

REPUBLIC OF THE PHILIPPINES  
SUPREME COURT  
MANILA

**RECEIVED**

by: DISINI & DISINI  
17 DEC 2012

*Angie*

EN BANC

LOUIS "BAROK" C. BIRAOGO,  
Petitioner,

- versus -

G.R. No. 203299

NATIONAL BUREAU OF INVESTIGATION,  
et al.,

Respondents.

X-----X

ALAB NG MAMAMAHAYAG (ALAM),  
et al.,

Petitioners,

- versus -

G.R. No. 203306

OFFICE OF THE PRESIDENT, etc., et al.,  
Respondents.

X-----X

JOSE JESUS M. DISINI, JR., et al.,  
Petitioners,

- versus -

G.R. No. 203335

THE SECRETARY OF JUSTICE, et al.,  
Respondents.

X-----X

SENATOR TEOFISTO DL GUINGONA, III,  
Petitioner,

- versus -

G.R. No. 203359

THE EXECUTIVE SECRETARY, et al.,  
Respondents.

X-----X

ALEXANDER ADONIS, et al.,  
Petitioners,

- versus -

G.R. No. 203378

THE EXECUTIVE SECRETARY, et al.,  
Respondents.

X-----X

HON. RAYMOND V. PALATINO,  
et al.

Petitioners,

- versus -

G.R. No. 203391

HON. PAQUITO N. OCHOA, JR., etc., et al.,  
Respondents.

X-----X

Biraogo, et al. vs. NBI, et al.  
G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

Bagong Alyansang Makabayan Secretary  
General RENATO M. REYES, JR. et al.,  
Petitioners,

- versus -

G.R. No. 203407

BENIGNO SIMEON C. AQUINO III, etc.,  
et al.,  
Respondents.

x-----x

MELENCIO S. STA. MARIA, et al.,  
Petitioners,

- versus -

G.R. No. 203440

HON. PAQUITO OCHOA, etc, et al.,  
Respondents.

x-----x

NATIONAL UNION OF JOURNALISTS OF  
THE PHILIPPINES, et al.,  
Petitioners,

- versus -

G.R. No. 203453

THE EXECUTIVE SECRETARY,  
et al.,  
Respondents.

x-----x

PAUL CORNELIUS T. CASTILLO, et al.,  
Petitioners,

- versus -

G.R. No. 203454

THE HON. SECRETARY OF JUSTICE,  
et al.,  
Respondents.

x-----x

ANTHONY IAN M. CRUZ, et al.,  
Petitioners,

- versus -

G.R. No. 203469

HIS EXCELLENCY BENIGNO S. AQUINO III,  
etc., et al.,  
Respondents.

x-----x

PHILIPPINE BAR ASSOCIATION, INC.,  
Petitioner,

- versus -

G.R. No. 203501

HIS EXCELLENCY BENIGNO S. AQUINO III,  
etc., et al.,  
Respondents.

x-----x

Biraogo, et al. vs. NBI, et al.  
G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

Bayan Muna Representative NERI J.  
COLMENARES,

Petitioner,

- versus -

G.R. No. 203509

THE EXECUTIVE SECRETARY PAQUITO  
OCHOA, JR.,

Respondent.

X-----X

NATIONAL PRESS CLUB OF THE  
PHILIPPINES, INC., etc.,

Petitioner,

- versus -

G.R. No. 203515

OFFICE OF THE PRESIDENT, PRESIDENT  
BENIGNO SIMEON AQUINO III, etc., et al.,

Respondents.

X-----X

PHILIPPINE INTERNET FREEDOM  
ALLIANCE, etc., et al.,

Petitioners,

- versus -

G.R. No. 203518

THE EXECUTIVE SECRETARY, et al.,  
Respondents.

X-----X

## CONSOLIDATED COMMENT WITH PARTIAL MANIFESTATION

**RESPONDENTS** and **THE OFFICE OF THE SOLICITOR**

**GENERAL** respectfully aver:

### PREFATORY STATEMENT

Penal laws are enacted to maintain minimum standards of decency, morality and civility in human society.<sup>1</sup>

---

<sup>1</sup> People vs. Siton, 600 SCRA 476, 495 [2009].

**Republic Act No. 10175, otherwise known as the Cyber Crime Prevention Act of 2012** is no different.

The advancement of information technology and communication has made man's vulnerability to cyber threats, cyber attacks and cyber crimes a real concern. Some have realized that actions in the virtual world have real consequences. Others still believe that all problems in the virtual world can be eradicated by pressing the reset button.

Acts penalized as crimes in the real world are also crimes when committed through cyber. This Honorable Court affirmed the conviction of an accused for violation of Section (5)(h) of R.A. No. 9262 "Anti-Violence Against Women and Their Children Act." The accused sent through SMS a picture of a naked woman's body with his former girlfriend's head.<sup>2</sup> Yet, existing law still does not punish many acts committed through the ICT which same acts when committed in the real world, are punished as crimes. There is, thus, an urgent need for the Philippines to enact a law which will address all

---

<sup>2</sup> Ang vs. Court of Appeals, 618 SCRA 592 [2010].

“legitimate concerns about criminal behavior on the internet and the effects of abusive behavior”.<sup>3</sup>

But the cyber world presents another distinct reality: the absence of borders.

Unlike in the real world where the effects of the crime are felt within the territory where it is committed, an offender’s cyber acts in one country can easily and immediately affect persons, natural or otherwise, in other and many countries. This borderless world presents special challenges for law enforcement, and which requires the cooperation of nations.

Thus, States began devising mechanisms to deter cybercrimes so that an orderly and vibrant digital environment can be nurtured, protected, and secured. Truly, extending the rule of law into cyberspace is a critical step to create a trustworthy environment for people and business.<sup>4</sup>

In 2001, the Council of Europe took an important step against cybercrime. It sponsored the *Budapest Convention on*

---

<sup>3</sup> <http://www.gov.ph/2012/10/03/statement-of-the-presidential-spokesperson-on-the-cybercrime-prevention-act-of-2012/> last accessed on October 25, 2012.

<sup>4</sup> Cyber Crime...and Punishment? - Archaic Laws Threaten Global Information, A Report prepared by McConnel International, December 2000.

*Cybercrime ("Convention")* which today is recognized as a model law for many countries and is an important international instrument in the fight against cybercrime.<sup>5</sup> It requires signatories to develop legislation to criminalize attacks against computer data and systems (*i.e.*, illegal access, illegal interception, data interference, system interference and the misuse of data); outlaw child pornography and its production, distribution and possession; and penalize offenses committed by means of computer systems (such as computer related forgery and fraud and infringement of copyright and related rights). The Convention also requires member States to put in place procedural law measures to enable its competent authorities to investigate cybercrime and secure volatile electronic evidence in an efficient manner (including expedited preservation of data, search and seizure of computer systems, interception of communications, etc.) and provides for cooperation between signatory States (including for extradition purposes and law enforcement). The Convention has been signed by 46 States, including the Council of

---

<sup>5</sup> There are thirty-three (33) parties to the *Budapest Convention* which include the member States of the Council of Europe, the United States of America, fourteen (14) signatories which include the member States of the Council of Europe, Canada, Japan and South Africa, and eight (8) states with invitations to accede, *i.e.* Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines and Senegal.

---

Europe's observer states Canada, Japan and the USA, and it came into force in 2004.<sup>6</sup>

In 2008, the Philippines was invited to accede to the Convention. In three years, the Congress produced R. A. No. 10175. But the constitutional challenges, through these fifteen (15) Petitions, made on R. A. No. 10175 stunts the process of accession.

R. A. No. 10175 is meant only to curb and fight the evil of cybercrime, nothing more and nothing less. It criminalizes conduct, not free speech or free expression.

In this Comment, the Office of the Solicitor General vigorously defends the constitutionality of R. A. No. 10175, in its entirety, except only as to Section 19, on restricting or blocking access. With all due respect to the Congress, the OSG submits that Section 19 is constitutionally impermissible, because it permits a form of final restraint on speech without prior judicial determination. As to Section 12, on the real time collection of traffic data, the OSG defends its constitutionality. However, again with all due deference to

---

<sup>6</sup> <http://www.fosigrid.org/europe/council-of-europe> last accessed on October 25, 2012.

Congress, the OSG submits that the Congress may, in its wisdom, consider amending the Section to provide for prior judicial authorization.

## ISSUES

Respondents, for clarity and expediency, consolidated the common or similar issues raised in the separate petitions and segregated the issues unique to each petition. Thus, the issues raised by the fifteen (15) separate petitions may be reduced, as follows:

### PROCEDURAL ISSUES

#### I

**WHETHER OR NOT PETITIONERS HAVE  
LOCUS STANDI TO BRING THE PETITIONS.<sup>7</sup>**

#### II

**WHETHER OR NOT THE ISSUES RAISED ARE  
RIPE FOR ADJUDICATION.<sup>8</sup>**

### SUBSTANTIVE ISSUES

#### III

**WHETHER OR NOT SECTION 4(a)(1) OF  
REPUBLIC ACT NO. 10175 WHICH TREATS  
AS A CYBERCRIME ACCESS TO THE WHOLE  
OR PART OF A COMPUTER SYSTEM  
WITHOUT RIGHT, IS UNCONSTITUTIONAL:**

---

<sup>7</sup> infra at pp. 39-46.

<sup>8</sup> infra at pp. 47-50.



- a. For failure to meet the strict scrutiny standards (PIFA, G.R. No. 203518).<sup>9</sup>

IV

WHETHER OR NOT SECTION 4(a)(3) OF R.A. NO. 10175, WHICH TREATS AS A CYBERCRIME 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, IS UNCONSTITUTIONAL:

- a. For violating the freedom of expression clause under Section 3, Article III of the 1987 Constitution (Reyes, et al., G.R. No. 203407).<sup>10</sup>

V

WHETHER OR NOT SECTION 4(a)(6), WHICH TREATS AS A CYBERCRIME THE ACQUISITION OF A DOMAIN NAME OVER THE INTERNET IN BAD FAITH TO PROFIT, MISLEAD, DESTROY REPUTATION AND DEPRIVE OTHERS FROM REGISTERING THE NAME, IS UNCONSTITUTIONAL:

- a. For violating the equal protection clause under Section 1, Article III of the 1987 Constitution (PIFA, G.R. No. 203518).<sup>11</sup>

VI

WHETHER OR NOT SECTION 4(b)(3) OF R.A. NO. 10175, WHICH TREATS AS A CYBERCRIME THE INTENTIONAL ACQUISITION, USE, MISUSE, TRANSFER, POSSESSION, ALTERATION OR DELETION OF IDENTIFYING INFORMATION BELONGING TO ANOTHER, WHETHER NATURAL OR JURIDICAL, WITHOUT RIGHT, IS UNCONSTITUTIONAL:

---

<sup>9</sup> infra at pp. 51-54.

<sup>10</sup> infra at pp. 54-56.

<sup>11</sup> infra at pp. 57-60.

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

- a. For violating the due process clause under Section 1, Article III of the 1987 Constitution (**Reyes, G.R. No. 203407**);
- b. For violating the right to privacy of communication clause under Section 3 Article III of the 1987 Constitution (**Reyes, G.R. No. 203407**);
- c. For violating the freedom of the press clause under Section 4, Article III of the 1987 Constitution (**Reyes, G.R. No. 203407**).<sup>12</sup>

VII

**WHETHER OR NOT SECTION 4(c)(1) OF R.A. NO. 10175, WHICH TREATS 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, IS UNCONSTITUTIONAL:**

- a. For violating the freedom of expression clause under Section 3, Article III of the 1987 Constitution (**Guingona, G.R. No. 203359; PIFA, G.R. No. 203518**).<sup>13</sup>

VIII

**WHETHER OR NOT SECTION 4(c)(3) OF R.A. NO. 10175, WHICH TREATS AS A CYBERCRIME THE TRANSMISSION OF COMMERCIAL ELECTRONIC COMMUNICATION WITH THE USE OF COMPUTER SYSTEM WHICH SEEK TO ADVERTISE, SELL, OR OFFER FOR SALE PRODUCTS AND SERVICES, IS UNCONSTITUTIONAL:**

---

<sup>12</sup> infra at pp. 61-65.

<sup>13</sup> infra at pp. 66-69.

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

- a. For violating the due process clause under Section 1, Article III of the 1987 Constitution (**Alab, G.R. No. 203306**).
- b. For violating the equal protection clause under Section 1, Article III of the 1987 Constitution (**PIFA, G.R. No. 203518**).<sup>14</sup>

IX

**WHETHER OR NOT SECTION 4(C)(4) OF R.A. NO. 10175, WHICH TREATS AS A CYBERCRIME LIBEL AS DEFINED UNDER ARTICLE 355 OF THE REVISED PENAL CODE WHEN COMMITTED THROUGH A COMPUTER SYSTEM OR ANY OTHER SIMILAR MEANS, IS UNCONSTITUTIONAL:**

- a. For violating the due process clause under Section 1, Article III of the 1987 Constitution (**Biraogo, G.R. No. 203299, Guingona, G.R. No. 203359, Adonis, G.R. No. 203378, Palatino, G.R. No. 203391, Reyes, G.R. No. 203407, Sta. Maria, G.R. No. 203440, Castillo, G.R. No. 203454, Cruz, G.R. No. 203469, PBA, G.R. No. 203501, NPCP, G.R. No. 203515**).
- b. For violating the equal protection clause under Section 1, Article III of the 1987 Constitution (**Guingona, G.R. No. 203359, Sta. Maria, G.R. No. 203440, Castillo, G.R. No. 203454, NPCP, G.R. No. 203515**).
- c. For abridging the constitutional right to free speech, expression and press under Section 4, Article III of the 1987 Constitution (**Biraogo, G.R. No. 203299, Disini, G.R. No. 203335, Adonis, G.R. No. 203378, Sta. Maria, G.R. No. 203440, NUJP, G.R. No. 203453, Cruz, G.R. No. 203469, PBA, G.R. No. 203501, NPCP, G.R. No. 203515**).

---

<sup>14</sup> infra at pp. 70-72.

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

- d. For violating the rule on double jeopardy under Section 21, Article III of the 1987 Constitution (**NPCP, G.R. No. 203515**).
- e. For being a bill of attainder (**NUJP, G.R. No. 203453**).
- f. For being an *ex post facto* law (**PIFA, G.R. No. 203518, PBA, G.R. No. 203501**).<sup>15</sup>
- g. For violating the International Covenant on Civil and Political Rights (ICCPR) (**Adonis, G.R. No. 203378, Reyes, G.R. No. 203407**).

**X**

**WHETHER OR NOT SECTION 5 OF R.A. NO. 10175, DECLARING THE AIDING OR ABETTING IN THE COMMISSION OF CYBERCRIME AND THE ATTEMPT IN ITS COMMISSION AS A CYBERCRIME OFFENSE, IS UNCONSTITUTIONAL:**

- a. For violating the due process clause under Section 1, Article III of the 1987 Constitution (**Reyes, G.R. No. 203407, Sta. Maria, G.R. No. 203440, Cruz, G.R. No. 203469, PBA, G.R. No. 203501, NPCP, G.R. No. 203515**).
- b. For violating the equal protection clause under Section 1, Article III of the 1987 Constitution (**NPCP, G.R. No. 203515**).
- c. For violating the freedom of expression clause under Section 3, Article III of the 1987 Constitution (**NUJP, G.R. No. 203453**).
- d. For violating the rule on double jeopardy under Section 21, Article III of the 1987 Constitution (**NPCP, G.R. No. 203515**).

---

<sup>15</sup> infra at pp. 72-84.

- e. For being a bill of attainder (**NUJP, G.R. No. 203453**).<sup>16</sup>

**XI**

**WHETHER OR NOT SECTION 6 OF R.A. NO. 10175, IMPOSING A PENALTY ONE DEGREE HIGHER FOR CRIMES PENALIZED BY THE REVISED PENAL CODE AND SPECIAL LAWS, IF COMMITTED WITH THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY, IS UNCONSTITUTIONAL:**

- a. For violating the due process clause under Section 1, Article III of the 1987 Constitution (**Guingona, G.R. No. 203359, NUJP, G.R. No. 203453, Cruz, G.R. No. 203469, NPCP, G.R. No. 203515**).
- b. For violating the equal protection clause under Section 1, Article III of the 1987 Constitution (**Guingona, G.R. No. 203359, Adonis, G.R. No. 203378, Sta. Maria, G.R. No. 203440, Cruz, G.R. No. 203469, PBA, G.R. No. 203501, NPCP, G.R. No. 203515**).
- c. For violating the freedom of expression clause under Section 4, Article III of the 1987 Constitution (**NUJP, G.R. No. 203453, Cruz, G.R. No. 203469, NPCP, G.R. No. 203515**).
- d. For violating the rule on Double jeopardy under Section 21, Article III of the 1987 Constitution (**Disini, G.R. No. 203335, Reyes, G.R. No. 203407, Sta. Maria, G.R. No. 203440, NPCP, G.R. No. 203515**).
- e. For being a Bill of attainder (**NUJP, G.R. No. 203453**).
- f. For being incompatible with Article 19, paragraph 3 of the International Covenant on Civil and Political

---

<sup>16</sup> infra at pp. 86-93.

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

Rights on freedom of expression  
(PIFA, G.R. No. 203518).<sup>17</sup>

## XII

**WHETHER OR NOT SECTION 7 OF R.A. NO. 10175, WHICH STATES THAT PROSECUTION UNDER SAID LAW IS WITHOUT PREJUDICE TO ANY LIABILITY FOR VIOLATION OF THE REVISED PENAL CODE OR SPECIALS LAWS, IS UNCONSTITUTIONAL:**

- a. For violating the due process clause under Section 1, Article III of the 1987 Constitution (**NUJP, G.R. No. 203453, Cruz, G.R. No. 203469**).
- b. For violating the equal protection clause under Section 1, Article III of the 1987 Constitution (**Disini, G.R. No. 203335, Sta. Maria, G.R. No. 203440, NUJP, G.R. No. 203453**).
- c. For violating freedom of expression (**NUJP, G.R. No. 203453, Cruz, G.R. No. 203469**).
- d. For violating the rule on double jeopardy under Section 21, Article III of the 1987 Constitution (**Disini, G.R. No. 203335, Guingona, G.R. No. 203359, Adonis, G.R. No. 203378, Reyes, G.R. No. 203407, Sta. Maria, G.R. No. 203440, NUJP, G.R. No. 203453, PBA, G.R. No. 203501**).<sup>18</sup>

## XIII

**WHETHER OR NOT THE PENAL PROVISIONS OF R.A. NO. 10175 ARE UNCONSTITUTIONAL (Biraogo, G.R. No. 203299);<sup>19</sup>**

---

<sup>17</sup> infra at pp. 93-106.

<sup>18</sup> infra at pp. 106-108.

<sup>19</sup> infra at pp. 108-112.

XIV

**WHETHER OR NOT SECTION 12 OF R.A. NO. 10175, WHICH AUTHORIZES LAW ENFORCEMENT AUTHORITIES, BY TECHNICAL OR ELECTRONIC MEANS, AFTER FINDING DUE CAUSE, TO COLLECT OR RECORD TRAFFIC DATA IN REAL-TIME, ASSOCIATED WITH SPECIFIED COMMUNICATION TRANSMITTED BY MEANS OF A COMPUTER SYSTEM, IS UNCONSTITUTIONAL:**

- a. For violating the due process clause under Section 1, Article III of the 1987 Constitution (**Castillo, G.R. No. 203454**).
- b. For violating freedom of speech under Section 3, Article III of the 1987 Constitution (**Biraogo, G.R. No. 203299, Castillo, G.R. No. 203454**).
- c. For being an unlawful search and seizure, under Section 3, Article III of the 1987 Constitution (**Reyes, G.R. No. 203407, NUJP, G.R. No. 203453, Castillo, G.R. No. 203454, Cruz, G.R. No. 203469, PBA, G.R. No. 203501**).
- d. For allowing warrantless electronic surveillance (**NUJP, G.R. No. 203453**).
- e. For violating the right to privacy under Section 3, Article III of the 1987 Constitution (**Reyes, G.R. No. 203407, NUJP, G.R. No. 203453, Castillo, G.R. No. 203454, Cruz, G.R. No. 203469, PBA, G.R. No. 203501**).<sup>20</sup>

XV

**WHETHER OR NOT SECTION 13 OF R.A. NO. 10175 ON PRESERVATION OF DATA, IS UNCONSTITUTIONAL:**

---

<sup>20</sup> infra at pp. 112-136.

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

- a. For violating the due process clause (**Palatino, et al., G.R. No. 203391**).
- b. For violating right to privacy (**PIFA, G.R. No. 203518**),<sup>21</sup>

**XVI**

**WHETHER OR NOT SECTION 14 OF R.A. NO. 10175, WHICH EMPOWERS LAW ENFORCEMENT AUTHORITIES, UPON SECURING A SEARCH WARRANT, TO ISSUE AN ORDER REQUIRING ANY PERSON OR SERVICE PROVIDER TO DISCLOSE OR SUBMIT TRAFFIC DATA WITHIN HIS POSSESSION OR CONTROL, IS UNCONSTITUTIONAL:**

- a. For being an undue delegation of judicial powers to PNP and NBI (**NUJP, et al., G.R. No. 203453**).<sup>22</sup>

**XVII**

**WHETHER OR NOT SECTION 15 OF R.A. NO. 10175, WHICH DEFINES THE POWERS AND DUTIES OF LAW ENFORCEMENT AUTHORITIES IN THE IMPLEMENTATION OF THE SEARCH AND SEIZURE WARRANT, IS UNCONSTITUTIONAL:**

- a. For being an undue delegation of judicial powers to the PNP (**NUJP, et al., G.R. No. 203453**).
- b. For being an unlawful search and seizure (**Palatino, et al., G.R. No. 203391**).<sup>23</sup>

**XVIII**

**WHETHER OR NOT SECTION 17 OF R.A. NO. 10175, WHICH AUTHORIZES SERVICE PROVIDERS AND LAW ENFORCEMENT AUTHORITIES, UPON EXPIRATION OF THE PERIODS UNDER SECTIONS 13 AND 15 TO**

---

<sup>21</sup> infra at pp. 136-141.

<sup>22</sup> infra at pp. 141-143.

<sup>23</sup> infra at pp. 143-147.



**IMMEDIATELY AND COMPLETELY DESTROY  
THE COMPUTER DATA SUBJECT OF A  
PRESERVATION AND EXAMINATION, IS  
UNCONSTITUTIONAL:**

- a. For violating the due process clause under Section 1, Article III of the 1987 Constitution (**Reyes, G.R. No. 203407, Palatino, G.R. No. 203391**).<sup>24</sup>

**XIX**

**WHETHER OR NOT SECTION 19 OF R.A. NO. 10175, WHICH AUTHORIZES THE DEPARTMENT OF JUSTICE TO ISSUE AN ORDER TO RESTRICT OR BLOCK ACCESS TO COMPUTER DATA FOUND *PRIMA FACIE* TO BE IN VIOLATION OF R.A. NO. 10175, IS UNCONSTITUTIONAL:**

- a. For violating the due process clause under Section 1, Article III of the 1987 Constitution (**Disini, G.R. No. 203335, Guingona, G.R. No. 203359, Sta. Maria, G.R. No. 203440, NUJP, G.R. No. 203453, Castillo, G.R. No. 203454, Cruz, G.R. No. 203469, PBA, G.R. No. 203501**).
- b. For constituting an unlawful search and seizure (**Guingona, G.R. No. 203359, Castillo, G.R. No. 203454, Cruz, G.R. No. 203469, NPCP, G.R. No. 203515**).
- c. For violating the right to privacy of communication under Section 3, Article III of the 1987 Constitution (**Sta. Maria, G.R. No. 203440, Castillo, G.R. No. 203454, NPCP, G.R. No. 203454**).
- d. For violating the freedom of speech clause under Section 4, Article III of the 1987 Constitution (**Sta. Maria,**

---

<sup>24</sup> infra at pp. 147-151.

