

# **Control Policy versus Internet Freedom**

**Brief introduction of the development and dynamics of regulation related to internet and human rights in Indonesia, Malaysia and Philippines**



Author

**Wahyudi Djafar**

**Institute for Policy Research and Advocacy [ELSAM]**

**2013**

# **Control Policy versus Internet Freedom**

**Brief introduction of the development and dynamics of regulation related to internet and human rights in Indonesia, Malaysia and Philippines**

Author:

**Wahyudi Djafar**

Editor:

**Triana Dyah**

Translator:

**Idaman Andarmosoko**

First published by:

**Institute for Policy Research and Advocacy [ELSAM]**

Jl. Siaga II No.31, Pejaten Barat, Pasar Minggu, Jakarta Selatan 12510

Tel. +62 21 7972662, 79192564, Fax. +62 21 79192519

email: [office@elsam.or.id](mailto:office@elsam.or.id), laman: [www.elsam.or.id](http://www.elsam.or.id), twitter: @elsamnews - @ElsamLibrary

*All ELSAM publication are dedicated to the victims of human rights violation as well as part of effort of promotion and protection of human rights in Indonesia.*

Except where otherwise noted, content on this report is licensed under a Creative Commons Attribution 3.0 License



Some rights reserved.

## Contents

A. Introduction .....	4
B. Trajectory of internet technology usage: initiative and development .....	5
C. Internet as communication and information access facility: regulation development .....	13
D. Control Policy versus Internet Freedom: Regulations Dynamic .....	21
Content restriction and dawn of criminalization .....	23
Ensuring the protection of privacy .....	31
E. Conclusion .....	36

## A. Introduction

The development of internet is now unstoppable in the world as well as in Asia. Indonesia, even, with population of 250 million had ranked into top eight world internet users, as well as the third in Asia. The large number of internet users in Indonesia, is also in line with the large number of active users of social media such as Facebook and twitter, as reflected on the high number of active account in those social media. Although there is a slight decrease, yet up to March 2013, there are 48,807,580 users<sup>1</sup>. Jakarta the capital city of Indonesia, ranks the second largest number of Facebook users in the world with 11,658,760 users, under Bangkok, Thailand with 12,797,500 users. In the case of twitter, the number of Indonesian twitter accounts grows steadily, reaching 29 millions in March 2013, ranking the fifth in the world, after US, Brazil, Japan and Britain<sup>2</sup>. The fast growth of internet users happened not only in Indonesia, but also in other Southeast Asian countries. Philippines, with 133 million population, had reached 33,600,000 internet users in 2012, while Malaysia have 17,723,000 internet users, with 60.71% penetration to the total population.

In the context of human rights, the development of internet technology adoption had contributed positive benefits to the needs fulfillment as well as promotion of human life qualities. Internet can deliver information, and connect distant separate communities rapidly. Internet had become important instrument in supporting the advances of nation development, yet internet brought also a number of negative impacts along with positive benefits. The negative impacts are amongst the new variant of crimes, known as virtual realm crimes, as well as new practices of human rights violation, unknown in the previous era.

Previous ELSAM Publication, the human rights and internet series, had discussed the strong relationship between internet and human rights fulfillment.<sup>3</sup> United Nation, through the human rights commission, in June 2012 had issued a resolution on The Promotion and Enjoyment of Human Rights in the Internet, that sternly stipulate internet access as part of human rights.<sup>4</sup> In line, the UN special *rapporteur* for freedom of expression and opinion, Frank La Rue stated that internet had became very important instrument to implement various human rights, eradicate injustice, and accelerate human development and progress. Therefore assuring the universal access to the internet should be priority for all states.<sup>5</sup>

Building on the previous ELSAM studies, as previously mentioned, this paper would look on the preliminary initiatives of utilization and development of information and communication technology, specially internet, in the southeast region, taking examples in three countries, Indonesia, Malaysia and Philippines. The paper would also discuss the framework and model adopted by each country in

1 See "Facebook Country Stats February 2013", in <http://www.quintly.com/blog/2013/02/facebook-country-stats-february-2013-top-10-countries-lose-users/>, accessed in August 1st 2013.

2 See "Social Media Statistics for Indonesia", in <http://socialmemos.com/social-media-statistics-for-indonesia/>, accessed in august 1st 2013.

3 See Indriaswati DS and Wahyudi Djafar, Tata kelola internet yang berbasis hak: Studi tentang permasalahan umum tata kelola internet dan dampaknya terhadap perlindungan hak asasi manusia, (Jakarta: Elsam, 2013).

4 See A/HRC/20/L.13, accessible at <http://daccess-dds ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement>.

5 ibid A/HRC/20/L.13. See "Facebook country Stats February 2013" in

governing use and development of Information and communication technology. Furthermore, as the use and development of ICT had expanded in the last few years, some crucial problem had arisen related with the use of this technology. To emphasize the previous point, besides of delivering various positive benefits for the advance of human life qualities and human rights fulfillment in general, the rapid growth of internet had also spurred negative impacts, putting everyone as potential victim of the impact. These negative impact had triggered the government to issue some regulations the specifically governs the use and control of this technology.

Viewing the situation, the paper would also examine the tendencies of countries to set national rules to limit the user in the use of internet technology. The limitation phenomena gained legitimacy from the raising issue of cyber sovereignty, which often propose nationalism slogan without closely and holistically examining every facet of cyber characteristic that hardly had any apparent territorial borders. The issue of limitation on usage of internet technology seems to complete the problem of internet access that are still primary problem in the third world countries, specially developing countries like Indonesia, Malaysia and Philippines.

### **B. Trajectory of internet technology usage: initiative and development**

The first initiatives of internet in Indonesia start from a group of people involved in nonprofit research and a group of hobby community (computer technology hobby). Merlyna lim notes that the initial internet connection appeared in 1983, pioneered by Joseph Luhukay that connected the computers in the computer science department of Universities Indonesia (UI), Jakarta with UUNet in United States through UUCP network.<sup>6</sup> In 1984 then Joseph Luhukay initiated to build the UINET, that connects the entire network in the Indonesia state university campus and formally connect with UUNet.<sup>7</sup> In June 24th 1988, UI NETLAB gained the first Internet Protocol address in Indonesia (192.41.206/24) on behalf of Indonesia State University, registered at ARIN (the American Registry for Internet Numbers).<sup>8</sup>

Besides the initiatives of community and education institution, in 1986, the minister of research and technology at that time, Baharuddin Jusuf Habibie also started to promote the Idea of IPTEKnet, building on the experience of NSFNET (National Science Foundation Network). The IPTEKnet project was officially launched in Bandung in 1994 using local node. Further in 1994, for the first time the IPTEKnet was connected to the internet, and the subsequent year, a limited public use of internet were started in Indonesia. The internet was connected through the Global One network in USA, with speed of only 14.4 Kbps, resulting in slow and unstable connection. Connection got better after in 1996, the Bandung Institute of technology collaborated with Japan Satellite Corporation (Jsat) in the WIDE project, boosting the connection speed to 1.5Mbps.<sup>9</sup>

Meanwhile the first internet service provider (ISP) in Indonesia is the Indo Internet (IndoNet), established in Jakarta in 1994. Indonet's early internet connection was through dial up, with text

6 See Merlyna Lim, *Archipelago Online: The Internet and Political Activism in Indonesia*, Doctoral Dissertation at School of Business, Public Administration and Technology, University of Twente, the Netherlands, 2005, page. 61.

7 See "The Internet History in Indonesia", in [http://www.apnic.net/\\_\\_data/assets/pdf\\_file/0010/27919/apster21-200702.pdf](http://www.apnic.net/__data/assets/pdf_file/0010/27919/apster21-200702.pdf), accessed in august 1st 2013.

8 See "Sejarah Perkembangan Internet di Indonesia", in <http://id.shvoong.com/internet-and-technologies/commercial-companies/2040621-sejarah-perkembangan-internet-di-indonesia/#ixzz108XRNW00>, accessed in August 1st 2013.

9 See The Internet History... *Loc.Cit.*

mode, shell account, lynx browser, and pine email client in the AIX10 server. This business grew in the subsequent years, in 1996 there are at least 20 ISP companies operating in Indonesia. In 1996 the Association of Indonesian Internet Service Providers (APJII) was established. The association was established is amongst geared for consultation and negotiation with government, policy makers, creating healthy environment for the ISP to operate, such as billing rate regulation for the ISP.<sup>11</sup>

In international context the APJII then joined the APNIC (Asia Pacific Network Information Center) in 1999, as a member of confederation, and obtain National Internet Registries (NIR) in 2002. Up to 2013, APJII had at least 289 ISP members. The success of APJII to establish local IIX (Internet Exchange Point) in 1998 had been the biggest achievement of the organization. The IIX enables the ISP to be connected to two nodes at the speed reaching the Gigabit Ethernet.<sup>12</sup>

The usage of internet technology increases more after the new order regime in power at that time disbanded a number of mass media, including Tempo weekly magazine in June 21st 1994. To respond the situation, the Tempo magazine embarked to the internet by launching Interactive Tempo in 1995. The internet based media business also raised with the establishment of Detik.com in July, 9th 1998, not long after the fall of Suharto's regime.<sup>13</sup>

Similar with the initiatives of internet technology in Indonesia, Malaysia also starts their internet development with limited use in the university circles. The Internet development initiatives started in Malaysia in 1988, when Malaysia Institute of Microelectronic Systems (MIMOS) established university computer network known as *Rangkaian Komputer Malaysia* (RangKom). This network is connected four dial-up lines to Australia, South Korea, Netherlands, and United States. The network offers also email and participation in mailing list group. Later the dial up proves to be too expensive, finally in 1992, it is replaced with satellite connection to United States, and since then Malaysia gains permanent connection to the Internet.<sup>14</sup>

MIMOS then establishes JARING (Joint Advanced Integrated Networking) as the first ISP in Malaysia. This network uses the satellite connection between Malaysia and United States so that internet users in Malaysia gains easy access to global internet connection.<sup>15</sup> JARING becomes a government ISP until in 1995 government established TMNet, which is a new business line of the Telkom Malaysia Berhad (TMB). TMNet obtained full license in July 1996 and start operating their public service provision in November 1996. Since then, the internet technology grew, although TMNet monopolize the new Internet. Only after 2000, new ISPs appeared, ending the TMNet monopoly.<sup>16</sup>

Five years after the appearance of ISPs, came the growth of Malaysian Internet users. According to the survey conducted by MIMOS and Beta Interactive Services, from October to November 1995, at

10 See The Internet History... *Loc.Cit*

11 <http://www.apjii.or.id/v2/index.php/read/page/halaman-tentang/1/latar-belakang-.html>, accessed in August 1st 2013

12 APJII also collaborate with APNIC, ISC and Autonomica, to build two root server in Indonesia. Root server F and I installed in 2004 and 2005. See Andy Kurniawan, Indonesia Internet eXchange (IIX), APJII (2007). See also Johar Alam, History of the Indonesia Internet eXchange (IIX), accessible at [http://www.iix.net.id/library/iix\\_history.pdf](http://www.iix.net.id/library/iix_history.pdf)

13 See Wahyudi Djafar, et al , 2000-2010 Kebebasan Internet Indonesia: Perjuangan Meretas Batas, (Jakarta: IMDLN and ICJR, 2011), accessible at [http://wahyudidjafar.files.wordpress.com/2011/12/briefing-paper-3\\_2011\\_kebebasan-internet.pdf](http://wahyudidjafar.files.wordpress.com/2011/12/briefing-paper-3_2011_kebebasan-internet.pdf)

14 See ITU, *Multimedia Malaysia: Internet Case Study*, (Geneve: International Telecommunication Union, 2002), page. 19.

15 See "The Internet in Malaysia", in [https://www.apnic.net/data/assets/pdf\\_file/0020/27920/apster9-200402.pdf](https://www.apnic.net/data/assets/pdf_file/0020/27920/apster9-200402.pdf), accessed in August 1st 2013

16 See ITU, *Multimedia... Op. Cit.*

least one of thousand Malaysian citizen had access to internet. This means the there are approximately 20,000 Internet users of the total 20,000,000 population of Malaysia. The figure grew further in 1998, with at least 2.6% of the population of Malaysia used the internet.<sup>17</sup>

The Malaysian government also provides significant support for the growth of internet technology. For the sake of developing the communication and information technology, the government had launched a national strategy in telecommunication, including the internet. The policies can be seen in amongst the Visi Malaysia 2020, launched in 1991 by Mahathir Mohammad. Next in 1994 the Malaysian government established the National Information Technology Council, a consultant team to determine the steps and strategies to achieve the Malaysian 2020 vision. Also in 1996 Malaysia launched National Information Technology Agenda, providing framework for the usage and development of information and communication technology in Malaysia from three perspectives, i.e. people, infrastructure and application.<sup>18</sup>

The active promotion of Malaysian government in increasing the internet and cellular phone access had resulted in stable growth of internet technology usage and development since the first ISP in 1990s. In supporting the internet usage, the Malaysian government had applied various policies, including investment in large projects such as Multi Media Super Corridor. This corridor is a high technology business center with communication infrastructure designed to put Malaysia into international lead position in usage of information technology. Internet Infrastructure development in Malaysia had become a strong priority, amongst is done through endorsing the citizen to buy personal computers and connect to the internet access.<sup>19</sup>

The ISPs in Malaysia joins together in organization called Malaysian Multimedia and Computer Industry Association (PIKOM), established in 1986. All the companies in Malaysia in the sector of computer and internet usage join this National ICT Association of Malaysia.<sup>20</sup> The association currently has 1400 members, 110 of it is in the communication network sector, and 33 are web hosting companies.<sup>21</sup> Five years after Indonesia, in November 2003, Malaysia succeeded to establish Malaysia Internet Exchange (MYIX). The establishment of MYIX is an important milestone in the Malaysia internet development history. The MYIX is the primary support for all the Malaysian ISPs and assures local internet defense.<sup>22</sup>

Philippines had rather similar experiences with Malaysia and Indonesia at the early stage of internet usage. Early in 1990, actually internet technology had penetrated Philippines, albeit only enjoyable by a handful of people. The first public internet connection only available in 1994, provided by Computer Network Systems Corporation (ComNet), in collaboration with Science and Technology Department of University of Philippines, through the project The Philippine Network Foundation

17 See John Paynter and Jackie Lim, Drivers and Impediments to e-Commerce in Malaysia, in *Malaysian Journal of Library and Information Science*, (Vol. 6, No. 2, December 2001), pages. 1-19

18 See Ali Salman, et al, Tracing the Diffusion of Internet in Malaysia: Then and Now, in *Asian Social Science*, (Vol. 9, No. 6, April 2013).

