civil liability for child pornography as follows:

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider and cannot be held civilly liable for any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene...whether or not such material is constitutionally protected.<sup>69</sup>

When a person replies to a Tweet containing child pornography, he effectively republishes it whether wittingly or unwittingly. Does this make him a willing accomplice to the distribution of child pornography? When a user downloads the Facebook mobile application, the user may give consent to Facebook to access his contact details. In this way, certain information is forwarded to third parties and unsolicited commercial communication could be disseminated on the basis of this information.<sup>70</sup> As the source of this information, is the user aiding the distribution of this communication? The legislature needs to address this clearly to relieve users of annoying fear of possible criminal prosecution.

Section 5 with respect to Section 4(c)(4) is unconstitutional. Its vagueness raises apprehension on the part of internet users because of its obvious chilling effect on the freedom of expression, especially since the crime of aiding or abetting ensnares all the actors in the cyberspace front in a fuzzy way. What is more, as the petitioners point out, formal crimes such as libel are not punishable unless consummated.<sup>71</sup> In the absence of legislation tracing the interaction of netizens and their level of responsibility such as in other countries, Section 5, in relation to Section 4(c)(4) on Libel, Section 4(c)(3) on Unsolicited Commercial Communications, and Section 4(c)(2) on Child Pornography, cannot stand scrutiny.

But the crime of aiding or abetting the commission of cybercrimes under Section 5 should be permitted to apply 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. None of these offenses borders on the exercise of the freedom of expression.

---

<sup>69</sup> Id., citing 47 U.S.C. 230.

<sup>70</sup> Bianca Bosker, Facebook To Share Users' Home Addresses, Phone Numbers With External Sites, [http://www.huffingtonpost.com/2011/02/28/facebook-home-addresses-phone-numbers\\_n\\_829459.html](http://www.huffingtonpost.com/2011/02/28/facebook-home-addresses-phone-numbers_n_829459.html) (last accessed July 18, 2013).

<sup>71</sup> G.R. No. 203440 (*Sta Maria*), MEMORANDUM, p. 14, citing Luis B. Reyes, *The Revised Penal Code: Book 1*, 118 (17<sup>th</sup> ed. 2008).

The crime of willfully attempting to commit any of these offenses is for the same reason not objectionable. A hacker may for instance have done all that is necessary to illegally access another party's computer system but the security employed by the system's lawful owner could frustrate his effort. Another hacker may have gained access to usernames and passwords of others but fail to use these because the system supervisor is alerted.<sup>72</sup> If Section 5 that punishes any person who willfully attempts to commit this specific offense is not upheld, the owner of the username and password could not file a complaint against him for attempted hacking. But this is not right. The hacker should not be freed from liability simply because of the vigilance of a lawful owner or his supervisor.

Petitioners of course claim that Section 5 lacks positive limits and could cover the innocent.<sup>73</sup> While this may be true with respect to cybercrimes that tend to sneak past the area of free expression, any attempt to commit the other acts specified in Section 4(a)(1), Section 4(a)(2), Section 4(a)(3), Section 4(a)(4), Section 4(a)(5), Section 4(a)(6), Section 4(b)(1), Section 4(b)(2), Section 4(b)(3), and Section 4(c)(1) as well as the actors aiding and abetting the commission of such acts can be identified with some reasonable certainty through adroit tracking of their works. Absent concrete proof of the same, the innocent will of course be spared.

### **Section 6 of the Cybercrime Law**

Section 6 provides:

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 (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

Section 6 merely makes commission of existing crimes through the internet a qualifying circumstance. As the Solicitor General points out, there exists a substantial distinction between crimes committed through the use of information and communications technology and similar crimes committed using other means. In using the technology in question, the offender often evades identification and is able to reach far more victims or cause greater harm. The distinction, therefore, creates a basis for higher penalties for cybercrimes.

---

<sup>72</sup> Shiresee Bell, Man Pleads Guilty to Attempted USC Website Hacking, Email Accounts, <http://columbia-sc.patch.com/groups/police-and-fire/p/man-pleaded-guilty-to-hacking-usc-website-email-accounts> (last accessed July 18, 2013); Peter Ryan, Hackers target Bureau of Statistics data, <http://www.abc.net.au/news/2013-04-26/abs-targeted-by-hackers/4652758> (last accessed July 18, 2013).

<sup>73</sup> *Supra* note 34, at 32.



### **Section 7 of the Cybercrime Law**

Section 7 provides:

Sec. 7. *Liability under Other Laws.* — A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws.

The Solicitor General points out that Section 7 merely expresses the settled doctrine that a single set of acts may be prosecuted and penalized simultaneously under two laws, a special law and the Revised Penal Code. When two different laws define two crimes, prior jeopardy as to one does not bar prosecution of the other although both offenses arise from the same fact, if each crime involves some important act which is not an essential element of the other.<sup>74</sup> With the exception of the crimes of online libel and online child pornography, the Court would rather leave the determination of the correct application of Section 7 to actual cases.