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

**G.R. No. 203440, Cruz, G.R. No. 203469).**

- e. For violating the rule on double jeopardy under Section 21, Article III of the 1987 Constitution (**Sta. Maria, G.R. No. 203440**).
- f. For being an undue delegation of legislative authority (**Disini, G.R. No. 203335**).
- g. For being a grant of unbridled power to the Secretary of Justice in that the latter acts as “judge, jury and executioner” of all cybercrime related complaint (**Disini, G.R. No. 203335, Reyes, et al., G.R. No. 203407**).
- h. For being an undue delegation of judicial function (**Adonis, G.R. No. 203378, NUJP, G.R. No. 203453**).<sup>25</sup>

**XX**

**WHETHER OR NOT SECTION 20 OF R.A. NO. 10175, WHICH PENALIZES AS A VIOLATION OF PRESIDENTIAL DECREE NO. 1829<sup>26</sup> ANY PERSON WHO FAILS TO COMPLY WITH THE ORDER FROM LAW ENFORCEMENT AUTHORITIES UNDER CHAPTER IV OF THE LAW, IS UNCONSTITUTIONAL:**

- a. For violating the right to the privacy of communication and correspondence (**Biraogo, G.R. No. 203299**).
- b. For violating the freedom of speech clause under Section 4, Article III of the 1987 Constitution (**Biraogo, G.R. No. 203299**).
- c. For being a bill of attainder (**NUJP, G.R. No. 203453**).<sup>27</sup>

---

<sup>25</sup> *infra* at pp. 151-157.

<sup>26</sup> *Penalizing Obstruction of Apprehension and Prosecution of Criminal offenses.*

<sup>27</sup> *infra* at pp. 157-162.

**XXI**

**WHETHER OR NOT SECTIONS 24 AND 26(a) OF R.A. NO. 10175, WHICH GAVE THE CICC THE POWER TO FORMULATE A NATIONAL CYBER SECURITY PLAN, IS AN UNDUE DELEGATION OF LEGISLATIVE POWER FOR LACK OF PARAMETERS OR STANDARDS IN FORMULATING SAID PLAN (NUJP, G.R. No. 203453).<sup>28</sup>**

**STATEMENT OF RELEVANT ANTECEDENTS**

1. On September 12, 2012, President Benigno S. Aquino, III signed into law **R. A. No. 10175**. R.A. No. 10175 seeks to address “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.”

2. The following acts are categorized as cybercrimes and made punishable under said law:

**Offenses against the confidentiality, integrity and availability of computer data and systems**

---



---

<sup>28</sup> infra at pp. 163-168.

Section 4(a)(1) Illegal Access;  
 Section 4(a)(2) Illegal Interception;  
 Section 4(a)(3) Data Interference;  
 Section 4(a)(4) System Interference;  
 Section 4(a)(5) Misuse of Devices; and  
 Section 4(a)(6) Cyber-squatting.

**Computer-related Offenses**

---

Section 4(b)(1) Computer-related Forgery;  
 Section 4(b)(2) Computer-related Fraud; and  
 Section 4(b)(3) Computer-related Identity Theft.

**Content-related Offenses**

---

Section 4(c)(1) Cybersex;  
 Section 4(c)(2) Child Pornography;  
 Section 4(c)(3) Unsolicited Commercial Communications; and  
 Section 4(c)(4) Libel.

3. Section 5 of R. A. No. 10175 also renders criminally liable any person who willfully abets or aids in the commission or attempts to commit any of the foregoing offenses. On the other hand, Section 6 of R. A. No. 10175 legislates that all crimes if committed through the use of information and communications technology (ICT) are covered by R.A. No. 10175. It also makes the use of ICT a qualifying circumstance of all crimes under the Revised Penal Code and special laws. Section 7 incorporates the doctrine that a single act may

constitute several offenses by expressly stating that a prosecution under R.A. No. 10175 is without prejudice to any liability for violation of the Revised Penal Code or special laws.

4. R.A. No. 10175 also devotes a chapter on enforcement and implementation in line with its policy “to 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.”

5. Between September 24, 2012 and October 8, 2012, fifteen (15) petitions were filed before this Honorable Court seeking to declare as unconstitutional the whole or portions of R. A. No. 10175. The petitions raise the following arguments:

**1. *Louis “Barok” C. Biraogo (Biraogo)*  
*G. R. No. 203299***

**I**

Section 4(c)(4), Section 12 and Section 20 of Republic Act No. 10175 abridge the constitutional right of free speech enjoyed by petitioner and the Filipino people.

**II**

Section 4(c)(4), Section 12 and Section 20 of Republic Act No. 10175 carry a heavy presumption that they are unconstitutional.

**III**

Section 12 and Section 20 of Republic Act No. 10175 abridge the constitutional right of petitioner and the Filipino people to the privacy of their communication and correspondence.

**IV**

Section 4(c)(4) and Section 12 of Republic Act No. 10175 are unconstitutional pursuant to the void for vagueness rule.

**V**

The penal provisions of Republic Act No. 10175 are unconstitutional.

**VI**

Petitioner has *locus standi*.

**VII**

Petitioner is entitled to the issuance of the writs of certiorari and prohibition.

**VIII**

The petitioner is entitled to the injunctive reliefs sought.

**2. Alab Ng Mamamahayag, et al. (ALAM)  
G.R. No. 203306**

**I**

Section 2 of R.A. No. 10175 which sets forth the State's objective of providing an environment conducive to the development, acceleration and rational application and exploitation of information and communications technology is not compelling enough to sacrifice the freedom of expression.

**II**

Section 4(c)(3) of R.A. No. 10175 defining “unsolicited advertisement” is not grounded on compelling interest to regulate such activity.

**III**

Section 6, R.A. No. 10175 increasing the penalty for crimes under the Revised Penal Code and special penal laws fails to provide a link between its objectives and the crimes enumerated in the RPC and special laws.

**IV**

Section 6 of R.A. No. 10175 is oversweeping, too general and overreaching for ordinary citizens to understand.

**V**

Section 6 of R.A. No. 10175 providing for a higher penalty for crimes committed through information and communications technology is not based on substantial distinction between online publishers and offline publishers.

**3. Jose Jesus M. Disini, Jr., et al. (Disini)  
G.R. No. 203335**

**I**

The Cybercrime Act violates free speech.

**II**

Sections 6 and 7 of the Cybercrime Act violate the double jeopardy and equal protection clauses of the Constitution.

**III**

The real time collection of traffic data violates the right to privacy and the right against unreasonable searches and seizure.

**IV**

The respondent DOJ Secretary's take down authority under Section 19 of the Cybercrime Act violates due process and is an undue delegation of legislative authority.

**4. Sen. Teofisto DL Guingona, III, et al. (Guingona)  
G.R. No. 203359**

**I**

Section 4(c)(4) in relation to Section 6 of "The Cybercrime Act" violates the constitutional guarantees on equal protection and due process of law.

**II**

Section 7 of "The Cybercrime Act" is contrary to the constitutional prohibition against double jeopardy.

**III**

Section 19 of "The Cybercrime Act" is violative of the constitutional prohibition against unlawful searches and seizure and the due process clause of the Constitution.

**5. Alexander Adonis, et al. (Adonis)  
G.R. No. 203378**

**PROCEDURAL MATTERS**

**I**

Petitioners have standing to file the instant petition for certiorari and prohibition.

**II**

The controversy is sufficiently ripe for the high court's adjudication.

**III**

The filing of the instant Petition does not violate the hierarchy of courts, given the urgency and the nature of the issues involved.



**IV**

The petition involves matters of public interest and transcendental importance such as would justify a relaxation of procedural requirements for constitutional adjudication.

**V**

In the very first place, any prosecution for criminal libel is a continuing violation of Philippine State obligations under the International Covenant of Civil and Political Rights (ICCPR) as the UN Human Rights Committee has so held in its view on *Adonis v. Republic of the Philippines*, where the committee stated that criminal libel in the Revised Penal Code is incompatible with freedom of expression.

**VI**

Section 4(c)(4) and Section 5 of R.A. 10175 violate the constitutional right to freedom of speech, of expression, and of the press enshrined in Article III, Section 4 of the Constitution as said Sections of the law are vague and overbroad.

**VII**

Section 6 of R.A. 10175 violates the equal protection clause enshrined in Article III, Section 1, of the Constitution – since it arbitrarily increases the penalty imposed on “cyber libel” as compared to the penalty for ordinary libel – without any valid legal basis for such a higher penalty.

**VIII**

Section 7 of R.A. 10175 violates the constitutional right against double jeopardy enshrined in Article III, Section 21 of the Constitution as it places an accused in double jeopardy.

**IX**

Section 19 of R.A. 10175 violates the constitutional principle of separation of powers as it delegates to the DOJ what is properly a judicial function.

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

## X

The presumption of constitutionality does not apply to R.A. 10175 since it violates constitutionally protected fundamental rights.

### **6. *Hon. Raymond V. Palatino, et al. (Palatino)* G.R. No. 203391**

#### I

All the requisites for the exercise of judicial review are present.

#### II

Sections 4(c)(4), 5 and 6 of R.A. No. 10175 relative to libel are unconstitutional due to vagueness.

#### III

Particular sections of Chapter IV of R.A. No. 10175 are unconstitutional for violating constitutional due process, among other rights.

### **7. *Bagong Alyansang Makabayan Secretary General* *Renato M. Reyes, et al. (Reyes)* G.R. No. 203407**

#### I

RA 10175 is not an ordinary penal statute as it involves, or rather infringes on, freedom of speech, of expression, and of the press and other fundamental rights of the People that are inherent in the exercise of freedom of speech clause in cyberspace, including the right against unreasonable searches and seizures and the right to privacy. As such, the doctrines of vagueness and overbreadth are applicable in the instant case, and Sections 4(a)(3), 4(b)(3), 4(c)(4), 5(a)(b), 6, 7, 12, 17, 19, and 20 of RA 10175 are hereby assailed either for being void-for-vagueness, overbreadth, constituting prior restraint or content-based restrictions on freedom of speech clause, violation of the right to privacy, right against unreasonable searches and seizures, right not to be subjected to double

jeopardy, or deprivation of property without due process of law, and thus unconstitutional.

## II

Section 4(a)(3) of RA 10175 suffers from overbreadth as the means employed in said provision sweep unnecessarily broadly and thereby invade the area of protected speech, in relation to the supposed purposes of RA 10175, and constitutes prior restraint and content based restrictions.

## III

Section 4(b)(3) of RA 10175 suffers from overbreadth as the means employed in said provision sweep unnecessarily broadly and thereby invade the area of protected speech and right to privacy, in relation to the supposed purposes of RA 10175, and constitutes prior restraint.

## IV

Section 4(c)(4) of RA 10175 suffers from vagueness as it lacks comprehensible standards that men of common intelligence must necessarily guess at its meaning and differ as to its application, and that infringes on protected speech.

## V

Section 4(c)(4) of RA 10175 suffers from overbreadth as the means employed in said provision sweep unnecessarily broadly and thereby invade the area of protected speech, in relation to the supposed purposes of RA 10175.

## VI

Section 5(a)(b) of RA 10175, in relation to the offenses that includes speech related matters under said statute, suffers from overbreadth as the means employed in said provision sweep unnecessarily broadly and thereby invade the area of protected speech, in relation to the supposed purposes of RA 10175.

## VII

Sections 6 and 7 of RA 10175 constitute a violation of the right of the people not to be

subjected to double jeopardy, and Section 6 suffers from overbreadth.

**VIII**

Section 12(1) of RA 10175 constitutes a patent violation of the right of the people against unreasonable searches and seizures and the right to privacy.

**IX**

Section 17 of RA 10175 constitutes deprivation of property without due process of law.

**X**

Section 19 of RA 10175 is a patent infringement of the freedom of speech clause and a grant of unbridled power to public respondent Secretary of Justice.

**8. Melencio S. Sta. Maria, et al. (Sta. Maria)  
G.R. No. 203440**

**I**

Section 19 of Republic Act No. 10175 violates Section 1 of Article 3 of the Bill of Rights of the 1987 Philippine Constitution.

**II**

Section 19 of Republic Act No. 10175 violates Section 4 of Article 3 of the Bill of Rights of the 1987 Philippine Constitution.

**III**

Section 19 of Republic Act No. 10175 violates Section 3 (1) of Article 3 of the Bill of Rights of the 1987 Philippine Constitution.

**IV**

Section 19 of Republic Act No. 10175 violates Section 21 of Article 3 of the Bill of Rights of the 1987 Philippine Constitution.

**V**

Section 5 of Republic Act No. 10175 violates Section I of Article 3 of the Bill of Rights of the 1987 Philippine Constitution.

**VI**

Section 6 of Republic Act No. 10175 violates Section 1 on equal protection and 21 on double jeopardy of Article 3 of the Bill of Rights of the 1987 Philippine Constitution.

**VII**

Section 7 of Republic Act No. 10175 violates Section 1 on equal protection and 21 on double jeopardy of Article 3 of the Bill of Rights of the 1987 Philippine Constitution.

**VIII**

Section 4(4) (*sic*) on Libel of Republic Act No. 10175 violates Sections 1 and 4 of Article 3 of the Bill of Rights of the 1987 Philippine Constitution.

**9. National Union of Journalists of the Philippines, et al. (NUJP)  
G.R. No. 203453**

**I**

Sections 4(c)(4), 5(a), 6, and 7 violate freedom of expression.

**II**

Section 4(c)(4), 5(a), 6 which criminalize the use of “Information and communications technologies” (ICT), render Republic Act No. 10175 a Bill of Attainder; Further, Sec. 20, which makes non-compliance with orders of law enforcement authorities punishable criminally also renders the law a bill of attainder.

**III**

Section 7 violates the constitutional guarantee of protection against double jeopardy.

**IV**

Sections 6, 7 and 19 violate due process and equal protection.

**V**

Sections 14, 15, 19, 24 and 26(a) violate separation of powers as judicial powers are unduly delegated to the Secretary of Justice, the PNP and the NBI.

**VI**

Section 12 violates the right of privacy of communication and correspondence as it allows the real-time collection of traffic data and effectively surveillance without a warrant.

**VII**

The Cybercrime Law is effective even without the implementing rules and regulations; unless the implementation of the law is restrained, petitioners stand to suffer grave and irreparable injury with no speedy or adequate remedy at law.

**10. Paul Cornelius T. Castillo, et al. (Castillo)  
G.R. No. 203454**

**I**

Section 4(c)(4) of the Cybercrime Act is unconstitutional for vagueness.

**II**

Section 6 of the Cybercrime Act is unconstitutional for violating the equal protection clause.

**III**

Section 12 of the Cybercrime Act is unconstitutional for being violative of the constitutionally guaranteed right to due process; freedom of speech; right against unreasonable searches and seizures; and the right to privacy.

**IV**

Section 19 of the Cybercrime Act is unconstitutional for being violative of the constitutionally guaranteed right to due process; right against unreasonable searches and seizures; and right to free speech. Section 19 is also an undue delegation of legislative authority.

**11. Anthony Ian M. Cruz, et al. (Cruz)  
G.R. No. 203469**

**I**

Section 12 of the Cybercrime Prevention Act is patently unconstitutional considering that it violates an individual's right to privacy and the privacy of communication and correspondence.

- a. An individual has a reasonable expectation of privacy of personal electronic data, as well as communication and correspondence.
- b. Section 12 of the Cybercrime Prevention Act constitutes an unreasonable government intrusion as it lacks safeguards against possible abuses by possessors of acquired data.
- c. Section 12 of the Cybercrime Prevention Act constitutes an unreasonable government intrusion as it renders existing safeguards against invasion of privacy, as well as communications and correspondence, nugatory.

**II**

Section 12 of the Cybercrime Prevention Act is patently unconstitutional considering that it violates an individual's right to unreasonable searches and seizures.

**III**

Section 19 of the Cybercrime Prevention Act is null and void for being unconstitutional considering that:

- a. Section 19 of the Cybercrime Prevention Act is violative of the due process clause under Section 1, Article III of the Constitution, for failing to provide any procedural safeguards in its implementation and/or enforcement.

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407, 203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

- b. Section 19 of the Cybercrime Prevention Act is violative of the right of citizens against unreasonable searches and seizures, as provided under Section 2, Article III of the Constitution.
- c. Section 19 of the Cybercrime Prevention Act is violative of the right of the People to freedom of speech, as provided under Section 4, Article III of the Constitution.

**IV**

Sections 4(c)(4), 5, 6, and 7 of the Cybercrime Prevention Act are null and void for being unconstitutional considering that said provisions are violative of the due process clause under Section 1, Article III of the Constitution and of the free speech clause under Section 4, Article III of the Constitution.

**V**

Section 6 of the Cybercrime Prevention Act is null and void for being unconstitutional considering that it is violative of the equal protection clause under Section 1, Article III of the Constitution.

**12. Philippine Bar Association, Inc., et al. (PBA)  
G.R. No. 203501**

**I**

Sections 4(c)(4) and 5 of RA 10175 violate the right to due process as well as the freedom of speech, of expression, and of the press guaranteed by the 1987 Constitution.

**II**

Section 6 of the Cybercrime Law violates the equal protection clause guaranteed in Section 1, Article III of the 1987 Constitution.

**III**

Section 7 of RA 10175 violates the Rule on Double Jeopardy guaranteed in Article III, Section 21 of the 1987 Constitution thus, void.



**IV**

Section 12 of the Cybercrime Law is patently unconstitutional considering that:

- a. Section 12 of the Cybercrime law violates an individual's right to privacy.
- b. Section 12 of the Cybercrime law violates an individual's right against unreasonable searches and seizures.

**V**

Section 19 of the Cybercrime law, which allows the DOJ to restrict or block access to computer data, is likewise constitutionally infirm.

**13. *Bayan Muna Representative Neri J. Colmenares, et al., (Colmenares) G.R. No. 203509***

**I**

A facial reading of the statute will lead the Honorable Court to conclude that the statute does not incorporate the multi-tiered proportionality analysis that ought to be deployed in free speech, especially e-speech, namely, proportionality analysis and probability analysis.

**II**

There is no question that the Cybercrime Prevention Law will reduce the sum total of internet speech and opinion among internet users great and small in the Philippines and beyond, because its Sections, read in their entirety, raise the constitutional price of an essential political good today.

**III**

On its face, the Cybercrime Statute is unconstitutional, because it does not incorporate possible defenses to the charge of e-libel as part of the statutory text, thus effectively passing a prohibitive burden to the defense attorney, if not the poor judge who works under an archaic analogue system, to make the proportionality analysis himself.

#### IV

The Congress must obviously decide, in the first instance, whether a danger exists which calls for a particular protective measure. But where a statute is valid only in case certain conditions exist, the enactment of the statute cannot alone establish the facts which are essential to its validity. These facts are absent.

#### V

For having failed to incorporate proportionality and probability analysis in free speech, especially the rapidly emerging area of e-speech, the Cybercrime Statute is unconstitutional for failing the sufficiency of standards test and the completeness test. Thus, the effect of the Cybercrime Statute is the undue delegation of too wide a legislative and policy making function to both the trier of fact and the law enforcer.

#### VI

The apparent rider on e-libel appears to be under the hearing "Content-Related Offenses" in Section 4(c), but this heading does not alert the trier of fact to the term of art 'Content-Based' within the meaning of the bill of rights, rather it is a caption meant to distinguish e-libel from the nomenclature of previously listed offenses such e-espionage and 'computer-related offenses.'

#### VII

On its face the Cybercrime Statute fails to incorporate reasonably sufficient standards that would aid the trier of fact to distinguish between e-speech in ordinary times and places and e-speech made in extraordinary times and places; in fact no such attempt can be made because e-speech is by nature not spatially constrained, nor can the speaker, endorser, actor, and receiver of such speech be conveniently located in time and place by the trier of fact.

#### VIII

Without manageable standards set forth in the Cybercrime Law in the name of proportionality and probability analysis that can meet the dynamic nature of e-speech, the modest provisions of the e-libel provision will operate as

essentially open-ended restrictions of expression.

**IX**

As a matter of fact, history would show that the Cybercrime Statute contains a similar rider on libel, recast in contemporary society as e-libel in Section 4(c), and may thus face a similar fate to the US Espionage Act of 1917 and Sedition Act of 1918.

**X**

If the interpretation of the e-libel provision of the cybercrime statute is in danger of open-ended interpretation by the trier of fact or law enforcer, then no matter how “special” the “Cybercrime Court” or “specially trained” their judges can be, there can be no avoidance to the result that the e-libel will allow for roving commissions if not roving warrants in implementation.

**XI**

In particular, no sufficient standard can be found in the cybercrime statute to assist the trier of fact whether to consider joint, cumulative action among ‘netizens’ in dynamic social media.

**XII**

Whether the statute is contrary to equal protection, unduly delegates legislative and policy making functions, violates the right of privacy of communication and correspondence, is void for being vague, is void for overbreadth thereby violating the basic constitutional requirements for a valid law.

**14. *National Press Club of the Philippines, Inc., et al. (NPC)*  
*G.R. No. 203515***

**I**

This Petition for Certiorari and Prohibition is anchored on the thesis that Sections 4(c)4, 5(a), 6 and 7 of R.A. No. 10175 are absolutely and unequivocally unconstitutional.

**II**

The Honorable Supreme Court has the duty to exercise its power of judicial review against the questioned provisions of the law.

**III**

Sections 4(c) 4, 5(a) 6 and 7 of RA 10175 infringed petitioners' freedom of speech, freedom of expression, freedom of the press, right to due process and equal protection of the law and right against double jeopardy.

**15. *Philippine Internet Freedom Alliance, et al. (PIFA)*  
*G.R. No. 203518***

**I**

The Cybercrime Prevention Act is an undue abridgment of the freedom of speech, expression, and of the press.

- a. The Cybercrime Prevention Act infringes on freedom of speech.
- b. The Cybercrime Prevention Act is constitutionally infirm on its face for being vague and overbroad.
- c. Cybercrime Prevention Act contradicts Constitutional mandate for balanced flow of information under policy respecting freedom of speech and of the press.

**II**

The Cybercrime Prevention Act of 2012 (The Cybercrime Prevention Act) authorizes government to conduct an unreasonable search and seizure.

- a. Section 12 grants unto the government the power to conduct warrantless electronic surveillance.
- b. Section 19 authorizes government to make an invalid seizure of one's data.

### III

The Cybercrime Prevention Act violates the constitutional right to privacy and the right to privacy of communication and correspondence.

- a. The Cybercrime Prevention Act of 2012 (the Cybercrime Prevention Act) violates the right to privacy.
- b. Sections 12 and 19 of the Cybercrime Prevention Act (the Cybercrime Prevention Act) violate the right to privacy of communications and correspondence.