19 See *The Internet in Malaysia*, Loc. Cit.

20 See <http://www.pikom.my/>, accessed in August 1st 2013.

21 See <http://pikom.org.my/cms/AllProductByCat.asp?CatID=53&type=>, accessed in August 1st 2013.

22 See The Malaysia Internet Exchange (MYIX), in <http://myix.my/about-myix/>, accessed in August 1st 2013.

(PHNet). PHNet itself is consortium comprises of government, specially the Science and Technology Department of University of Philippines, some other universities, and some private companies.<sup>23</sup>

The first internet access in Philippines is connected by PHNet through 64kb/s link to Sprint in United States, connected first time in March 29th 1994. Since that day, Philippines got permanent internet connection, while the first commercial ISP in Philippines appeared in August 1994, with Mosaic Corporation (Moscom), that launched their service at that month.<sup>24</sup>

It needs some time for the internet usage to be something common in Philippines. This is primarily due to the expensive cost of internet usage at that time. The cost problem is due to the hierarchical Philippine internet market structure, in which the Value Added Service (VAS) internet providers had to lease communication infrastructure from a licensed telecommunication operators, and only 13 companies have their own network. Nearly all international telecommunication operators leased international bandwidth for consumer end ISP. The large ISP then sells the connection to smaller provincial ISPs.<sup>25</sup>

Despite of this situation, some groups, including intermediary groups started to use this new information resource. They started to prefer to use electronic mail and publish various materials through email centers established by Roberto Verzola, and developed by Caucus of Development NGO Network and the Foundation for Media Alternatives. Another important note in the internet development in Philippine is related to content. Although 90% of the internet traffic from Philippines is bound to United States, yet various institution and mass media in Philippines contributes largest portion of local content accessible in the internet.<sup>26</sup>

At the early stages of internet development in Philippines, there are only a few ISPs, only 19 ISP in 1995, then grew into 88 ISPs in 1996, and more than 160 at end of 1997. Up to 2006 at least there are 408 ISPs registered at the National Telecommunication Commission (NTC).<sup>27</sup> Besides obliged to be registered and verified by NTC, these ISP also have to deal with The Commission on Information and Communication Technology (CICT), established in 2004. The ISP companies also joined in the Philippine Internet Service Organization (PISO). The PISO was established in 1996 with initial members of 30 ISPs. Initially the members of PISO are only access provider companies, but later on non access companies such as web design, software development, domain registration, wireless, and hosting companies also joined the PISO. The model is similar with the PIKOM in Malaysia. PIKOM had the vision of promoting the development and growth of internet industry and related sector, by protecting the stakeholders and beneficiaries, promoting sustainable technology innovation, healthy competition and supporting entrepreneurship in the ISP communities in Philippines.<sup>28</sup>

23 See ITU, *Pinoy Internet: Philippines Case Study*, (Geneva: International Telecommunication Union, 2002).

24 See Emmanuel C. Lallana and Cheryll Ruth Soriano, *Towards Universal Internet Access in the Philippines*, (Manila: ideacorp and Intel Technology Philippines, Inc, 2007). Accessible at <http://www.unapcict.org/ecohub/resources/towards-universal-internet-access-in-the-philippines>, accessed in August 1st 2013

25 See ITU, *Pinoy Internet... Op. Cit.*

26 See A. Pabico, Online advocacy, in S. S. Coronel (Ed.), *From Loren to Marimar: The Philippine media in the 1990s*. (Quezon City: Philippine Center for Investigative Journalism, 1999)

27 See Erwin A. Alampay, *Telecom Regulatory and Policy Environment in the Philippines: Results and Analysis of the 2008 TRE Survey*, accessible at [http://limeasia.net/wp-content/uploads/2009/07/TRE\\_Philippines\\_final\\_2008Nov29.pdf](http://limeasia.net/wp-content/uploads/2009/07/TRE_Philippines_final_2008Nov29.pdf).

28 See <http://www.ncc.gov.ph/default.php?a1=2&a2=5&a3=1&a4=PQRS&a5=37>. See also "Information Technology in The Philippines", in <http://www1.american.edu/carmel/bree/internet.html>, accessed in August 1st 2013.



In the context of local internet network empowerment, in July 1997, for the first time, Philippine launched Philippine Internet Exchange (PHIX). The PHIX is a network access point that enables Philippine ISP to exchange local internet traffic in Philippine without having to connect to overseas host server. PHIX was established by several ISP, amongst PLDT (Philippines Long Distance Telephone Company) and interconnects Infocom, Iphil, Moscom, Virtualink, and WorldTel. The Idea had actually been launched 1995, pioneered by PLDT, and formally presented October, 26th 1996 to 15 local ISPs, each having their own connection to other countries.<sup>29</sup>

**Table 1: Number of users and Internet penetration in Southeast Asia**

Country	Population (2012)	Internet users (2000)	Internet users (2012)	Penetration (% Population)	Facebook (2012)
Brunei Darussalam	408.786	30	318.900	78.0 %	25.476
Cambodia	14.952.665	6	66.284	4.4 %	74.222
Indonesia	248.645.008	2.000.000	55.000.000	22.1 %	51.096.860
Laos	6.586.266	6	592.764	9.0 %	25.588
Malaysia	29.179.952	3.700.000	17.723.000	60.7 %	13.589.520
Myanmar	54.584.650	1	53.493	1.0 %	n/a
Philippines	103.775.002	2.000.000	33.600.000	32.4 %	29.890.900
Singapore	5.353.494	1.200.000	4.015.121	75.0 %	2.915.640
Thailand	67.091.089	2.300.000	20.100.000	30.0 %	17.721.480
Timor-Leste	1.143.667	0	10.293	0.9 %	n/a
Vietnam	91.519.289	200	31.034.900	33.9 %	10.669.880

Source: <http://www.internetworldstats.com/stats3.htm>

Furthermore, if we compare the growth of internet users in the Southeast Asia regions, we can find that of the 3 countries (Indonesia, Malaysia, and Philippines), at the early stages of internet technology introduction, Malaysia rank the highest in the internet usage. The figures above shows even early in 1995, one of thousand Malaysian population uses internet, which means at that time the number of users is approximately 20,000. Five years later in 2000 according to data from Internet World Stat, the internet users in Malaysia reaches 3.7 million people, highest compared to other Southeast Asian countries. The number rises rapidly in next five years, in 2005 Malaysia had approximately 11 million internet users with penetration level of 42% of the population. The penetration level of 42% put Malaysia in the second rank in Southeast Asia, one level under Singapore, but in the following years, growth of internet users are no longer significant, although still rising. In 2012, the number of internet users in Malaysia is 17.723 millions, penetrating 60% of the population. Malaysia is third rank under Brunei Darussalam (78%) and Singapore (75%) in terms of internet penetration level in Southeast Asian countries.

The high penetration at the early stage of internet development in Malaysia was possible due to high commitment of the government in building the internet infrastructure, as indicated by the existence of National Information Technology Agenda (NITA) in 1996. This agenda is integral part of Malaysia

29 See <http://www.phix.net.ph/>. See also Grace In Mono, Localizing the Internet in the Philippines, in <http://www.telecomasia.net/>, April 24th 2012.

2020 vision. Even in the most technical level the Malaysian government endorses the citizen to buy personal computers and connect it to the internet. The program is famously known as “One Home, One computer.” Through this program every Malaysian who have Employee Provident Fund (EPF) are allowed to withdraw part of the fund to buy computer. The government also endorses every Malaysian family to buy domestic PC through a credit scheme from their retirement fund.<sup>30</sup>

Nevertheless, Malaysia also had to address the problem of digital divide between urban and rural areas. Internet penetrations are only big in cities, especially in west Malaysia such as Kuala Lumpur and other states such as Negeri Sembilan and Selangor. Other areas, east Malaysia have low penetration, such as Sarawak and Sabah that had penetration of only 5.9% of the population.<sup>31</sup> Addressing digital divide, in 2010, Malaysian government had launched National Broadband Initiative that is expected to increase the internet penetration and decrease digital divide.<sup>32</sup>

The Philippines had slower internet usage growth than Malaysia. In early stages of internet adoption in Philippines, in 1994, according to International Telecommunication Union (ITU), Philippines only have 4,000 user or penetration of only 0.005% of the total population. To endorse the growth of internet technology in Philippines, in 1993, president Fidel Ramos issued two executive orders (EO), mandating the provision of interconnection and expansion of telecommunication services through competition and market liberalization in Philippines. One of the EO, is EO number 59 that obliged the interconnection between local telecommunication companies, and cheaper telecommunication subscription rates. The other EO, number 109, mandated the improvement of Local Exchange Carrier (LEC). Through this EO, Service Area Scheme (SAS) was established that divided Philippines into 11 geographic service zones. At the following period, after the republic Act 7925 in 1995, telecommunication regulation is handed over fully to the National Telecommunication Commission, including service rate setting.<sup>33</sup>

After the issue of EO 109 that calls for expansion of telecommunication services to remote areas, then the penetration of internet in Philippines slowly rises. The EO also endorses competition in the information technology business sector, nevertheless, a study released by NTC in 2003, showed that only 78.7% network were established under the EO 109, the rest are failed to be build by public telecommunication entity, due to various factors, such as lengthy conflicts in South Philippines, and the Asian economic crisis at that time.<sup>34</sup> Despite of the situation, Ramos government efforts at least had increased the internet penetration level in the Philippines. Up to year 2000, at least 2 million Philippines had enjoyed internet, an increase compared to previous five years, that were only thousands.<sup>35</sup> Up to 2012, there are 33.6 million internet users in the Philippines, ranking second

---

30 See Ali Salman, et al, *Tracing ... OP .Cit.*

31 See <http://www.newmediatrendwatch.com/markets-by-country/11-long-haul/55-malaysia>, accessed in August 1st 2013

32 See “Target: Broadband Penetration to Go Up to 50% by Next Year”, in <http://malaysiakini.com/news/117064>, accessed in August 1st 2013.

33 See Cheryl Ruth R. Soriano, Universal Access in the Philippines: A Review of Policies and Strategies, Paper for the CPRsouth2 2007: Research for Improving ICT governance in the Asia Pacific, December 2007, Chennai, India. Accessible at [http://www.cprsouth.org/wp-content/uploads/drupal/Cheryl\\_Soriano.pdf](http://www.cprsouth.org/wp-content/uploads/drupal/Cheryl_Soriano.pdf).

34 See Mary Grace P. Mirandilla, Achieving Universal Access through Liberalization, Regulation, and Deregulation: The Case of the Philippine Telecommunications and ICT Sector, Paper in the Communication Policy Research (CPR) south2 conference on December 15-17, 2007 in Chennai, India. Accessible at [http://www.cprsouth.org/wp-content/uploads/drupal/Grace\\_Mirandilla.pdf](http://www.cprsouth.org/wp-content/uploads/drupal/Grace_Mirandilla.pdf)

35 See ITU, Pinoy Internet... Op. Cit.

largest in Southeast Asia after Indonesia, with penetration of 32.4%, ranking the fourth in all Southeast Asia.<sup>36</sup>

Digital divide also one of the primary problem in Philippines, internet is only concentrated in large cities such as Manila. One of the survey notes that half of the internet users are in Manila.<sup>37</sup> It seems that one of the factors that contributed low internet penetration in Philippines is the minimal number of household that own a computer in the rural areas, besides that, lack of infrastructure is also a factor. Internet penetration rises sharply after 2008, after the coming of new players in the telecommunication industry and the expansion of cellular phones, although it is still concentrated in the large cities where people have much larger income than those in the rural areas.

The internet technology in Indonesia also developed in slow pace. As in Philippines, Infrastructure is also a primary challenge in the internet development in Indonesia. Up to year 1998, according to International Telecommunication Union (ITU), the number of internet subscribers in Indonesia is only 134,000 or 0.07 per 100 people, i.e. the number of internet users per 100 people is 0.26%. This is a small figure compared to Malaysia of 405,000 people and Philippines of 300,000 people.<sup>38</sup> The figures increases significantly year by year, in year 2000, APJII data showed that the internet users in Indonesia reaches 1.9 million users, five years later, in 2005 reaches 20 million user, and rises sharply in 2010 to 42 million users. As at the end of 2012, according to APJII calculation, there are already 63 million internet users in Indonesia, with penetration level of 24.23%.<sup>39</sup> These figures are not so high compared to the total population of 250 million people.

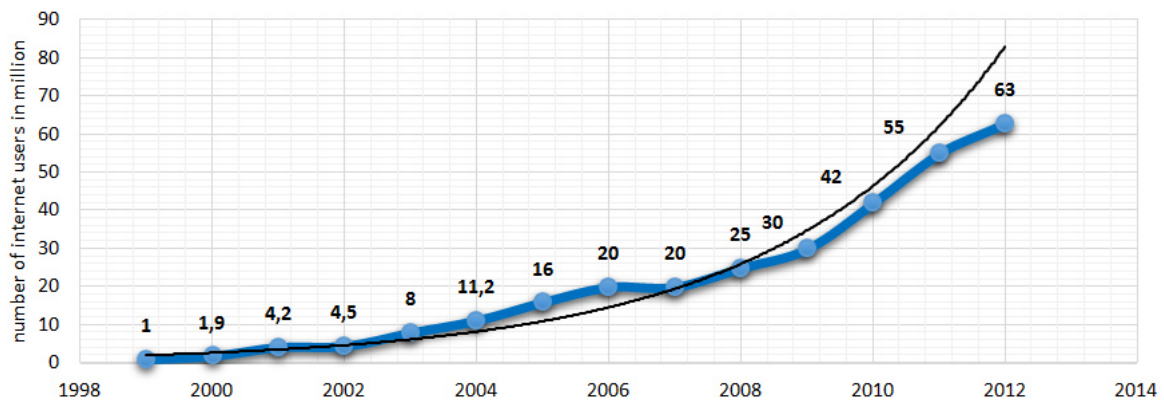
At the early stage of internet development, the internet growth is not too significant. As an archipelago country like Indonesia, the largest obstacle for internet expansion is infrastructure issues. The difficulties of building inter-island (telecommunication) infrastructures limits the concentration of internet connection only in major cities, especially Java, it should be admitted that all this time network infrastructures development were majorly done in Java. The fantastic growth of Internet user in Indonesia happened after 2009, surging from 30 million to 40 million in 2010. The surge of internet users in Indonesia was influenced by the popular use of mobile internet, and appearance of unlimited service package from certain service providers. The surge of blackberry product and smart phones produced in china also contributed to the increase of internet users in Indonesia. The details of internet user growth in Indonesia according to APJII can be viewed in the following graph:

36 See <http://www.internetworldstats.com/stats3.htm>, accessed in August 1st 2013.

37 See Emmanuel C. Lallana and Cheryll Ruth Soriano, *Towards ... Op. Cit.*

38 See [http://www.itu.int/ITU\\_D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP\\_intYear=1998&RP\\_intLanguageID=1&RP\\_bitLiveData=False](http://www.itu.int/ITU_D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=1998&RP_intLanguageID=1&RP_bitLiveData=False), accessed in August 1st 2013.

39 See "2013, Pengguna Internet Indonesia Bisa Tembus 82 Juta", in <http://www.apjii.or.id/v2/index.php/read/content/apjii-at-media/139/2013-pengguna-internet-indonesia-bisa-tembus-82-ju.html>, accessed in August 1st 2013.

**Figure 1: The growth of internet user in Indonesia**

Source: <http://www.apjii.or.id/v2/index.php/read/page/halaman-data/9/statistik.html>.

The problem of digital gap is also inevitable problem in Indonesia, as well as other developing countries. As mentioned, the access to internet in Indonesia is only concentrated in major cities, especially Java, even in those areas, the penetration has reached 57% of the population.<sup>40</sup> To address this problem of access due to scarce infrastructure, the government of Indonesia, through the Ministry of Communication and Information, has launched a Palapa Ring project. The project focuses on the deployment of 36,000 miles of fiber optic cable throughout Indonesia, consisting of seven circular fiber optic (for Sumatra, Java, Borneo, Lesser Sunda Islands, Celebes, and Moluccas) and a backhaul connecting this entire network. This project is expected to reach out to all the sub-provinces/cities in Indonesia, so all citizens can have equal communication access, especially Internet.<sup>41</sup>

After the network infrastructure development, the Indonesian government, through the Ministry of Communication and Information, since 2010 has been deploying the Universal Service Obligation (USO), which attempts to build infrastructures to the remote areas of Indonesia. The program is carried out through the village telephone and village internet programs, village internet service center and mobile village internet service center. The funding of the program is collected from various telecommunication operators equivalent to 1.25% of the annual total revenue of the companies.<sup>42</sup> Nevertheless, the program implementation is also under some criticism as well as problems such as allegations of corruption in the implementation of village internet service center and mobile internet

40 See "Mobile overtakes internet cafes as primary access point", in <http://www.emarketer.com/Article/Indonesias-Cities-Mobile-Boosts-Internet-No-2-Media-Spot/1009637>, accessed in August 1st 2013.