Online libel is different. There should be no question that if the published material on print, said to be libelous, is again posted online or vice versa, that identical material cannot be the subject of two separate libels. The two offenses, one a violation of Article 353 of the Revised Penal Code and the other a violation of Section 4(c)(4) of R.A. 10175 involve essentially the same elements and are in fact one and the same offense. Indeed, the OSG itself claims that online libel under Section 4(c)(4) is not a new crime but is one already punished under Article 353. Section 4(c)(4) merely establishes the computer system as another means of publication.<sup>75</sup> Charging the offender under both laws would be a blatant violation of the proscription against double jeopardy.<sup>76</sup>

The same is true with child pornography committed online. Section 4(c)(2) merely expands the ACPA's scope so as to include identical activities in cyberspace. As previously discussed, ACPA's definition of child pornography in fact already covers the use of "electronic, mechanical, digital, optical, magnetic or any other means." Thus, charging the offender under both Section 4(c)(2) and ACPA would likewise be tantamount to a violation of the constitutional prohibition against double jeopardy.

### **Section 8 of the Cybercrime Law**

Section 8 provides:

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

<sup>74</sup> Supra note 51, at 49, citing *People v. Doriquez*, 133 Phil. 295 (1968).

<sup>75</sup> Office of the Solicitor General, MEMORANDUM, p. 49.

<sup>76</sup> Section 21, Article III, 1987 CONSTITUTION: "No person shall be twice put in jeopardy of punishment for the same offense. If an act is punished by a law and an ordinance, conviction or acquittal under either shall constitute a bar to another prosecution for the same act."

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

Any person found guilty of the punishable act under Section 4(a)(5) shall be punished with imprisonment of *prision mayor* or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both.

If punishable acts in Section 4(a) are committed against critical infrastructure, the penalty of *reclusion temporal* or a fine of at least Five hundred thousand pesos (PhP500,000.00) up to maximum amount commensurate to the damage incurred or both, shall be imposed.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(1) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos (PhP200,000.00) but not exceeding One million pesos (PhP1,000,000.00) or both.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(2) of this Act shall be punished with the penalties as enumerated in Republic Act No. 9775 or the “Anti-Child Pornography Act of 2009:” *Provided*, That the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775, if committed through a computer system.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(3) shall be punished with imprisonment of *arresto mayor* or a fine of at least Fifty thousand pesos (PhP50,000.00) but not exceeding Two hundred fifty thousand pesos (PhP250,000.00) or both.

Any person found guilty of any of the punishable acts enumerated in Section 5 shall be punished with imprisonment one (1) degree lower than that of the prescribed penalty for the offense or a fine of at least One hundred thousand pesos (PhP100,000.00) but not exceeding Five hundred thousand pesos (PhP500,000.00) or both.

Section 8 provides for the penalties for the following crimes: Sections 4(a) on Offenses Against the Confidentiality, Integrity and Availability of Computer Data and Systems; 4(b) on Computer-related Offenses; 4(a)(5) on Misuse of Devices; when the crime punishable under 4(a) is committed against critical infrastructure; 4(c)(1) on Cybersex; 4(c)(2) on Child Pornography; 4(c)(3) on Unsolicited Commercial Communications; and Section 5 on Aiding or Abetting, and Attempt in the Commission of Cybercrime.

The matter of fixing penalties for the commission of crimes is as a rule a legislative prerogative. Here the legislature prescribed a measure of severe penalties for what it regards as deleterious cybercrimes. They appear proportionate to the evil sought to be punished. The power to determine penalties for offenses is not diluted or improperly wielded simply because at some prior time the act or omission was but an element of another offense or

might just have been connected with another crime.<sup>77</sup> Judges and magistrates can only interpret and apply them and have no authority to modify or revise their range as determined by the legislative department. The courts should not encroach on this prerogative of the lawmaking body.<sup>78</sup>

### **Section 12 of the Cybercrime Law**

Section 12 provides:

Sec. 12. *Real-Time Collection of Traffic Data.* — Law enforcement authorities, with due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system.

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

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

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

The court warrant required under this section shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce and the showing: (1) that there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, or is being committed, or is about to be committed; (2) that there are reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and (3) that there are no other means readily available for obtaining such evidence.

Petitioners assail the grant to law enforcement agencies of the power to collect or record traffic data in real time as tending to curtail civil liberties or provide opportunities for official abuse. They claim that data showing where digital messages come from, what kind they are, and where they are destined need not be incriminating to their senders or recipients before they are to be protected. Petitioners invoke the right of every individual to privacy and to be protected from government snooping into the messages or information that they send to one another.

The first question is whether or not Section 12 has a proper governmental purpose since a law may require the disclosure of matters normally considered private but then only upon showing that such

---

<sup>77</sup> *Baylosis v. Hon. Chavez, Jr.*, 279 Phil. 448 (1991).

<sup>78</sup> *People v. Dela Cruz*, G.R. No. 100386, December 11, 1992, 216 SCRA 476, citing *People v. Millora*, 252 Phil. 105 (1989).

requirement has a rational relation to the purpose of the law,<sup>79</sup> that there is a compelling State interest behind the law, and that the provision itself is narrowly drawn.<sup>80</sup> In assessing regulations affecting privacy rights, courts should balance the legitimate concerns of the State against constitutional guarantees.<sup>81</sup>

Undoubtedly, the State has a compelling interest in enacting the cybercrime law for there is a need to put order to the tremendous activities in cyberspace for public good.<sup>82</sup> To do this, it is within the realm of reason that the government should be able to monitor traffic data to enhance its ability to combat all sorts of cybercrimes.