### IV

Section 12 is an impermissible intrusion into the right of privacy of communication and correspondence.

### V

Section 19 is an impermissible intrusion into the right of privacy of communication and correspondence.

### VI

The Cybercrime Prevention Act of 2012 (the Cybercrime Prevention Act) is contrary to the guarantee of equal protection under the law.

### VII

The Cybercrime Prevention Act of 2012 violates our legal obligations under public international law.

### VIII

The Cybercrime Prevention Act acts as an *ex post facto* law.

## IX

The implementation of the Cybercrime Prevention Act will clog the dockets of our courts arising from a deluge of frivolous lawsuits.

### SUMMARY OF ARGUMENTS

#### PROCEDURAL ISSUES

The president cannot be sued for actions taken while in the office (pp. 41-42).

- I. Petitioners have no standing to file the present case (pp. 42-50).
- II. The issues raised are not ripe for adjudication (pp. 50-54).

#### SUBSTANTIVE ISSUES

- 4(a) Offenses against the confidentiality, integrity and availability of computer data and systems.
  - III. The application of strict scrutiny is not called for because Section 4(a)(1) regulates hacking, a socially harmful conduct; it does not regulate, prevent or punish speech (pp. 54-58).
  - IV. Section 4(a)(3) of the Cybercrime Prevention Act of 2012 does not violate the exercise of free speech (pp. 53-60).
  - V. Section 4(a)(6) of the Cybercrime Prevention Act of 2012 does not violate the equal protection clause of the Constitution (pp. 60-64).
- 4(b) Computer-related Offenses:
  - VI. Section 4(b)(3) of R.A. No. 10175 does not violate the Bill of Rights (pp. 64-69).
- 4(c) Content-related Offenses.
  - VII. Section 4(c)(1) does not abridge freedom of expression nor is it a prior restraint on the exercise of said freedom (pp. 69-73).

VIII. Section 4(c)(3) does not violate the constitutional provisions on deprivation of one's right to liberty without due process and equal protection of the law (pp. 73-76).

IX. Section 4(c)(4), making expressed the use of computer system as another avenue of committing libel under Article 353 of the Revised Penal Code, does not violate the 1987 Constitution (p. 76).

a. Section 4(c)(4) is valid, complete and clear, and does not violate due process of law (pp. 76-78).

b. Section 4(c)(4) does not abridge the constitutional right to free speech, freedom of expression and of the press (pp. 78-83).

c. Section 4(c)(4) of R.A. No. 10175 does not violate the Equal Protection Clause of the Constitution (pp. 83-84).

d. Section 4(c)(4) of R.A. No. 10175 is not *ex post facto* law (pp. 84-85).

e. Section 4(c)(4) does not violate the Philippines' international treaty obligations (pp. 85-89).

X. Section 5, which penalizes the acts of aiding or abetting and attempting the commission of cybercrimes, is valid and constitutional.

Section 5 does not suffer from vagueness.

Section 5 does not constitute prior restraint or subsequent punishment in the exercise of the freedom of expression over the internet (pp. 89-95).

XI. Section 6 is valid (pp. 95-96).

The first sentence of Section 6 is clear. The term Information and Communication Technology has long been used; its short version is I.T. or Information Technology (pp. 96-98).

The first sentence of Section 6 does not violate Section 21, Article III of the 1987 Constitution (pp. 98-99).

The second sentence of Section 6 does not suffer from any constitutional infirmity (pp. 99-101).

Section 6 of R.A. No. 10175 does not violate the equal protection clause of the 1987 Constitution (pp. 101-106).

Effect of the Second Sentence of Section 6 on the crime of Libel (pp. 106-107).

Section 6 of R.A. No. 10175 is not a bill of attainder (pp. 108-109).

**XII. Section 7 of R.A. No. 10175 does not violate Section 21, Article III of the 1987 Constitution (pp. 109-111).**

**XIII. The fixing of penalties for the violation of statutes is primarily a legislative function (pp. 111-115).**

**XIV. The collection of traffic data will not result in any search or seizure of petitioners' persons and/or properties (pp. 115-119).**

*Ephemeral traffic data: challenges for law enforcement* (pp. 119-124).

Rule against unreasonable searches and seizures (pp. 124-126).

*Inside/Outside Distinction translated in the communications network context* (pp. 126-136).

**R.A. No. 10175 provides for statutory protection; OSG is of the view that the Congress may consider more robust procedural protections (pp. 136-139).**

**XV. Section 13 on preservation of data does not violate the provisions of the Constitution.**

Section 13 does not violate the due process clause of the Constitution (pp. 140-143).

**Section 13 does not infringe on one's right to privacy (pp. 143-144).**

**XVI. Section 14 does not encroach upon judicial process. The order referred to therein is to be issued upon securing a court warrant. Nonetheless, the power to issue subpoena is inherent in the power to investigate and may thus be exercised by the law enforcement authorities (pp. 144-146).**

**XVII. Section 15 of R.A. No. 10175 is not an undue delegation of judicial and legislative powers to NBI and PNP (pp. 146-151).**

**XVIII. Petitioners do not have any interest relative to destruction of computer data under Section 17 (pp. 151-154).**



**XIX. Section 19 of R.A. No. 10175 violates the freedom of speech and expression clauses of the Constitution (pp. 154-161).**

**XX. Section 20, which treats as obstruction of justice the non-compliance with orders of the Law Enforcement Agencies, observes substantial due process and is not a bill of attainder (pp. 161-163).**

**XXI and XXII. The authority granted to CICC under Sections 24 and 26(a) has parameters and standards. It is embodied in Sections 2 and 26-A of R.A. No. 10175 (pp. 163-165).**

## **DISCUSSION**

**The President cannot be sued for actions taken while in the office.**

---

Petitioners Alab, Reyes, Cruz, PBA and NPC impleaded President Benigno Simeon Aquino III for having signed into law R.A. No. 10175 and the Office of the President, represented by President Benigno Simeon Aquino III, for being one of the office tasked to implement the same.

These five (5) petitions are suits against an incumbent President. An incumbent President is immune from suit or from being brought to court during the period of his incumbency and tenure.

In **David vs. Arroyo**,<sup>29</sup> this Honorable Court held that the President enjoys immunity during incumbency. One of the underlying reason for the grant of said immunity is that the demands of his Office require the President to be free from unnecessary distractions so that he can have his undivided attention and time to the concerns of the nation. This Honorable Court said:

xxx Settled is the doctrine that the President, during his tenure of office or actual incumbency, may not be sued in *any* civil or criminal case, and there is no need to provide for it in the Constitution or law. It will degrade the dignity of the high office of the President, the Head of State, if he can be dragged into court litigations while serving as such. Furthermore, it is important that he be freed from any form of harassment, hindrance or distraction to enable him to fully attend to the performance of his official duties and functions. Unlike the legislative and judicial branch, only one constitutes the executive branch and anything which impairs his usefulness in the discharge of the many great and important duties imposed upon him by the Constitution necessarily impairs the operation of the Government. However, this does not mean that the President is not accountable to anyone. Like any other official, he remains accountable to the people but he may be removed from office only in the mode provided by law and that is by impeachment.

Verily, the suits against the President must be dismissed outright.

**I. Petitioners have no standing to file the present case.**

-----

---

<sup>29</sup> 489 SCRA 160, 224-225 [2006].

*Locus standi* or legal standing requires a personal stake in the outcome of the controversy as to assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends for the illumination of difficult constitutional questions.<sup>30</sup>

Petitioners NUJP,<sup>31</sup> Disini,<sup>32</sup> Castillo,<sup>33</sup> PBA<sup>34</sup> and NPCP<sup>35</sup> assert *locus standi* on the basis of the “transcendental importance” doctrine.

While **Chavez vs. PCGG**<sup>36</sup> holds that transcendental public importance dispenses with the requirement that petitioner has experienced or is in actual danger of suffering direct and personal injury, cases involving the constitutionality of *penal* legislation belong to an altogether different genus of constitutional litigation. Compelling State

---

<sup>30</sup> Southern Hemisphere Engagement Network, Inc. vs. Anti-Terrorism Council, 632 SCRA 146 [2010], citing Integrated Bar of the Philippines vs. Zamora, 338 SCRA 81 [2000], which made reference to Baker vs. Carr, 369 US 186 [1962].

<sup>31</sup> G.R. No. 203469, pp. 15-16,

<sup>32</sup> G.R. No. 203335, p. 2

<sup>33</sup> G.R. No. 203454, p. 3

<sup>34</sup> G.R. No. 203501, p. 9.

<sup>35</sup> G.R. No. 203515, pp. 3-4.

<sup>36</sup> 299 SCRA 744 [1998].

and societal interests in the proscription of harmful conduct necessitate a closer judicial scrutiny of *locus standi*.<sup>37</sup>

The following are determinants of whether a matter is of transcendental importance: (1) the character of the funds or other assets involved in the case; (2) the presence of a clear case of disregard of a constitutional or statutory prohibition by the public respondent agency or instrumentality of the government; and, (3) the lack of any other party with a more direct and specific interest in the questions being raised.<sup>38</sup> None of the foregoing determinants are established by petitioners.

Petitioners who invoke the “transcendental importance” doctrine have not identified their *personal stake in the outcome of the controversy*. They fail to particularize how the implementation of specific provisions of RA No. 10175 would result in direct injury to their organization and members.<sup>39</sup> R.A. No. 10175 does not disregard the provisions of the Constitution, as in fact, it protects petitioners’ right and

---

<sup>37</sup> Southern Hemisphere, *supra*.

<sup>38</sup> *c.f.*, CREBA vs. ERC and MERALCO, 624 SCRA 556 [2010].

<sup>39</sup> *c.f.*, CREBA vs. ERC, *supra*.

freedom by establishing minimum standards of decency and civility for an orderly and safe virtual environment.

There are other parties not before the Court with **direct and specific interests** in the questions being raised. Prior to October 9, 2012, when this Honorable Court issued a temporary restraining order (TRO) against the implementation of R.A. No. 10175, the National Bureau of Investigation (NBI) started investigating members of *Anonymous Philippines*, a group that has claimed on its Facebook account that it hacked the website of the NBI and those of other agencies. The members of *Anonymous Philippines* were charged with hacking in violation of R.A. No. 10175.<sup>40</sup> None of the petitioners were previously investigated or may be prospectively charged with violation of R.A. No. 10175 before they filed their respective petitions.

Petitioners in G.R. No. 203518, PIFA, claim that upon the effectivity of R.A. No. 10175, they will be subjected to “*unwarranted electronic surveillance*” twenty-four (24) hours a day, seven (7) days a week that is violative of their

---

<sup>40</sup> <http://technology.inquirer.net/17976/nbi-says-it-has-traced-at-least-20-hacktivists>, accessed on November 21, 2012.

constitutional right to privacy, free speech, free expression and their rights to unreasonable searches and seizures.<sup>41</sup> Petitioners' apprehension cannot substantiate their plea. They have not shown any connection between the purported "*surveillance*" and the implementation of R.A. No. 10175.

Petitioner Philippine Bar Association, Inc.<sup>42</sup> (PBA) and petitioner-lawyers Ronaldo E. Renta, Cirilo P. Sabarre, Jr., David Castro,<sup>43</sup> Harry L. Roque, Jr., Romel R. Bagares, Gilbert T. Andres,<sup>44</sup> and Marlon Anthony Romasanta Tonson<sup>45</sup> base their claim of *locus standi* on their sworn duty as officers of the court to uphold the Constitution.

In **Southern Hemisphere Engagement Network, Inc.**, *supra*, this Honorable Court held that mere invocation of the duty to preserve the rule of law does not suffice to clothe the Integrated Bar of the Philippines or petitioners-lawyers with standing. Herein petitioners PBA and the petitioners-lawyers also failed to demonstrate how the assailed statute violates their "mandate" to uphold constitutional rights.

---

<sup>41</sup> Petition, G.R. No. 203518, p. 9.

<sup>42</sup> G.R. No. 203501, pp. 8-9.

<sup>43</sup> G.R. No. 203306, par. 28.

<sup>44</sup> G.R. No. 203378, p. 4.

<sup>45</sup> G.R. No. 203518, p. 4.

Petitioner-organizations *Alab ng Mamahayag (ALAM)*, *Hukuman ng Mamamayan Movement, Inc. (HMMI)*,<sup>46</sup> National Union of Journalist of the Philippines (NUJP), Philippine Press Institute (PPI), Center for Media Freedom and Responsibility (CMFR),<sup>47</sup> Philippine National Press Club of the Philippines (NPC),<sup>48</sup> Dakila and Partido Lakas ng Masa<sup>49</sup> contend that as media advocacy groups of journalist, media practitioners and advocates of the Jury System, they are committed to defend press freedom, freedom of expression, speech, due process and right to privacy.

Mere invocation of media advocacy does not clothe litigants with *locus standi*. Petitioners must show an actual, or immediate danger of sustaining, direct injury as a result of the law's enforcement. To rule otherwise would be to corrupt the settled doctrine of *locus standi*, as every worthy cause is an interest shared by the general public.<sup>50</sup>

---

<sup>46</sup> G.R. No. 203306, par. 24.

<sup>47</sup> G.R. No. 203453, p. 6.

<sup>48</sup> G.R. No. 203515, p. 4.

<sup>49</sup> G.R. No. 203518, pp. 3-4.

<sup>50</sup> Southern Hemisphere, *supra* at p. 174.

Senator Teofisto DL Guingona III,<sup>51</sup> Representatives Raymond V. Palatino,<sup>52</sup> Antonio Tinio<sup>53</sup> and Neri J. Colmenares<sup>54</sup> cite their being senators and congressmen, respectively, and oppositors to the passage of R. A. No. 10175. As this Honorable Court ruled in **Southern Hemisphere, supra**, being a lawmaker, sans showing of concrete injury, does not vest standing.<sup>55</sup>

Neither can *locus standi* be conferred upon individual petitioners as *taxpayers* and *citizens*. A taxpayer suit is proper only when there is an exercise of the spending or taxing power of Congress, whereas citizen standing must rest on direct and personal interest in the proceeding.<sup>56</sup> None of the individual petitioner-citizens has alleged any direct and personal interest in the implementation of the law. Generalized interests, albeit accompanied by the assertion of a public right, do not establish *locus standi*. Evidence of a direct and personal interest is key.<sup>57</sup>

---

<sup>51</sup> G.R. No. 203359, p. 7.

<sup>52</sup> G.R. No. 203391, p. 2.

<sup>53</sup> G.R. No. 203391, p. 2.

<sup>54</sup> G.R. No. 203509, p. 4.

<sup>55</sup> *Supra* at p. 174.

<sup>56</sup> *Supra* at pp. 174-175.

<sup>57</sup> *Supra* at p. 175.



Several individual petitioners sue in their capacities as journalists, columnists, bloggers, internet users, internet subscribers, social media account holders, broadcasters, professors, freelance writers. Such claims are also insufficient to clothe petitioners with *locus standi*. R. A. No. 10175 regulates and penalizes acts defined as cybercrime. It does not prevent petitioners from using the internet and from expressing their thoughts and opinion. Thus, they can still publish articles online, post and comment on social medias, research and surf.

Likewise, petitioners cannot claim the protection of the constitutional right against an unreasonable search and seizure because there has been no search and seizure on their property. **Stonehill vs. Diokno**<sup>58</sup> held that the right to object to an unlawful search and seizure is a purely personal right that can only be claimed by the party whose right has been impaired.

Traffic data, which is the subject of petitioners' objections on Section 12 of the law, are information logged, stored and

---

<sup>58</sup> 20 SCRA 383 [1967].

kept by service providers,<sup>59</sup> and not by private individuals. These logs constitute the **business records** of the service providers. No service provider has raised any objection to Section 12.

## II. The issues raised are not ripe for adjudication.

-----

Petitioners Biraogo's,<sup>60</sup> Reyes'<sup>61</sup> and Castillo's<sup>62</sup> prayer for the *facial invalidation* of Section 4 of R.A. No. 10175 is without merit because the said doctrine does not apply to penal statutes.

As this Honorable Court explained in **Estrada vs. Sandiganbayan**, penal statutes have general *in terrorem* effect resulting from its very existence, and if a facial challenge is allowed for this reason alone, the State may well be prevented from enacting laws to deter socially harmful conduct.<sup>63</sup>

---

<sup>59</sup> Section 3 (n) reads:

Service provider refers to:

- (1) Any public or private entity that provides to users of its service the ability to communicate by means of a computer system;
- (2) Any other entity that processes or stores computer data on behalf of such communication service or users of such service.

<sup>60</sup> G.R. No. 203299, pp. 20-21.

<sup>61</sup> G.R. No. 203407, p. 12.

<sup>62</sup> G.R. No. 203454, pp. 5-6.

<sup>63</sup> 369 SCRA 394, 441 [2001].

In **Sps. Romualdez vs. COMELEC**,<sup>64</sup> this Honorable Court again emphasized that "on-its-face" invalidation of penal statutes are not allowed in this jurisdiction.

The void-for-vagueness doctrine holds that a law is facially invalid if men of common intelligence must necessarily guess at its meaning and differ as to its application. However, this Court has imposed certain limitations by which a criminal statute, as in the challenged law at bar, may be scrutinized. This Court has declared that facial invalidation or an "on-its-face" invalidation of criminal statutes is not appropriate. We have so enunciated in no uncertain terms in *Romualdez v. Sandiganbayan*, thus:

In sum, the doctrines of strict scrutiny, overbreadth, and vagueness are analytical tools developed for testing "on their faces" statutes in free speech cases or, as they are called in American law, First Amendment cases. They cannot be made to do service when what is involved is a criminal statute. With respect to such statute, the established rule is that 'one to whom application of a statute is constitutional will not be heard to attack the statute on the ground that impliedly it might also be taken as applying to other persons or other situations in which its application might be unconstitutional.' As has been pointed out, 'vagueness challenges in the First Amendment context, like overbreadth challenges typically produce facial invalidation, while statutes found vague as a matter of due process typically are invalidated [only] 'as applied' to a particular defendant.'" (underscoring supplied)

"To this date, the Court has not declared any penal law unconstitutional on the ground of ambiguity." While mentioned in passing in some cases, the void-for-vagueness concept has yet to find direct application in our jurisdiction. In *Yu Cong Eng v. Trinidad*, the Bookkeeping Act was found unconstitutional because it violated the equal protection clause, not because it was vague. *Adiong v. Comelec* decreed as void a mere Comelec Resolution, not a statute. Finally, *Santiago v. Comelec* held that a portion of RA

---

<sup>64</sup> 573 SCRA 639, 643-644 [2008].

6735 was unconstitutional because of undue delegation of legislative powers, not because of vagueness.

**Indeed, an "on-its-face" invalidation of criminal statutes would result in a mass acquittal of parties whose cases may not have even reached the courts. Such invalidation would constitute a departure from the usual requirement of "actual case and controversy" and permit decisions to be made in a sterile abstract context having no factual concreteness.** In *Younger v. Harris*, this evil was aptly pointed out by the U.S. Supreme Court in these words:

"[T]he task of analyzing a proposed statute, pinpointing its deficiencies, and requiring correction of these deficiencies before the statute is put into effect, is rarely if ever an appropriate task for the judiciary. The combination of the relative remoteness of the controversy, the impact on the legislative process of the relief sought, and above all the speculative and amorphous nature of the required line-by-line analysis of detailed statutes, x x x ordinarily results in a kind of case that is wholly unsatisfactory for deciding constitutional questions, whichever way they might be decided."

**For this reason, generally disfavored is an on-its-face invalidation of statutes, described as a "manifestly strong medicine" to be employed "sparingly and only as a last resort." In determining the constitutionality of a statute, therefore, its provisions that have allegedly been violated must be examined in the light of the conduct with which the defendant has been charged.** (Emphasis supplied.)

In **Southern Hemisphere Engagement vs. Anti-Terrorism Council**,<sup>65</sup> citing **Holder vs. Humanitarian Law Project**,<sup>66</sup> this Honorable Court ruled that under the “**as applied doctrine**” the burden is on petitioners, assailing the constitutionality of a penal statute, to indubitably show the presence of all the following requisites before said law may be reviewed and struck down, to wit:

1. Petitioners must demonstrate an actual and personal interest over the matter in question;
2. Must clearly show the existence of a credible threat of criminal prosecution; and
3. Must clearly show that the implementation of the challenged penal statute forbids the performance of a constitutionally protected activity or conduct.

None of the petitioners raised the existence of the above required requisites to challenge the subject penal statute.

Petitioners merely claim that they are suing in their respective capacities as: citizen, netizen, legislator, internet blogger, internet user, multimedia journalist, media organization, or person maintaining a twitter or facebook account.

---

<sup>65</sup> *Supra.*

<sup>66</sup> Argued February 23, 2010--Decided June 21, 2010, No. 08-1498.

Though generally petitioners are frequent internet users, or subscribers, they do not show how their use is actually impeded or affected by any of the questioned provisions of R.A. No. 10175.

Petitioners also fail to establish that there is an imminent threat of an actual filing of a criminal offense against them for violation of the assailed law to warrant its review.

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

---

III. The application of strict scrutiny is not called for because Section 4(a)(1) regulates hacking, a socially harmful **conduct**; it does not regulate, prevent or punish speech.

---

(1) Illegal Access. - The access<sup>67</sup> to the whole or any part of a computer system without right.

Section 4(a)(1) punishes the illegal intrusion into a computer system or network, a form of hacking.

---

<sup>67</sup> Section 3(a) of R.A. No. 10175 defines access as instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network.

Petitioner PIFA contends that Section 4(a)(1) does not meet the *strict scrutiny standards*. Allegedly, Section 4(a)(1) was not narrowly tailored to exclude the “ethical hacker”<sup>68</sup> and may lead him to lose a profession (Petitioner PIFA, G.R. No. 203518, p. 50).

Petitioner PIFA’s apprehensions are misplaced.

In terms of judicial review of statutes or ordinances, strict scrutiny refers to the standard for determining the quality and the amount of governmental interest brought to justify the regulation of fundamental freedoms. Strict scrutiny is used today to test 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>69</sup>

The application of strict scrutiny is not called for because Section 4(a)(1) regulates hacking, a socially harmful **conduct**; it does not regulate, prevent or punish speech.

---

<sup>68</sup> Allegedly “a computer security professional, who by his knowledge of a computer’s systems must test an organization’s security without authority in order to enhance its defenses.

<sup>69</sup> White Light Corporation vs. City of Manila, 576 SCRA 416 [2009].

The inclusion of the qualifying phrase “without right,” which has a clear statutory definition, ensures that legitimate conduct would not be ensnared within the penal provisions of the Cybercrime law.

“Illegal access” is among the offenses against the confidentiality, integrity and availability of computer data and systems under the *Budapest Convention on Cybercrime*, to wit:

*Title 1 – Offenses against the confidentiality, integrity and availability of computer data and systems*

**Article 2 – Illegal access**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

The Explanatory Report on the Convention on Cyber Crime said that illegal access seeks to prevent intrusions which may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment, or even encourage hackers to commit more dangerous forms of



computer-related offenses, like computer-related fraud or forgery. The Report recognizes that the most effective means of preventing unauthorized access is the introduction and development of effective security measures. However, a comprehensive response has to include also the threat and use of criminal law measures and a criminal prohibition of unauthorized access is able to give additional protection to the system and the data as such and at an early stage against the dangers described above. The report underscored that *Illegal Access* does not seek to criminalize legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices.<sup>70</sup>

Illegal access is one of the offenses often implemented by countries using the words of the *Budapest Convention*. Seventy percent (70%) of the countries have implemented illegal access to computer system in line with the *Budapest Convention*.