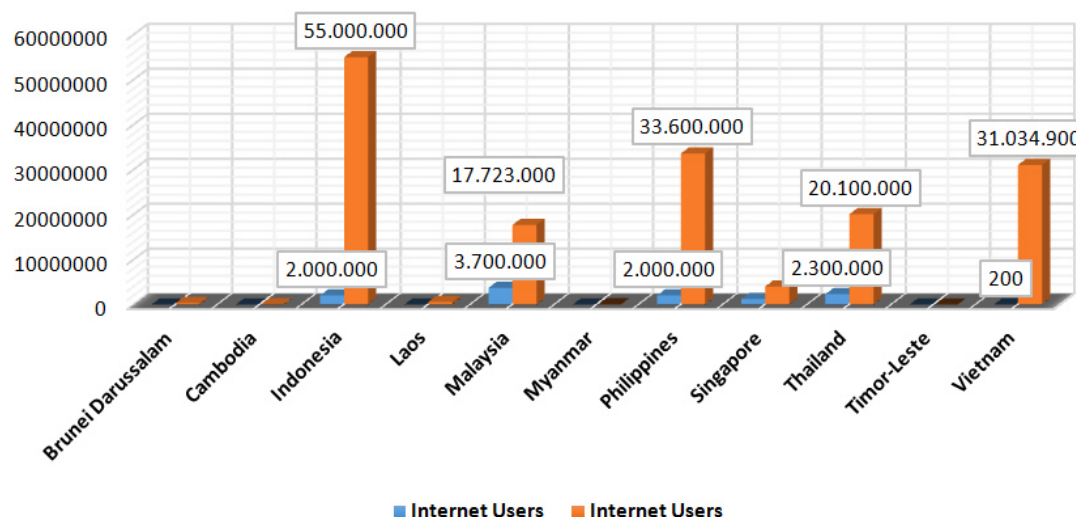
41 See "Palapa Ring", in <http://www.detiknas.org/index.php/flagship/c/14/>, accessed in August 1st 2013.

42 See "Penyebaran PLIK dan M-PLIK Wujud Hak Masyarakat Peroleh Informasi", in [http://kominfo.go.id/berita\\_kemendrian/detail/4005/Penyebaran+PLIK+dan+MPLIK+Wujud+Hak+Masyarakat+Peroleh+Informasi](http://kominfo.go.id/berita_kemendrian/detail/4005/Penyebaran+PLIK+dan+MPLIK+Wujud+Hak+Masyarakat+Peroleh+Informasi), accessed in August 1st 2013.

service center projects.<sup>43</sup> Meanwhile on the village internet program, up to second semester of 2011, only 107 villages had been installed with the equipments.<sup>44</sup>

Based on the previous treatise, compared to internet penetration in Indonesia and Philippines, Malaysia is in the highest rank position at 60% of the total population. The second rank is Philippines at 32.4%, while Indonesia is the last position with penetration of 24.23% of the total population, yet looking at the number of users, Indonesia is the largest compared to other countries.

**Figure 2: comparison of the growth of internet users in Southeast Asia**



Source: <http://www.internetworldstats.com/stats3.htm>.

Examining the figure, referring the data released by Internet World Stats, compared to early internet use in year 2000, the number of internet users in Indonesia had a big surge from two millions to 55 millions. Philippines also had surge from 2 million to 33.6 million, while Malaysia had been growing fast from the early stages in terms of population but yet still plagued by digital gap issues, like Indonesia and Philippines. In the future, Malaysia might reach saturation point in terms of penetration, while Indonesia according to APJII would continue to grow to 139 million users in 2015, equivalent to 50% of the population.

### C. Internet as communication and information access facility: regulation development

The use of internet technology in Indonesia as tool of communication and search and dissemination of information is relatively new. The regulation related to information technology made after internet age, even had not specifically governs the internet technology. At that time the Indonesian government had not yet prepared long term plan to develop and expand internet access in

43 See "Graft suspected in Rp 40 trillion IT project", in <http://www.thejakartapost.com/news/2013/07/11/graft-suspected-rp-40-trillion-it-project.html>. See also response of ministry of communication and information to that news, in the press release. Number 55/PIH/KOMINFO/7/2013, Available at <http://kominfo.go.id/berita/detail/4057/Siaran+Pers+No.+55-PIH-KOMINFO-7-2013+tentang+Tanggapan+Terhadap+Berita+Mengenai+Potensi+Penyalah+Gunaan+Anggaran+di+Kementerian+Kominfo>, accessed in August 1st 2013.

44 See "Desa Pinter yang Terpasang", in <http://statistik.kominfo.go.id/site/data?idtree=244&iddoc=789>, accessed in August 1st 2013.

Indonesia. Initially the regulation of internet as communication and telecommunication facility refers to act number 3 of 1989 on telecommunication. The act replaces act number 5 of 1964 on Telecommunication that approves substitute act number 1963 on telecommunication into act. The act was regarded irrelevant to the technology advances of the late 1980s. The regulation that appeared at the new order reign in general governs all the telecommunication apparatus, so all the apparatus used in the telecommunication wire, optic, radio or any other electromagnetic system although not explicitly mentioned abides to this law.<sup>45</sup>

In 1996, after the use of internet flourish in many cities, Indonesian government finally issued a regulation on the rate of internet service price, through the decree of ministry of tourism and telecommunication number KM.59/PR.301/MPT-96. In this price regulation, three price scheme are regulated namely, the registration, subscription, and usage price.<sup>46</sup> At that time internet was regarded as a special broadcasting, so its regulation obeys to the existing schemes of regulations under the directorate general of post office and telecommunication. This institution has also the authority to issue a license for the establishment of ISP companies. A team formed by ministry of tourism, post office and telecommunication was given a special authority to select and evaluate all the proposal of license, including the business plan of each ISP. After being established, the ISP companies are obliged to report their activities regularly, and their license would be reviewed every five years.

After the fall of Suharto, in 1999, The government of Indonesia, under the president Habibie's power, changed the Telecommunication Act number 3 1999 into Act number 36 1999 on Telecommunication. Judging the scope, i.e. the communication apparatus, there is not significant change. The new act also does not specifically discuss even the use and development of internet technology, let alone specifically the content. The regulation and usage of the whole telecommunication apparatus and technology were still placed under a very general framework as the previous act.<sup>47</sup> Based on the Act number 36 of 1999, some derived regulations were issued related to the telecommunication provision, including internet. One of the derivate regulation is government bill number 52 of 2000 on the telecommunication provision. According to this regulation, internet is categorized under multimedia service, including voice over internet (VoIP), internet, intranet, data communication and video conference.<sup>48</sup> Subsequently some regulations to regulate internet business and traffic in Indonesia, through ministry level and related official regulations.<sup>49</sup>

In 2008 the government issued a new regulation related to the use of information technology, i.e. the act number 11 of 2008 on Electronic information and transaction (Known as UU ITE). This regulation had been constructed at least since 2003. At the draft stage there were two draft produced, namely the draft of information technology usage (RUU PTI), and the draft of electronic information and transaction (RUU IETE). Judging the content of regulation, both draft apparently were responses to information technology development that through cyberspace had impacted the global and national trade and economy. The importance of legal response to the technology

45 See general provision Article 1 points 1, 2, and 3 act Number. 3 of 1989 on telecommunication.

46 Available at [http://www.apjii.or.id/v2/upload/Regulasi/KM59\\_1996.pdf](http://www.apjii.or.id/v2/upload/Regulasi/KM59_1996.pdf).

47 Available at [http://pkps.bappenas.go.id/dokumen/uu/Uu%20Sektor/Telekomunikasi/20.%20uu\\_36\\_1999.pdf](http://pkps.bappenas.go.id/dokumen/uu/Uu%20Sektor/Telekomunikasi/20.%20uu_36_1999.pdf).

48 Available at [http://www.apjii.or.id/v2/upload/Regulasi/PP\\_52\\_2000.html](http://www.apjii.or.id/v2/upload/Regulasi/PP_52_2000.html)

49 Available at <http://www.apjii.or.id/v2/index.php/read/page/halaman-data/8/regulasi.html>



advances impact on various economic and social dimensions implies the need of legal regulation of the cyberspace. In March 2003, the ministry of Communication and information starts to design the draft of Electronic Information and Transaction act (RUU ITE).<sup>50</sup>

Based on the problem identification by RUU ITE drafter team, there are at least five issues of the RUU ITE, namely:

1. Principles and regulations
2. Favorable regulation model for use of information technology and electronic transaction
3. Content of the regulation
4. International Instrument to be referred
5. Scope of offences to be regulated

In general, the content of academic text shows a broad spectrum that governs the Cyberspace Act in Indonesia as reflected by rigorous references to various international instruments and law practices in various countries as the foundation vision to formulate the regulation. RUU ITE also governs the position of electronic document, electronic information, and electronic signature in law, and the usage, electronic system institutionalization, electronic certification provision, electronic transaction aspects, domain name, intellectual property rights, privacy protection, and regulation of society and government participation. Basically nearly all the articles in the UU ITE were geared to rule the excesses of the rapid global information technology advance to the economy and trade.

After being issued, this regulation triggered controversies, as this act, besides recognizing and protecting the electronic information, document, signature and transaction, also stipulates penal sanctions. The formulation of this regulation, does not bear the spirit of expanding the electronic trade, but instead sternly limits it. The strong limitation is reflected in the penal sanctions in internet content, namely expansion of defamation, hate speech, and obscenity into information technology. The formulation in that regulation could lead to multiple interpretations, violates the *lex certa* principle in penal law, with serious implication to Indonesian social politic life.<sup>51</sup>

The strictly limiting formulations, is an interesting fact related to the general explanation of the UU ITE that states UU ITE is a synergy of three approaches, namely legal approach, technology approach, and social cultural ethical approach, with amongst, consideration of religious values and Indonesian social cultural values in the use of information technology. This is the context that resulted some controversial articles in UU ITE, specially concerning internet content.

In Malaysia, the regulation related to the use of computer and internet technology came about initially in 1997, when the government of Malaysia issued Act number 563 of 1997 on computer crimes. The regulation governs amongst networked computer, defined as interconnected communication and electronic circuit consisting of two or more connected computers.<sup>52</sup> This regulation amongst governs illegal access prohibition, illegal forms of communication using computer networks. According to the computer crime regulation, anyone performing illegal

50 See Wahyudi Djafar, et al, Hak Asasi Manusia in Pusaran Politik Transaksional: Penilaian terhadap Kebijakan HAM in Produk Legislasi and Pengawasan DPR RI Periode 2004-2009, (Jakarta: Elsam: 2012). Available at [http://elsam.or.id/article.php?lang=in&id=1731&act=content&cat=401#UjaFj9L\\_wQ0](http://elsam.or.id/article.php?lang=in&id=1731&act=content&cat=401#UjaFj9L_wQ0)

51 See Article 27, 28, and 29 Electronic Transaction and Information Act (UU ITE)

52 See Article 2 Item (1) Malaysia Computer Crime Act

communication, using numbers, code, or crypt or accessing other people computer without permission of the owner can be sanctioned as much as twenty five thousands ringgit fine or maximum three years sentence, or could be both fined and sentenced.<sup>53</sup>

Later on, along with the advances of information and computer technology, in order to develop as well as to control the usage of information technology, the Malaysian parliament had approved a series of regulations related to the information and communication technology. After the computer crime act, in 1998, the Malaysian government approved Act number 588 of 1998 on communication and multimedia, and Act number 589 of 1998 on Multimedia commission, effectively establishing the Malaysian multimedia commission. The two acts directly governs matters related to telecommunication, broadcasting, and internet, including the internet service and content, while the communication and multimedia commission have the mandate of governing the information and communication technology industry in Malaysia.

In February 2001, based on mandate of both act (CMA and CMCA), the commission had also established Malaysian communication and multimedia content forum (CMCF). The forum is aimed to endorse the communication and multimedia forum in Malaysia to establish self regulation. The forum is managed by a chair person and 18 members selected for two years period, representing service providers, content providers, advertising agencies, and other groups including civil society groups. Referring to the CMA, the communication and multimedia industry in Malaysia is responsible for setting the content code or any other codes relevant to the possible need in communication and multimedia. This forum also receives communication and multimedia consumer and industry complaints, related to electronic contents.<sup>54</sup>

The next discussion is on the information and communication technology system in the Philippines. Philippines is one of the pioneering countries establishing independent body to regulate telecommunication. At the time Philippines is still under 1973 constitution, in July 23rd 1979, The Philippines government issued Executive Order number 546 on the Establishment of National Telecommunication Commission. This is a quasi-judicial body under the coordination of ministry of transport and communication. This commission had the authority amongst to certify communication services using any devices. This body also governs the operational territory of telecommunication companies, allocates frequency, control of communication activities, and other functions governed by law.<sup>55</sup> Later on in Corazon Aquino's rule, based on executive order number 125-A issued in April 13th 1987, the commissions quasi-judicial position is merged into integral part of ministry of transport and communication.<sup>56</sup>

Outside the function of the ministry of transport and communication that supervise all the telecommunication activities in the Philippines, including internet, in the year 2000, at the era of President Joseph Estrada, the National Information Technology Council (NTIC) was established, directly answerable to the president's office. The president then merged this council with National Electronic Transaction Council (NTEC), into the National Electronic Information and Transaction

53 See Article 6 Item (1) and (2) Malaysia Computer Crime Act.

54 For complete see <http://www.cmcf.my/home.php>.

55 See part 15 Executive Order No. 546 of year 1979, Available at [http://www.lawphil.net/executive/execord/eo1979/eo\\_546\\_1979.html](http://www.lawphil.net/executive/execord/eo1979/eo_546_1979.html)

56 See part 13 Executive Order No. 125-A of year 1987, Available at [http://www.lawphil.net/executive/execord/eo1987/eo\\_125\\_a\\_1987.html](http://www.lawphil.net/executive/execord/eo1987/eo_125_a_1987.html)



Council (ITECC), through executive order number 264 year 2000.<sup>57</sup> Later on another change is in 2001, at the era of President Gloria Macapagal-Arroyo, in which ITECC was put directly under president as the chair person of the commission, based on the executive order number 18 year 2001, practically giving her powers to supervise the direction of ITECC and the development of information and communication technology in the Philippines.<sup>58</sup>

In January 12th, 2004, President Gloria Macapagal Arroyo issued Executive order number 269 on the Establishment of Communication and Information Technology Commission (CICT). After this commission was established, the function of National communication Commission (NTC) that previously attached to the ministry of transportation and communication is moved to become part of the CICT. The members of CICT are from NTC as well as from National Computer Center (NCC), Telecommunication Office (TELOF), Office of telecommunication policy and planning, and Philippine postal company.<sup>59</sup> Based on the regulation that formed it, the commission had a very broad authority, covering the planning, control and supervision of the use of information and communication technology in the Philippines. This commission also have the mandate to assure strategic information provision, including information and communication technology infrastructure, endorse and accelerate convergence beyond just the network development, assuring universal access, building strong and effective regulation system that recognizes consumer protection, protecting individual rights, specially related to privacy and confidentiality.<sup>60</sup>

The structure of National Telecommunication Commission was changed again in 2005. President Gloria Macapagal Arroyo reassigns the function of NTC into the ministry of transportation and communication through the Executive order number 454 of year 2005.<sup>61</sup> Before two years, again President Arroyo reassigns NTC function from ministry of transportation and communication back to CICT through executive order number 648 of 2007.<sup>62</sup> President Arroyo also reassigns the function of telecommunication office (TELOF) into part of the Communication and Information Technology Commission through executive order number 780 year 2009.<sup>63</sup>

The last restructurization is made by President Benigno S. Aquino in 2011, with the executive order number 47 2011. Through this executive order, President Aquino changed the Communication and Information Technology Commission into Information and Communication Technology Office (ICTO), under the coordination of ministry of knowledge and technology, while the National Telecommunication commission and Philippine postal company stays under the president office, while the telecommunication office (TELOF) and National Computer Center (NCC), previously under the CICT, is returned to the ministry of science and technology.<sup>64</sup>

57 See part 1 Executive Order No. 264 year 2000, Available at <http://www.itecc.gov.ph/files/eo%20264.pdf>.

58 See part 3 Executive Order No. 18 year 2001, Available at <http://www.itecc.gov.ph/files/eo%2018.pdf>. See also <http://www.itecc.gov.ph/about.htm>

59 See part 3 Executive Order No. 269 year 2004, Available at [http://www.lawphil.net/executive/execord/eo2004/eo\\_269\\_2004.html](http://www.lawphil.net/executive/execord/eo2004/eo_269_2004.html)

60 Information and communication technology, in this regulation is defined as all the electronic facilities to gather, store, process and present information to end user to support their activities. This includes, computer system, electronic system, and information network infrastructure, components covering telephone, internet, fax and computer system, see part 2 Executive Order No. 269 year 2004.