Chapter IV of the cybercrime law, of which the collection or recording of traffic data is a part, aims to provide law enforcement authorities with the power they need for spotting, preventing, and investigating crimes committed in cyberspace. Crime-fighting is a state business. Indeed, as Chief Justice Sereno points out, the Budapest Convention on Cybercrimes requires signatory countries to adopt legislative measures to empower state authorities to collect or record “traffic data, in real time, associated with specified communications.”<sup>83</sup> And this is precisely what Section 12 does. It empowers law enforcement agencies in this country to collect or record such data.

But is not evidence of yesterday’s traffic data, like the scene of the crime after it has been committed, adequate for fighting cybercrimes and, therefore, real-time data is superfluous for that purpose? Evidently, it is not. Those who commit the crimes of accessing a computer system without right,<sup>84</sup> transmitting viruses,<sup>85</sup> lasciviously exhibiting sexual organs or sexual activity for favor or consideration;<sup>86</sup> and producing child pornography<sup>87</sup> could easily evade detection and prosecution by simply moving the physical location of their computers or laptops from day to day. In this digital age, the wicked can commit cybercrimes from virtually anywhere: from internet

---

<sup>79</sup> Supra note 14, at 436-437.

<sup>80</sup> *Ople v. Torres*, 354 Phil. 948, 974-975 (1998).

<sup>81</sup> *In the Matter of the Petition for Habeas Corpus of Capt. Alejano v. Gen. Cabuay*, 505 Phil. 298, 322 (2005); *Gamboa v. Chan*, G.R. No. 193636, July 24, 2012, 677 SCRA 385.

<sup>82</sup> SEC. 2. *Declaration of Policy*. — The State recognizes the vital role of information and communications industries such as content production, telecommunications, broadcasting electronic commerce, and data processing, in the nation’s overall social and economic development. The State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology (ICT) to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts. In this light, the State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.

<sup>83</sup> Convention on Cybercrime, Art. 20, *opened for signature November 23, 2001*, ETS 185.

<sup>84</sup> Cybercrime Law, Section 4(a)(1),.

<sup>85</sup> *Id.*, Section 4(a)(3)

<sup>86</sup> *Id.*, Section 4(c)(1)

<sup>87</sup> *Id.*, Section 4(c)(2)

cafés, from kindred places that provide free internet services, and from unregistered mobile internet connectors. Criminals using cellphones under pre-paid arrangements and with unregistered SIM cards do not have listed addresses and can neither be located nor identified. There are many ways the cyber criminals can quickly erase their tracks. Those who peddle child pornography could use relays of computers to mislead law enforcement authorities regarding their places of operations. Evidently, it is only real-time traffic data collection or recording and a subsequent recourse to court-issued search and seizure warrant that can succeed in ferreting them out.

Petitioners of course point out that the provisions of Section 12 are too broad and do not provide ample safeguards against crossing legal boundaries and invading the people's right to privacy. The concern is understandable. Indeed, the Court recognizes in *Morfe v. Mutuc*<sup>88</sup> that certain constitutional guarantees work together to create zones of privacy wherein governmental powers may not intrude, and that there exists an independent constitutional right of privacy. Such right to be left alone has been regarded as the beginning of all freedoms.<sup>89</sup>

But that right is not unqualified. In *Whalen v. Roe*,<sup>90</sup> the United States Supreme Court classified privacy into two categories: decisional privacy and informational privacy. Decisional privacy involves the right to independence in making certain important decisions, while informational privacy refers to the interest in avoiding disclosure of personal matters. It is the latter right—the right to informational privacy—that those who oppose government collection or recording of traffic data in real-time seek to protect.

Informational privacy has two aspects: the right not to have private information disclosed, and the right to live freely without surveillance and intrusion.<sup>91</sup> In determining whether or not a matter is entitled to the right to privacy, this Court has laid down a two-fold test. The first is a subjective test, where one claiming the right must have an actual or legitimate expectation of privacy over a certain matter. The second is an objective test, where his or her expectation of privacy must be one society is prepared to accept as objectively reasonable.<sup>92</sup>

Since the validity of the cybercrime law is being challenged, not in relation to its application to a particular person or group, petitioners' challenge to Section 12 applies to all information and communications technology (ICT) users, meaning the large segment of the population who use all sorts of electronic devices to communicate with one another. Consequently, the expectation of privacy is to be measured from the general

---

<sup>88</sup> Supra note 14.

<sup>89</sup> Id. at 433-437.

<sup>90</sup> 429 U.S. 589 (1977).

<sup>91</sup> Id. at 599.

<sup>92</sup> Supra note 13, at 206.

public's point of view. Without reasonable expectation of privacy, the right to it would have no basis in fact.