Considering that illegal access is globally recognized as an offense against the confidentiality, integrity and availability

---

<sup>70</sup> <http://conventions.coe.int/Treaty/EN/Reports/html/185.htm>.

of computer data and systems, the Philippines has no reason not to include the same in R.A. No. 10175.

**IV. Section 4(a)(3) of the  
Cybercrime Prevention Act  
of 2012 does not violate the  
exercise of free speech.**

---

**(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.<sup>71</sup>

Section 4(a)(3) penalizes conduct, not speech. It criminalizes another form of hacking, *i.e.*, the unauthorized destruction of data, computer programs, or supporting documents residing or existing internal or external to a computer, computer system or computer network.

Petitioners Reyes, et al. argue that Section 4(a)(3), **a)** intrudes the area of protected speech as it suffers from overbreadth, constitutes prior restraint and content-based restrictions; **b)** suffers from vagueness. According to petitioners Reyes, the term computer data is broad and includes any electronic document or electronic data message

---

<sup>71</sup> Section 4(a)(3) also refers to what is commonly labelled as "hacking".

stored in any device or online. Petitioners Reyes, et al. believe that internet memes and online posters that may alter photos of politicians or statements of politician will be covered by the assailed provision.<sup>72</sup>

Section 4(a)(3) regulates data interference because it is socially harmful **conduct**. It does not regulate, prevent or punish speech.

Data interference is also a *Budapest Convention* offense against the confidentiality, integrity and availability of computer data and systems. Article 4 of the Convention reads:

**Article 4 – Data interference**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

---

<sup>72</sup> G.R. No. 203407, pp. 12-15.

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

Article 4 of the *Budapest Convention*, in criminalizing the destruction of data, aims “to provide computer data and computer programs with protection similar to that enjoyed by” tangible objects against the intentional infliction of damage.<sup>73</sup> The protected legal interest here is the integrity and proper functioning or use of stored computer data or computer programs.

Seventy percent (70%) of the parties, signatories and states with invitation to accede to the *Budapest Convention* have criminalized the offense of data interference.<sup>74</sup>

**V. Section 4(a)(6) of the Cybercrime Prevention Act of 2012 does not violate the equal protection clause of the Constitution.**

---

**(6) Cyber-squatting.**- The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy 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;

---

<sup>73</sup> Keyser, Mike, “The Council of Europe Convention”, *Journal of Transnational Law & Policy*, Vol. 12:2, p. 302, citing Explanatory Note of the Comm. Of Ministers (of the Convention on Cybercrime), 109<sup>th</sup> Sess. (adopted on November 8, 2001), Art. 1(a), par. 23.

<sup>74</sup> The Global State of Cybercrime Legislation by Cristina Schulman, [www.coe.int/cybercrime](http://www.coe.int/cybercrime).

- (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.

Petitioner PIFA contends that failure to narrowly tailor Section 4(a)(6) will cause a user using his real name to suffer more than those who use *aliases*, or take the name of another in satire, parody, or any other literary device.<sup>75</sup>

Petitioner PIFA is mistaken.

The difficulty in tracing the real perpetrators of cybercrimes or persons using *aliases* cannot be a deterrent to the passage and implementation of a law. The cybercrime law was enacted precisely to allow law enforcement authorities to go after the perpetrators of cybercrime whether they be known or hidden under the veil of pseudonyms. Besides, a person who commits a crime using his actual name is as guilty as a person who commits a crime using an *alias*.

---

<sup>75</sup> G.R. No. 203518, Petition, p. 50.

Section 4(a)(6) is intended to protect intellectual property and other property rights of persons, natural or juridical and at the same time stem the use of deceptive internet addresses. The activity prohibited by Section 4(a)(c) is usually perpetrated by criminals engaged in online financial fraud.

Cybersquatting is the oldest and best-known *form of nuisance in cyber space*. Cybersquatters will generally either offer to sell the name back to the trademark owner for an extortionate price, or make money from internet traffic accidentally landing on their page. The practice is a nuisance for the growing number of companies that do business over the internet and are loath to lose valuable traffic to rogue websites.

In the United States, the **Anticybersquatting Consumer Protection Act (ACPA)**, 15 U.S.C. § 1125(d), was enacted in 1999 and it established a cause of action for registering, trafficking in, or using a domain name confusingly similar to, or dilutive of, a trademark or personal name. The law was designed to thwart "cybersquatters" who register Internet domain names containing trademarks with no intention of creating a legitimate web site, but instead plan to sell the

domain name to the trademark owner or a third party. Under the ACPA, a trademark owner may bring a cause of action against a domain name registrant who (1) has a bad faith intent to profit from the mark and (2) registers, traffics in, or uses a domain name that is (a) identical or confusingly similar to a distinctive mark, (b) identical or confusingly similar to or dilutive of a famous mark, or (c) is a trademark protected by 18 U.S.C. § 706 (marks involving the Red Cross) or 36 U.S.C. § 220506 (marks relating to the "Olympics").

In **Virtual Works, Inc. vs. Volkswagen of America, Inc.** (a dispute over the domain vw.net), the U.S. Fourth Circuit Court of Appeals created a common law requirement that the cybersquatter must exhibit a bad faith intent in order to confer liability. This means that domain names bearing close resemblance to trademarked names are not per se impermissible. Rather, the domain name must have been registered with the bad faith intent to later sell it to the trademark holder.<sup>76</sup>

Similarly, Section 4(a)(6) punishes cybersquatting only if they are made in bad faith to profit, mislead, destroy

---

<sup>76</sup> 238 F.3d 264.

reputation, and deprive others from registering the same. Consequently, petitioner's contention, that failure to narrowly tailor Section 4(a)(6) has caused a user using his real name to suffer more than those who use aliases, or take the name of another in satire, parody, or any other literary device, is baseless.

In our jurisdiction, Article 694 of the Civil Code defines a nuisance as "any act, omission, establishment, condition of property, or anything else which shocks, defies, or disregards decency or morality," the remedies for which are a prosecution under the Revised Penal Code or any local ordinance, a civil action, or abatement without judicial proceedings.<sup>77</sup>

**(b) Computer-related Offenses:**

**VI. Section 4(b)(3) of R.A. No. 10175 does not violate the Bill of Rights.**

---

**(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.<sup>78</sup>

---

<sup>77</sup> Ang Ladlad LGBT Party vs. COMELEC, 618 SCRA 32 [2010].

<sup>78</sup> R.A. No. 10175.



Petitioners Reyes, et al. argue that “identity theft,” as defined under Section 4(b)(3), suffers from overbreadth and constitutes prior restraint on free speech because mere “acquisition,” “possession,” or “transfer” of identifying information *without right* is prohibited. As such, petitioners claim, “persons must exercise restraint in order not to be personally aware of the contents of such identifying information in his possession”.<sup>79</sup> Petitioners Reyes, et al. also posit that the use of “identifying information” available in *Facebook* such as a politician’s full name, age, education background, parents, children, etc. even for journalistic investigations will constitute identity theft.<sup>80</sup> Hence, petitioners Reyes, et al. conclude that Section 4 (b)(3) constitutes a prior restraint on the press in its information gathering activities for journalistic and news purposes.

Petitioners Reyes’ arguments are misleading.

The term “identity theft” has gained an accepted technical definition long before the advent of the information age. Identity theft is defined under Oxford Dictionary as the

---

<sup>79</sup> G.R. No. 203407, pp. 15-16.

<sup>80</sup> G.R. No. 203407, p. 16.

fraudulent acquisitorial use of a person's private identifying information, usually for financial gain.

In the U.S., "Identity Theft" is committed when someone uses another person's identifying information, such as name, social security number, or credit card number, without permission, to commit fraud or any criminal act.<sup>81</sup>

Phishing and spoofing are common means of cyber identity theft. Phishing refers to fraudulent electronic communications appearing to be genuine legitimate source inducing the recipient to disclose sensitive "identifying information."<sup>82</sup> On the other hand, spoofing refers to a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.<sup>83</sup>

In the Philippines, Congress recently enacted R.A. No. 10173, or the Data Privacy Act of 2012, to ensure that

---

<sup>81</sup> [www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html](http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html)

<sup>82</sup> pp. 126-128, First Edition, Cyberlaw: Law of the Internet and Information Technology, Brian Craig.

<sup>83</sup> <http://www.cwu.edu/~its/cybersecurity/def.html> last accessed on November 13, 2012.

personal information in information and communications system in the government and private sector are secured and protected.

Identity theft covers “identifying information.” It does not simply refer to one’s personal profile but pertains to a combination of data which can uniquely identify a person and may include a personal identification number.

In the U.S., identifying information includes any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any – (1) Name, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (3) Unique electronic identification number, address or routing code; or (4) Telecommunication identifying information or access device.<sup>84</sup>

---

<sup>84</sup> Fair Credit Reporting Act (16 C.F.R. §603.2).

In the Philippines, personal information refers to 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 identity holding the information, or when put together with other information would directly and certainly identify an individual.<sup>85</sup>

Section 4(b)(3) is intended to protect one's right to privacy and to protect one's right to property. The offender's rights to privacy and protected speech are irrelevant in computer-related offenses.

Petitioners Reyes' fear focus on the words "acquisition" "transfer" and "possession" in relation to journalists' fundamental work of reporting information is unfounded.<sup>86</sup>

Petitioners Reyes' fear can be easily soothed when the principle *noscitur a sociis* is applied. By *noscitur a sociis*, the correct construction of a word or phrase susceptible of various meanings may be made clear and specific by considering the company of words in which it is found or with which it is

---

<sup>85</sup> Section 3(g), R.A. No. 10173.

<sup>86</sup> G.R. No. 203407, p. 16.

associated.<sup>87</sup> Here, the words “intentional acquisition,” “transfer,” and “possession,” must be associated with the term “identity theft” and must be understood to mean any such acts done with the intention of appropriating another’s identity for acquisitorial use.

Journalists can take comfort that the government continues to recognize the privilege of journalists to gather information as R.A. No. 10173, the Data Privacy Act of 2012, exempts from its coverage personal information processed for journalistic, artistic, literary or research purposes.<sup>88</sup>

**(c) Content-related Offenses.**

**VII. Section 4(c)(1) does not abridge freedom of expression nor is it a prior restraint on the exercise of said freedom.**

---

**(1) Cybersex.**- the wilful 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 favour or consideration.

Petitioner Guingona claims that Section 4(c)(1) is legally

---

<sup>87</sup> People vs. Flores, 629 SCRA 478 [2010].

<sup>88</sup> Section 4(d), R.A. No. 10173.

infirm for being too broad. According to petitioner Guingona, the law “failed to provide for the parameters that constitute the crime and “did not provide any standard or limitation, as it encompasses any and all sexual acts, for as long as they were exhibited online. As such, mere publication of nude materials in the internet is already considered punishable even if they are classified as artistic works”.<sup>89</sup>

Petitioner Guingona further argues that R.A. No. 10175 legislates morality. According to him, a law to be effective should not plead to the legislator to determine what is moral and what is not as defining standards of morality is not a function of congress but should be better left in the hands of our religious leaders.”<sup>90</sup>

Petitioner PIFA, likewise, claims that the definition of “cybersex” is vague as it a) makes no distinction on what is obscene and what is merely indecent; b) one cannot determine what types of persons are regulated, what conduct is prohibited or what punishment may be imposed; and c) it includes the punishment of “lascivious exhibition of sexual

---

<sup>89</sup> G.R. No. 203351, pp. 26-28.

<sup>90</sup> G.R. No. 203351, p. 29.

organs or sexual activity” even in commercially available cinematic films which feature adult subject matter and artistic, literary or scientific material and instructional material for married couples.<sup>91</sup>

Congress, in enacting Section 4(c)(1), seeks to punish cyber prostitution, white slave trade and pornography for favour and consideration. This includes interactive prostitution and pornography, *i.e.*, by webcam. This is confirmed by the discussion during the Bicameral Conference Committee:

THE CHAIRMAN (REP. TINGA). You know, after reviewing the House and the Senate versions, there is a difference in how we define cybersex, ‘no. The Senate version reads, “The wilful 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.” Would that mean that I would need to be engaging in a business for it to be considered illegal?

The House version says, “Includes any form of interactive prostitution and other forms of obscenity through the cyberspace as the primary channel with the use of webcams by inviting people either here or other country to watch men, women and children perform sexual acts.” What I am trying to get at, Mr. Chairman, is we have to make it clear that you are engaging in a business for it to be illegal.

THE CHAIRMAN (SEN. ANGARA). That’s correct.

THE CHAIRMAN (REP. TINGA). The mere showcasing

---

<sup>91</sup> G.R. No. 203518, p. 21.

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

of the sexual act between two parties would not constitute an illegal act.

THE CHAIRMAN (SEN. ANGARA). That's correct.

THE CHAIRMAN (REP. TINGA). That's what you were saying here, Mr. Chairman.

THE CHAIRMAN (SEN. ANGARA). That's correct. And that's why we have this classification. This classification "for favour or consideration," yeah.

THE CHAIRMAN (REP. TINGA). Agreed, Mr. Chairman.

So that will be enough to -

THE CHAIRMAN (SEN. ANGARA). Yes, yeah. So that private showing, as you cited, between and among two private persons would not constitute an illegal act although that may be a form of obscenity to some.

THE CHAIRMAN (REP. TINGA). Agreed, Mr. Chairman.

(pp. 5-6, Bicameral Conference Committee)

Petitioner Guingona and PIFA do not challenge the right of the State to punish prostitution, white slavery and pornography. They merely raised issues about the distinction between what is "obscene," "indecent" and "artistic".<sup>92</sup> The last word on this matter was expressed by this Honorable Court in **Pita vs. Court of Appeals**.<sup>93</sup> In that case, the petitioner did not dare challenge "the right of the State, in the legitimate exercise of police power to suppress smut - provided it is smut." As to what constitutes "smut", or merely "obscene", this Honorable Court held that the same be

---

<sup>92</sup> G.R. No. 203359, pp. 27-28; G.R. No. 203518, p. 21.

<sup>93</sup> 178 SCRA 512 [1989].



determined by a judge subject to judicial review. This Honorable Court said that, in a proper case, the defendant can raise “defenses, under the Constitution,” including freedom of expression. Thus, the matters raised by petitioners Guingona and PIFA are matters of defenses to be raised in the event of a trial.

The risks to publishers of publishing “nude materials” in the internet or to film producers of creating “artistic works” is no different or greater than the “risks” presently confronting them under Article 201 of the Revised Penal Code. Since 1932, Article 201 punishes “obscene publications and exhibitions and indecent shows.” To date, Article 201 has not been declared unconstitutional.

**VIII. Section 4(c)(3) does not violate the constitutional provisions on deprivation of one’s right to liberty without due process and equal protection of the law.**

---

**(3) Unsolicited Commercial Communications.**

— The transmission of commercial electronic communication with the use of computer system which seek to advertise, sell, or offer for sale products and services are prohibited unless:

XXX      XXX      XXX

Petitioners Alab, et al. argue that there is no compelling interest to regulate “unsolicited advertisement” as it does not affect the efficiency of computers.<sup>94</sup> Allegedly, “unsolicited advertisements” or SPAM is a “form of expression” and the interest affected is the right to liberty of the concerned individual - a fundamental right.<sup>95</sup>

Petitioner PIFA, et al. also assert that Section 4(c)(3) failed to meet the requirements of equal protection as it does not distinguish between unsolicited commercial communication systems and that done through other communication system such as telemarketing. They contend that Section 4(c)(3) prohibits and penalizes commercial acts of marketing and sales which are perfectly legitimate. They add that Section 4(c)(3) treats unsolicited private commercial communication and unsolicited private political communication differently.<sup>96</sup>

Unsolicited Commercial Communications or “SPAM” is outlawed because worldwide, SPAM messages waste the

---

<sup>94</sup> G.R. No. 203306, p. 11.

<sup>95</sup> G.R. No. 203306, p. 12.

<sup>96</sup> G.R. No. 203518, Petition, pp. 46-48.

storage and network capacities of Internet Service Providers (ISPs), and are simply offensive to the unwilling recipient.<sup>97</sup>

Flooding the internet with useless and nuisance bulk emails burden the internet networks and reduce the efficiency of commerce and technology. They also result to tremendous losses in revenue if left unpunished.<sup>98</sup>

Spam can, in principle, properly be considered a type of trespass—since it is a means by which the spammer uninvitedly use another’s property.<sup>99</sup> Spam can also be considered a nuisance because of its substantial interference with the peaceful enjoyment of a property, which causes considerable amount of damage consisting of clogged disc spaces, network congestions, financial loss and loss of productivity.<sup>100</sup>

Spamming is at most commercial speech not worthy of constitutional protection. It is intrusive to the privacy of the internet users and unlawfully appropriates the storage and network of ISPs without compensation and for profit. The

---

<sup>97</sup> <http://www.britannica.com/EBchecked/topic/130595/cybercrime/235710/Spam>.

<sup>98</sup> Record of the Philippine Senate, taken on May 11, 2011, pp. 38-44; and Record taken on September 12, 2011, pp. 22-23.

<sup>99</sup> <http://archive.mises.org/4201/spyware-and-trespass>.

<sup>100</sup> Snehashish Ghosh, Spam: A Cyber Age Nuisance, March 26, 2011.

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

government has an interest in the free, efficient flow of information, commercial technology in the Internet.<sup>101</sup>

**IX. Section 4(c)(4), making expressed the use of computer system as another avenue of committing libel under Article 353 of the Revised Penal Code, does not violate the 1987 Constitution.**

---

**(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.

**b. Section 4(c)(4) is valid, complete and clear, and does not violate due process of law.**

---

Petitioners<sup>102</sup> claim that Section 4(c)(4) of R.A. No. 10175 violates due process for being vague and overbroad as there is no comprehensible standard provided by the law. Allegedly, Section 4(c)(4) failed to provide fair notice of the conduct to avoid as it did not define who may be liable; how such person committing the act may be identified; and how and when they

---

<sup>101</sup> See *Lee Central Hudson Gas and Electric Corp. vs. Public Service Commission*, 447 US 557 [1980].

<sup>102</sup> *Palatino, et al.; Reyes, et al.; Castillo; Adonis, et al.; Biraogo; Cruz, et al.; PBA and NPCP.*

may be criminally liable.

Petitioners' contentions are untenable.

Online libel is not a new crime. Online libel is a crime punishable under the Articles 353, in relation to Article 355 of the Revised Penal Code. Section 4(c)(4) just made express an avenue<sup>103</sup> already covered by the term "similar means" under Article 355, to keep up with the times. This would immediately negate the oft-used defense that libel committed through the use of the internet is not punishable. That said, the relevant provisions of the Revised Penal Code on libel and jurisprudence on the subject gives ascertainable standards and well-defined parameters which would enable an accused to determine the nature of his violation.

Libel has the same meaning and has the same elements no matter the means of publication. The computer system is just another means of "publication."

Libel is defined as a public and malicious imputation of a

---

<sup>103</sup> Senator Angara pointed out that cyberspace is just a new avenue for publicizing or communicating a libelous statement which is subject to prosecution and punishment as defined by the Revised Penal Code.

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 (**Article 353 of the Revised Penal Code**).

“Libel committed through a computer system” can therefore be defined as a 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,<sup>104</sup> committed through a computer system or any other similar means which may be devised in the future.<sup>105</sup>

**b) Section 4(c)(4) does not abridge the constitutional right to free speech, freedom of expression and of the press.**

---

Petitioners<sup>106</sup> assail the constitutionality of Section 4(c)(4) on the ground that it abridges the constitutionally protected

---

<sup>104</sup> Article 353 of the Revised Penal Code.

<sup>105</sup> Section 4(c)(4) of R.A. No. 10175.

<sup>106</sup> Cruz, G.R. No. 203469; Philippine Bar Association, G.R. No. 203501; National Press Club, G.R. No. 203515; Biraogo, G.R. No. 203299; Adonis, G.R. No. 203378; Sta.

right to free speech, of expression and of the press under Section 4, Article III of the 1987 Constitution on the following grounds:

1. It is a form of prior restraint to regulate freedom of speech, expression, and of the press exercised through the internet or communications technologies; and
2. It broadens the definition of libel by adding the use of computer system or any other similar means, and in the process singles out netizens in their chosen medium of expression.

Libel is not constitutionally protected speech.

As this Honorable Court held in **Guingging vs. Court of**

**Appeals:**<sup>107</sup>

Criminal libel laws at face value, might strike as laws passed that abridge the freedom of speech, expression, or the press. Whatever seeming conflict between these two precepts has long been judicially resolved with the doctrine that libelous speech does not fall within the ambit of constitutional protection.

**Chaplinsky vs. New Hampshire,**<sup>108</sup> explained at length:

There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never

---

Maria, G.R. No. 203440 and National Union of Journalists of the Philippines, G.R. No. 203453.

<sup>107</sup> 471 SCRA 196 [2005].

<sup>108</sup> 315 U.S. 568, 571-572 [1942].

been thought to raise any constitutional problem. These include xxx the libelous xxx. It has been well observed that such utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to test truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality.

As above discussed, online libel is punishable under Article 353 of the Revised Penal Code. The modes of publication is listed under Article 355, thus:

**Article 355. Libel by Means 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 *prisión correccional* in its minimum and medium periods or a fine ranging from 200 to 6,000 pesos, or both, in addition to the civil action which may be brought by the offended party.

Publication, as an element of libel, has been given a wide range of application by this Honorable Court. In **U.S. vs. Escobañas**,<sup>109</sup> it was held that an unsealed defamatory letter dropped in a street in front of a store where the parties lived is libelous. In **Magno vs. People**,<sup>110</sup> this Honorable Court, citing **People vs. Silvela**,<sup>111</sup> held that sending an unsealed libelous letter to the offended party constitutes publication. In **People**

---

<sup>109</sup> 12 Phil. 80 [1908].

<sup>110</sup> 480 SCRA 276 [2006], citing also *People vs. Silvela*, 103 Phil. 773 [1958].

<sup>111</sup> 103 Phil. 773 [1958]



**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

**vs. Casten**,<sup>112</sup> the Court of Appeals ruled that defamatory statements made on television constitutes libel, even if television is not one of the modes enumerated under Article 355, as it squarely falls within that category other similar means. This Honorable Court has said that a statement made to a person other than the person defamed is sufficient to constitute publication. In short, publication is not limited to mass media, print, television or radio. Publication in libel means making the defamatory matter, after it has been written, known to someone other than the person to whom it has been written.<sup>113</sup>

Thus, even without Section 4(c)(4), a 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, made with the use of computer system already constitutes libel.

---

<sup>112</sup> CA G.R. No. 07924-CR, promulgated December 13, 1974.

<sup>113</sup> Alcantara vs. People, 517 SCRA 74 [2007].