61 See EO No. 454 year 2005, Available at <http://www.gov.ph/2005/08/16/executive-order-no-454-s-2005/>

62 See EO No. 648 year 2007, Available at <http://www.gov.ph/2007/08/06/executive-order-no-648-s-2007/>

63 See EO No. 780 year 2009, Available at <http://www.gov.ph/2009/01/29/executive-order-no-780-s-2009/>

64 See part, 1, 3, and 4 EO No. 47 year 2011, Available at <http://www.gov.ph/2011/06/23/executive-order-no-47/>

Referring to the Executive Order number 47 2011, ICTO has the functions of amongst, formulating and recommending and implementing information and communication technology, assuring provision of information and efficient and effective information technology infrastructure, conducting research and development on information and communication technology, in multi party collaboration, building the capacity of public sector institutions in the use of Information and communication technology, preparing plans for e-governance based information and budgeting systems, and other possible functions.<sup>65</sup> The license and permit issues related to the use of information and communication technology remains as the function of NTC, as well as the function of supervision on all the telecommunication and broadcasting activities.<sup>66</sup>

The situation shows the frequent changes in the policies related to use and development of information and communication technology in Philippines. The ICT policies always change with the change of national leadership, indicating direct interest and influence of each president in governing and controlling the use of ICT. Through the presidential administrative authority to issue executive order, President can issue any regulation to establish institution that deals with control, usage and development of ICT, including ICT policy itself. This is actually a situation vulnerable to abuse, as the ICT policy depends on the ruling president. The ICT policy, including usage and control model would follow the president's political intention.<sup>67</sup>

The frequent changes in the ICT policies in Philippines, especially in the institutions that governs usage and control of ICT reflects the intense government, especially president's interest in ICT sector in the Philippines. Nevertheless, viewing the regulations jointly issued by both legislative and executive (acts), the early stages in Philippines are not as dynamic as Malaysia. On the expansion of access, policy reform to accelerate the growth of telecommunication development and universal access to ICT, Philippines issued the Act number 7925 year 1995 on Public Telecommunication Policy (Republic Act 7925), in March 1995 after the issue of Executive order number 109 year 1993. This telecommunication policy act enables competition between private sector in Philippines in the development of ICT infrastructure.

Republic Act 7925 had provided broad authority for the National Telecommunication Commission in Philippines. This act affirms NTC as the primary administration in act implementation, thus NTC can take the necessary measure to carry the legal mandate. The Republic Act 7925 states that NTC had the responsibilities of: regulating the telecommunication price policy; ensuring the quality and safety of telecommunication services, including issuing the license; ensuring fair and sensible competition between telecommunication service providers; protecting the consumer from monopoly of telecommunication services; supervision of operation of telecommunication service provider.<sup>68</sup>

Aside of regulating on a set of authority owned by NTC and telecommunication service provider entities, the law will also regulate the rights of any telecommunication service end users. According to this regulation, end user rights comprises a non-discriminative access to quality service

65 See part 2 EO No. 47 year 2011. See also <http://icto.dost.gov.ph/index.php/home>.

66 See [http://www.ntc.gov.ph/about\\_functions\\_01.php](http://www.ntc.gov.ph/about_functions_01.php)

67 See Mary Grace P. Mirandilla, *Achieving Universal Access ...* Op. Cit.

68 See Article 3 part 5 RA 7925. Available at <http://ntc.gov.ph/laws/laws/LAW%207925.pdf>

conforming with the minimum standard set by the Commission (NTC). End users also have the right for a thorough and punctual investigation should they reported any complaints related to services.<sup>69</sup>

Next in Year 1998 law, on 11 February 1998, the Congress of Philippines successfully approved the formation of Act No. 8484 Year 1998 on the Regulation of Access Devices (Republic Art 8484). Access devices referred in this Act is all type of cards, discs, code, account number, electronic serial numbers, personal identification number or other telecommunication services, devices or instrumental identifier, or other ways that can be utilized to access an account, for the goal of gain money, services or other valuables or to do a fund transfer.<sup>70</sup> Furthermore the Act regulate the publishing and the use of access device, banning illegal access and fraud using access device, and threat of fine if the regulation is violated, also other criminal punishment as it is regulated by the Philippines Penal Code and other specific law regulation.<sup>71</sup>

The new era of regulation on information and communication technology utilization in the Philippines, took place in year 2000, with the urgency to prevent cyber crime. The urgency was at least prominence after Onel de Guzman, a Philippine student; spread a computer virus known as "i love you" virus to the global computer network. The virus caused damage to computers of many corporations, private and government institutions in Asia. The losses caused by the computer virus attack were approximately ten billion US dollar. The virus sent through electronic mails was able to delete and blur out graphics and computer data, it was also able to access all contacts at the computer directory and sent out similar e-mail--virus to all contacts. Because of his action Guzman was apprehended by the Philippines police force, involving the international police, but in the process the Guzman case had to be stopped due to the *nullum crimen, nulla poena sine lege* principle (there aren't any act of crime without pre-existing law of crime), which applies to the Philippines penal code.<sup>72</sup>

Following the incidence, on 14 June 2000, the Congress of Philippines finally approved the passing of Act No. 8792 Year 2000 on Electronic Trades (Republic Act 8792). The passing of this act aimed among other to prevent cyber crime threats, the effort to increase e-commerce in the Philippines, which enables consumers to find and buy products in the network. From the stand point of administering government, the establishment of developing electronic system is hoped to reduce bribery and corruption within the government, because the process in the network at least reduces personal interaction between the government agents and the personal citizen. From the stand point of substance, the Act is a mark of legal recognition on letters, data, documents and electronic hand signature, also can be used as evidence in the court of law.<sup>73</sup> Apart from recognizing electronic documents, RA 8792 also provides legal threat for cyber criminals in the network, such as hacking, spreading computer virus, and copyright violation. Threat for such crime is one hundred thousand Philippine pesos legal fine or commensurate to the damage caused by the crime. Other applicable criminal punishment threat is imprisonment between six months to three years.<sup>74</sup>

69 See Article 7, section 20 of RA. 7925.

70 See Section 3 letter a. RA. 8484. Available at <http://www.pctc.gov.ph/initiatv/RA8484.htm>.

71 See Section 9 and section 17 RA. 8484.

72 See Gilbert C. Sosa, Country Report on Cybercrime: The Philippines, Participating paper in The Criminal Justice Response to Cybercrime, course Tokyo, December 2009. Can be accessed on [http://www.unafei.or.jp/english/pdf/RS\\_No79/No79\\_00All.pdf](http://www.unafei.or.jp/english/pdf/RS_No79/No79_00All.pdf).

73 See Chapter II RA 8792.

74 See Sub-section V Part 33 RA 8792.

The argument on regulation information and communication technology in the Philippines is back on the spotlight with the passing of Act No. 10175 Year 2012 on Prevention of Cyber Crime, on 12 September 2012 by the President Benigno S. Aquino (Republic Act 10175). Despite the Act being made to prevent, detect, investigate, and cyber crime litigation, also ensuring constitutional protection to the digital world in the Philippines, yet the materials are considered opposing the protection on the freedom of expression, freedom of speech, freedom of opinion and data protection in the Philippines.<sup>75</sup>

The Act material regulates more on the types of cyber crime and violation, which are divided into three categories of violations: first, breach of confidentiality, integrity and data availability, and computer system; second, violations related to computer device; and third, violation related to content. Included in the first category violation according to this law: illegal access, illegal wiretapping, data interference, system interference, misuse of device, and cyber-squatting. The followings are included into the second category violation: forgery related to computer, fraud related to computer, and identity theft. While violation related to content includes: cybersex, child pornography, unwanted commercial communication, and contempt.<sup>76</sup>

Several days after the Act was passed, fifteen lawsuits were brought separately to the Supreme Court (SC) opposing at least fourteen provisions in the law.<sup>77</sup> Responding the petition, the Philippines SC on 9 October 2012 finally issued a suspension of the Cyber Crime Prevention Law execution for 120 days.<sup>78</sup> After hearing testimonies of the plaintiffs on 15 January 2013, and explanation from the government represented by the Attorney General on 22 January 2013, in the proceedings on 5 February 2013, SC decided to impede/stop the execution of the Republic Act 10175, until the next ruling on the law.<sup>79</sup>

In its development, in 24 May 2013, President Aquino administration through the Department of Justice, decided to erase the provisions of criminal contempt in Republic Act 10175. Hereafter the threat of criminal contempt penalties refers to regulations in the Philippines Penal Code, and other laws that already exist, such as Child Pornography and cyber squatting laws. Moreover, the Department of Justice also stated their support to the revision of Cyber Crime Prevention Law in the next Congress (the 16th assembly).<sup>80</sup>

One of the important changes according to the government is the regulation on contempt crime, as it is considered to be not aligned with the Philippines Constitution, and in fact creating a double threat for the Philippines, because similar crime regulation has already been made under Philippines Penal Code. Yet, internet freedom activists in the Philippines believed, revision dedicated to erase the regulation on contempt crime is not enough. A total cancelation of Republic Act 10175 should

75 See *"Internet Law in Philippines Takes Effect, Raising Fears"*, in <http://www.nytimes.com/2012/10/04/world/asia/new-internet-law-gets-hostile-reception-in-philippines.html>, accessed on 1 August 2013

76 See Chapter II section 5 RA. 10175. Can be accessed on <http://www.gov.ph/2012/09/12/republic-act-no-10175/>.

77 Summary of the lawsuits of the plaintiffs can be accessed on <http://sc.judiciary.gov.ph/microsite/cybercrime/203469.php>.

78 See *"Cybercrime law is suspended by Philippines court"*, in <http://www.bbc.co.uk/news/world-asia-19881346>, accessed on 1 August 2013.

79 See *"Supreme Court extends TRO on cybercrime law"*, on <http://www.gmanetwork.com/news/story/293478/news/nation/supreme-court-extends-tro-on-cybercrime-law>, accessed on 1 August 2013.

80 See *"DOJ to drop online libel from revised cybercrime law"*, on <http://www.gmanetwork.com/news/story/309704/scitech/technology/doj-to-drop-online-libel-from-revised-cybercrime-law>, accessed on 1 August 2013.

take place, and replacing it with law material that upholds civil and political rights in the network field, also ensuring ICT can be used in improving administration, economic development promotion and safeguarding the national security. They affirmed, each regulation proposal that aren't maturely arranged, and not carefully considering the bases of information and communication technology must be denied, since it will create public threats and risks.<sup>81</sup>

After the implementation of Cyber Crime Prevention Law was suspended by the Philippines Supreme Court, recently a new bill initiative emphasizing internet usage and freedom, to replace the Republic Act 10175 that's considered too repressive. The Bill was proposed by Senator Miriam Defensor Santiago,<sup>82</sup> and representative of the Kabaatan Party in the House of Representatives, Raymond Palatino.<sup>83</sup> Senator Santiago proposed Senate Bill 3327 about Magna Charta Philippine Internet Freedom (MCPIF), as the Senate proposal to the Congress,<sup>84</sup> and Palatino of the Kabaatan Party proposed the House Bill 6818 about Magna Charta Internet Users as the Lower Assembly (House of Representatives) Proposal to the Congress,<sup>85</sup> for discussion in the 16th Assembly. The drafting of both bills were admitted to have used a multi-party participation strategy, especially the stakeholders of information and communication strategy, including the business sectors, bloggers, and internet freedom activists. Experiences from many countries, the drafting of ICT sector regulation involving multi-parties is considered to be more successful compared to when it's a mere initiative of the government or legislative.<sup>86</sup>

#### D. Control Policy versus Internet Freedom: Regulations Dynamic

The use of internet technology as part of the development of information technology is closely related to the fulfillment of the right to information, which will be the key suggestion in fulfilling other human rights. It is in line with the statement of the UN General Assembly in its Resolution No. 59 (I) of 1948 which stated that *"the right to information is a fundamental human right and ...a touchstone of all freedoms to which the United Nations is consecrated"*. Frank La Rue, UN Special Rapporteur on the Right to Freedom of Opinion and Expression, said that the fulfillment of right to information – including the right to opinion and expression should be seen as an essential instrument in the promotion and protection of other human rights, and it is also an important tool for combating impunity and corruption.<sup>87</sup>

The beginning of this essay has, at least, provided a brief overview of the initial initiatives of internet technology utilization in Southeast Asia countries, especially Indonesia, Malaysia and the Philippines. There were also appeared a variety of responses from the governments of each country in the early development of this technology. The experiences in the three countries show that the initiative on the utilization of internet technology begin from a multi-party cooperation, including the

81 See ["DOJ deletes libel from new anti-cybercrime bill"](http://www.businessmirror.com.ph/index.php/en/news/nation/13927-doj-deletes-libel-from-new-anti-cybercrime-bill), on <http://www.businessmirror.com.ph/index.php/en/news/nation/13927-doj-deletes-libel-from-new-anti-cybercrime-bill>, accessed on 1 August 2013.

82 See *"After the RH Law: Magna Charta for Internet Freedom is Miriam's new pet bill"*, on [http://www.senate.gov.ph/press\\_release/2013/0703\\_santiago1.asp](http://www.senate.gov.ph/press_release/2013/0703_santiago1.asp), accessed on 1 August 2013.

83 See *"Kabataan Partylist files Magna Charta of Internet Users"*, on <http://kabataanpartylist.com/blog/kabataan-partylist-files-magna-charta-of-internet-users/>, accessed on 1 August 2013.

84 The Bill can be accessed on <http://www.senate.gov.ph/lisdata/1446312119!.pdf>.

85 The Bill can be accessed on <http://kabataanpartylist.com/files/2013/01/HB-6818-Internet-Freedom.pdf>.

86 See *"Pinoy netizens welcome Miriam's online rights bill"*, in <http://www.abs-cbnnews.com/nation/07/03/13/pinoy-netizens-welcome-miriams-online-rights-bill>, accessed on 1 August 2013.

87 A/HRC/14/23

government, private sectors, civil society and universities, with the dominant role of university academics. The situation has made the government has lessen its intervention in regulating the utilization and development of the technology at the time.

In the context of Southeast Asia, Malaysia may be said as one of the first country to respond on the negative impact of the use of ICT. When Indonesia and the Philippines were still struggling to create regulations intended to expand internet access to their population, Malaysia had already issued several regulations with materials containing the authority of state control and penalties for service providers and users in the event of a breach of the utilization of internet technology. For example, Malaysia has issued the Computer Crime Act and Communications and Multimedia Act, which specifically intended to regulate and monitor the use of this technology. Although it must be recognized as well that the Malaysian government also has a very big concern on the utilization of this technology, they even have an aspiration to one of the leaders in the use of ICT in the world, through the Malaysian Vision 2020.

To this day, the major problem faced by developing countries such as Indonesia, Malaysia and the Philippines, in relation to the utilization of ICT, is certainly still struggling with digital divide issues. Various policies created were directed in order of universal access of the utilization of ICT. On the other side, there was also an increase in the number and types of cyber crimes, which led to the birth of a number of policies, intended to control and supervise the use of ICT, along with threats of criminal prosecution. In most countries, including Southeast Asia, there is a tendency to create a variety of new regulations specifically intended to control and narrow the space on the use of internet technology. This tendency became stronger with the growing issues and interests of those countries in the context of sovereignty of cyber space (cyber sovereignty).