As the Solicitor General points out, an ordinary ICT user who courses his communication through a service provider, must of necessity disclose to the latter, a third person, the traffic data needed for connecting him to the recipient ICT user. For example, an ICT user who writes a text message intended for another ICT user must furnish his service provider with his cellphone number and the cellphone number of his recipient, accompanying the message sent. It is this information that creates the traffic data. Transmitting communications is akin to putting a letter in an envelope properly addressed, sealing it closed, and sending it through the postal service. Those who post letters have no expectations that no one will read the information appearing outside the envelope.

Computer data—messages of all kinds—travel across the internet in packets and in a way that may be likened to parcels of letters or things that are sent through the posts. When data is sent from any one source, the content is broken up into packets and around each of these packets is a wrapper or header. This header contains the traffic data: information that tells computers where the packet originated, what kind of data is in the packet (SMS, voice call, video, internet chat messages, email, online browsing data, etc.), where the packet is going, and how the packet fits together with other packets.<sup>93</sup> The difference is that traffic data sent through the internet at times across the ocean do not disclose the actual names and addresses (residential or office) of the sender and the recipient, only their coded internet protocol (IP) addresses. The packets travel from one computer system to another where their contents are pieced back together. Section 12 does not permit law enforcement authorities to look into the contents of the messages and uncover the identities of the sender and the recipient.

For example, when one calls to speak to another through his cellphone, the service provider's communication's system will put his voice message into packets and send them to the other person's cellphone where they are refitted together and heard. The latter's spoken reply is sent to the caller in the same way. To be connected by the service provider, the sender reveals his cellphone number to the service provider when he puts his call through. He also reveals the cellphone number to the person he calls. The other ways of communicating electronically follow the same basic pattern.

In *Smith v. Maryland*,<sup>94</sup> cited by the Solicitor General, the United States Supreme Court reasoned that telephone users in the '70s must realize that they necessarily convey phone numbers to the telephone company in order to complete a call. That Court ruled that even if there is an expectation

---

<sup>93</sup> Jonathan Strickland, How IP Convergence Works, <http://computer.howstuffworks.com/ip-convergence2.htm> (last accessed May 10, 2013).

<sup>94</sup> 442 U.S. 735 (1979).

that phone numbers one dials should remain private, such expectation is not one that society is prepared to recognize as reasonable.

In much the same way, ICT users must know that they cannot communicate or exchange data with one another over cyberspace except through some service providers to whom they must submit certain traffic data that are needed for a successful cyberspace communication. The conveyance of this data takes them out of the private sphere, making the expectation to privacy in regard to them an expectation that society is not prepared to recognize as reasonable.

The Court, however, agrees with Justices Carpio and Brion that when seemingly random bits of traffic data are gathered in bulk, pooled together, and analyzed, they reveal patterns of activities which can then be used to create profiles of the persons under surveillance. With enough traffic data, analysts may be able to determine a person's close associations, religious views, political affiliations, even sexual preferences. Such information is likely beyond what the public may expect to be disclosed, and clearly falls within matters protected by the right to privacy. But has the procedure that Section 12 of the law provides been drawn narrowly enough to protect individual rights?

Section 12 empowers law enforcement authorities, "with due cause," to collect or record by technical or electronic means traffic data in real-time. Petitioners point out that the phrase "due cause" has no precedent in law or jurisprudence and that whether there is due cause or not is left to the discretion of the police. Replying to this, the Solicitor General asserts that Congress is not required to define the meaning of every word it uses in drafting the law.

Indeed, courts are able to save vague provisions of law through statutory construction. But the cybercrime law, dealing with a novel situation, fails to hint at the meaning it intends for the phrase "due cause." The Solicitor General suggests that "due cause" should mean "just reason or motive" and "adherence to a lawful procedure." But the Court cannot draw this meaning since Section 12 does not even bother to relate the collection of data to the probable commission of a particular crime. It just says, "with due cause," thus justifying a general gathering of data. It is akin to the use of a general search warrant that the Constitution prohibits.

Due cause is also not descriptive of the purpose for which data collection will be used. Will the law enforcement agencies use the traffic data to identify the perpetrator of a cyber attack? Or will it be used to build up a case against an identified suspect? Can the data be used to prevent cybercrimes from happening?

The authority that Section 12 gives law enforcement agencies is too sweeping and lacks restraint. While it says that traffic data collection should

not disclose identities or content data, such restraint is but an illusion. Admittedly, nothing can prevent law enforcement agencies holding these data in their hands from looking into the identity of their sender or receiver and what the data contains. This will unnecessarily expose the citizenry to leaked information or, worse, to extortion from certain bad elements in these agencies.

Section 12, of course, limits the collection of traffic data to those “associated with specified communications.” But this supposed limitation is no limitation at all since, evidently, it is the law enforcement agencies that would specify the target communications. The power is virtually limitless, enabling law enforcement authorities to engage in “fishing expedition,” choosing whatever specified communication they want. This evidently threatens the right of individuals to privacy.