In fact, in **Bonifacio vs. RTC of Makati**,<sup>114</sup> an online libel case, this Honorable Court did not rule on the ground raised by petitioners therein that “the acts alleged in the information” are not punishable by law.<sup>115</sup> Instead, this Honorable Court ruled that venue was improperly laid and recognized that “there would be no way of determining the *situs* of printing and first publication” “when it pertains to defamatory material appearing in a website in the internet”:

If the circumstances as to where the libel was printed and first published are used by the offended party as basis for the venue in the criminal action, the Information must allege with particularity where the defamatory article was printed and first published, as evidenced or supported by, for instance, the address of their editorial or business offices in the case of newspapers, magazines or serial publications. This pre-condition becomes necessary in order to forestall any inclination to harass.

The same measure cannot be reasonably expected when it pertains to defamatory material appearing on a website on the internet as there would be no way of determining the *situs* of its printing and first publication. To credit Gimenez’s premise of equating his first access to the defamatory article on petitioners’ website in Makati with “printing and first publication” would spawn the very ills that the amendment to Article 360 of the RPC sought to discourage and prevent. It hardly requires much imagination to see the chaos that would ensue in situations where the website’s author or writer, a blogger or anyone who posts messages therein could be sued for libel anywhere in the Philippines that the

---

<sup>114</sup> 620 SCRA 268 [2010].

<sup>115</sup> Then Secretary of Justice Raul Gonzalez reversed the finding of probable cause opining that the crime of “internet libel” was non-existent and hence, the respondents could not be charged with libel under Article 353 of the Revised Penal Code. Judge Cesar Untalan of the Regional Trial Court in Makati disagreed and found that probable cause existed; *supra* at p. 276.

private complainant may have allegedly accessed the offending website.<sup>116</sup>

It is, thus, clear that prior to the enactment of R.A. No. 10175, online libel was already a crime punished under Articles 353 to 362 of the Revised Penal Code, and to date, has never been declared unconstitutional on the ground of abridging the right to free speech, freedom of expression and of the press.

**c. Section 4(c)(4) of R.A. No. 10175 does not violate the Equal Protection Clause of the Constitution.**

-----

Petitioners Alam, Adonis, Guingona, National Press Club, Castillo, and Philippine Bar Association, alleged that Section 4(c)(4) violates the equal protection clause of the 1987 Constitution as it is discriminatory because there is no reason to make cyber libel a crime, distinct from libel punishable by the Revised Penal Code.

Petitioners' arguments constitute an unwitting admission that online defamation is a crime even under the Revised Penal Code.

---

<sup>116</sup> *Supra* at p. 281; underscoring supplied.

But it must be emphasized that cyber libel was not given a higher penalty under Section 4(c)(4). Notably, R.A. No. 10175 did not provide for a distinct penalty for Section 4(c)(4). The “one degree higher penalty” was imposed under Section 6 for all the crimes under the Revised Penal Code and special penal laws committed with the use of ICT. For an orderly discussion and to avoid repetition, the refutation of this argument will be made under the arguments for Section 6.

**d. Section 4(c)(4) of R.A. No. 10175 is not *ex post facto* law.**  
-----

Petitioners Biraogo and PBA argue that Section 4(c)(4) is an *ex post facto* legislation since the phrase “similar means which may be devised in the future,” found under Section 4(c)(4), covers all future developments in communications technology.<sup>117</sup> On the other hand, petitioner PIFA is of the view that Section 4(c)(4) constitutes *ex post facto* legislation because a person responsible for uploading a certain data or

---

<sup>117</sup> Biraogo’s Petition (G.R. No. 203299), p. 13 and Philippine Bar Association’s Petition (G.R. No. 203501), pp. 16-17.

digital content before October 3, 2012 may be held liable under the Cybercrime Prevention Act.<sup>118</sup>

The arguments lack basis.

*Ex post facto* law is one which punishes an act, which when committed was not yet criminal.<sup>119</sup> As previously discussed, libel committed by using computer system is punishable under Articles 353-362 of the Revised Penal Code. Section 4(c)(4) merely made expressed another avenue for the commission of libel. Said addition does not make said provision *ex post facto*. Libelous statements made through computer systems prior to the enactment of R.A. No. 10175 are already considered punishable under the Revised Penal Code.

By the same token, neither would the use of the phrase “similar means which may be devised in the future” made Section 4(c)(4) *ex post facto*.

**e. Section 4(c)(4) does not violate the Philippines’ international treaty obligations.**

---

<sup>118</sup> Philippine Internet Freedom Alliance’s Petition (G.R. No. 203518), pp. 54-55.

<sup>119</sup> Salvador vs. Mapa, 539 SCRA 34 [2007].

Petitioners Adonis, et al.,<sup>120</sup> Reyes, et al.<sup>121</sup> and PIFA<sup>122</sup> claim that criminalizing libel published through the internet violates the Philippines' treaty obligation under Article 19 of the International Covenant on Civil and Political Rights (ICCPR). Petitioners Adonis, Reyes and PIFA cite the view of the UN Human Rights Committee (UNHRC) that: a) the imprisonment imposed on Mr. Adonis for libel under the Philippines Revised Penal Code is "*incompatible with Article 19, paragraph three of the International Covenant on Civil Political Rights,*" or freedom of expression; and, b) the Philippines is "*also under an obligation to take steps to prevent similar violations occurring in the future, including by reviewing the relevant libel legislation.*"

PIFA also argues that:

162. The criminalization of libel over the Internet and other communications media violates the rights of free speech, free expression and press freedom enshrined in the Universal Declaration of Human Rights...<sup>123</sup>

PIFA points out that:

164. On 29 June 2012, the Human Rights

---

<sup>120</sup> G.R. No. 203378, pp. 21-27.

<sup>121</sup> G.R. No. 203407, p. 21.

<sup>122</sup> G.R. No. 203518, pp. 52-54.

<sup>123</sup> *Ibid*, pp. 52-53.

Council of the United Nations General Assembly passed Resolution No. A/HRC/20/L.13 **recognizing the freedom of expression on the Internet as a basic human right.** Thus, a member-State of the United Nations, such as the Philippines, now has an obligation *erga omnes*, that is, an *obligation owed to humanity*, to promote and protect the right to freedom of opinion and expression on the Internet on the part of its citizens. The same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with Articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.<sup>124</sup>

Libel is unprotected speech. It remains to be a crime in many nations.

The text of the ICCPR does not mandate the decriminalization of libel. In fact, ICCPR recognizes that the freedom of expression carries with it special duties and responsibilities and may be subject to certain restrictions as are provided by law and as are necessary for the respect of the rights or reputations of others, *viz*:

#### Article 19

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the

---

<sup>124</sup> *Ibid*, p. 53.

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

- (a) For respect of the rights or reputations of others;

- (b) For the protection of national security or of public order (order public), or of public health or morals.

Articles 353-362 of the Revised Penal Code and Section 4(c)(4) of R.A. No. 10175 were enacted for the respect of the rights and reputations of others.

Further, the UNHRC statement did not mandate the decriminalization of libel but only advised States to “consider the decriminalization of libel.” The UNHRC said:

- 50) Recalling its General Comment No. 34, the UN body stressed that defamations laws should not stifle freedom of expression. “Penal defamation laws should include defense of truth,” it said.

- 51) “[In] comments about public figures, consideration should be given to avoiding penalties or otherwise rendering unlawful untrue statements that have been published in error but without malice. In any event, a public interest in the subject matter of the criticism should be recognized as a defense. State parties should consider the decriminalization of libel (Adonis’ Petition, p. 21).



There is, therefore, no basis to the contention that Section 4(c)(4) violates Philippines' international obligations.

**X. Section 5, which penalizes the acts of aiding or abetting and attempting the commission of cybercrimes, is valid and constitutional.**

---

Section 5 does not suffer from vagueness.

---

Section 5 does not constitute prior restraint or subsequent punishment in the exercise of the freedom of expression over the internet.

---

**Section 5. Other Offenses.** - The following acts shall also constitute an offense:

- (a) Aiding or Abetting in the Commission of Cybercrime.-Any person who wilfully 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 wilfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

Petitioners argue that Section 5 violates due process of law and constitute prior restraint on the exercise of the freedom of expression for:

- a. Being overbroad as it lacks comprehensible standards and fails to define, describe and enumerate with specificity the persons who will be held criminally responsible and when they will

become liable (Petitioners Cruz, Reyes, PBA and National Press Club; Adonis, NUJP).

- b. Rendering irrelevant the defense of good faith, lack of intention to injure and ignorance of the law (Petitioners Sta. Maria, et al.)

The terms *aiding*, *abetting* and *attempt* are clear and need no express definition.

A criminal statute does not become void just because of its reference to general terms, or in this case, of its use of the terms “aid” or “abet,” and “attempt.” There is no constitutional or statutory duty on the part of the lawmakers to define every word in a law, as long as the intent can be gathered from the entire act.<sup>125</sup>

The test in determining the ambiguity of a statute is whether the words convey a sufficiently definite warning with respect to the proscribed conduct based on common understanding and practice.<sup>126</sup> The words of a statute are interpreted in their plain and ordinary meaning.<sup>127</sup> There is no need for absolute precision in order to appreciate the words

---

<sup>125</sup> Perez vs. LPG Refillers Association of the Philippines, Inc., 531 SCRA 431 [2007].

<sup>126</sup> Estrada vs. Sandiganbayan, supra, citing State v. Hill, 189 Kan 403, 369 P2d 365, 91 ALR2d 750.

<sup>127</sup> Mustang Lumber, Inc. vs. Court of Appeals, 257 SCRA 430 [1996].

of the statute. A reasonable degree of certainty and flexibility, with clearly delineated limitations, is acceptable.<sup>128</sup>

### Aiding and abetting

First, penalizing people who are aiding and abetting in the commission of a crime is not a new concept in Philippine laws. There are various laws<sup>129</sup> penalizing the “aiding and abetting” of criminal acts.

Second, a person who is guilty of *aiding* and *abetting* is simply considered an accomplice. Section 5, when read

---

<sup>128</sup> Estrada vs. Sandiganbayan, *supra*.

- <sup>129</sup> a. Republic Act No. 3701, in relation to Section 2751, Revised Administrative Code. - Unlawfully occupying or destroying public forest;
- b. Presidential Decree No. 532, Section 2 - Piracy and highway robbery/brigandage;
- c. National Internal Revenue Code, Section 253(b). - Committing a crime penalized by the National Internal Revenue Code;
- d. Tariff and Custom Code, Section 3609. - Fraudulently removing or concealing warehoused articles;
- e. Labor Code, Article 264(b), in relation to Article 272. - Obstructing, impeding or interfering with by force, violence, coercion, threats or intimidation any peaceful picketing by employees during any labor controversy or in the exercise of the right to self-organization;
- f. Republic Act No. 8293, Section 217.- Infringing copyright;
- g. Republic Act No. 8799, Section 51.3. - Violating the Securities Regulation Code;
- h. Republic Act No. 9266, Section 23(d). - Practicing architecture in the Philippines without authorization;
- i. Republic Act No. 10088, Section 3(c). - Possessing, using and/or controlling audiovisual recording devices without authorization.

together with Section 8, last paragraph of R.A. No. 10175, shows that a person guilty of aiding and abetting is penalized as an accomplice.

**Section 8** reads:

xxx xxx xxx

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.

As defined under the Revised Penal Code, accomplices are those persons who, not being principals, cooperate in the execution of the offense by previous or simultaneous acts.<sup>130</sup>

To be considered an accomplice, the offender must have known of the criminal design of the principal by direct participation and concurs therein, that he cooperates in the execution of the offense by prior or simultaneous acts, and there is a relation between the acts done by the principal and those of the accomplice.<sup>131</sup>

---

<sup>130</sup> Article 18, Revised Penal Code.

<sup>131</sup> People vs. Tamayo, 44 Phil 38 [1922].

Section 5, in relation to Section 8, is consistent with the decision of this Honorable Court in **People vs. De Vera**,<sup>132</sup> which regarded the person who *aided or abetted* in the commission of the crime<sup>133</sup> as an accomplice, having knowledge of the criminal design, concurs with the principal's purpose by performing previous or simultaneous acts not indispensable to the commission of the crime.<sup>134</sup>

Attempted Felony

Similarly, there is no confusion in the use of the term "attempt" under paragraph 2 of Section 5, R.A. No. 10175. The Revised Penal Code defines "attempt", as follows:

**Article 6. Consummated, frustrated, and attempted felonies. -**

xxx                      xxx                      xxx

There is an attempt when the offender commences the commission of a felony directly by overt acts, and does not perform all the acts of execution which should produce the felony by reason of some cause or accident other than his own spontaneous desistance.

---

<sup>132</sup> 312 SCRA 640 [1999].

<sup>133</sup> Murder.

<sup>134</sup> People vs. Tamayo, 389 SCRA 540 [2002].

Attempt, aiding and abetting are concepts in the *Budapest Convention* which treaty countries are to adopt in their cybercrime law:

**Article 11 – Attempt and aiding or abetting**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.
3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Petitioners Adonis<sup>135</sup> and NUJP<sup>136</sup> posit that Section 5 violates freedom of expression for lack of comprehensible standard to guide the authorities and citizens as to what acts constitute “aiding or abetting in the commission of libel” or

---

<sup>135</sup> G.R. No. 203378, pp. 27-28.

<sup>136</sup> G.R. No. 203453, pp. 10-12

“attempted libel” and such being the case, violates freedom of expression for being a prior restraint.

The laws on libel (under Article 353 to 362 of the Revised Penal Code) and now as contained in Section 4(c)4 of R.A. No. 10175 do not operate as “prior restraints” to speech. These libel acts provide for “subsequent punishment”. Thus, petitioners are free to exercise their right to speak out. If what they express is libelous, then they risk subsequent oppunishment.

**XI. Section 6 is valid.**

-----

Section 6. All crimes as 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 portions 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 as the case may be.

The first sentence of Section 6 declares that all acts which are considered a crime if committed in the real world are also treated as a crime if committed in the cyber world.<sup>137</sup>

---

<sup>137</sup> Bicameral Conference Committee on Disagreeing Provisions of Senate Bill 2796 and House Bill No. 5808 (Cybercrime Prevention Act of 2012), May 31, 2012, pp. 175-179.

The second sentence of Section 6 effectively makes the commission of a crime with the use of ICT a qualifying circumstance.

**The first sentence of Section 6 is clear. The term Information and Communication Technology has long been used; its short version is I.T. or Information Technology.**

-----

Petitioners claim that Section 6 is overbroad as it failed to define the term “Information and Communications Technology.”

That R.A. No. 10175 did not define “Information and Communications Technology” (ICT) would not make Section 6 void for being vague.

Information and Communications Technology is just the full text of *Information Technology* and has been in use since the 1980s. Information and Communication Technology is a technical term defined as an *electronic means of capturing, processing, storing, and disseminating information.*



Our law's definition of Information and Communications Technology as found in Executive Order No. 269<sup>138</sup> dated January 12, 2004 provides a similar, albeit more detailed, definition of *Information and Communications Technology*, viz: the totality of *electronic means to collect, store, process and present information to end-users in support of their activities and which consists, among others, of computer systems, office systems and consumer electronics, as well as networked information infrastructure, the components of which include the telephone system, the Internet, fax machines and computers.* Reference can also be made to Republic Act No. 8792's<sup>139</sup> definition of *Information and Communications System*: A system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or in which data is recorded or stored and any procedures related to the recording or stage of electronic data message or electronic document.

The presumption is that the language used in a statute, which has a technical or well known legal meaning, is used in

---

<sup>138</sup> Creating the Commission on Information and Communications Technology.

<sup>139</sup> E-Commerce Act.

that sense by legislation.<sup>140</sup>

Thus, the first sentence of Section 6 is clear, delimited in scope and is valid.

The first sentence of Section 6 does not violate Section 21, Article III of the 1987 Constitution.  
-----

According to petitioner Disini, et al., the cybercrimes defined and punished under Section 6 of R. A. No. 10175 are absolutely identical to the crimes defined in the Revised Penal Code and special laws. Since the acts and essential elements of both offenses are basically the same, an accused faces the possibility of being punished twice for the same offense, in violation of the constitutional prohibition of double jeopardy.<sup>141</sup>

**Article III, Section 21** provides:

Section 21. 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.

---

<sup>140</sup> Estrada vs. Sandiganbayan, 369 SCRA 394, 436-438 [2001].

<sup>141</sup> Disini Petition, p. 20.

The rule on double jeopardy has a settled meaning in this jurisdiction. Double jeopardy is inherently a “procedural defense” or a shield that forbids a defendant from being subjected to the possibility of being penalized twice, or being tried again on the same (or similar) charge following a legitimate acquittal or conviction.<sup>142</sup> It is not a constitutional prohibition against laws that may present possible prosecution for an offense penalized under other laws or statutes.

Hence, the mere possibility of prosecution for two separate offenses by itself would not render either law unconstitutional.

The second sentence of Section 6 does not suffer from any constitutional infirmity.

---



---

<sup>142</sup> In the case of **Guerrero vs. Hon. Court of Appeals, 257 SCRA 703, 712 [1996]**:

It is a settled rule that to raise the defense of double jeopardy, the following requisites must concur: (1) a first jeopardy must have attached prior to the second; (2) the first jeopardy must have been validly terminated; and (3) the second jeopardy must be for the same offense, or the second offense includes or is necessarily included in the offense charged in the first information, or is an attempt to commit the same or is a frustration thereof (citations omitted).

And legal jeopardy attaches only: (a) upon a valid indictment; (b) before a competent court; (c) after arraignment; (d) a valid plea having been entered; and e) the case was dismissed or otherwise terminated without the express consent of the accused (citation omitted).

Petitioner NUJP argues that by making the use of ICT a qualifying circumstance, Congress made an omnibus amendment not covered by the title and scope of the bill and not deliberated in Congress and public hearings.

Petitioner's argument is without merit.

This Honorable Court, as early as 1947 and reiterated in subsequent cases, has subscribed to the conclusiveness of an enrolled bill. It has consistently refused to invalidate a law or provision of law, on the ground that the bill from which it originated contained no such provision, and was merely inserted by the Bicameral Conference Committee of both Houses.<sup>143</sup> In **Tolentino vs. Secretary of Finance**,<sup>144</sup> this Honorable Court refused to depart from the rule that an enrolled copy of a bill is conclusive, not only of its provisions, but also of its due enactment:

Whatever doubts there may be as to the formal validity of Republic Act No. 7716 must be resolved in its favor. Our cases manifest firm adherence to the rule that an enrolled copy of a bill is conclusive not only of its provisions but also of its due enactment. Not even claims that a proposed constitutional amendment was invalid because the requisite votes for

---

<sup>143</sup> *Central Bank Employees Association vs. Bangko Sentral ng Pilipinas*, 446 SCRA 299, 346 [2004].

<sup>144</sup> 235 SCRA 630, 672 [1994].

its approval had not been obtained or that certain provisions of a statute had been “smuggled” in the printing of the bill have moved or persuaded us to look behind the proceedings of a coequal branch of the government. There is no reason now to depart from this rule.

No claim is here made that the “enrolled bill” rule is absolute. In fact in one case we “went behind” an enrolled bill and consulted the Journal to determine whether certain provisions of a statute had been approved by the Senate in view of the fact that the President of the Senate himself, who had signed the enrolled bill, admitted a mistake and withdrew his signature, so that in effect there was no longer an enrolled bill to consider.

But where allegations that the constitutional procedures for the passage of bills have not been observed have no more basis than another allegation that the Conference Committee “surreptitiously” inserted provisions into a bill which it had prepared, we should decline the invitation to go behind the enrolled copy of the bill. To disregard the “enrolled bill” rule in such cases would be to disregard the respect due the other two departments of our government.

- b. Section 6 of R.A. No. 10175 does not violate the equal protection clause of the 1987 Constitution.
- 

Petitioners Guingona,<sup>145</sup> Sta. Maria,<sup>146</sup> Cruz,<sup>147</sup> PBA<sup>148</sup> and NPCP<sup>149</sup> argue that Section 6 violates the equal protection clause because it discriminates against those who use ICT. Allegedly, there is no substantial distinction between offenders committing a crime using ICT and those who do not use ICT.

---

<sup>145</sup> G.R. No. 203359, p. 19.

<sup>146</sup> G.R. No. 203440, pp. 29-31.

<sup>147</sup> G.R. No. 203469, pp. 65-68.

<sup>148</sup> G.R. No. 203501, pp. 22-25.

<sup>149</sup> G.R. No. 203515, pp. 20-21.

Also, petitioners claim that the increased penalty is not germane to the purpose of the law nor is there a reasonable connection between the increased penalty and the use of ICT. Petitioners call special attention to the effects of Section 6 on the crime of libel.

The equal protection clause means that "no person or class of persons shall be deprived of the same protection of laws which is enjoyed by other persons or other classes in the same place and in like circumstances." The guaranty of the equal protection of the laws is not violated by a legislation based on a reasonable classification. The equal protection clause, therefore, does not preclude classification of individuals who may be accorded different treatment under the law as long as the classification is reasonable and not arbitrary.<sup>150</sup>

The classification, to be reasonable, (1) must rest on substantial distinctions; (2) must be germane to the purposes

---

<sup>150</sup> NPC vs. Pinatubo, 616 SCRA 611, 621 [2010].

of the law; (3) must not be limited to existing conditions only; and (4) must apply equally to all members of the same class.<sup>151</sup>

The classification rests on substantial distinction.

**Scope of reach.** Cybercrimes are not bound by time and geography.<sup>152</sup> These crimes, accomplished through ICT, can reach the world instantly without limitation as to its scope. On the other hand, ordinary crimes are limited by resources, distance, border security, various regulations, and time.

**Accessibility.** Cybercrimes are easily committed due to its accessibility. There are approximately thirty (30) million internet users in the country and hundreds of millions more in the world.

Thus, due to this nature of the internet, any person with minimal equipment and once online can have the opportunity to create worldwide chaos or intrude into the privacy of others without much obstacle.

---

<sup>151</sup> People vs. Cayat, 68 Phil. 12, 18 [1939].

<sup>152</sup> Sponsorship speech of Sen. Edgardo Angara, May 11, 2011 (Minutes of the Senate, p. 39).

**Effect.** Criminal purpose is easily accomplished with greater impact than ordinary crimes. Any person, once online, may perform activities which can affect private lives or public safety. On the other hand, the commission of ordinary crimes have physical limitations.

The classification is germane to the purpose of the law.

As previously explained, R.A. No. 10175 was enacted for several reasons, the principal of which is to maintain minimum standards of decency, morality and civility in human society. The qualifying circumstance of use of ICT was included in Section 6 as a means to deter the increasing commission of cyber offenses. Senator Angara, in his sponsorship speech<sup>153</sup> observed that “Internet usage – as well as abuse – has skyrocketed in the absence of any appropriate legal framework. The ubiquity of the Internet has given rise to the proliferation of cybercrime... This can be attributed to the inherent lack of security of the Internet architecture and the relative anonymity of users. The increase in penalties under

---

<sup>153</sup> From the Senate Journal, May 11, 2011, pp. 1321-1323; <http://www.gov.ph/2012/10/03/for-the-record-public-records-of-senate-deliberations-on-the-cybercrime-prevention-bill/>.



Section 6 of R.A. No. 10175 is, therefore, justified and consistent with the policy of the law.

This Honorable Court has upheld as valid qualifying circumstances, objects of a crime (coconut) because of the industry that it is supposed to protect and develop (coconut industry);<sup>154</sup> and tools of the crime (unlicensed firearm, negotiable instruments, specifically commercial checks<sup>155</sup>).