The situation is also recognized by the UN Special Rapporteur on Freedom of Opinion and Expression, Frank La Rue. In his report, released in 2011, La Rue argues that current problems on use of internet technology, besides problem of digital divide, is the strengthening efforts on content restrictions. It tends to limit human rights, especially rights of internet access. Some of the acts on content restrictions were regulated specifically in national legislation, while some were purely policies of the government. La Rue identifies the forms of content restrictions, among others, manifested in the form of: (a) arbitrary blocking and filtering of internet content; (b) criminalization of legitimate expression; (c) imposition of intermediary liability (ISP); (d) disconnecting users from internet access, including on the basis of intellectual property rights; (e) inadequate protection on privacy and personal data. These various practices related to content restrictions, according to La Rue, contradict the human rights, especially the right to freedom of expression and the right to privacy.<sup>88</sup>

This phenomenon has become prominent in Southeast Asia region, including Indonesia, Malaysia, and the Philippines. The countries, not only creating new regulations specifically on the purpose of regulating and monitoring the ICT sector, were also applying a number of rules which are not specifically regulate the ICT sector, but the material can be an instrument to restrict it, just like Indonesian Criminal Code or ISA in Malaysia.

---

88 See, [http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27\\_en.pdf](http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf)



## Content restriction and dawn of criminalization

Provisions of the law in Indonesia provide a strong enough protection to exercise the right to freedom of opinion, as defined in Article 28E paragraph (3) of the 1945 Constitution. In addition, Article 28F of the Indonesian Constitution, with sufficient details, also regulates the guarantee on protection of the rights to information, including an element on protection of the right to freedom of expression. The provision in Article 28F of 1945 Constitution mentions that:

Every person has the right to communicate and gain information to develop personal and social environment, and the right to seek, obtained, possess, keep, process, and convey information by using all lines available

In 2005, Indonesian government has also ratified the International Covenant on Civil and Political Rights into its domestic laws, through Law No. 12 of 2005<sup>89</sup>. The Ratification of the covenant implies that all instruments of national legislation created must be in accordance to the provisions contained in the covenant, including rules concerning the right to freedom of opinion, expression, and information, as set forth in Article 19 of the covenant. Indonesia has also issued a number of laws and regulations that were created specifically to ensure on the implementation of these rights, among others: Law No. 39 of 1999 on Human Rights<sup>90</sup>, Law No. 40 of 1999 on Press, Law No. 32 of 2002, and Law No. 14 of 2008 on Public Information Disclosure.

As mentioned above, Indonesia has also issued regulations that were specifically intended to regulate the use of ICT, through Law No. 11 of 2008 on Electronic Information and Transactions. Unfortunately, the law, which was expected to boost and extend the use of ICT as well as to provide adequate protection to users, has several formulas that threaten civil liberties. Among these formulas, there was a specific one on provisions on criminal defamation, in Article 27 paragraph (3) juncto Article 45 of Electronic Information and Transaction Law.<sup>91</sup> In addition to the threat of criminal defamation, which is not in line with the principles of protection of the right to freedom of speech and expression, the law also contains threats on hate crimes, which was often applied incorrectly.<sup>92</sup> This law also regulates the provisions of prohibitions along with its criminal threats, based on moral reasons.

<sup>89</sup> See, [http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg\\_no=IV-4&chapter=4&lang=en#EndDec](http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en#EndDec)

<sup>90</sup> See the decree on Article 14 of Law No. 39 of 1999 on Human Rights

<sup>91</sup> Article 27 paragraph (3) mentioned that any person intentionally and without right to distribute and / or transmit and / or make accessible of an electronic information and / or electronic documents that have contents of insult and / or libel. While the provisions of Article 45 set criminal threats in the form of imprisonment of six years and / or a maximum fine of one billion dollars. In 2009, the provisions of this Article proposed a judicial review to the Constitutional Court (MK), after several bloggers were charged with Article 27 paragraph (3) Electronic Information and Transactions Law for their posts in their blogs. However in its decision, the Constitutional Court rejected the petition, the main reason that the Court stated in their consideration of legal decision, to reject this petition is that contempt which was regulated in Criminal Code (off line contempt) cannot reach libel and defamation committed in cyber world (online contempt). The provisions of Article 27 paragraph (3) of the Electronic Information and Transactions Act dragged many victims in online activities in Indonesia, one of the high profile cases is the case of Prita Mulyasari, a housewife punished and detained, after sending an email to a mailing list, criticizing the services of a private hospital in Tangerang, Banten. More description about this case please observe the Elsam Briefing Paper No. 2 of 2010, Criminal defamation is an unconstitutional restriction of freedom of speech: Amicus Curiae (written comments) in Case No. 1269/PEN.PID.B/2009/PN.TNG with the defendant Prita Mulyasari, can be accessed at [http://elsam.or.id/article.php?lang=in&id=616&act=content&cat=401#UjZkwdL\\_wQQ](http://elsam.or.id/article.php?lang=in&id=616&act=content&cat=401#UjZkwdL_wQQ)

<sup>92</sup> The provisions is set out in Article 28 paragraph (2) EIT Act, with a penalty similar to Article 27 paragraph (3). Similar provisions were also regulated in Article 156 Criminal Code and Article 156a if the action is considered to disfiguring

Content restrictions based on moral reasons are also regulated in Law No. 44 of 2008 on Pornography. The law provides authority to the government to block internet content that includes pornography.<sup>93</sup> Other provision in Indonesian laws and regulations which often became a threat to internet users is the provisions on insult which is still valid in Criminal Code.<sup>94</sup> Internet users accused of criminal contempt are usually punishable by two laws at once: Criminal Code and Electronic Information and Transactions Law.

Internet users in Indonesia are becoming even more vulnerable when charged with criminal acts, upon the enactment of Law No. 17 of 2011 on State Intelligence. There are provisions in this law that threatens a person / entity who intentionally or negligently leaked state intelligence secrets.<sup>95</sup> The criminal threat becomes very arbitrary because the secret intelligence category was made too wide in Article 25 paragraph (2) State Intelligence Law. In this article, the limitation to intelligence secret was too general, for example it only states that those included in secret intelligence category are information that endangers national defense and security, revealing Indonesia's natural wealth which were protected in secrecy, and harm the interest of national economy.<sup>96</sup>

In Malaysia, the country also provide guaranteed constitutional protection to freedom of speech and expression, as confirmed in the provision of Article 10 paragraph (1) letter (a) of Malaysian Constitution, which stated that every citizen has the right to freedom of speech and expression. However, restrictions to the guaranteed freedom are still possible to be done by relying on several reasons. For example, the Parliament, with a reason to protect the interests of the Malaysian Federation's security which are related to public order, may place a restriction on free speech by issuing a rule of law – an act. Moreover, with reasons of for the fight against practice of contempt of the court, defamation, and hate crime, restrictions can be done.<sup>97</sup> In addition to the guaranteed constitutional protection, the Malaysian government to this day has not ratified or even signed the International Convention on Civil and Political Rights.<sup>98</sup>

At the beginning of this writings, it was already mentioned about the creation of a number of regulations which regulate the use of internet technology in Malaysia, including policies with materials that arrange the authority of restrictions and control from the state for the use of internet technology. To be precise, the Malaysian government has enacted a series of laws that allows the

---

officially recognized religions in Indonesia. An example of an arbitrary application of this law was experienced by Alexander An also known as Aan (Minang Atheist case) in West Sumatera. Aan was sentenced to 2,5 years in prison and a fine of 100 million rupiah for his writings on his Facebook account. Further review on this case may be observed on Wahyudi Djafar and Roichatul Aswidah's Intimidation and Freedom of Variety, Style and Issue on Freedom of Expression in Five Provinces (Jakarta: Elsam, 2013). Available at [http://elsam.or.id/article.php?lang=in&id=2307&act=content&cat=401#.UjZl59L\\_wQ0](http://elsam.or.id/article.php?lang=in&id=2307&act=content&cat=401#.UjZl59L_wQ0). Similar case was also experienced by Sebastian Joe, in Ciamis, West Java, who was sentenced in prison for writing a status on his Facebook account which was considered sacrilege to religion. In his Facebook account Joe wrote status "God is miser".

93 See, Article 18 (a) and article 19 (a) of Law on Pornography

94 See, Article 310, Article 311, Article 315, Article 207, and Article 208 of Criminal Code.

95 This penal provision appears in chapter 26 juncto. Article 44 and article 45 State intelligence act. Anyone deliberately spill the state intelligence can be sentence maximally 10 years and or fine of five hundred million rupiahs, while state secret spill due to negligence is sentenced maximally 7 years and or fine of three hundred millions rupiah.

96 In 2012, after the approval of State Intelligence act, the civil society alliance submitted request of review to the constitutional court, amongst requesting to cancel the clause secret information, but the constitution court reject the request. One of the argument of the constitutional court is that rights to information is a derogable one.

97 See, Article 10 par. 2 (a) and par. 4 of Malay Constitution.

98 See, [http://www.suhakam.org.my/c/document\\_library/get\\_file?p\\_l\\_id=30276&folderId=24703&name=DLFE-9701.pdf](http://www.suhakam.org.my/c/document_library/get_file?p_l_id=30276&folderId=24703&name=DLFE-9701.pdf)



state control the exercise of the right to speech and expression. The cyber laws package includes the Computer Crime Law, Communications and Multimedia Act, as well as Communications and Multimedia Commission Act.<sup>99</sup>

On the issue of internet freedom, the Malaysian government alone, through Communication and Multimedia Commission, has taken a stand that internet content should be regulated and controlled. The stance sets out based on reasons related to issues on access, privacy and security, as well as protection on individual rights. In order to manage and control the internet content, the Commission is provided with considerable authority, which includes: (a) advise the Minister on all matters concerning the national policy objectives for communications and multimedia activities; (b) implement and enforce the provisions of the communications and multimedia law; (c) regulate all matters relating to communications and multimedia activities not provided for in the communications and multimedia law; (d) consider and recommend reforms to the communications and multimedia law; (e) supervise and monitor communications and multimedia activities; (f) encourage and promote the development of the communications and multimedia industry; (g) encourage and promote self-regulation in the communications and multimedia industry.<sup>100</sup>

The Commission is also provided with authority to oversee the internet content. The law states that every content provider and user is prohibited to provide and access contents which are offensive, indecent, false, menacing, or offensive with the intent to annoy, threaten or harass individuals.<sup>101</sup> Any person who violates the prohibition may be liable to a fine of fifty thousand Malaysian ringgit or imprisonment for a maximum of one year. Content service providers will also be fined one thousand ringgit every day, if the content contains the elements above has already been banned, yet may still be accessed.<sup>102</sup>

Another threat that has surfaced for the internet users in Malaysia is the enactment of Law No. 88 year 1972 on Official Secret (Official Secret Act – OSA), which contains prohibitions to retrieve and contribute documents which are considered detrimental to the interests and security of Malaysia. The documents can be in the forms of maps, plans, photographs, compact discs, tapes, films, or other visual images, including documents that can be published in the network.<sup>103</sup> OSA is a major

99 Apart from the three acts, Regulations in the cyber space in Malaysia also have Act number 562 of 1997 (Digital Signature Act), Act Number 564 of 1997 (Telemedicine Act), and Act number 658 of 2006 (Electronic Commerce Act).

100 See Article 16 of Malaysian Communications and Multimedia Commission Act

101 See Article 211 par. 1 of Malaysian Communications and Multimedia Commission Act

102 See Article 211 par. (2) Malaysia Communication and Multimedia Act. In July 2013, two bloggers Vivian Lee and Alvin Tan, known as "Alvivi" had been arrested by Malaysian Police due to their posting in their blog and Facebook. They are charged with Malaysian Communication and Multimedia act as well as Hate speech act, with heavier sentence. Their posting is considered to trigger hate on behalf of religion, and create social disharmony. See complete material at "*Malaysian police may arrest sex bloggers*", in <http://www.todayonline.com/world/asia/malaysian-police-may-arrest-sex-bloggers>. Previously, two blogger, in March 2013, Papagomo and King Jason also arrested by Malaysia Police, with charges of spreading racial hate at the time of election, due to their posting in social media. Papagomo is charged with Malaysian Communication and Multimedia act as well as Hate speech act. See the complete version in "*Malaysian elections: Bloggers arrested after police reports lodged against them*", in <http://news.asiaone.com/News/AsiaOne+News/Malaysia/Story/A1Story20130508-420987.html>.

103 See article 2 Malaysia state secret act. Previously Malaysia also applied Act No. 82 of 1960 (Internal Security Act—ISA). In chapter III this act governs the special authority related to subversive publication, etc. This Rule, even initially aimed at printed publications, but in the development presently also became threat to internet users should they upload publication, specially political publication out of line with the interest of the ruling government. This Act enable one to be sanctioned of one thousands Malaysian ringgit fine and maximally three years if the publication threatens the state. Included in the category are the contents of incitement to violence, opposing the law, threatens peace, public order, and harms national security. Not only publication, the ownership of document in network that

instrument in the Malaysian government to protect, or exactly, to cover information, matters and documents with confidential status according to the government. While the internet has become a free information exchange space so free that OSA is applied in the use of the internet.<sup>104</sup> A person who is considered to be leaking a secret information or disseminate information that is considered sensitive, which fall into the information category in Article 8 of this Law, is punishable with imprisonment for at least one year and a maximum of seven years.<sup>105</sup>

Malaysia even specifically has laws that regulate defamation, as regulated in Law No. 286 of 1957 on Defamation (Defamation Act). Defamation, according to this law, is an expression done either verbally or in written form that reflects and tends to injure a person's reputation and puts a person in a situation where he is judged by public on a particular action, or make the people avoid the person concerned. Further emphasized in this law, defamation is categorized into two kinds, namely slander and libel. While the media which are considered to be the space for a defamation action may include print media, broadcast media – in its development, it also includes information and communications technology (internet), as well as meetings in public spaces (public meetings).<sup>106</sup>

Up to this day, Malaysia also still applies Law No. 15 of 1948 on Sedition (Sedition Act)<sup>107</sup>. The law prohibits any form of action, speech and publications either in written or in any other forms of similar nature<sup>108</sup>, which material is considered to be inciting others and contain hatred or contempt against the ruler, the government, or the administration of justice, or spreading hostility between different races or classes<sup>109</sup>. This law also prohibits every citizen to question matters related to rights, status, position, Malay privileges, and sovereignty or prerogative rights of the ruler, as protected by the provisions of Part III of the Federal Constitution or Article 152, 153 or 181 of the Federal Constitution<sup>110</sup>.

In 2012, Malaysia has also amended their copyright law, from Law No. 332 of 1987 on Copyright<sup>111</sup> to Law No. A1420 of 2012 on the Amendment of the Copyright Act<sup>112</sup>. Changes to the law have

---

contains such material also can be sentenced based in ISA. In 2008, a very influential political blogger in Malaysia, Raja Petra Kamarudin was detained based on ISA, due to his posting that were regarded to be anti government. Petra was detained for an unclear period of time, based in ISA rule. See complete version at *"Malaysia blogger arrested for posting anti-government comments"*, in <http://www.theguardian.com/world/2008/sep/12/malaysia.pressandpublishing>. In April 2012 Malaysia government cancels the ISA, but at the same month the government also issued Act No. 747 of 2012 on security offence (Special measure) to replace ISA.

104 See the full version of Official Secrets Act at <http://www.agc.gov.my/Akta/Vol.%202/Act%2088.pdf>.

105 See Article 9 of Malaysia Official Secret Act. In July 2012, a blogger, Syed Abdullah Hussein Al-Attas, popularly known as 'Uncle Seekers', arrested by Malaysian police, with charges of violating chapter 8 of the Malaysian Official Secret Act (OSA) due to his posting of controversial information about Sultan of Johor in his blog page. See *"Blogger held under OSA over articles against Johor sultan"*, in <http://www.malaysiakini.com/news/202760>, accessed in August 1st 2013.