The Solicitor General points out that Section 12 needs to authorize collection of traffic data “in real time” because it is not possible to get a court warrant that would authorize the search of what is akin to a “moving vehicle.” But warrantless search is associated with a police officer’s determination of probable cause that a crime has been committed, that there is no opportunity for getting a warrant, and that unless the search is immediately carried out, the thing to be searched stands to be removed. These preconditions are not provided in Section 12.

The Solicitor General is honest enough to admit that Section 12 provides minimal protection to internet users and that the procedure envisioned by the law could be better served by providing for more robust safeguards. His bare assurance that law enforcement authorities will not abuse the provisions of Section 12 is of course not enough. The grant of the power to track cyberspace communications in real time and determine their sources and destinations must be narrowly drawn to preclude abuses.<sup>95</sup>

Petitioners also ask that the Court strike down Section 12 for being violative of the void-for-vagueness doctrine and the overbreadth doctrine. These doctrines however, have been consistently held by this Court to apply only to free speech cases. But Section 12 on its own neither regulates nor punishes any type of speech. Therefore, such analysis is unnecessary.

This Court is mindful that advances in technology allow the government and kindred institutions to monitor individuals and place them under surveillance in ways that have previously been impractical or even impossible. “All the forces of a technological age x x x operate to narrow the area of privacy and facilitate intrusions into it. In modern terms, the capacity to maintain and support this enclave of private life marks the difference between a democratic and a totalitarian society.”<sup>96</sup> The Court

---

<sup>95</sup> Supra note 80, at 983.

<sup>96</sup> Supra note 14, at 437, citing Emerson, *Nine Justices in Search of a Doctrine*, 64 Mich. Law Rev. 219, 229 (1965).



must ensure that laws seeking to take advantage of these technologies be written with specificity and definiteness as to ensure respect for the rights that the Constitution guarantees.

**Section 13 of the Cybercrime Law**

Section 13 provides:

Sec. 13. *Preservation of Computer Data.* — The integrity of traffic data and subscriber information relating to communication services provided by a service provider shall be preserved for a minimum period of six (6) months from the date of the transaction. Content data shall be similarly preserved for six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation.

Law enforcement authorities may order a one-time extension for another six (6) months: Provided, That once computer data preserved, transmitted or stored by a service provider is used as evidence in a case, the mere furnishing to such service provider of the transmittal document to the Office of the Prosecutor shall be deemed a notification to preserve the computer data until the termination of the case.

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

Petitioners in G.R. 203391<sup>97</sup> claim that Section 13 constitutes an undue deprivation of the right to property. They liken the data preservation order that law enforcement authorities are to issue as a form of garnishment of personal property in civil forfeiture proceedings. Such order prevents internet users from accessing and disposing of traffic data that essentially belong to them.

No doubt, the contents of materials sent or received through the internet belong to their authors or recipients and are to be considered private communications. But it is not clear that a service provider has an obligation to indefinitely keep a copy of the same as they pass its system for the benefit of users. By virtue of Section 13, however, the law now requires service providers to keep traffic data and subscriber information relating to communication services for at least six months from the date of the transaction and those relating to content data for at least six months from receipt of the order for their preservation.

Actually, the user ought to have kept a copy of that data when it crossed his computer if he was so minded. The service provider has never assumed responsibility for their loss or deletion while in its keep.

At any rate, as the Solicitor General correctly points out, the data that service providers preserve on orders of law enforcement authorities are not made inaccessible to users by reason of the issuance of such orders. The

---

<sup>97</sup> G.R. No. 203391 (*Palatino v. Ochoa*).

process of preserving data will not unduly hamper the normal transmission or use of the same.

### **Section 14 of the Cybercrime Law**

Section 14 provides:

Sec. 14. *Disclosure of Computer Data.* — Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.

The process envisioned in Section 14 is being likened to the issuance of a subpoena. Petitioners' objection is that the issuance of subpoenas is a judicial function. But it is well-settled that the power to issue subpoenas is not exclusively a judicial function. Executive agencies have the power to issue subpoena as an adjunct of their investigatory powers.<sup>98</sup>

Besides, what Section 14 envisions is merely the enforcement of a duly issued court warrant, a function usually lodged in the hands of law enforcers to enable them to carry out their executive functions. The prescribed procedure for disclosure would not constitute an unlawful search or seizure nor would it violate the privacy of communications and correspondence. Disclosure can be made only after judicial intervention.

### **Section 15 of the Cybercrime Law**

Section 15 provides:

Sec. 15. *Search, Seizure and Examination of Computer Data.* — Where a search and seizure warrant is properly issued, the law enforcement authorities shall likewise have the following powers and duties.

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

- (a) To secure a computer system or a computer data storage medium;
- (b) To make and retain a copy of those computer data secured;
- (c) To maintain the integrity of the relevant stored computer data;

---

<sup>98</sup> *Biraogo v. Philippine Truth Commission*, G.R. Nos. 192935 and 193036, December 7, 2010, 637 SCRA 78, 143; ADMINISTRATIVE CODE of 1987, Book I, Chapter 9, Section 37, and Book VII, Chapter 1, Section 13.

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

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

Pursuant thereof, the law enforcement authorities may order any person who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the search, seizure and examination.