Here, ICT, as a tool of the crime, is treated as a qualifying circumstance to deter the commission of crimes using said platform so as to protect and develop the ICT Industry. Congress, as seen in Section 2 of R.A. No. 10175, 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 and sees the need to protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and

---

<sup>154</sup> People vs. Isnain, 85 Phil. 648, 650-651 [1950].

<sup>155</sup> Lim vs. People, 390 SCRA 194, 199 [2002].

availability of information and data stored therein, from all forms of misuse, abuse, and illegal access.<sup>156</sup>

Petitioners do not question the presence of the third and fourth elements as in fact, the classification is not be limited to existing conditions only; and it applies equally to all members of the same class, *i.e.*, criminal offenders using ICT.

Effect of the Second Sentence  
of Section 6 on the crime of  
Libel.

---

Petitioners Adonis, et al.<sup>157</sup> and Biraogo<sup>158</sup> contend that by providing for use of ICT as a qualifying circumstance, Section 6 effectively disqualified those convicted of cyber libel from applying for probation. Petitioners point out that those convicted for ordinary libel can apply for probation since it is punishable only by *prision correccional* in its minimum to medium periods, or for six (6) months and one (1) day to six (6) years.

---

<sup>156</sup> Section 2, RA 10175.

<sup>157</sup> G.R. No. 203378, p. 33.

<sup>158</sup> G.R. No. 203299, p. 11.

Probation is a special privilege by the State.<sup>159</sup> The State's discretion to penalize criminal acts cannot be stifled just to make sure that crimes which are probationable would always remain to be so.

But more importantly, petitioners overlooked Supreme Court Circular No. 08-08, *Guidelines in the Observance of a Rule of Preference in the Imposition of Penalties in Libel Cases*. This Honorable Court advised judges that certain cases that this Honorable Court has resolved "indicate an emergent rule of preference for the imposition of fine only rather than imprisonment in libel cases under the circumstances therein specified." "The Judges concerned may, in the exercise of sound discretion, and taking into consideration the peculiar circumstances of each case, determine whether the imposition of a fine alone would best serve the interests of justice or whether forbearing to impose imprisonment would depreciate the seriousness of the offense, work violence on the social order, or otherwise be contrary to the imperatives of justice."

---

<sup>159</sup> Sable vs. People, 584 SCRA 619, 625-626 [2009].

c. Section 6 of R.A. No. 10175  
is not a bill of attainder

---

Petitioners NUJP, et al. contend that Section 6 is a bill of attainder because those who use information and communication technology are singled out and subjected to a new penalty that is one degree higher.

Section 6 does not fall under the category of a bill of attainder. A bill of attainder is a legislative act which inflicts punishment without judicial trial.<sup>160</sup> Essential to a bill of attainder are a specification of certain individuals or a group of individuals, the imposition of a punishment, penal or otherwise, and the lack of judicial trial.<sup>161</sup>

None are present in R.A. No. 10175.

Section 6 does not seek to punish a status or a group but the action, *i.e.*, using ICT to commit crimes.

---

<sup>160</sup> Bernas, Joaquin J., *The 1987 Constitution of the Republic of the Philippines: A Commentary*, 2003 Edition, p. 604.

<sup>161</sup> *Bureau of Customs Employees Association vs. Hon. Teves*, 661 SCRA 589, 614-615 [2011].

Section 6 does not punish internet users without the benefit of a trial. It merely makes the use of ICT a qualifying circumstance for all crimes and offenses. All elements, including the use of ICT, must be established by proof beyond reasonable doubt.

**XII. Section 7 of R.A. No. 10175  
does not violate Section 21,  
Article III of the 1987  
Constitution.**

-----

**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.

Petitioners Guingona, Disini, et al. and Adonis, et al. alleged that Section 7 of R.A. No. 10175 is a direct violation of the constitutional prohibition against double jeopardy. Petitioners are of the view that penalizing one for both the print and the online versions of papers they write for is a clear violation of the right against double jeopardy.<sup>162</sup>

Section 7 merely expressly included in R.A. No. 10175 what is actually a settled doctrine, *i.e.*, “a single set of acts

---

<sup>162</sup> Adonis Petition, p. 35; Bayan Petition, pp. 22-23.

may be prosecuted and penalized simultaneously under two laws, a special law and the Revised Penal Code.”<sup>163</sup>

Admittedly, the doctrine is subject to conditions. In **People vs. Doriquez, 24 SCRA 163, 171 [1968]**, this Honorable Court said that when two different laws defines 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, involve some important act which is not essential element of the other, the protection against double jeopardy is only for the same offense.

But Section 7 does not remove the above condition. Hence, if a person is prosecuted for two offenses, for the same act, and he believes that the elements of both crimes are exactly alike and there is no essential element of one which is not present in the other, he can raise it as a defense. But it is not right to burden this Honorable Court, at this point, to try all different permutations to determine if each cybercrime has the same essential elements as the other offenses punishable under the Revised Penal Code and special laws.

---

<sup>163</sup> People vs. Sandoval, 254 SCRA 436 [1996].

The wisdom of the “as applied doctrine” precisely addresses such types of arguments.

On the other hand, petitioners’ concerns on whether an article printed online would be separately penalized from an article printed on the broadsheet were not brought about by R.A. No. 10175. In libel, the settled rule is each publication constitutes a single offense.<sup>164</sup>

**XIII. The fixing of penalties for the violation of statutes is primarily a legislative function.**

-----

**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 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.

---

<sup>164</sup> Soriano vs. IAC, 167 SCRA 222, 228 [1988].

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

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.

Petitioner Biraogo argues that the penalty provisions in R.A. No. 10175 are unconstitutional citing **Reno vs. American Civil Liberties Union**<sup>165</sup> wherein the United States Supreme Court declared a statute prohibiting the use of

---

<sup>165</sup> 521 U.S. 844 [1997].



telecommunications devise to transmit obscene materials unconstitutional.<sup>166</sup>

Petitioner Biraogo's arguments do not deserve merit.

In **Baylosis vs. Chavez**,<sup>167</sup> the Honorable Court declared that it is within the power of the legislature to determine what acts or omissions other than those set out in the Revised Penal Code or other existing statutes are to be condemned as separate, individual crimes and what penalties should be attached thereto. This legislative power is not diluted or improperly wielded simply because at some prior time the act or omission was but an element or ingredient of another offense, or might usually have been connected with another crime.

Petitioner could not rely on **Reno vs. American Civil Liberties Union**<sup>168</sup> since resort to foreign jurisprudence would be proper only if no law or jurisprudence is available locally to

---

<sup>166</sup> Biraogo's Petition (G.R. No. 203299), pp. 21-22.

<sup>167</sup> 202 SCRA 405, 415-416 [1991].

<sup>168</sup> *Supra*.

settle a controversy and even in the absence of local statute and case law, foreign jurisprudence is only persuasive.<sup>169</sup>

Also, in **Reno**, the United States Supreme Court said, in refusing to validate the content-based restriction, that there were no special justifications in regulating cyberspace because the internet is not as “invasive” as radio or television.<sup>170</sup> However, this is no longer the case.

**Reno** was a 1997 U.S. Supreme Court case which is no longer applicable in our time. Notably, the United States ratified the *Budapest Convention on Cybercrime* in August 2006. Since then, US has actively participated in the fight against cybercrime.

In addition, this Honorable Court, in **People vs. Punto**, **68 Phil. 481, 482 [1939]**, said that the punishment provided by a wholesome purpose, namely to effectuate early repression of an evil that, in the opinion of the Legislature, undermines the social, moral and economic growth of the nation and is “. . . best calculated to answer the ends of precaution necessary to deter others from the commission of like offenses . . .”

---

<sup>169</sup> *Philippine Airlines, Inc. vs. Court of Appeals*, 185 SCRA 110, 121 [1990].

<sup>170</sup> *Janet Reno vs. Civil Liberties Union*, 521 U.S. 868 [1997].

In the Philippines, an estimated twenty nine (29) million Filipinos use the internet. From desk top computers, tablets, cellular phones and laptops, Filipinos have a wide array of gadgets which connect them to the internet. As more Filipinos leave for better economic opportunities abroad, the internet becomes an indispensable tool for families to stay in touch.<sup>171</sup> Given the reach and speed by which information is disseminated, and the ease of committing illegal acts on the internet, the government found a need to regulate it. Thus, R.A. No. 10175 was enacted to serve as deterrent to potential cyber criminals.

**XIV. The collection of traffic data  
will not result in any search  
or seizure of petitioners'  
persons and/or properties.**

---

**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.

XXX XXX XXX

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

---

<sup>171</sup> Smart, Need for Connectivity grows as more Filipinos Work Abroad, accessed on October 23, 2012 from <https://secure.smart.com.ph/corporate/newsroom/I4AOFW.htm>.

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 will be 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 Reyes,<sup>172</sup> NUJP,<sup>173</sup> Castillo,<sup>174</sup> Cruz<sup>175</sup> and PBA<sup>176</sup> claim that Section 12, which allows the real-time collection of **traffic data** sans warrant and based only on due cause, infringes their rights to privacy and their rights against unreasonable searches and seizures.

Petitioners fail to understand the **nature** of traffic data and how its ephemeral character presents law enforcement challenges that require extraordinary measures. Understandably, they mistakenly conclude that its collection constitutes an unjustified infringement on their right against unreasonable searches and seizures.

---

<sup>172</sup> G.R. No. 203407, pp. 24-25.

<sup>173</sup> G.R. No. 203453, pp. 16-17.

<sup>174</sup> G.R. No. 203454, pp. 11-14.

<sup>175</sup> G.R. No. 203469, pp. 39-41.

<sup>176</sup> G.R. No. 203501, p. 31.

Respondents and the OSG submit: (1) The constitutional right to privacy does **not** extend to traffic data; (2) Real-time collection of traffic data is akin to the collection of information derived from visual surveillance of an **open** physical space. As such, it does **not** intrude into “private” space, and thus its retrieval does not call for the constitutional requirement of a prior judicial warrant.

#### Nature of Traffic Data

Every communications network features two types of information: the contents of communications (“**content/inside information**”), and the addressing and routing information that the networks use to deliver the contents of communications (“**envelope/outside information.**”)<sup>177</sup> In *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn’t*, Harvard University Professor and commentator on US Internet surveillance laws, Orin S. Kerr explains:

---

<sup>177</sup> Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn’t*. *Northwestern University Law Review*, Vol. 97, No. 2, p. 611, (2003).

Biraogo, et al. vs. NBI, et al.

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

**The essential distinction between content and envelope information remains constant across different technologies, from postal mail to email.** With postal mail, the content information is the letter itself, stored safely inside its envelope. The envelope information is the information derived from the outside of the envelope, including the mailing and return addresses, the stamp and postmark, and the size and weight of the envelope when sealed.

Similar distinctions exist for telephone conversations. The content information for a telephone call is the actual conversation between participants that can be captured by an audio recording of the call. The envelope information includes the number the caller dials, the number from which the caller dials, the time of the call and its duration. This calling information is not visible in the same way that the envelope of the letter is, but it equates roughly with the information derived from the envelope of a letter. In both cases, the envelope information contains to-and-from addressing, data about the time the communication was sent, and information about the communication's size and length.

These principles translate to the Internet quite readily in the case of email. The content information for an email is the message in the body of the email itself, much like the phone conversation or the letter in the envelope. The email also carries addressing information in a "mail header." Mail headers are digital postmarks that accompany every email and carry information about the delivery of the mail. Many email programs show users only some of this information by default, but can be configured to reveal the full mail header.<sup>178</sup>

Traffic data are *data generated by computers in the chain of communication to route a communication from its origin to its*

---

<sup>178</sup> Id., pp. 611-612.

*destination*.<sup>179</sup> By nature, and as expressed in Section 3(p) of R.A. No. 10175, traffic data is **non-content** data that consists of the origin, destination, route, time and date of the communication. It is **auxiliary** to the communication and is necessarily shared with a service provider who is a third party.<sup>180</sup>

*Ephemeral traffic data:  
challenges for law enforcement*

---

The collection and preservation of traffic data is an important investigative measure which, considering the fleeting life of internet data, require extraordinary legal measures. As the *Explanatory Note* of the *Budapest Convention on Cybercrime* (upon which R.A. No. 10175 is largely based) explains:

§ 217. Traditionally, the collection of traffic data in respect of telecommunications (e.g., telephone conversations) has been a useful investigative tool to determine the source or destination (e.g., telephone numbers) and related data (e.g., time, date and duration) of various types of illegal communications (e.g., criminal threats and harassment, criminal conspiracy, fraudulent misrepresentations) and of communications affording evidence of past or future crimes (e.g., drug trafficking, murder, economic crimes, etc.)

---

<sup>179</sup> Explanatory Note on the Convention on Cybercrime, ETS No. 185, par. 28.

<sup>180</sup> Id.

§ 218. Computer communications can constitute or afford evidence of the same types of criminality. However, given that computer technology is capable of transmitting vast quantities of data, including written text, visual images and sound, it also has **greater potential** for committing crimes involving distribution of illegal content (e.g., child pornography). Likewise, as computers can store vast quantities of data, often of a private nature, **the potential for harm**, whether economic, social or personal, can be **significant** if the integrity of this data is interfered with. Furthermore, as the science of computer technology is founded on the processing of data, both as an end product and as part of its operational function (e.g., execution of computer programs), any interference with this data can have disastrous effects on the proper operation of computer systems. When an illegal distribution of child pornography, illegal access to a computer system or interference with the proper functioning of the computer system or the integrity of data, is committed, particularly from a distance such as through the Internet, **it is necessary and crucial to trace the route of the communications back to the victim of the perpetrator. Therefore, the ability to collect traffic data in respect of computer communications is just as, if not more, important as it is in respect of purely traditional telecommunications. This investigative technique can correlate time, date and source and destination of the suspect's communications with the time of the intrusions into the systems of victims, identify other victims or show links with associates.**<sup>181</sup>

Considering the breadth and speed of technology, time becomes of utmost essence in cybercrime law enforcement. Anything that is posted online can be accessed by anyone with

---

<sup>181</sup> Explanatory Note to the Convention on Cybercrime, ETS 185.



great facility while anything that is stored in a local computer or to any of its system can be disseminated or destroyed just as easily. Indeed, the maximum exposure the Internet provides is a significant consideration in crafting the provisions of R.A. No. 10175.

In a way, it can be argued that the rationale for the collection of traffic data is analogous to the one used and recognized in a valid warrantless search of a moving vehicle and to that under exigent circumstances.

The warrantless search of a moving vehicle had been justified on the ground that the **mobility** of motor vehicles makes it possible for the vehicle sought to be searched to move out of the locality or jurisdiction in which the warrant must be sought.<sup>182</sup> Over the years, the rules governing search and seizure have been steadily liberalized whenever a moving vehicle is the object of the search on the basis of practicality. **“This is so considering that before a warrant could be obtained, the place, things and persons to be searched must be described to the satisfaction of the issuing judge — a requirement which borders on the impossible in**

---

<sup>182</sup> People vs. Mariacos, 621 SCRA 327, 339-342 [2010].

**instances where moving vehicle is used to transport contraband from one place to another with impunity.”<sup>183</sup>**

This exception is easy to understand. A search warrant may readily be obtained when the search is made in a store, dwelling house or other immobile structure. But it is impracticable to obtain a warrant when the search is conducted on a mobile ship, on an aircraft, or in other motor vehicles since they can quickly be moved out of the locality or jurisdiction where the warrant must be sought.<sup>184</sup>

In the same vein, in cybercrime law enforcement under existing technology, it is quite impossible (not to mention impractical) to describe the place, things and persons to be searched because what is originally posted or made available online or stored in local computer systems may be changed, removed or passed on to another instantaneously.

So, too, a warrantless seizure of computer data is valid on the ground of exigency. The requirement of a warrant to collect traffic data, which, in the first place, involves non-

---

<sup>183</sup> *Ibid*, p. 341.

<sup>184</sup> *Ibid*, p. 342.

content information, could hamper or derail prosecution altogether.

The technological revolution, which encompasses the “electronic highway” where numerous forms of communication and services are interrelated and interconnected through the sharing of common transmission media and carriers, has altered the sphere of criminal law and criminal procedure. The ever-expanding network of communications opens new doors for criminal activity in respect of both traditional offences and new technological crimes. Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques.<sup>185</sup>

Prescinding from its nature as “outside” and “envelope” information, the retrieval of traffic data does not require, as a matter of constitutional law, the application with, and issuance by, a judge of a search and seizure warrant. This is because traffic data does not constitute “inside” information. Its collection does not involve any intrusion into an

---

<sup>185</sup> Section 2 – Procedural Law, 132, Explanatory Report, Convention on Cybercrime, ETS No. 185.

individual’s private space. Its timely collection, an exigency inherent in the ephemeral character of computer data, argues against the requirement of a judicial warrant.

Rule against unreasonable searches and seizures

---

**Section 2, Article III of the Constitution** requires:

Section 2.

The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.

Section 2, Article III mandates that where there is an intrusion into “persons, houses, papers and effects,” it must be conducted under the authority of a warrant issued by a disinterested person, who could be trusted to act with sufficient discretion to weigh the competing demands of personal liberty *vis-à-vis* those of governmental interest in law enforcement.<sup>186</sup>

---

<sup>186</sup> Posadas vs. Ombudsman, 341 SCRA 388, 397-398 [2000].

Conversely, where there is no intrusion, no search or seizure, the warrant requirement does not apply. This is because “(m)erely to observe and look at that which is in plain sight is not a ‘search.’ It is not a search to observe that which occurs **openly** in a public place and which is **fully disclosed to visual observation.**”<sup>187</sup> The principle therefore is that there is no necessity to secure a warrant where there is no **invasion** of personal space. Thus, surveillance activities, limited as they are to surveillance over “outside” facts/spaces, do not require the prior issuance of a warrant. In fact, in our jurisdiction, it appears that the practice has been to conduct surveillance activities for purposes of determining probable cause without the necessity for a warrant application.<sup>188</sup>

The Court in *Valmonte vs. Villa* said that there is as yet no cause for the application of the constitutional rule when what are involved are routine checks consisting of “a brief question or two.” **For as long as the vehicle is neither searched nor its occupants subjected to a body search, and the inspection of the vehicle is limited to a visual search, said routine checks cannot be regarded as violative of an individual’s right against unreasonable searches and seizures.**<sup>189</sup>

(Emphasis and underscoring supplied)

<sup>187</sup> Bobby Chadwick vs. State of Tennessee, 4 29 S.W.2d 135 (1968) cited by the Philippine Supreme Court in the case People of the Philippines vs. Andre Marti, 193 SCRA 57, 66 [1991].

<sup>188</sup> People of the Philippines vs. Arnold Martinez y Angeles, et al., 637 SCRA 791, 806 [2010] citing People of the Philippines vs. Zenaida Bolasa, et al., 321 SCRA 459, 466 [1999]. See also Benjamin Kho, et al. vs. Hon. Roberto Makalintal, et al., 306 SCRA 70 [1999].

<sup>189</sup> Joaquin G. Bernas, S.J., The 1987 Constitution of the Philippines: A Commentary, (Manila: Rex Bookstore), pp. 168.

Thus, while government intrusion into **personal** (“**inside**”) spaces must be by authority of a court warrant, no such requirement applies for governmental actions short of actual intrusion into personal space, (*i.e.*, surveillance of **public/”outside**” spaces.) This is also necessitated by practical considerations. Requiring law enforcement authorities to obtain a warrant for the conduct of **non-intrusive activities** (*i.e.*, over “outside” information) in relation to a criminal investigation would seriously disrupt (if not unduly burden) the conduct of routine law enforcement.

*Inside/Outside Distinction  
translated in the  
communications network  
context*

---

The “**inside/outside**” distinction in the context of physical spaces (for purposes of applicability of warrant requirement) is functionally translated in the communications network setting into a distinction between “**content/non-content**” information. In *Applying the Fourth Amendment to the Internet: A General Approach*, Professor Kerr writes:

Biraogo, et al. vs. NBI, et al.

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

This translation is accurate because the distinction between content and non-content information serves the same function online that the inside/outside distinction serves in the physical world. Non-content information is analogous to outside information; it concerns where a person is and where a person is going. Consider what the police can learn by watching a suspect in public. Investigating officers can watch the suspect leave home and go to different places. They can watch him go to lunch, go to work, and go to the park; they can watch him drive home; and they can watch him park the car and go inside. In effect, this is to/from information about the person's own whereabouts.

On the other hand, content information is analogous to inside information. The contents of communications reveal the substance of our thinking when we assume no one else is around. It is the space for reflection and self-expression when we take steps to limit the audience to a specific person or even just to ourselves. The contents of Internet communications are designed to be hidden from those other than the recipients, much like property stored inside a home is hidden from those who do not live with us. xxx

The connection between content/non-content on the Internet and inside/outside in the physical world is not a coincidence. Addressing information is itself a network substitute for outside information, and contents are a network substitute for inside information. Recall the basic function of communications networks: they are systems that send and receive communications remotely so that its users do not have to deliver or pick up the communications themselves. The non-content information is the information the network uses to deliver communications, consisting of where the communication originated, where it must be delivered, and in some cases, the path of delivery. This information is generated in lieu of what would occur in public; it is information about the path and timing of delivery. In contrast, the contents are the private communications themselves that would have been inside in a physical network.

Consider the postal network. In a world without the postal network, a person who wanted to deliver a letter would have to deliver it himself. He would take the letter, travel to the destination, and leave the letter there. All of this would be open to surveillance; if the

police wanted to, they could watch him travel from the origin to the destination point. Envelope addressing information is the information that a person tells the postal network when he wants the postal network to do the job for him. The sender gives the postal service the information it needs, such as the "to" address and "from" address. The postal service then does the work: the mail carrier is the one who goes out and travels from the origin to the destination, using the information provided by the sender. In effect, the use of the service of the network substitutes the previously public information about the person's whereabouts in the delivery of the letter for the addressing information of the letter's delivery. The outside information turns into the addressing information, and the inside information becomes the content of the communication.

In light of this, a technologically neutral way to translate the Fourth Amendment from the physical world to the Internet would be to treat government collection of the contents of communications as analogous to the government collection of information inside and the collection of non-content information as analogous to the collection of information outside.

xxx

xxx

xxx

This approach would mirror the line that the Fourth Amendment imposes in the physical world. **In the physical world, the inside/outside distinction strikes a sensible balance. It generally lets the government observe where people go, when they go, and to whom they are communicating while protecting the actual substance of their speech from government observation without a warrant unless the speech is made in a setting open to the public. The content/non-content distinction preserves that function. It generally lets the government observe where people go in a virtual sense, and to observe when and with whom communications occur.** The essentially transactional information that would occur in public in a physical world has been replaced by the non-content information in a network environment, and the content/non-content line preserves that treatment. At the same time, the distinction permits individuals to communicate with others in ways that keep the government at bay. The Fourth Amendment ends up respecting private rights where people can share their most



**private thoughts without government interference  
both in the physical space and cyberspace alike.**<sup>190</sup>

(Emphasis and underscoring supplied)

Thus, because traffic data is non-content (“outside”) information, the Constitution does not require that it may be collected only upon the prior authority of a judicial warrant.