106 See the full version of Defamation Act in <http://www.agc.gov.my/Akta/Vol.%206/Act%20286.pdf>.

107 See the full version of Sedition Act in <http://www.agc.gov.my/Akta/Vol.%201/Act%2015.pdf>

108 See Section II of Sedition Act

109 See Section III par.. 1 (a-e) of Sedition Act.

110 See Part 3 paragraph (1) letter (f) Malaysia Sedition Law. A blogger, Mohd Nur Hanief Abdul Jalil in March 2011 was arrested and detained by Police and Malaysian commission for multimedia and communication, based on Incitement Act, as his posting was regarded to demean the Sultan of Selangor. He wrote in his blog, a suspicion of sexual scandal under Sultan of Selangor and a Malaysian actress. See full version at *"Blogger 'arrested' at midnight under Sedition Act"*, in <http://www.malaysia-today.net/mtcolumns/from-around-the-blogs/38903-blogger-arrested-at-midnight-under-sedition-act>, accessed in August 1st 2013.

111 See the full version of Copyright Act in <http://www.agc.gov.my/Akta/Vol.%207/Act%20332.pdf>

expanded the scope of copyright protection, which also has implications to the growing extent on the forms of copyright infringement. The amended law also includes copyright protection related to information and communications technology. According to this law, transmitting a copyrighted work illegally using the internet is an act of violation of intellectual property rights<sup>113</sup>.

It is a different situation in the Philippines, whose constitution is far more lenient to human rights. The Philippine Constitution of 1987 is not absolutely regulated on the rights to information for citizens, but it is said in it that the right of the people to information on matters of public concern shall be recognized. It also affirms that access to official records, documents and papers pertaining to official acts, transactions, or decisions, as well as government data used as basis for policy development, shall be given to the citizens. But these are still subject to the restrictive measures that can be done by basing it on a law<sup>114</sup>. Paying attention to this clause, the Philippine Constitution has mentioned in detail the forms of information that are part of public information and may be accessed by every citizen of the Philippines.

The Philippine Constitution has also provided a guaranteed protection to each of its citizen of the right to freedom of speech and expression. It is asserted that there is no law that can narrow the freedom of speech, of expression, freedom of the press, or the right of the people to assemble and to petition the government to demand compensation<sup>115</sup>. The Philippine government has even ratified the International Covenant on Civil and Political Rights since 1986<sup>116</sup>; the second country in Southeast Asia that ratify ICCPR into its domestic law, after Thailand acceded since 1966.

In the early development of the internet in the Philippine, like Indonesia, the Philippine government was not responsive in creating regulations in order to control the use of this technology. Although the control function of the internet actually has been done by National Telecommunication Commission (NTC), who controls all telecommunication activities in the Philippines. In 2000, when President Estrada was in rule, the monitoring of the internet usage was even performed directly by the Office of the President, through National Information Technology Council. In addition to creating a road map of information and communication technology development in the Philippine, the board is also overseeing its utilization. When President Arroyo came to power, the Board was changed to the Commission on Information and Communication Technology. As concluded above, the policy on the development and monitor on the use of information and communication technology in the Philippines, is very dependent on the interests of the president in power.

On the issue of internet freedom in the Philippine, before the enactment of Cybercrime Prevention Act, there is not one policy with materials that restrain the right to freedom of speech and expression in a network. Moreover, although the provisions of Article 353 and Article 360 of the Philippine Criminal Code is still regulating on criminal threats, both fines and imprisonment, for act of contempt, the Philippine Department of Justice confirmed that the provisions does not applied to postings on websites, or forms in other network<sup>117</sup>. In his statement in October 2009, the Minister of

112 See the full version of Law No. A1420 of 2012 on the Amendment of the Copyright Act in [http://www.federalgazette.agc.gov.my/outputaktap/20120209\\_%20A1420\\_BI\\_JW001763%20Act%20A1420-BI.pdf](http://www.federalgazette.agc.gov.my/outputaktap/20120209_%20A1420_BI_JW001763%20Act%20A1420-BI.pdf)

113 See section IV b limitation and responsibilities of service provider in the Copyright law modification.

114 See the decree on Article 3 (Bill of Rights) section 7 of Philippine Constitution 1987.

115 See the decree on Article 3 (Bill of Rights) section 4 of Philippine Constitution 1987

116 See, [http://treaties.un.org/Pages/ViewDetails.aspx?mtldsg\\_no=IV-4&chapter=4&lang=en%23EndDec#EndDec](http://treaties.un.org/Pages/ViewDetails.aspx?mtldsg_no=IV-4&chapter=4&lang=en%23EndDec#EndDec)

117 See Freedom House, Philippines Freedom on the Net 2012, (New York: Freedom House, 2012), p. 7. Available on <http://www.freedomhouse.org/report/freedom-net/2012/philippines>.

Justice said that an action of contempt must be in written form, printed, through lithography, engravings, radio, phonograph, paintings, theatrical performances, cinematographic exhibition, or other similar means, and not including those in a network<sup>118</sup>.

However, cases charged with threats against internet users still occur. In 2010, a blogger was reported by the Secretary of the Department of Social Welfare for his posting that accused the Department of Social Welfare for hoarding aids for Parma storm victims. As a result, the blogger was accused of defamation actions<sup>119</sup>. A similar case occurred in 2011, when a Facebook user was reported for an act of defamation by a renowned plastic surgeon in the Philippines, due to his postings. But then the court terminated the case, stating that defamation in the network was not included in the court's jurisdiction<sup>120</sup>.

Such situation has also become one of the reasons for the enactment of Law No. 8792 of 2000 on Electronic Trades (Republic Act 8792). At the beginning of this paper, it has already been mentioned on the cause of the enactment of RA 8792, which stems from the emergence of virus 'I love you' in the Philippines. Creator and disseminator, Onel de Guzman, who has cost the world billions of dollars, cannot be punished, as it collided with the principle of *nullum crimen, nulla poena sine lege*, which is applicable in the Philippine criminal law. As a follow-up, on June 14, 2000, the Philippine Congress agreed to ratify the Republic Act 8792, with one of its purposes is to prevent threats of cybercrimes. The law threatens the perpetrators of crime in the network, such as hacking, virus dissemination, and copyright infringements. The offender shall be punished by a fine of up to one hundred thousand Philippine pesos or commensurate with the damage caused by the crime. Other criminal sanctions that can be applied are in the form of imprisonment for six months up to three years<sup>121</sup>.

Whereas on the provisions on contempt according to RA 8792, the person or party acting as the service provider has no civil or criminal liability in the creation, publication, dissemination or distribution of the contempt materials, if: (a) does not have any knowledge nor awareness on the facts or clear state that the creation, publication, dissemination or distribution of such material is illegal or violating the rights; (b) accidentally receives a direct financial benefit from an act of infringement; (c) does not directly commit violations or criminal activities nor encourage others to commit acts of violations. Should a service provider know that content contains elements of contempt, and then access to the content must immediately be closed.<sup>122</sup>

In the Philippines, the use and content of the internet is regulated quite strictly, specifically those which are related to child pornography, in Law No. 9775 of 2009 on Anti Child Pornography

118 According to the Philippines penal code, defamation can be sanctioned 6 month to 6 years imprisonment, or fine of 200 to 6000 Philippine peso, or both, for full version see "*Defamation and the internet: the multiple publication rule*", in <http://www.commentonthis.com/defamation/>.

119 See "*Solons defend blogger sued by DSWD for libel*", in <http://newsinfo.inquirer.net/breakingnews/nation/view/20100125-249403/Solons-defend-blogger-sued-by-DSWD-for-libel>, accessed on August 1, 2013.

120 See, "*BMGI Inc. vs. Gueverra: first Facebook libel case in the Philippines dismissed by court*", in <http://technogra.ph/2011/07/30/bmgi-inc-vs-gueverra-first-facebook-libel-case-in-the-philippines-dismissed-by-court/>, accessed on August 1, 2013.

121 See, sub-chapter V section 33 of Act No. 8792 of 2000 on Electronic Trades

122 See article 30 Republic Act 8792.

(Republic Act 9775)<sup>123</sup>. This Act provides a number of obligations for internet hosts, internet service providers, and internet cafe owners, as well as regulates a series of penalties in case of infringements. According to the law, every internet service provider (ISP) is obliged to report to Philippine National Police (PNP) or National Bureau of Investigation (NBI), whenever they find a content containing child pornography, by making use of a server or its services. However, this law still prohibits ISPs to perform observation / monitoring of the internet users, including personal communication of the users. As long as there is a good will from them, the ISPs will not be liable for anything. Furthermore, the ISPs must also install the available technology in the form of software in order to filter and block access to any form of child pornography<sup>124</sup>. Any ISP that violates the above obligations will be fined between five hundred thousand pesos to one million Philippine pesos. Should the ISP repeat the offense, he will again be fined between one million to two million Philippine pesos as well as a revocation of their business license<sup>125</sup>.

Then, according to the provisions of this law, every internet hosting provider is obliged to report content that contains elements of child pornography, maximum within seven days and accompanied with evidences. Furthermore, within a maximum of forty eight hours, hosting provider should also cut off access to the content containing elements of child pornography. If it is not done, then the hosting provider may be said to have intentionally violate the law<sup>126</sup>. Internet hosting provider who commits an offense may be punished with a medium sentence of imprisonment, as well as a fine between one million to two million Philippine pesos. If he commits the same offense, he is punishable with fines between two million and three million Philippine pesos, as well as a revocation of his operating license and business permits. While on the owners of internet cafes, the supervision over them is delegated to each local government, with provisions restricted according to this law (RA9775).

Strict controls on the content and use of internet in the Philippines occurred when the government along with the Congress approved the Act No. 10175 of 2012 on the Prevention of Cyber Crime (Republic Act 10175). On the previous section, it has been mentioned that even though the formation of this Act is to minimize the act of cyber crime, the content of the material tends to limit the freedom of speech, opinion and expression, which was guaranteed by the Philippines Constitution. This Act confirms that every crime as stipulated by the Philippines Penal Code and other special laws, if performed with the use of information and communication technology, then the penalty will be one degree higher than the penalty stated in the Penal Code.<sup>129</sup> In addition to giving a higher degree of penalty, it is worsen by the penalty based on RA 10175 which does not abolish penalty in the Penal Code as well as other special laws, if the offense is also committed offline (in print) and in a network.<sup>130</sup>

Republic Act 10175 also regulates specifically the provisions of criminal contempt, as provided in Article 355 of the Philippines Penal Code. On previous occasions, the Philippine court refused to hear

---

123 See the full version of Law No. 9775 of 2009 on Anti Child Pornography in [http://www.lawphil.net/statutes/repacts/ra2009/ra\\_9775\\_2009.html](http://www.lawphil.net/statutes/repacts/ra2009/ra_9775_2009.html)

124 See section 9 of Republic act no 9775

125 See section 15 (k) of Republic Act 9775. After notification from ISP, in the maximal of 90 days, National Telecommunication Commission would block the access to transmission of the content with child pornography.

126 See section 11 of Republic Act 9775

129 . See Section 6 RA 10175

130 . See Section 7 RA 10175

a case on insults committed in a network, with an excuse that it is not within their jurisdiction, since the Penal Code does not include network insults.<sup>131</sup> So through this Law, network insults may be charged with a criminal penalty. Besides, RA 10175 also threatens anyone who intentionally assists or conspires in committing a criminal offense as set out in this law.<sup>132</sup> Interpretation flexibility of “intentionally assisting an offense” may result in a sentence to the application providers on the internet, such as Google, Facebook and Twitter. In the case of network insult, for example, the application providers could be accused of taking part to help publicize a content which contains elements of criminal offense. Such situation has certainly gave birth to a real threat to the functions of internet.<sup>133</sup>

Cyber Crime Prevention Act also authorizes the Justice Department to issue a warrant for blocking and termination of access to a content whose materials are considered a violation to the provisions of this law.<sup>134</sup> Granting absolute authority to the Department of Justice, which is part of a political institution, is certainly dangerous, as it has the potential to be misused for power interests. Content blocking and termination should be done through a judicial process in line with the principles of restriction to the rights of freedom of expression. Another problem that arises is the enforcement of universal jurisdiction of this Act,<sup>135</sup> which seems to place the Philippines authorities as the inspectors of all internet contents in the world, and even a person who only visited the Philippines (not a citizen of the Philippines), and had uploaded a content with a prohibited materials according to RA 10175, may be convicted by the Philippine court. To support the implementation of the law, this act has even specifically mandates the establishment of a Cyber Crime Special Court, with trained judges to handle these cases.<sup>136</sup>

The formulation, which was too repressive and deemed inconsistent with the guaranteed protection of the freedom of speech, opinion, and expression regulated in the Philippine Constitution, has given rise to many protests and oppositions to this legislation. As described earlier in this article, a number of civil societies have filed a petition to the Philippines Supreme Court to reject this legislation. The Supreme Court then declared to stop the enactment of this Act indefinitely (until a new resolution on its judicial review). Meanwhile, the Justice Department addresses the protest by declaring that it has revised the law by abolishing the provisions on contempt.

In response to the situation, a member of the Senate and a member of the Lower House (House of Representatives) of the Philippines, proposed a bill on the freedom of the internet (Magna Charta for Philippine Internet Freedom), to be discussed in Congress. Once approved, the bill will replace RA 10175, and ensure the freedom of the internet in Philippine. The formulation of the bill includes, among others, ensuring the freedom of speech and expression in the network in the Philippines, and

---

131 . See Section 4 Number (4) RA 10175

132 . See Section 5 letter (a) RA 10175

133. See Center for Law and Democracy, Philippines, Analysis of the Cybercrime Prevention Act of 2012, November 2012, page 6

134. See Section 19 RA 10175

135. See Section 21 RA 10175

136. Complete critical notes against Cybercrime Prevention Act of the Philippines, see Center for Law and Democracy, Philippines, Analysis of the Cybercrime Prevention Act of 2012, November 2012, may be accessed at [http://www.law-democracy.org/live/wp-content/uploads/2012/08/Phil.Cybercrime.final\\_.pdf](http://www.law-democracy.org/live/wp-content/uploads/2012/08/Phil.Cybercrime.final_.pdf).



a confirmed that all forms of restriction should be done through a court order and only applicable in certain circumstances, et cetera.<sup>137</sup>

### Ensuring the protection of privacy

Another issue raised in the utilization of internet technology is the susceptibility of intervention on privacy, including easier exposure on a person's private data. UN special *rapporteur* for freedom of opinion and expression Frank La Rue gave a special attention to the issue, considering the heights of practices on surveillance, citizens' private communication interceptions, as well as personal data transfers which were done arbitrarily. In his report, La Rue confirmed on the needs for each country to have its own laws, which should clearly describe the conditions that the rights for individual privacy may be limited under certain terms, and measurements on this rights should be taken based on a special decision. This decision should be taken by the state authorities guaranteed by law to perform the act.<sup>138</sup>

Between the three countries, Indonesia, Malaysia and the Philippines, Indonesia may be said as the most vulnerable in terms of its framework of privacy protection. Before the amendment to Indonesia 1945 Constitution, protection on a person's private communication in Indonesia was regulated in Chapter XXVIII Penal Code on Official Crime, specifically in Article 430 to 434. Especially with regard to tapping on long distance communication through a device is regulated in Article 433, which prohibits telephone and telegraph tapping illegally. This provision is then reinforced by the enactment of Act No. 36, 1999, on Telecommunication. One of the new things appeared in the Act is related with the prohibition to commit telecommunication wire tapping. In the provisions of Article 40 of Act No. 36, 1999, it is stated that *"Every person is prohibited in committing a wire tapping action on information channeled through a telecommunication network in any forms"*. It is confirmed in the explanation of the law, that the information is a personal right that must be protected, therefore tapping should be banned.<sup>139</sup> But in terms of law enforcement, specifically for a particular offense with a penalty of imprisonment for more than five years, information tapping as an attempt to uncover crime and to gather evidence may be performed. Telecommunication operator who conduct the tapping rests on a written request of the Attorney General, Chief of Police, or an investigator, for certain offenses as regulated by the law.<sup>140</sup>

Post-amendment of the Constitution, the right to privacy is recognized in Indonesia as one of the citizens' constitutional rights that must be protected. The protection is asserted in Article 28 G paragraph (1) of 1945 Constitution, which stated among others, that every person has the right for a protection to himself, family, honor, dignity and properties (including personal data). This statement is also affirmed in Article 32 Act No. 39/1999 on Human Rights, which stated, among others, that the freedom and confidentiality of communications through electronic means should not be disturbed except by order of a judge or other authority authorized by law.