Law enforcement authorities may request for an extension of time to complete the examination of the computer data storage medium and to make a return thereon but in no case for a period longer than thirty (30) days from date of approval by the court.

Petitioners challenge Section 15 on the assumption that it will supplant established search and seizure procedures. On its face, however, Section 15 merely enumerates the duties of law enforcement authorities that would ensure the proper collection, preservation, and use of computer system or data that have been seized by virtue of a court warrant. The exercise of these duties do not pose any threat on the rights of the person from whom they were taken. Section 15 does not appear to supersede existing search and seizure rules but merely supplements them.

### **Section 17 of the Cybercrime Law**

Section 17 provides:

*Sec. 17. Destruction of Computer Data.* — Upon expiration of the periods as provided in Sections 13 and 15, service providers and law enforcement authorities, as the case may be, shall immediately and completely destroy the computer data subject of a preservation and examination.

Section 17 would have the computer data, previous subject of preservation or examination, destroyed or deleted upon the lapse of the prescribed period. The Solicitor General justifies this as necessary to clear up the service provider's storage systems and prevent overload. It would also ensure that investigations are quickly concluded.

Petitioners claim that such destruction of computer data subject of previous preservation or examination violates the user's right against deprivation of property without due process of law. But, as already stated, it is unclear that the user has a demandable right to require the service provider to have that copy of the data saved indefinitely for him in its storage system. If he wanted them preserved, he should have saved them in his computer when he generated the data or received it. He could also request the service provider for a copy before it is deleted.

**Section 19 of the Cybercrime Law**

Section 19 empowers the Department of Justice to restrict or block access to computer data:

*Sec. 19. Restricting or Blocking Access to Computer Data.—*  
When a computer data is prima facie found to be in violation of the provisions of this Act, the DOJ shall issue an order to restrict or block access to such computer data.

Petitioners contest Section 19 in that it stifles freedom of expression and violates the right against unreasonable searches and seizures. The Solicitor General concedes that this provision may be unconstitutional. But since laws enjoy a presumption of constitutionality, the Court must satisfy itself that Section 19 indeed violates the freedom and right mentioned.

Computer data<sup>99</sup> may refer to entire programs or lines of code, including malware, as well as files that contain texts, images, audio, or video recordings. Without having to go into a lengthy discussion of property rights in the digital space, it is indisputable that computer data, produced or created by their writers or authors may constitute personal property. Consequently, they are protected from unreasonable searches and seizures, whether while stored in their personal computers or in the service provider's systems.

Section 2, Article III of the 1987 Constitution provides that the right to be secure in one's papers and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable. Further, it states that no search warrant shall issue except upon probable cause to be determined personally by the judge. Here, the Government, in effect, seizes and places the computer data under its control and disposition without a warrant. The Department of Justice order cannot substitute for judicial search warrant.

The content of the computer data can also constitute speech. In such a case, Section 19 operates as a restriction on the freedom of expression over cyberspace. Certainly not all forms of speech are protected. Legislature may, within constitutional bounds, declare certain kinds of expression as illegal. But for an executive officer to seize content alleged to be unprotected without any judicial warrant, it is not enough for him to be of

---

<sup>99</sup> Computer data is defined by R.A. 10175 as follows:

“SEC. 3. Definition of Terms. x x x

x x x x

(e) Computer data refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system including a program suitable to cause a computer system to perform a function and includes electronic documents and/or electronic data messages whether stored in local computer systems or online.”

the opinion that such content violates some law, for to do so would make him judge, jury, and executioner all rolled into one.<sup>100</sup>

Not only does Section 19 preclude any judicial intervention, but it also disregards jurisprudential guidelines established to determine the validity of restrictions on speech. Restraints on free speech are generally evaluated on one of or a combination of three tests: the dangerous tendency doctrine, the balancing of interest test, and the clear and present danger rule.<sup>101</sup> Section 19, however, merely requires that the data to be blocked be found *prima facie* in violation of any provision of the cybercrime law. Taking Section 6 into consideration, this can actually be made to apply in relation to any penal provision. It does not take into consideration any of the three tests mentioned above.

The Court is therefore compelled to strike down Section 19 for being violative of the constitutional guarantees to freedom of expression and against unreasonable searches and seizures.

### **Section 20 of the Cybercrime Law**

Section 20 provides:

Sec. 20. *Noncompliance.* — Failure to comply with the provisions of Chapter IV hereof specifically the orders from law enforcement authorities shall be punished as a violation of Presidential Decree No. 1829 with imprisonment of prision correccional in its maximum period or a fine of One hundred thousand pesos (Php100,000.00) or both, for each and every noncompliance with an order issued by law enforcement authorities.

Petitioners challenge Section 20, alleging that it is a bill of attainder. The argument is that the mere failure to comply constitutes a legislative finding of guilt, without regard to situations where non-compliance would be reasonable or valid.

But since the non-compliance would be punished as a violation of Presidential Decree (P.D.) 1829,<sup>102</sup> Section 20 necessarily incorporates elements of the offense which are defined therein. If Congress had intended for Section 20 to constitute an offense in and of itself, it would not have had to make reference to any other statute or provision.