**Katz vs. United States**<sup>191</sup> held that the existence of privacy right under prior decisions involved a two-fold requirement: first, that a person has exhibited an actual (subjective) expectation of privacy; and second, that the expectation be one that society is prepared to recognize as reasonable (objective).<sup>192</sup>

Traffic data is non-content/”envelope”/“outside” information. In contrast to content information, traffic data are information necessarily shared with third parties (other than the ultimate recipient) for purposes of delivering a particular communication. As such, and unlike content information, a person has no legitimate expectation of privacy in said

---

<sup>190</sup> Kerr, Orin S. Applying the Fourth Amendment to the Internet: A General Approach, *Stanford Law Review*, 62 STAN. L. REV. 1005 (2010), pp. 1020-1022.

<sup>191</sup> 389 U.S. 347 [1967].

<sup>192</sup> At p. 361, concurring opinion of Justice Harlan.

“outside” information revealed or is available to third parties.<sup>193</sup>

Inasmuch as traffic data is “shared” or made available to service providers who, in turn, log, store and keep traffic data for business purposes, petitioners cannot claim any legitimate expectation of privacy over traffic data.

In **Smith vs. Maryland**,<sup>194</sup> the US Supreme Court analyzed privacy rights vis-à-vis non-invasive technological surveillance of police authorities. In **Smith**, a telephone company, at police request, installed at its central office a pen register for Smith’s home phone number. A pen register is a device that will record all the numbers dialed by a person in a phone. *It does not overhear oral communications and does not indicate whether calls are actually completed.*<sup>195</sup> Smith, at that time, was being investigated for robbery. He moved to suppress “all fruits derived from” the pen register. The Maryland district court denied the motion. The US Supreme Court affirmed the denial and held:

---

<sup>193</sup> Smith vs. Maryland, 442 U.S. 735 [1979].

<sup>194</sup> *Supra.*

<sup>195</sup> United States vs. New York Tel. Co., 434 U.S. 159, 161 [1977].

Biraogo, et al. vs. NBI, et al.

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

xxx First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies for purposes of checking billing operations, detecting fraud, and preventing violations of law.<sup>196</sup>

Respondents submit that the analysis and logic of **Smith** apply with equal cogency to Section 3, Article III of our Constitution. Petitioners cannot claim a legitimate expectation of privacy with respect to the traffic data generated on account of their use of a particular technology/device.

*Internet communications necessitate sharing content and data with third parties.*<sup>197</sup> In an ordinary Internet transaction, each data or message is copied and routed through a series of interdependent networks.<sup>198</sup> When a person uses the Internet, he will connect to an Internet Service Provider which will link the user to a host of his desired websites.<sup>199</sup> In the process,

<sup>196</sup> Smith vs. Maryland, *supra*, at p. 742, citing United States vs. New York Tel. Co., *supra*, at pp. 174-175; emphasis and underscoring supplied.

<sup>197</sup> Jonathan Brick, *Internet Communications Privacy Rights*, *New Jersey Law Journal*, Volume 195, No 11, Index 793.

<sup>198</sup> *Supra*.

<sup>199</sup> <http://www.mediacollege.com/internet/intro/thewww2.html>, October 24, 2012.

**data and information are necessarily duplicated by third parties in the chain of transaction.**<sup>200</sup> Hence, each party receives, logs and stores the data to form the sequence of Internet activity.

Petitioners, in using technology to communicate, relay information to a service provide to complete the transaction. Clearly, the involvement of the service provider, a third party, in their communications defeats any claim of expectation of privacy.

Even assuming, for the sake of argument, that petitioners harbored subjective expectations of privacy over traffic data, by authority of the analysis enunciated in **Katz**, such expectation is not one society is prepared to recognize as reasonable.

When a person uses the services of a service provider, he is aware that the provider has access to traffic data generated on account of his use of a particular communication service and, thus, he assumes the risk that the latter may, *under*

---

<sup>200</sup> *Supra*.

*certain conditions*, reveal said traffic data to government authorities.

In the analogous case of **US vs. Miller**,<sup>201</sup> the US Supreme Court denied a motion to suppress bank documents alleged to have been unlawfully seized. Therein respondent alleged that, although the documents were seized by virtue of several subpoenae, said subpoenae were defective for having been issued only by a United States Attorney and not by a court. The US Supreme Court held:

...the depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. **This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities,** even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.<sup>202</sup>

Petitioners know, or ought to know, that traffic data over their communications are necessarily “shared” with service providers. While they may assume that the data is not easily accessible to the public as a whole, they cannot insist that said information, which — more often than not — is part of the business records of the service providers, will remain

---

<sup>201</sup> 425 U.S. 435 [1976].

<sup>202</sup> At p. 443; citations omitted; underscoring and emphasis supplied.

undiscoverable forever. When they chose to use the service, they took on the risk that traffic data covering their communications may be revealed to parties other than the service provider.

On this score, we again quote **Smith**:

xxx Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.<sup>203</sup>

**Smith** and **Miller** emphasize with compelling analytic persuasiveness and common sense cogency that no privacy can be expected from information revealed to or made available to a third party.

In our jurisdiction, this Honorable Court, in the context of secrecy of bank deposits, has declined to declare that Section 2, Article III of the Constitution creates a constitutional right to privacy governing bank accounts. This Honorable Court would go only so far as to recognize a right to privacy

---

<sup>203</sup> At p. 743.

governing bank accounts sourced on statute. In the 2008 case of **Republic of the Philippines vs. Hon. Antonio M. Eugenio, et al.**,<sup>204</sup> this Honorable Court held:

The Court's construction of Section 11 of the AMLA is undoubtedly influenced by right to privacy considerations. If sustained, petitioner's argument that a bank account may be inspected by the government following an *ex parte* proceeding about which the depositor would know nothing would have significant implications on the right to privacy, a right innately cherished by all notwithstanding the legally recognized exceptions thereto. The notion that the government could be so empowered is cause for concern of any individual who values the right to privacy which, after all, embodies even the right to be "let alone," the most comprehensive of rights and the right most valued by civilized people. (Citation omitted)

**One might assume that the constitutional dimension of the right to privacy, as applied to bank deposits, warrants our present inquiry. We decline to do so.** Admittedly, that question has proved controversial in American jurisprudence. Notably, the United States Supreme Court in *U.S. v. Miller* held that there was no legitimate expectation of privacy as to the bank records of a depositor. Moreover, **the text of our Constitution has not bothered with the triviality of allocating specific rights peculiar to bank deposits.**(Citations omitted.)

**However, sufficient for our purposes, we can assert there is a right to privacy governing bank accounts in the Philippines, and that such right finds application to the case at bar. The source of such right is statutory, expressed as it is in R.A. No. 1405 otherwise known as the Bank Secrecy Act of 1955.** The right to privacy is enshrined in Section 2 of that law, to wit:

SECTION 2. All deposits of whatever nature with banks or banking institutions in the Philippines including investments in bonds issued by the Government of the Philippines, its political subdivisions and its instrumentalities, are hereby considered as of

---

<sup>204</sup> 545 SCRA 384 [2008].

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

an absolutely confidential nature and may not be examined, inquired or looked into by any person, government official, bureau or office, except upon written permission of the depositor, or in cases of impeachment, or upon order of a competent court in cases of bribery or dereliction of duty of public officials, or in cases where the money deposited or invested is the subject matter of the litigation.<sup>205</sup>

The core submission of respondents, on the challenges to the constitutionality of Section 12 of R.A. No. 10175 on traffic data, is that based on the analysis and logic of **Miller** and **Eugenio**, the Constitution does not provide for a constitutional right to privacy over traffic data. But as next discussed, there is a privacy right to traffic data based on statute, *i.e.*, R.A. No. 10175.

**R.A. No. 10175 provides for statutory protection; OSG is of the view that the Congress may consider more robust procedural protections.**

---

Congress legislated, under Section 12 of R.A. No. 10175, a statutory right of privacy over the traffic data.

---

<sup>205</sup> Emphasis and underscoring supplied.



Section 12 of R.A. No. 10175 conditions the collection of traffic data to a prior determination by “law enforcement authorities” that there is “due cause” for its collection. There is no requirement though of judicial intervention. The threshold to trigger collection is low, namely “due cause.” Also, a wide range of law enforcement personnel will determine due cause. Still, this type of statutory protection, minimalist as it is, is some protection. Were there no statutory protection at all, the discretion of law enforcement authorities would be unfettered.

The American experience with traffic data collection is instructive.

To recall, **Smith** validated the use of a pen register to record calls made to and from a particular phone number without need of a court warrant. In apparent response to the **Smith** ruling, the US Congress enacted the Pen Register Law in 1986 to cover telephone traffic data surveillance and, much later, the USA Patriot Act in 2001 to cover internet traffic data surveillance.

Both laws gave the people of the United States of America statutory rights over the collection of **non-content** electronic information. They both require the issuance of a judicial warrant before electronic surveillance over traffic data may be conducted. Under the Pen Register Law, a United States Attorney must first apply with a judge for the issuance of a judicial warrant. The court may issue the warrant only after the United States Attorney's certification, that the "information likely to be obtained" is "relevant to the subject investigation."<sup>206</sup> Only then can law enforcement authorities commence traffic data surveillance. The USA Patriot Act, enacted more than twenty years later, expanded the allowable use of the collection of traffic data to include Internet communications under the same conditions, *i.e.*, requiring a judicial warrant.<sup>207</sup>

Petitioners Reyes,<sup>208</sup> NUJP,<sup>209</sup> PIFA<sup>210</sup> and PBA<sup>211</sup> question Section 12 on account of the "sweeping authority" given to law enforcement agents" and/or the "low threshold" necessary to trigger the real-time collection of traffic data. Indeed,

---

<sup>206</sup> 18 U.S.C.A. § 3123.

<sup>207</sup> § 216 of the USA Patriot Act.

<sup>208</sup> G.R. No. 203407, pp. 24-25.

<sup>209</sup> G.R. No. 203453, p. 16.

<sup>210</sup> G.R. No. 203518, pp. 27-29.

<sup>211</sup> G.R. No. 203501, pp. 32-33 and 40.

-----

compared to the statutory protection afforded by the Pen Register Act and the Patriot Act to the collection of traffic data in the United States, the protection afforded by Section 12 of R.A. No. 10175 is minimal. Still, they afford some protection. The decision on the range of the protection resides in the wisdom of the Congress. This Honorable Court “does not pass upon question of wisdom, justice or expediency of legislation.”<sup>212</sup>

Having said the above, the Office of the Solicitor General, with utmost respect to the Congress submits that the law could have been crafted to provide **more** robust procedural safeguards respecting the collection of traffic/non-content data, *i.e.*, at a minimum requiring that the request be made by an attorney of the Department of Justice to a judge; that the information likely to be obtained is relevant to an ongoing investigation; and that the collection be made only after the issuance of a judicial warrant.

---

<sup>212</sup> Morfe vs. Mutuc, 22 SCRA 424 [1968] citing Angara vs. Electoral Commission, 63 Phil. 139 [1936].

**XV. Section 13 on preservation of data does not violate the provisions of the Constitution.**

Section 13 does not violate the due process clause of the Constitution.

---

**Section 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 Palatino, et al.<sup>213</sup> asserts that the preservation of computer data order, including its extension, under Section 13, R.A. No. 10175, does not provide the owner or possessor of computer data even the minimum requirements of due process, particularly notice and the opportunity to be heard as to why his computer data is being ordered preserved and his use and disposition restricted.

---

<sup>213</sup> G.R. No. 203391, pp. 16-17.

Petitioners' contentions are misplaced.

First, it must be pointed out that Section 13 is directed to a "service provider," not to the individual users.

Second, the requirement under the first sentence of Section 13 is a mere amendment to the franchise of telephone companies. It requires service providers to preserve, for a minimum of 6 months from date of transaction, the integrity of all traffic data and subscriber information relating to communication services it provides.

Third, Section 13 only calls for the preservation of traffic data and subscriber information, under the first sentence, and content data, under the second sentence. The subscriber's use and disposition of the preserved data are not being restricted.

Thus, the explanatory report of the *Budapest Convention on Cybercrime* said that preservation does not necessarily

mean that the data be frozen (*i.e.*, rendered inaccessible) and that it, or copies thereof, cannot be used by legitimate users.<sup>214</sup>

During the Senate Joint Committee Public Hearings<sup>215</sup> on this matter, one of the resource persons, DOJ Assistant Secretary G. L. Sy, during questioning by Committee Chair Sen. Edgardo Angara, explained that a preservation order sans judicial intervention and issued only by law enforcement agencies is necessary because of the ephemeral nature of computer data, to wit:

MR. SY: Yes sir, two aspects sir, sir(*sic*). And, sir, if we may address the earlier comment of the NTC, it's true now that the law enforcement, especially the NBI and PNP are experiencing extremely difficult situation to require cooperation from the telcos based on the standard reply **that a warrant is needed. But in the nature of electronic evidence, it's ephemeral. It's very easy to just disappear. And the requirement of a warrant unduly restricts this particular type of law enforcement.** What the law – the provision of the law says (*sic*) that there is an intermediary aspect called the **preservation order** that tells the telco, **“Hey, this particular number 0917123 has been used to commit a crime. Just hold on to the data that you have there, preserve it.”** That is the intermediary step that is absent in our present legal framework.

THE CHAIRMAN (SEN. ANGARA): **Who will issue that preservation order**, the law enforcer or the NTC?

MR. SY: **It should be law enforcement officials, sir.**  
(Emphasis and underscoring supplied)

---

<sup>214</sup> *Supra*.

<sup>215</sup> p. 35, February 28, 2011.

Thus, it can be assumed based on the above transcript that, in the pursuit of cyber-criminals, the requirement of a Notice and Hearing prior to any action to “preserve” the data, will clearly be inadequate because of the volatility of ICT data.

**Section 13 does not infringe on  
one’s right to privacy.**

---

Petitioner PIFA also contends that Section 13 violates an individual’s Right to Privacy<sup>216</sup> because “traffic data is private and personal information which belongs to the Internet user”.

PIFA’s contention is untenable.

As previously discussed, **traffic data** or **non-content data** is defined as any computer data **other than the content of the communication including**, but not limited to, the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

---

<sup>216</sup> Section 3.

(1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law.

(2) Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.

---

Preservation of computer data is a *Budapest Convention on Cybercrime* provision.

The Convention recognizes that traffic data lasts only for a short period of time, hence, there is a compelling need to make service providers responsible for preservation of data.<sup>217</sup> Article 17 of the Convention on Cybercrime establishes obligations on its member states in relation to the preservation of traffic data and provides for expeditious disclosure of some traffic data so as to identify the other service providers who were involved in the transmission of specified communications.

**XVI. Section 14 does not encroach upon judicial process. The order referred to therein is to be issued upon securing a court warrant. Nonetheless, the power to issue subpoena is inherent in the power to investigate and may thus be exercised by the law enforcement authorities.**

---

**Section. 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

---

<sup>217</sup> *Supra.*



investigation and the disclosure is necessary and relevant for the purpose of investigation.<sup>218</sup>

Petitioners NUJP, et al. assail Section 14 as it allegedly allows the PNP and NBI to issue a “subpoena” to require persons or service providers to disclose or submit subscriber’s information, traffic data or relevant data in his/its possession. Petitioners argue that Section 14 has delegated to said law enforcement authorities, a process that *allegedly* can only be exercised by the judiciary.<sup>219</sup>

This argument deserves no merit.

First, it must be pointed out that the “order” referred to in Section 14 issued by the law enforcement authority is to be made only upon securing a court warrant.

As there is no need to actually conduct the “search and seizure” themselves, law enforcement agencies will just require or order the data custodian/s to produce the relevant data. Thus, the order is actually done pursuant to a court issued warrant.

---

<sup>218</sup> Underscoring supplied.

<sup>219</sup> G.R. No. 203453, pp. 15-16.

Nonetheless, even if this be in the nature of a subpoena power, the same does not make it illegal. Investigating agencies, such as the PNP and NBI, are granted by law the power to issue subpoena and subpoena *duces tecum*.

And, having subpoena powers does not necessarily clothe law enforcement agencies with judicial power. In **Biraogo vs. Philippine Truth Commission**,<sup>220</sup> this Honorable Court said that although the Truth Commission may have subpoena powers, it has no power to cite people in contempt, much less order their arrest. If at all and if such is the case, the exercise of power to issue subpoena is merely an adjunct of the law enforcement agencies' power to investigate.

**XVII. Section 15 of R.A. No. 10175 is not an undue delegation of judicial and legislative powers to NBI and PNP**

---

**Section 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:

---

<sup>220</sup> 637 SCRA 78 [2010].

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

- 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;
- 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 NUJP, et al.<sup>221</sup> and Palatino, et al.<sup>222</sup> also asserts that Section 15 violates the doctrine of separation of powers as judicial and legislative powers are unduly delegated to the PNP and NBI. Petitioners Palatino, et al. insist that Section 15 violates the constitutional right against unreasonable searches and seizure.

Petitioners' contentions are without merit.

---

<sup>221</sup> G.R. No. 203453, pp. 14-15.

<sup>222</sup> G.R. No. 203391, pp. 17-18

Search and seizure is plainly a law enforcement function. The powers and duties enumerated in said section is a necessary adjunct of the exercise of such function bearing in mind the nature of the object to be seized. Hence, for purposes of seizing computer data, the securing and copying thereof is an important aspect of its seizure.

Search and seizure of computer data is a *Budapest Convention on Cybercrime* procedural provision. Its Explanatory Report explains that many of the characteristics of traditional search remain, such as: a) gathering of data occurs during the period of the search; b) in respect of data that exists at that time; c) preconditions for obtaining legal authority to undertake a search remain the same; d) the degree of belief required for obtaining legal authorization to search is no different. However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. There are several reasons for this.<sup>223</sup>

First, the data is in intangible form, such as in an

---

<sup>223</sup> *Supra.*

electromagnetic form.<sup>224</sup>

Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record. The physical medium on which the intangible data is stored (e.g., the computer hard-drive or a diskette) must be seized and taken away, or a copy of the data must be made in either tangible form (e.g., computer print-out) or intangible form, on a physical medium (e.g., diskette), before the tangible medium containing the copy can be seized and taken away. In the latter two situations, where such copies of the data are made, a copy of the data remains in the computer system or storage device. Domestic law should provide for a power to make such copies.

Third, due to the connectivity of computer systems, data may not be stored in the particular computer that is searched, but such data may be readily accessible to that system. It could be stored in an associated data storage device that is connected directly to the computer, or connected to the computer indirectly through communication systems, such as the Internet. This may or may not require new laws to permit

---

<sup>224</sup> *Supra.*

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

an extension of the search to where the data is actually stored (or the retrieval of the data from that site to the computer being searched), or the use traditional search powers in a more co-ordinated and expeditious manner at both locations.<sup>225</sup>

This Honorable Court, in **Nogales vs. Court of Appeals**,<sup>226</sup> already recognized the authority of law enforcement agencies to seize, retain and destroy computer hardware and software containing pornographic materials in violation of Article 201 of the Revised Penal Code.

xxx be released in their favor with only the hard disk removed from the CPUs and destroyed. If the softwares are determined to be violative of Article 201 of the RPC, unlicensed or pirated, they should also be forfeited and destroyed in the manner allowed by law. The law is clear. Only licensed softwares that can be used for legitimate purposes should be returned to petitioners.

To stress, P.D. No. 969 mandates the forfeiture and destruction of pornographic materials involved in the violation of Article 201 of the Revised Penal Code, *even if the accused was acquitted*. Taking into account all the circumstances of this case, the Court holds that the destruction of the hard disks and the softwares used *in any way* in the violation of the subject law addresses the purpose of minimizing if not totally eradicating pornography. This will serve as a lesson for those engaged *in any way* in the proliferation of pornography or obscenity in this country. The Court is not unmindful of the concerns of petitioners but their

---

<sup>225</sup> *Supra*.

<sup>226</sup> 660 SCRA 475 [2011].

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

supposed property rights must be balanced with the welfare of the public in general.

**XVIII. Petitioners do not have any interest relative to destruction of computer data under Section 17.**

---

**Section 17. Destruction of Computer Data. –**  
Upon expiration of the periods as provided in Section 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.

Petitioners Reyes, et al.,<sup>227</sup> and Palatino, et al.<sup>228</sup> argue that Section 17 of R.A. No. 10175 constitutes deprivation of property without due process of law because the owner of the computer data to be destroyed has not been convicted by a proper court. Petitioners raised the possibility of the complaint or criminal case being dismissed after the destruction of the computer data.

Petitioners likewise point out that Section 15 does not distinguish between computer data that have the nature of a “contraband” or data that are speech related which are of significant importance to the owner.

---

<sup>227</sup> G.R. No. 203407, pp. 25-26.

<sup>228</sup> G.R. No. 203391, p. 18.

Biraogo, et al. vs. NBI, et al.

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

Section 17 of R.A. No. 10175 does not constitute a deprivation of property without due process of law. Section 17 pertains to the traffic data, subscribe information data and content data ordered preserved under Section 13 and the copies of computer data made during the search and seizure under Section 15(b).

Section 17 merely provides for a process of clearing up – the telcos' systems to avoid overloading their storage capacity. As gleaned from the deliberations in the Bicameral Conference Committee, *viz*:

REP. GOLEZ. The preservation of computer data, the Senate version is for six months.

THE CHAIRMAN (SEN. ANGARA). Yes.

REP. GOLEZ. And the House version is for ...

THE CHAIRMAN (SEN. ANGARA). Ninety days, three months ...

REP. GOLEZ. ... 90 days or three months. I am just concerned about the overload on the...

THE CHAIRMAN (SEN. ANGARA). On the system.

REP. GOLEZ. ...on the system.

THE CHAIRMAN (SEN. ANGARA). There's now the cloud computing, eh. So –

REP. GOLEZ. No. But the cloud is still limited.

xxx

xxx

xxx



Biraogo, et al. vs. NBI, et al.

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

THE CHAIRMAN (SEN. ANGARA) I am just trying to ...

REP. GOLEZ. I don't know whether ...

THE CHAIRMAN (SEN. ANGARA). ...find the rationale for -

REP. GOLEZ. ...the system is capable of this overload.

THE CHAIRMAN (SEN. ANGARA) Yeah, But, you know, we are now talking of storage, eh. And as I understand it, you know, cloud computing has really expanded the capacity to hold as much data almost infinitely as possible because you just throw it up to the sky and the wide, wide world just keep it. And unless you -

xxx

xxx

xxx

THE CHAIRMAN (SEN. ANGARA). ... figure out, Roi, why we chose six months-

THE CHAIRMAN (REP. TINGA). Well, let me just clarify this, Mr. Chairman.

THE CHAIRMAN (SEN. ANGARA). Oo. Oo.

THE CHAIRMAN (REP. TINGA). The preservation of computer data would be subject to an order.

THE CHAIRMAN (SEN. ANGARA). Yes.

THE CHAIRMAN (REP. TINGA). So, it would not mean all computer data, but only a specific user, 'no.

THE CHAIRMAN (SEN. ANGARA) Yes.

THE CHAIRMAN (REP. TINGA). And while we, in the House, had originally gone for six months as well. There was a request to bring it down to three months or 90 days. But again, having reviewed current practice, and I think this is where you're getting your six months, 'no? Having reviewed current practice in Europe and other countries, we found out it was six months, Mr. Chairman.

THE CHAIRMAN (SEN. ANGARA). Oo, oo.