137 Further review on this bill, see [Jillian C. York](https://www.eff.org/deeplinks/2013/07/brief-analysis-magna-carta-philippine-internet-freedom), A Brief Analysis of the Magna Charta for Philippine Internet Freedom, in <https://www.eff.org/deeplinks/2013/07/brief-analysis-magna-carta-philippine-internet-freedom>.

138 See Frank La Rue Report paragraph 59, A/HRC/14/23

139 Tapping, according to this law, is an activity of installing a device or an additional equipment to a telecommunication network for the purpose to gain illegal information

140 See Article 42 Law No. 36 of 1999 on Telecommunications

Illegal communication interception committed on the internet is also prohibited according to Indonesian laws. The prohibition is asserted in Article 31 paragraph (1) Act No. 11/2008 on Electronic Information and Transactions. In its provisions, it is stated that every person is prohibited in committing interceptions or tapping on information or electronic documents in a computer or other person's electronic system. Communication interception is only allowed in the context of law enforcement at the request of the police, prosecutors, or other law enforcement agencies. Violation of the provision may be punished with imprisonment for up to 10 years maximum and/or fines up to 800 million rupiah.<sup>141</sup>

However, the absence of a single rule on procedures to interception in Indonesia has created vulnerability against acts of interceptions on citizens' personal communications, including internet-based communications, such as email, as well as other social media tools. To date, Indonesia has at least twelve laws on regulations of communication interceptions and tapping with different manners. The differences in the regulations of tapping are very clear, for example, between the Anti Terrorism Act, Narcotics Acts, the Law on Corruption Eradication Commission, and the State Intelligence Law. These scattered and fragmented tapping laws in Indonesia has opened a wide gap where practices of interference on citizens' private communications, including those using the internet.<sup>142</sup>

In addition to this scattered and fragmented tapping laws, another problem has surfaced on the issue protection of privacy in Indonesia that is inadequate protection on citizen's personal data. Even until now Indonesia has no legislation that specifically ensures the protection of a person's personal data. Provisions on protection of a person's personal data specifically in electronic forms is strictly regulated in Article 26 Electronic Information and Transactions Law. In the decree, it is affirmed that one's personal data transfer should be performed based on the consent of the person concerned, unless otherwise provided by the regulation. But the violation of this provision is not threatened with a punishment; instead the person who committed the violation is given space to do a compensation.<sup>143</sup> The lame regulations on the protection of personal data results in a widespread practices of personal data transfers and leakage in Indonesia, especially for commercial purposes.<sup>144</sup>

Malaysia, until now, has a Constitution that does not firmly grant the right to the protection of privacy for its citizens. While Malaysia Penal Code is limited only in regulating that a person who interferes in other person's privacy may receive a penalty of fine or imprisonment for up to five years maximum, or both.<sup>145</sup> Like Indonesia, the regulation of communication interception in Malaysia is scattered into several laws. In Malaysia, there is no single rule on tapping, so that there is an open space for interference (interception) against one's personal communication.

In June 2012, the Malaysian government has passed the Act No. 747/2012 on Security Breach (Special Measures)<sup>146</sup>, which gives enormous powers to the security forces and law enforcement

141. See Article 31 paragraph (20) juncto. Article 47 Electronic Information and Transactions Law

142. See Wahyudi Djafar, Protecting Privacy Rights from Wiretapping, The Jakarta Post, 21 February 2013, may be accessed at <http://www.thejakartapost.com/news/2013/02/21/protecting-privacy-rights-wiretapping.html>.

143. See Article 26 paragraph (2) Electronic Information and Transactions Law

144. See Wahyudi Djafar, We Need Protection on Personal Data Law, in <http://www.hukumpedia.com/ham/kita-perlu-uu-perlindungan-data-pribadi-hk51da54d24bb82.html>

145. See Section 509 Malaysia Penal Code

146. Complete version of the law may be accessed at [http://www.federalgazette.agc.gov.my/outputaktap/20120622\\_747\\_BI\\_Act%20747%20BI.pdf](http://www.federalgazette.agc.gov.my/outputaktap/20120622_747_BI_Act%20747%20BI.pdf).



agencies to perform communication interceptions, without a proper authorization.<sup>147</sup> Under the terms of this law, prosecutors are given the authority to conduct wiretapping and recording of communications in any forms, which are being sent and received by all types of communication media including the internet. Prosecutors are also equipped with the authority to grant authorization for police officers to carry out similar actions. This Act also provides space for the government to control communications using various electronic means, through a court order.<sup>148</sup>

Besides giving authorization for communication interceptions to prosecutors and the police, Malaysian laws also authorize communication interceptions to several other state institutions. Just like in Indonesia, tremendous authority to conduct wiretaps was given to Malaysian Anti-Corruption Commission, as stipulated in Act No. 575 of 1997 on Anti-Corruption,<sup>149</sup> and the Act No. 694 of 1999 on Malaysian Anti-Corruption Commission.<sup>150</sup> While the prosecutor, in addition to being given substantial powers over Security Breach Act, and is also given the authority to conduct communication tapping through Act No. 365 of 1961 on Kidnapping.<sup>151</sup> Based on this Act as well, Malaysian Ministry of Home Affairs can also perform an act of communication interceptions.

The prosecutors also have the authority to tap communications through Act No. 340 /1988 on Dangerous Drugs, which also provides authority to perform communication interception for National Anti Narcotics and Malaysian Ministry of Home Affairs.<sup>152</sup> Prosecutor's authority to conduct communication interceptions is also set in Act No. 708/2010 on Strategic Trade. This authority is given whenever the prosecutor is investigating a crime under this Act (trade related crimes).<sup>153</sup> Besides communication interception authority, according to the Strategic Trade Act, the Prosecutor is also given the authority to access the computer data of the party being investigated, access to necessary passwords and all data, including those encrypted.<sup>154</sup>

Communication interception is also arranged specifically in the use of information and communication technologies, as stipulated in Act No. 558/1998 on Communication and Multimedia. However, just as the Laws on Electronic Communication and Transactions in Indonesia, besides providing tremendous authority to perform communication interceptions, especially those which uses computer technology, to the security forces and law enforcement,<sup>155</sup> the law is actually provides a guarantee to Malaysian citizen that they are not being intercepted illegally.<sup>156</sup>

In terms of the citizens' personal data protection, the Parliament of Malaysia has passed Act no. 709/2010 on Protection of Personal Data in 2010, and becomes effective as of August 16, 2013, with a transition period of three months.<sup>157</sup> These laws regulate in detail the principles of personal data protection, the rights of the owner of the data;<sup>158</sup> procedures in data transfer, as well as the

147 See Section II Article 6 Authorization for communication interception, Security Breach Law

148 See Section III Special Procedures related with supervision on electronic devices, Article 7, Security Breach Law

149 See Section 38 Malaysia Anti Corruption Act

150 See Section 43 Malaysia Anti Corruption Commission Act

151 See Section 11 Malaysia Kidnapping Act

152 See Section 20 and 51 Malaysia Dangerous Drugs Act

153 See Section 37 Malaysia Strategic Trade Act

154 See Section 32 Malaysia Strategic Trade Act

155 See Section 252 Malaysia Communication and Multimedia Act

156 See Section 234 Malaysia Communication and Multimedia Act

157 See: "New enforcement date of the Personal Data Protection Act 2010 announced in <http://www.lexology.com/library/detail.aspx?q=9aa430a4-d841-4cb6-9e2d-911c71a24b17>.

158 See Article 30 Malaysia Personal Data Protection Act

obligations of the parties performing data storage.<sup>159</sup> The Act also regulates the complaint mechanism for a person whose personal data has not been properly transferred.<sup>160</sup>

Advisory Committee on Personal Data Protection was also established through this Law, whose duty is to receive reports on cases of abusive and illegal personal data transfers,<sup>161</sup> as well as establishing appeal courts to reach a judicial settlement.<sup>162</sup> The Act does not only provide rooms to complain, it also provides criminal sanctions to any person who violates the provisions of personal data protection. The heaviest threat, for example, is aimed to any party accessing a person's personal data without permission, or collecting personal data against the law, may be sanctioned with fines up to five hundred Malaysian ringgit, and/or imprisonment for up to three years maximum.<sup>163</sup>

Unlike Indonesia and Malaysia, the Philippines may be considered as the most advanced throughout Southeast Asia in terms of its citizens' privacy protection. Article III of the 1987 Philippines Constitution (Bill of Rights), Section 2, boldly states that a person's private communications and correspondences should not be interfered by anyone except by court's order or due to public safety reasons, or any other instructions set by the laws. One of this Constitutional guarantees is implemented by the 1965 Anti Wiretapping Act No. 4200 (Republic Act No. 4200), which was approved in June 1965. The Act regulates on prohibitions and penalties against a person who violates the prohibition by intercepting communications illegally. According to the Law, all acts of communication interceptions or any other acts that invades a person's privacy must have prior written permission and authorization from the court. Without any permission from the court, the action may be categorized as an offense.<sup>164</sup>

Communication interceptions in communications and information technology done illegally are also prohibited by the laws of the Philippines. This prohibition is as stated in Section 4 numbers (2) Cyber Crime Prevention Act. Interception of communication itself, according to the law, is the act of listening, recording, monitoring or controlling the content of communications, including data content, either directly or indirectly, with the use of a computer system or any other electronic devices, during the occurrence of the communication.<sup>165</sup> During its development, strict authorization on the use of wiretapping authority, including tapping on the internet, which was given to law enforcement, suffered a setback with the enactment of Act No. 9372/2007, on Human Security (Republic Act 9372). Rests on the arguments of anti-terrorism interests, the security forces are given great authority to carry out communication interceptions during the process of their investigation.<sup>166</sup> The effect to the enactment of this law is that the use of communication interception methods arose sharply in crime investigations.<sup>167</sup>

Cybercrime Prevention Act also prohibits the act of interference against a person's privacy. The Act prohibits any person to perform unauthorized acts to alter, destroy, or remove computer data,

159 Complete version of the law may be accessed at <http://www.kppk.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf>.

160 See Article 31 and Article 104 Malaysia Personal Data Protection Act

161 See Section VI Malaysia Personal Data Protection Act

162 See Section VII Malaysia Personal Data Protection Act

163 See Article 130 Malaysia Personal Data Protection Act

164 See Section 3 Philippine Anti Wiretapping Law

165 See Section 3 letter (m) Philippine Cybercrime Prevention Act

166 See Section 20 Philippine Human Security Act

167 Kristhoper A. Nelson, Transnational Wiretaps and the Fourth Amendment, *Hasting Constitutional Law Quarterly*, Vol 36. 2 Winter 2009, pages 340-341

electronic documents, or electronic data message. The protection of one's personal data is also confirmed in the Electronic Commerce Act (Republic Act 8792), as set forth in Section 31 and Section 32 of this law, which asserts that electronic data and documents can only be accessed by authorized parties (owners or parties authorized by law). Violation of such protection (data interference) may be imposed with a fine as much as one hundred Philippine pesos and/or imprisonment of at least six months and three years maximum.<sup>168</sup>

On August 15, 2012, President Benigno Aquino has also signed the Act No. 10173/2012 on Personal Data (Republic Act 10173), which was approved by the Philippine Congress. Although previously the Philippine legislation has set the protection for the security of one's personal data, but this Act is the first to introduce data privacy regime in the Philippines. According to this law, all forms of data transfer will be subject to the principles of accountability. This principle asserts that any party who keeps or have authority over personal information, is responsible for the information under its control, including the information that has been transferred to a third party to be processed, both domestically and internationally.<sup>169</sup>

This Act applies to all kinds of information and all entities, individuals, public and private, involved in the management of personal information. Subject within the scope of this regulation also includes the server providers, outside of the Philippines or those who simply have representative offices in the Philippines.<sup>170</sup> All information owned by journalists along with their sources is also protected by this law.<sup>171</sup> The provisions in this Act also regulates in details on the rights of the owner of personal data (data subject), such as the right to be notified whenever his personal data is being processed, prior approval request before his personal data were entered into the system, and a number of things, including: (a) Personal information to be incorporated into the system; (b) purpose of the process; (c) scope and methods of personal information processing; (d) recipients or level of recipients of the information; (e) methods used for an automatic access, should it be allowed by the owner, and the extent of such access allowed; (f) identity contact details of the personal information manager, or his representative; (g) the length of retention period of the personal information; and (h) the rights of the data owner to access, to correct, and the rights to file a complaint to the Commission.<sup>172</sup>

The Commission referred to in this Act is the National Privacy Commission within the Department of Transportation and Communications, which was established by Chapter II Section 7 of Data Privacy Act. The Commission itself serves to administer and implement the provisions of the law, as well as to monitor and to ensure the state compliances towards the international standards set out in data protection. Furthermore, this institution functions as any other quasi-judicial agency in charge of receiving complaints, conducting an investigation for a complaint, and should there be a violation, the institution will also facilitate an alternative dispute resolution process in determining the amount of feasible compensation. The Commission also has authorization to issue a temporary or permanent ban on a personal data processing, should the process is considered to be detrimental to national security and public interests. The Commission is also responsible to coordinate all stakeholders in

---

168 See Section 33 Philippine Electronic Commerce Act

169 See Chapter VI Section 21 Philippine Data Privacy Act

170 See Section 4 Philippine Data Privacy Act

171 See Section 5 Philippine Data Privacy Act

172 See Chapter IV Section 16 Philippine Data Privacy Act

preparing plans for policies on domestic data protection, includes providing proposals on personal data related amendments to the law. Privacy terms used by a public or private entity in processing one's personal data will also be examined by the Commission.<sup>173</sup>

Criminal provisions are also regulated in this law, as formulated in Chapter VIII, which mentions on details of penalties for violation of the law, as well as threats on imprisonment. Violation of Data Privacy Act includes unauthorized processing of a personal information, unauthorized access, inappropriate destruction of personal information, security breaches to sensitive information, and unauthorized disclosure of personal information. Violation on the provision of the Act is imposed to a fine of five hundred thousand up to five million Philippine peso, as well as imprisonment for at least six months up to a maximum of seven years. If the offense is committed by a corporation, then the criminal liability falls to the individuals who are responsible to the data processing, or parties participating in sponsoring the violation. Moreover, under this Act, the court may also suspend the license and rights owned by the corporation. If the perpetrator is a foreign citizen, then he should be deported after serving his sentences.<sup>174</sup>

## E. Conclusion

The internet has become an important medium in the fulfillment of the rights for information in this era. It has also become a diverse actualization to various human rights, such as the rights to freedom of speech, opinion, and expression. Furthermore, technology is recognized as one of the key instruments in the fulfillments of human rights as a whole, including the economic, social and cultural rights. This narrative experiences from three Southeast Asian countries above, Indonesia, Malaysia, and the Philippines, showed the existence of an enormous leap in the use of internet technology, upon observing the development, from the early initiatives of the use of technology to its development today.

The history in those three countries presents a similar situation. The early use of internet technology was not a state project, but was a result of a multi-party collaboration, between universities, civil society, business groups, and government agencies. Initially, these countries were not very responsive in creating policies to expand the use of internet technology. Internet had not been placed as an important instrument for statehood at that time, and was seen as a small part of the overall telecommunication device commonly used by people. The condition was particularly visible in Indonesia and the Philippines. It was slightly different to Malaysia, where the government has already had big ambitions on the use of internet technology since the beginning, that the policies constructed were directed to the development of the technology.