P.D. 1829 states:

Section 1. The penalty of prision correccional in its maximum period, or a fine ranging from 1,000 to 6,000 pesos, or both, shall be imposed upon any person who knowingly or willfully obstructs, impedes, frustrates or delays the apprehension of suspects and the investigation and

<sup>100</sup> *Pita v. Court of Appeals*, supra note 30, at 151.

<sup>101</sup> *Chavez v. Gonzales*, 569 Phil. 155 (2008).

<sup>102</sup> Entitled PENALIZING OBSTRUCTION OF APPREHENSION AND PROSECUTION OF CRIMINAL OFFENDERS.

prosecution of criminal cases by committing any of the following acts:  
x x x.

Thus, the act of non-compliance, for it to be punishable, must still be done “knowingly or willfully.” There must still be a judicial determination of guilt, during which, as the Solicitor General assumes, defense and justifications for non-compliance may be raised. Thus, Section 20 is valid insofar as it applies to the provisions of Chapter IV which are not struck down by the Court.

**Sections 24 and 26(a) of the Cybercrime Law**

Sections 24 and 26(a) provide:

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

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

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

Petitioners mainly contend that Congress invalidly delegated its power when it gave the Cybercrime Investigation and Coordinating Center (CICC) the power to formulate a national cybersecurity plan without any sufficient standards or parameters for it to follow.

In order to determine whether there is undue delegation of legislative power, the Court has adopted two tests: the completeness test and the sufficient standard test. Under the first test, the law must be complete in all its terms and conditions when it leaves the legislature such that when it reaches the delegate, the only thing he will have to do is to enforce it. The second test mandates adequate guidelines or limitations in the law to determine the boundaries of the delegate’s authority and prevent the delegation from running riot.<sup>103</sup>

Here, the cybercrime law is complete in itself when it directed the CICC to formulate and implement a national cybersecurity plan. Also, contrary to the position of the petitioners, the law gave sufficient standards for the CICC to follow when it provided a definition of cybersecurity.

---

<sup>103</sup> *Gerochi v. Department of Energy*, 554 Phil. 563 (2007).

Cybersecurity refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect cyber environment and organization and user's assets.<sup>104</sup> This definition serves as the parameters within which CICC should work in formulating the cybersecurity plan.

Further, the formulation of the cybersecurity plan is consistent with the policy of the law to "prevent and combat such [cyber] 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."<sup>105</sup> This policy is clearly adopted in the interest of law and order, which has been considered as sufficient standard.<sup>106</sup> Hence, Sections 24 and 26(a) are likewise valid.

**WHEREFORE, the Court DECLARES:**

1. **VOID** for being **UNCONSTITUTIONAL**:
  - a. Section 4(c)(3) of Republic Act 10175 that penalizes posting of unsolicited commercial communications;
  - b. Section 12 that authorizes the collection or recording of traffic data in real-time; and
  - c. Section 19 of the same Act that authorizes the Department of Justice to restrict or block access to suspected Computer Data.
  
2. **VALID** and **CONSTITUTIONAL**:
  - a. Section 4(a)(1) that penalizes accessing a computer system without right;
  - b. Section 4(a)(3) that penalizes data interference, including transmission of viruses;
  - c. Section 4(a)(6) that penalizes cyber-squatting or acquiring domain name over the internet in bad faith to the prejudice of others;
  - d. Section 4(b)(3) that penalizes identity theft or the use or misuse of identifying information belonging to another;
  - e. Section 4(c)(1) that penalizes cybersex or the lascivious exhibition of sexual organs or sexual activity for favor or consideration;
  - f. Section 4(c)(2) that penalizes the production of child pornography;
  - g. Section 6 that imposes penalties one degree higher when crimes defined under the Revised Penal Code are committed with the use of information and communications technologies;
  - h. Section 8 that prescribes the penalties for cybercrimes;

---

<sup>104</sup> REPUBLIC ACT 10175, Section 3(k).

<sup>105</sup> Supra note 94.

<sup>106</sup> *Gerochi v. Department of Energy*, supra note 103, at 586, citing *Rubi v. Provincial Board of Mindoro*, 39 Phil. 660 (1919).

- i. Section 13 that permits law enforcement authorities to require service providers to preserve traffic data and subscriber information as well as specified content data for six months;
- j. Section 14 that authorizes the disclosure of computer data under a court-issued warrant;
- k. Section 15 that authorizes the search, seizure, and examination of computer data under a court-issued warrant;
- l. Section 17 that authorizes the destruction of previously preserved computer data after the expiration of the prescribed holding periods;
- m. Section 20 that penalizes obstruction of justice in relation to cybercrime investigations;
- n. Section 24 that establishes a Cybercrime Investigation and Coordinating Center (CICC);
- o. Section 26(a) that defines the CICC's Powers and Functions; and
- p. Articles 353, 354, 361, and 362 of the Revised Penal Code that penalizes libel.