THE CHAIRMAN (REP. TINGA). Six Months po. So, that is -

REP. GOLEZ. In that case, I concur.

THE CHAIRMAN (SEN. ANGARA). O, sige.

REP. GOLEZ. I am just concerned about the ability of the system to handle this load.

THE CHAIRMAN (SEN. ANGARA). Okay. So, the Senate version will be adopted.  
Section 13, any question on Disclosure of Computer Data?

THE CHAIRMAN (REP. TINGA). It's the same, Mr. Chairman.

THE CHAIRMAN (SEN. ANGARA). The same, So, okay. Search, seizure and Examination of Computer Data.. Any question?  
Section -

THE CHAIRMAN (REP.TINGA). Agreed, Mr. Chairman

THE CHAIRMAN (SEN. ANGARA). Section 15, we will adopt the House-Destruction of Computer Data, we'll adopt the House version.

(pp. 62-67, Bicameral Conference Committee on the Disagreeing Provisions of Senate Bill No. 2796 and House Bill No. 5808 [Cybercrime Prevention Act of 2012], May 31, 2012)

The destruction of computer data within the periods provided under Sections 13 and 15 also serves a second purpose. The clean up protects individuals from unnecessary delay in the investigation and prosecution of a cybercrime.

**XIX. Section 19 of R.A. No. 10175 violates the freedom of speech and expression clauses of the Constitution.**

---

**Section 4, Article III of the Constitution** provides:

No law shall be passed abridging the freedom of speech, of expression, or of the press, or the right of the people peaceably to assemble and petition the government for redress of grievances.

The Office of the Solicitor General, with utmost respect to the Congress, is of the view that Section 19 of R.A. No. 10175 is an impermissible **final** restraint on the freedoms of speech and of expression.

**Section 19 of R.A. No. 10175** provides:

**Section 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.

Section 19 seeks to restrain access to, circulation and dissemination of computer data *prima facie* found to be violative of the provisions of R.A. No. 10175. It covers not just conduct but broadly and dangerously sweeps speech, as well.

A governmental purpose may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms.<sup>229</sup> The possible harm to society in permitting some unprotected speech to go unpunished is outweighed by the possibility that the protected speech of others may be deterred and perceived grievances left to fester because of possible inhibitory effects of overly broad statutes.<sup>230</sup>

Though governmental purposes be legitimate and substantial, they cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved. For precision of regulation is the touchstone in an area so closely related to our most precious freedoms.<sup>231</sup>

As Justice Vicente V. Mendoza has stated, authoritative interpretations of the free speech clause consider as invalid two types of prior restraints, namely, those which are imposed prior to the dissemination of any matter **and those imposed**

---

<sup>229</sup> *Gonzales vs. Comelec*, 27 SCRA 835 [1969] citing *NAACP vs. Alabama*, 377 US 288 [1964].

<sup>230</sup> Separate Opinion of Mr. Justice Mendoza in *Estrada vs. Sandiganbayan*, 421 Phil. 290, 430 [2001].

<sup>231</sup> *Gonzales vs. Comelec*, 27 SCRA 835 [1969].

prior to an adequate determination that the expression is not constitutionally protected.<sup>232</sup> The Winconsin Supreme Court put the matter, thus: “[A] prohibited ‘prior restraint’ is not limited to the suppression of a thing before it is released to the public. Rather, an invalid prior restraint is an infringement upon the constitutional right to disseminate matters that are ordinarily protected by the first amendment without there first being a judicial determination that the material does not qualify for first amendment protection.”<sup>233</sup>

Under Section 19 of R.A. No. 10175, the DOJ’s finding based on *prima facie* evidence that computer data are violative of the provisions of R.A. No. 10175 effectively rules with finality that said computer data are unprotected speech or expression. This impinges on freedom of speech and expression because **“only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a**

---

<sup>232</sup> Separate Opinion of Mr. Justice Mendoza in Estrada vs. Sandiganbayan, 421 Phil. 290, 430 [2001]].

<sup>233</sup> State v. I, a Woman, Part II, 53 Wis. 102, 191 N.W. 2d 897, 902-903 [1971]; Laurence H. Tribe, American Constitutional Law, 1041-42 [1988]; Separate Opinion of Mr. Justice Mendoza in Iglesia ni Cristo vs. Court of Appeals, 259 SCRA 529 [1996]; emphasis supplied.

**judicial determination suffices to impose a valid final restraint.”<sup>234</sup>**

Under the Constitution, courts are the exclusive arbiters of controversies affecting the civil and political rights of persons. Our courts that determine whether or not certain forms of speech and expression have exceeded the bounds of correctness, propriety or decency as to fall outside the area of protected speech. In the meantime, the liberties protected by the speech and expression and free exercise clauses are so essential to our society that they should be allowed to flourish unobstructed and unmolested.<sup>235</sup>

Thus, in **Pita vs. Court of Appeals**,<sup>236</sup> this Honorable Court was not convinced that therein private respondents had shown the required proof to justify a ban and to warrant confiscation of reading materials alleged to be obscene, *viz*:

**First of all, they were not possessed of a lawful court order: (1) finding the said materials to be pornography, and (2) authorizing them to carry out a search and seizure, by way of a search warrant.**

---

<sup>234</sup> *Freedman vs. Maryland*, 380 U.S. 51 [1965]; Emphasis supplied.

<sup>235</sup> Concurring and Dissenting Opinion of Justice Kapunan in *INC vs. CA*, 259 SCRA 529 [1996], citing *Cantwell v. Connecticut*, 310 U.S. 296, at 310 [1939].

<sup>236</sup> 178 SCRA 362 [1989].

The Court of Appeals has no “quarrel that...freedom of the press is not without restraint, as the state has the right to protect society from pornographic literature that is offensive to public morals.” Neither do we. But it brings us back to square one: were the “literature” so confiscated “pornographic”? That “we have laws punishing the author, publisher and sellers of obscene publications (Sec. 1, Art. 201, Revised Penal Code, as amended by P.D. No. 960 and P.D. No. 969),” is also fine, but the question, again, is: Has the petitioner been found guilty under the statute?

xxx xxx xxx

It is basic that searches and seizures may be done only through a judicial warrant, otherwise, they become unreasonable and subject to challenge. xxx The fact that the instant case involves an obscenity rap makes it no different from *Burgos*, a political case, because, as we have indicated, **speech is speech, whether political or “obscene.”**

xxx xxx xxx

xxx To say that the respondent Mayor could have validly ordered the raid without a lawful search warrant because in his opinion, “violation of penal laws” has been committed, is to make the respondent Mayor judge, jury, and executioner rolled into one.

(Emphasis supplied)

Section 19 of R.A. No. 10175 impermissibly dispenses with obtaining prior judicial intervention and determination before speech or expression may be adjudged to be outside the protection of the Constitution.

It thus does not provide for constitutionally mandated procedural safeguards that would justify final restraint.

First, once the DOJ rules that a computer data is *prima facie* violative of the any of R.A. No. 10175's provisions and effectively blocks access thereto, the exhibitor must assume the burden of instituting judicial proceedings and of persuading the courts that such computer data is protected expression. Second, once the DOJ has acted against a computer data, exhibition is prohibited pending judicial review, however protracted. Third, Section 19 of R.A. No. 10175 provides no assurance of prompt judicial determination.<sup>237</sup>

Censorship may be allowed only in a narrow class of cases involving pornography, excessive violence, and danger to national security. Even in these cases, only courts can prohibit the showing of a film or the broadcast of a program. In all other cases, the only remedy against speech which

---

<sup>237</sup> See *Freedman vs. Maryland*, 380 U.S. 51 [1965].



Biraogo, et al. vs. NBI, et al.

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

creates a clear and present danger to public interests is through subsequent punishment.<sup>238</sup>

**XX. Section 20, which treats as obstruction of justice the non-compliance with orders of the Law Enforcement Agencies, observes substantial due process and is not a bill of attainder.**

---

**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 argue that Section 20 constitutes a violation of substantive and procedural due process and is a bill of attainder as the said provision does not consider instances of a valid and lawful “non-compliance” of a person against whom an order has been issued by law enforcement authorities such as when the order is not supported by a court warrant, the order contains matters beyond the scope of the court warrant; the court warrant itself is patently illegal and

---

<sup>238</sup> Separate Opinion of Mr. Justice Mendoza in *Iglesia ni Cristo vs. Court of Appeals*, 259 SCRA 529 [1996].

unconstitutional.<sup>239</sup> Petitioners contend that under Section 20,<sup>240</sup> mere “failure to comply” with orders of the law enforcement authority is a prohibited act<sup>241</sup> and singles out a specific class of offenders for punishment based on legislative determination of guilt.<sup>242</sup>

Petitioners’ contentions are without merit.

Section 20, by its reference to Presidential Decree (PD) No. 1829, clearly set the definitive elements that will constitute non-compliance. **Section 1(b) of PD 1829** defines obstruction of justice, which equally applies in case of non-compliance.

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

xxx

xxx

xxx

(b) altering, destroying, suppressing or concealing any paper, record, document, or object, with intent to impair its verity, authenticity, legibility, availability, or admissibility as evidence in any investigation of or official proceedings in, criminal cases, or to be used in the

---

<sup>239</sup> *Supra.*

<sup>240</sup> Penalizing Obstruction of Apprehension and Prosecution of Criminal Offenders.

<sup>241</sup> p. 27, Bagong Alyansang Makabayan Secretary General Renato M. Reyes, Jr., et al. vs. Benigno Simeon C. Aquino, et al.

<sup>242</sup> p. 13, National Union of Journalists of the Philippines (NUJP), et al. vs. The Executive Secretary, et al.

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

investigation of, or official proceedings in,  
criminal cases; (Underscoring supplied.)

xxx

xxx

xxx

If any of the acts mentioned herein is  
penalized by any other law with a higher  
penalty, the higher penalty shall be  
imposed.

Thus, a person must still be prosecuted for obstruction of  
justice and thereafter, proven to have **knowingly or willfully**  
defied the orders of law enforcement authorities before he will  
be penalized for non-compliance.

**XXI and XXII. The authority  
granted to CICC under  
Sections 24 and 26(a) has  
parameters and standards. It  
is embodied in Sections 2  
and 26-A of R.A. No. 10175.**

---

**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.

xxx xxx xxx

**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 for the suppression  
of real-time commission of cybercrime offenses

through a computer emergency response team (CERT).

Petitioners NUJP, et al.<sup>243</sup> assail Sections 24 and 26(a) of R.A. 10175. Allegedly, both give the Cybercrime Investigation and Coordination Center (CICC) the power to formulate a *national cybersecurity plan* and implement the same. They assert that such delegation is unconstitutional as it amounts to an abdication of legislative power, allegedly for having no parameters or standards.

Such contention deserves scant consideration.

**Cybersecurity** refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

Two tests determine the validity of delegation of legislative power: (1) the completeness test and (2) the sufficient standard test. A law is complete when it sets forth therein the policy to be executed, carried out or implemented by the delegate. It lays down a sufficient standard when it

---

<sup>243</sup> G.R. No. 203453, p. 16.

provides adequate guidelines or limitations in the law to map out the boundaries of the delegate's authority and prevent the delegation from running riot. To be sufficient, the standard must specify the limits of the delegate's authority, announce the legislative policy and identify the conditions under which it is to be implemented.<sup>244</sup>

The CICC is not given unbridled legislative powers. In fact, the powers of the CICC with respect to enactment of relevant laws, issuances, measures and policies is merely recommendatory. Moreover, the powers and functions given to the CICC including the formulation of a cybersecurity plan merely relates to the prevention and suppression of Cybercrime as clearly specified under Sections 2 and 2(b) of R.A. No. 10175.

A perusal of Section 2 of R.A. No. 10175 readily reveals that the policy of the State deals with the "interest of law and order,"<sup>245</sup> "public interest,"<sup>246</sup> and "justice and equity."<sup>247</sup> Clearly, there are sufficient standards.

---

<sup>244</sup> BOCEA vs. Teves, 661 SCRA 589 [2011] citing ABAKADA GURO PARTY LIST vs. Purisima, 562 SCRA 251 [2008].

<sup>245</sup> Rubi vs. Provincial Board of Mindoro, 39 Phil. 660 [1919].

<sup>246</sup> People vs. Rosenthal, 68 Phil. 328 [1939].

<sup>247</sup> International Hardwood vs. Pang, 70 Phil. 602 [1940].

**PETITIONERS ARE NOT ENTITLED TO A  
WRIT OF INJUNCTION.**

The mere fact that a statute is alleged to be unconstitutional or invalid will not of itself entitle a litigant to have its enforcement enjoined.<sup>248</sup> It is required that further circumstance must, of necessity be present as to bring the case under some recognized head of equity jurisdiction, and there must appear some actual or threatened and irreparable injury to complainant's rights for which there is no adequate remedy.

The question as to whether an injunctive writ may be issued to restrain the enforcement of a law enacted by the lawmaking body would depend on circumstances that portend no less than extreme urgency, and should not rest merely upon asserted transgression on the constitutional protection against self-incrimination and against unreasonable searches and seizure.

In other words, it is imperative that a party seeking this extraordinary remedy which the courts have been enjoined to

---

<sup>248</sup> Co Chiong vs. Dinglasan, 96 SCRA 139 [1980].

issue with “circumspection,” must show that his right is clear and unmistakable and supported by indubitable proof that he is entitled to the relief demanded. His complaint must also show facts entitling him to such relief.

Thus, the issuance of injunction to restrain the enforcement of a law should not be made to rest merely on purely legal arguments, without evidence being introduced, for or against the validity of a challenged statute. For it is to be understood that there is always a presumption of validity that attaches to every legislative act rendered more effective upon the time-honored doctrine that the “task of suspending the operation of the law is a matter of extreme delicacy because that is an interference with the official acts not only with the duly elected representatives of the people in Congress but also of the highest magistrate of the land.”<sup>249</sup>

Thus, in **Vera vs. Arca**,<sup>250</sup> this Honorable Court upheld the well-settled doctrine that the power to issue preliminary injunctions is not to be availed of indiscriminately, and that such a power could not be exercised to restrain the Tax

---

<sup>249</sup> Ermita vs. Eldecoa-Delorino, 651 SCRA 128 [2011].

<sup>250</sup> 28 SCRA 351 [1969].


Census Act under facts and circumstances attendant in this case (Commentaries and Jurisprudence on Injunction by Laretta, pp. 275-298).

Likewise, there is a need for factual basis to overthrow the presumption of constitutionality of a law.<sup>251</sup>

**PRAYER**

**WHEREFORE**, it is respectfully prayed that a) the Petitions be **DISMISSED** for lack of merit; and, b) the Temporary Restraining Order be **IMMEDIATELY LIFTED**.

Makati City for Manila, December 3, 2012.



**FRANCIS H. JARDELEZA**

Solicitor General

Roll No. 25719/IBP Life Member Roll No. 00037

MCLE Exemption No. III-008523

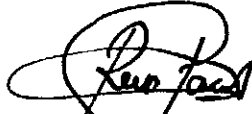
---

<sup>251</sup>Bautista vs. Junio, 127 SCRA 329 [1984].



Biraogo, et al. vs. NBI, et al.

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407, 203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

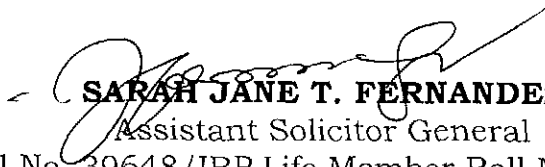


**REX BERNARD L. PASCUAL**

Assistant Solicitor General

Roll No. 38914/IBP Life Member Roll No. 01997

MCLE Exemption No. III-000368



**SARAH JANE T. FERNANDEZ**

Assistant Solicitor General

Roll No. 39648/IBP Life Member Roll No. 00824

MCLE Exemption No. III-001054



**MARSHA C. RECON**

Senior State Solicitor

Roll No. 41169/IBP Life Member Roll No. 883342

MCLE Compliance No. IV-0009083



**RAYMUND I. RIGODON**

Senior State Solicitor

Roll No. 39730/IBP No. 867929, 10-3-11

MCLE Compliance No. III-003833



**JOAN V. RAMOS-FABELLA**

State Solicitor

Roll No. 47418/IBP Life Member Roll No. 09134

MCLE Compliance No. III-0003829



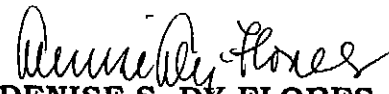
**MA. RITA CECILIA C. DE LEON-ABAD**

State Solicitor

Roll No. 47379

IBP Lifetime No. 08749/01-14-10

MCLE Compliance No. III-0003777



**DENISE S. DY-FLORES**

Associate Solicitor

Roll No. 57316/Life Member Roll No. 010412

MCLE Compliance No. III-0011975



**MOSES V. FLORENDO**

Associate Solicitor

Roll No. 50941/IBP Life Member Roll No. 08382

MCLE Compliance No. IV-0009082

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

  
**JONATHAN HONORATO D. LOCK**

Associate Solicitor

Roll No. 52038/IBP Life Member Roll No. 05786  
MCLE Compliance No. IV-0009080

  
**SAMANTHA P. CAMITAN**

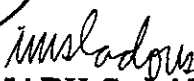
Associate Solicitor

Roll No. 54185/IBP Life Member Roll No. 08750  
MCLE Compliance No. IV-0009081

  
**JOSE CARLO H. NIEBRES**

Associate Solicitor

Roll No. 54093/IBP No. 902346, 8-2-12  
MCLE Compliance No. IV-0009197

  
**IVAN MARK S. LADORES**

Associate Solicitor

Roll No. 56801/IBP Life Member Roll No. 09526  
MCLE Compliance No. IV-0007603

  
**MA. CRISTINA T. NAVARRO**

Associate Solicitor

Roll No. 56704/IBP Life Member Roll No. 08851  
MCLE Compliance No. III-0011955

  
**DONNA S. SORIANO-VAN HAUTE**

Associate Solicitor

Roll No. 57002/IBP No. 888796, 02-09-12  
MCLE Compliance No. IV-0009144

  
**JOEL N. VILLASERAN**

Associate Solicitor

Roll No. 55935/IBP Lifetime No.08748  
MCLE Compliance No. IV-0009196

  
**GIANCARLO L. YUSON**

Associate Solicitor

Roll No. 59248  
IBP Life Member Roll No. 010029  
MCLE Compliance No. IV-0009147

  
**ELVIRA JOSELLE R. CASTRO**

Roll No. 57165/IBP Life Member Roll No. 010429  
MCLE Compliance No. III-0006576

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

**EXPLANATION**

(Pursuant to Section 11, Rule 13 of the 1997 Rules of Civil Procedure)

The foregoing **Consolidated Comment with Partial Manifestation** is being served by registered mail, personal service not being practicable due to distance and lack of personnel.

  
**JOAN V. RAMOS-FABELLA**  
State Solicitor

**COPY FURNISHED:**

**Louis "Barok C. Biraogo**

No. 115 Mariveles Street, San Jose Village 3  
Barangay Biñan, City of Biñan  
Laguna Province  
**G.R. No. 203299**

**Attys. Berteni Cataluna Causing, Cirilo P. Sabarre, Jr.,  
and Dervin V. Castro**

Renta Pe Causing Sabarre Castro & Associates  
Unit 1, 2368 JB Roxas Street corner Leon Guinto Street  
Malate, Manila  
**G.R. No. 203306**

**Atty. Jose Jesus M. Disini, Jr., Rowena S. Disini  
and Lianne Ivy Pascua-Medina**

Disini & Disini Law Office  
320 Philippine Social Science Center  
Commonwealth Avenue, Diliman, Quezon City  
**G.R. No. 203335**

**Attys. Alex O. Avisado, Jr., Raymond M. Cajucom,  
Ronald Michel R. Ubaña, María Cristina B. Garcia-Ramirez  
and Rose Anne P. Rosales**

Gana Atienza Avisado Law Offices  
3<sup>rd</sup> Floor HPL Building  
No. 60 Sen. Gil Puyat Avenue, Makati City  
**G.R. No. 203359**

**Atty. H. Harry L. Roque, Jr., Romel Regalado Bagares  
and Gilbert Teruel Andres**

Roque & Butuyan Law Offices  
1904 Antel 2000 Corporate Center  
121 Valero St., Salcedo Village, Makati City  
**G.R. No. 203378**

**Atty. James Mark Terry L. Ridon**

89 K-7 St., Kamias, Quezon City  
**G.R. No. 203391**

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

**Attys. Julius Garcia Matibag, Carlos Isagani T. Zarate,  
Gregorio Y. Fabros and Maria Cristina P. Yambot**

National Union of People's Lawyers

3<sup>rd</sup> Floor, Erythrina Building

No. 1 Maaralin cor. Matatag Sts.

Central District, Quezon City

**G.R. No. 203407**

**Attys. Melencio Sta. Maria, Sedfrey M. Candelaria,  
Amparita delos Santos-Sta. Maria, Gilbert V. Sembrano,  
Ryan Jeremiah D. Quan, Maria Patricia R. Cervantes,  
Ray Paolo J. Santiago and Nina Patricia D. Sison-Arroyo**

Ateneo Human Rights Center

G/F Ateneo Professionals Schools Building

20 Rockwell Drive, Rockwell Center, Makati City

**G.R. No. 203440**

**Atty. Theodore O. Te**

Free Legal Assistance Group (FLAG)

Room 201, Malcom Hall,

University of the Philippines

Diliman, Quezon City

**G.R. No. 203453**

**Attys. Paul Cornelius T. Castillo and Ryan D. Andres**

6<sup>th</sup> Floor, Tuscan Building

114 V.A. Rufino Street, Makati City

**G.R. No. 203454**

**Atty. Kristoffer James E. Purisima**

6/F LTA Building, 118 Perea Street

Legaspi Village, Makati City

**G.R. No. 203469**

**Attys. Rico A. Limpingco,**

**Arthur Anthony S. Alicer and**

**Michelle Anne S. Lapuz**

Solis Medina Limpingco and Fajardo Law Offices

1106 East Tower, Philippine Stock Exchange Centre

Exchange Road, Ortigas Commercial Center

Pasig City

**G.R. No. 203501**

**Atty. Rodel A. Cruz**

Suite 347 Valero Plaza

124 Valero Street, Salcedo Village

Makati City 1200

**G.R. No. 203501**

**Atty. Edsel F. Tupaz**

41 N. Romualdez Street

BF Homes Subdivision, 1120 Quezon City

**G.R. No. 203509**

**Biraogo, et al. vs. NBI, et al.**

G.R. Nos. 203299, 203306, 203335, 203359, 203378, 203391, 203407,  
203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518

---

**Atty. Michael J. Mella**

Santillan-Felix Magbanua and Mella Law Office  
Unit 1106, Prestige Tower  
F. Ortigas Jr. Road, Ortigas Center  
Pasig City

**G.R. No. 203515**

**Atty. Renecio S. Espiritu, Jr.**

Guevarra Mendoza and Espiritu Law Offices  
Suite 602 Richmonde Plaza Hotel  
21 San Miguel Avenue, Ortigas Center  
Pasig City

**G.R. No. 203518**

**Atty. Kelvin Lester K. Lee**

San Juan Tayag Lee and Vergara Law Office  
Unit 804 Xavierville Square, Xavierville Avenue  
Quezon City

**G.R. No. 203518**