Further, the Court **DECLARES**:

1. Section 4(c)(4) that penalizes online libel as **VALID** and **CONSTITUTIONAL** with respect to the original author of the post; but **VOID** and **UNCONSTITUTIONAL** with respect to others who simply receive the post and react to it; and

2. Section 5 that penalizes aiding or abetting and attempt in the commission of cybercrimes as **VALID** and **CONSTITUTIONAL** 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** and **UNCONSTITUTIONAL** with respect to Sections 4(c)(2) on Child Pornography, 4(c)(3) on Unsolicited Commercial Communications, and 4(c)(4) on online Libel.

Lastly, the Court **RESOLVES** to **LEAVE THE DETERMINATION** of the correct application of Section 7 that authorizes prosecution of the offender under both the Revised Penal Code and Republic Act 10175 to actual cases, **WITH THE EXCEPTION** of the crimes of:


1. Online libel as to which, charging the offender under both Section 4(c)(4) of Republic Act 10175 and Article 353 of the Revised Penal Code constitutes a violation of the proscription against double jeopardy; as well as



2. Child pornography committed online as to which, charging the offender under both Section 4(c)(2) of Republic Act 10175 and Republic Act 9775 or the Anti-Child Pornography Act of 2009 also constitutes a violation of the same proscription,

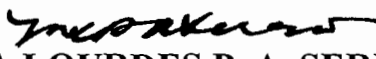
and, in respect to these, is **VOID** and **UNCONSTITUTIONAL**.

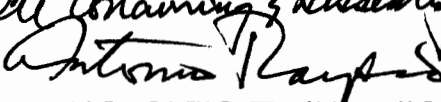
**SO ORDERED.**

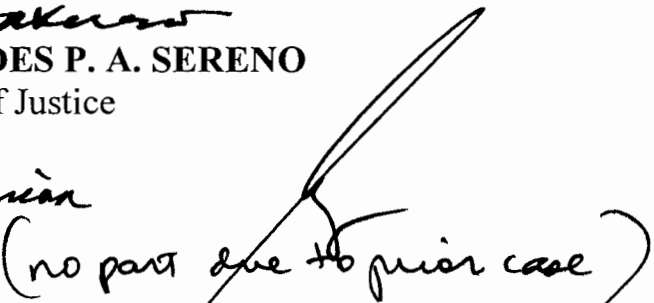
  
**ROBERTO A. ABAD**  
Associate Justice

**WE CONCUR:**

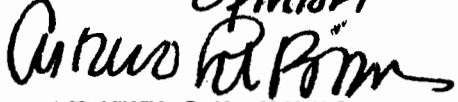
*See Concurring & Dissenting Opinion*

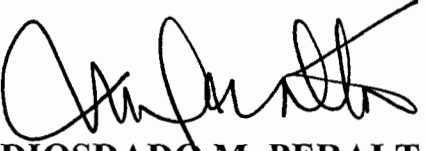
  
**MARIA LOURDES P. A. SERENO**  
Chief Justice

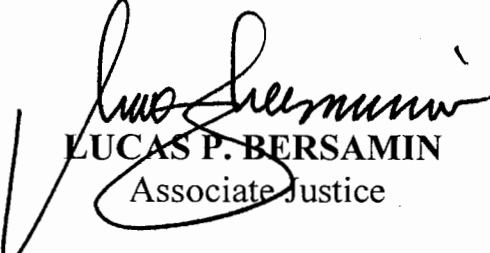
*See Concurring & Dissenting Opinion*  
  
**ANTONIO T. CARPIO**  
Associate Justice

*(no part due to prior case)*  
  
**PRESBITERO J. VELASCO, JR.**  
Associate Justice

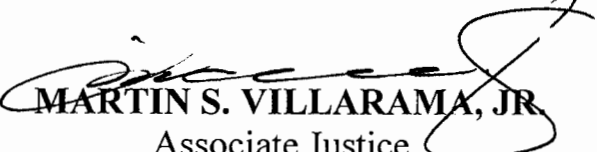
*Teresito Leonardo de Castro*  
**TERESITA J. LEONARDO-DE CASTRO**  
Associate Justice


*See Separate Concurring Opinion*  
  
**ARTURO D. BRION**  
Associate Justice


  
**DIOSDADO M. PERALTA**  
Associate Justice


  
**LUCAS P. BERSAMIN**  
Associate Justice

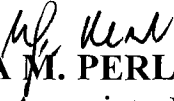
  
**MARIANO C. DEL CASTILLO**  
Associate Justice

  
**MARTIN S. VILLARAMA, JR.**  
Associate Justice

  
**JOSE PORTUGAL PEREZ**  
 Associate Justice

*I join Justice Brion in all his positions*  
  
**JOSE CATRAL MENDOZA**  
 Associate Justice


  
**BIENVENIDO L. REYES**  
 Associate Justice

*No Part*  
  
**ESTELA M. PERLAS-BERNABE**  
 Associate Justice

*See separate dissenting and concurring opinion*  
  
**MARVIC MARIO VICTOR F. LEONEN**  
 Associate Justice

**CERTIFICATION**

Pursuant to Section 13, Article VIII of the Constitution, it is hereby certified that the conclusions in the above Decision had been reached in consultation before the case was assigned to the writer of the opinion of the Court.

  
**MARIA LOURDES P. A. SERENO**  
 Chief Justice