From the point of view of the regulation creation specifically regulations on computer technology, including the internet, Malaysia may also be considered as the initiator. When the governments of Indonesia and the Philippines were still busy doing their telecommunications regulatory reforms, which manages the entire telecommunication mediums in general, the Malaysian government has devised an array of special regulations intended to regulate the use of the internet, including its supervision, which at certain point tends to restrict the freedom to browse the internet. Since 1997

173 Complete details on duties and functions of Philippines National Privacy Commission can be reviewed in Section 7 Philippine Data Privacy Act

174 Complete version may be reviewed in Chapter VII Philippine Data Privacy Act

– 1998, Malaysia had established regulations that give recognition to various activities in a network, as well as supervising these activities. The Philippines started in 2000, and had to pay dearly, as the enactment of a special regulation to regulate the internet, was prone to cyber crime incidents. These incidents caused many losses, as there were no laws created yet, so the culprit cannot be punished. While Indonesia has given recognition to the wide range of activities based on the information and communication technology in 2008 with the enactment of Electronic Information and Transactions Law, and the materials received many public criticisms.

Another thing that should be highlighted is related to the tendency of the creation of regulations that restrict the internet contents, and that is not in line with the principles of the protection of freedom of information, freedom of speech, opinion and expression. This phenomenon has certainly become an irony amongst the ever-growing number of internet audience in the world, including the developing countries, such as Indonesia, Malaysia and the Philippines. After the enactment of the Law on Electronic Information and Transactions in 2008 in Indonesia, victims of the law began to collapse, the internet users were forced to deal with the authorities, as the internet activities were deemed inconsistent with the formulation of the legislation. It was even worse in Malaysia, where due to political situation, it was not as free as in Indonesia. Internet users, especially social media lovers and bloggers, have experienced detention due to materials they had uploaded on the internet were in violation to the law. Internet users in Malaysia were not only charged with violation on the laws that specifically regulate the internet sector (Communications and Multimedia Act), but also had to deal with a variety of other laws which have general settings, but applicable to the activity on the network. While in the Philippines, a country that were previously friendly towards the rights of the internet users, due to a strong constitutional guarantee, later also began to create policies that tend to be repressive, especially after the release of Cyber Crime Prevention Act. Fortunately, the Supreme Court then freezes the enactment of this law, as it is not in line with the guaranteed protection of human rights in the Philippine Constitution. Interestingly, at the moment, a new initiative appeared in Congress to discuss a bill that focuses on protection to internet freedom.

The experience in the Philippines proves that the model to establish a regulation is with a top-down nature in the internet sector, will only create a repressive rule and poses a risk to the public. Therefore, the most appropriate way is to create rules for internet sector by involving many stakeholders, so the rule created is one that upholds internet freedom, but on the other hand, it should also be able to minimize the negative impacts of this technology. Strictly speaking, important multi-party scheme should be implemented in creating internet-related regulations, considering the large parties involved in the utilization of this technology, as well as the impacts caused. In conclusion, in line with the recommendation from the UN, it is a must to ensure that all international human rights instruments are inherent in any regulations on internet. Certainty in such instrument adoption will guarantee the protection on the rights for individuals to surf the internet, especially the rights to freedom of expression and the right to privacy, as well as a guaranteed universal access. This exposure on the dynamics of regulations related to the use of internet technology in three Southeast Asian countries, is expected to give a complete picture in preparing and formulating policies that correlate to the internet and human rights, for now and henceforth.

## Bibliography

- After the RH Law: Magna Carta for Internet Freedom is Miriam's new pet bill. (2013). Accessed at August 1, 2013, from [http://www.senate.gov.ph/press\\_release/2013/0703\\_santiago1.asp](http://www.senate.gov.ph/press_release/2013/0703_santiago1.asp)
- Alam, J. (2007). History of the Indonesia Internet eXchange (IIX). may be take from [http://www.iix.net.id/library/lix\\_history.pdf](http://www.iix.net.id/library/lix_history.pdf).
- Alampay, E. A. (2008). *Telecom Regulatory and Policy Environment in the Philippines: Results and Analysis of the 2008 TRE Survey*. may be take from [http://lrneasia.net/wp-content/uploads/2009/07/TRE\\_Philippines\\_final\\_2008Nov29.pdf](http://lrneasia.net/wp-content/uploads/2009/07/TRE_Philippines_final_2008Nov29.pdf).
- Ali Salman, d. (2013, April). Tracing the Diffusion of Internet in Malaysia: Then and Now. *Asian Social Science*, Vol. 9(No. 6).
- APJII. (2013). 2013, Pengguna Internet Indonesia Bisa Tembus 82 Juta. Accessed August 1, 2013, dari <http://www.apjii.or.id/v2/index.php/read/content/apjii-at-media/139/2013-pengguna-internet-indonesia-bisa-tembus-82-ju.html>
- APNIC. (2004). *The Internet in Malaysia*. Accessed at August 1, 2013, from [https://www.apnic.net/\\_\\_data/assets/pdf\\_file/0020/27920/apster9-200402.pdf](https://www.apnic.net/__data/assets/pdf_file/0020/27920/apster9-200402.pdf)
- APNIC. (2013, August 1). The Internet History in Indonesia. may be take from [http://www.apnic.net/\\_\\_data/assets/pdf\\_file/0010/27919/apster21-200702.pdf](http://www.apnic.net/__data/assets/pdf_file/0010/27919/apster21-200702.pdf).
- Blogger 'arrested' at midnight under Sedition Act. (2011). Accessed at August 1, 2013, from <http://www.malaysia-today.net/mtcolumns/from-around-the-blogs/38903-blogger-arrested-at-midnight-under-sedition-act>
- Blogger held under OSA over articles against Johor sultan. (2012). may be take from <http://www.malaysiakini.com/news/202760>
- BMGI Inc. vs. Gueverra: first Facebook libel case in the Philippines dismissed by court. (2011). Accessed at August 1, 2013, dari <http://technogra.ph/2011/07/30/bmgi-inc-vs-gueverra-first-facebook-libel-case-in-the-philippines-dismissed-by-court/>
- Center for Law and Democracy. (2012, December). Philippines, Analysis of the Cybercrime Prevention Act of 2012.
- Center for Law and Democracy. (2012, November). Philippines, Analysis of the Cybercrime Prevention Act of 2012. may be take from dari [http://www.law-democracy.org/live/wp-content/uploads/2012/08/Phil.Cybercrime.final\\_.pdf](http://www.law-democracy.org/live/wp-content/uploads/2012/08/Phil.Cybercrime.final_.pdf).
- Communications and Multimedia Content Forum of Malaysia. (2013). <http://www.cmcf.my/home.php>.
- Constitution of Malaysia. (1963).
- Cybercrime law is suspended by Philippines court. (2012). Accessed at August 1, 2013, from <http://www.bbc.co.uk/news/world-asia-19881346>
- Defamation and the internet: the multiple publication rule. (2009). may be take from <http://www.commentonthis.com/defamation/>
- Desa Pinter yang Terpasang. (2011). Accessed at August 1, 2013, from <http://statistik.kominfo.go.id/site/data?idtree=244&iddoc=789>
- Dewan Teknologi Informasi dan Komunikasi Nasional (Detiknas). (2013). Palapa Ring. Accessed at August 1, 2013, from <http://www.detiknas.org/index.php/flagship/c/14/>
- Djafar, Wahyudi, et.al. (2011). 2000-2010 Kebebasan Internet Indonesia: Perjuangan Meretas Batas. Jakarta: IMDLN;ICJR. Accessed at 2013, from [http://wahyudidjafar.files.wordpress.com/2011/12/briefing-paper-3\\_2011\\_kebebasan-internet.pdf](http://wahyudidjafar.files.wordpress.com/2011/12/briefing-paper-3_2011_kebebasan-internet.pdf).
- Djafar, Wahyudi, et.al. (2012). *Hak Asasi Manusia dalam Pusaran Politik Transaksional: Penilaian terhadap Kebijakan HAM dalam Produk Legislasi dan Pengawasan DPR RI Periode 2004-2009*. Jakarta: ELSAM. may be take from <http://elsam.or.id/article.php?lang=in&id=1731>
- Djafar, Wahyudi, et.al. (2013, Februari 21). Protecting privacy rights from wiretapping. *The Jakarta Post*. may be take from <http://www.thejakartapost.com/news/2013/02/21/protecting-privacy-rights-wiretapping.html>.

- Djafar, Wahyudi. (t.thn.). Kita Perlu UU Perlindungan Data Pribadi. may be take from <http://www.hukumpedia.com/ham/kita-perlu-uu-perlindungan-data-pribadi-hk51da54d24bb82.html>.
- DOJ deletes libel from new anti-cybercrime bill. (2013). Accessed at August 1, 2013, from <http://www.businessmirror.com.ph/index.php/en/news/nation/13927-doj-deletes-libel-from-new-anti-cybercrime-bill>
- DOJ to drop online libel from revised cybercrime law. (2013). Accessed at August 1, 2013, from <http://www.gmanetwork.com/news/story/309704/scitech/technology/doj-to-drop-online-libel-from-revised-cybercrime-law>
- Executive Order No. 780 Tahun 2009. (2009). may be take from <http://www.gov.ph/2009/01/29/executive-order-no-780-s-2009/>
- Facebook Country Stats February 2013. (2013, February). Accessed at August 1, 2013, from <http://www.quintly.com/blog/2013/02/facebook-country-stats-february-2013-top-10-countries-lose-users/>
- Freedom House. (2012). *Philippines Freedom on the Net 2012*. New York: Freedom House. may be take from <http://www.freedomhouse.org/report/freedom-net/2012/philippines>
- Gmanetwork. (2013). Supreme Court extends TRO on cybercrime law. Accessed at August 1, 2013, from <http://www.gmanetwork.com/news/story/293478/news/nation/supreme-court-extends-tro-on-cybercrime-law>
- Graft suspected in Rp 40 trillion IT project. (2013). Accessed at August 1, 2013, from <http://www.thejakartapost.com/news/2013/07/11/graft-suspected-rp-40-trillion-it-project.html>
- <http://www.apjii.or.id/v2/index.php/read/page/halaman-data/8/regulasi.html>. (2013). Accessed at August 1, 2013, dari <http://www.apjii.or.id>.
- <http://www.apjii.or.id/v2/index.php/read/page/halaman-data/9/statistik.html>. (2013). may be take from <http://www.apjii.or.id/>.
- <http://www.apjii.or.id/v2/index.php/read/page/halaman-tentang/1/latar-belakang-.html>. (2013). Accessed at August 1, 2013, from <http://www.apjii.or.id/>.
- [http://www.apjii.or.id/v2/upload/Regulasi/KM59\\_1996.pdf](http://www.apjii.or.id/v2/upload/Regulasi/KM59_1996.pdf). (1996). Accessed at August 1, 2013, from <http://www.apjii.or.id/>.
- [http://www.apjii.or.id/v2/upload/Regulasi/PP\\_52\\_2000.html](http://www.apjii.or.id/v2/upload/Regulasi/PP_52_2000.html). (2000). Accessed at August 1, 2013, from <http://www.apjii.or.id>.
- [http://www.federalgazette.agc.gov.my/outputaktap/20120622\\_747\\_BI\\_Act%20747%20BI.pdf](http://www.federalgazette.agc.gov.my/outputaktap/20120622_747_BI_Act%20747%20BI.pdf). (2012). may be take from <http://www.federalgazette.agc.gov.my>.
- <http://www.internetworldstats.com/stats3.htm>. (2013).
- [http://www.suhakam.org.my/c/document\\_library/get\\_file?p\\_l\\_id=30276&folderId=24703&name=DFFE-9701.pdf](http://www.suhakam.org.my/c/document_library/get_file?p_l_id=30276&folderId=24703&name=DFFE-9701.pdf). (t.thn.). may be take from <http://www.suhakam.org.my>.
- Indonesia. Law Number 3 Tahun 1989 about Telecommunication
- Indonesia. Law Number 11 Tahun 2008 about Information and Elektronik Transaction
- Indonesia. Law Number 44 Tahun 2008 about Pornography
- Information Technology and Electronic Commerce Council. (2013). <http://www.itecc.gov.ph/about.htm>.
- Information Technology in The Philippines. (t.thn.). Accessed at August 1, 2013, from <http://www1.american.edu/carmel/bree/internet.html>
- International Telecommunication Union. (2013). [http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP\\_intYear=1998&RP\\_intLanguageID=1&RP\\_bitLiveData=False](http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=1998&RP_intLanguageID=1&RP_bitLiveData=False),. accessed at August 1, 2013, from <http://www.itu.int/>.
- International Telecommunication Union. (2002). Multimedia Malaysia: Internet Case Study. 19. Geneva: International Telecommunication Union.

- International Telecommunication Union. (2002). Pinoy Internet: Philippines Case Study. Geneva: International Telecommunication Union.
- Internet Law in Philippines Takes Effect, Raising Fears. (2012). Accessed at August 1, 2013, from <http://www.nytimes.com/2012/10/04/world/asia/new-internet-law-gets-hostile-reception-in-philippines.html>
- Kabataan Partylist files Magna Carta of Internet Users. (2013). Accessed at August 1, 2013, from <http://kabataanpartylist.com/blog/kabataan-partylist-files-magna-carta-of-internet-users/>
- Kementerian Komunikasi dan Informatika. (2013). Penyebaran PLIK dan M-PLIK Wujud Hak Masyarakat Peroleh Informasi. Accessed at August 1, 2013, from [http://kominfo.go.id/berita\\_kemendrian/detail/4005/Penyebaran+PLIK+dan+MPLIK+Wujud+Hak+Masyarakat+Peroleh+Informasi](http://kominfo.go.id/berita_kemendrian/detail/4005/Penyebaran+PLIK+dan+MPLIK+Wujud+Hak+Masyarakat+Peroleh+Informasi)
- Kementerian Komunikasi dan Informatika. (2013). Siaran Pers No. 55/PIH/KOMINFO/7/2013. Accessed at August 1, 2013, from <http://kominfo.go.id/berita/detail/4057/Siaran+Pers+No.+55-PIH-KOMINFO-7-2013+tentang+Tanggapan+Terhadap+Berita+Mengenai+Potensi+Penyalah+Gunaan+Anggaran+di+Kementerian+Kominfo>
- Kitab Undang-undang Hukum Pidana (KUHP) Art. 310, 311, 315, 207, and 208. (s.a).
- Kurniawan, A. (2007). *Indonesia Internet eXchange (IIX)*. Jakarta: APJII.
- Laws of Malaysia Act 234 of Dangerous Drugs. (1952).
- Laws of Malaysia Act 286 of Defamation. (2006). may be take from <http://www.agc.gov.my/Akta/Vol.%206/Act%20286.pdf>.
- Laws of Malaysia Act 365 of Kidnapping. (1961).
- Laws of Malaysia Act 562 of Digital Signature . (1997).
- Laws of Malaysia Act 747 of Security Offences (Special Measures). (2012).
- Laws of Malaysia Act 88 Official Secrets Act. (1972).
- Laws of Malaysia Act A1420 of Copyright. (2012). may be take from [http://www.federalgazette.agc.gov.my/outputaktap/20120209\\_A1420\\_BI\\_JW001763%20Act%20A1420-BI.pdf](http://www.federalgazette.agc.gov.my/outputaktap/20120209_A1420_BI_JW001763%20Act%20A1420-BI.pdf).
- Laws of Malaysia Act Personal Data Protection. (2010).
- Laws of Malaysia Act 15 Sedition Act. (2006). may be take from <http://www.agc.gov.my/Akta/Vol.%201/Act%2015.pdf>
- Laws of Malaysia Act 563 of Computer Crimes Act 1997. (1997).
- Laws of Malaysia Act 564 of Telemedicine Act. (1997).
- Laws of Malaysia Act 589 of Communications and Multimedia Act. (1998).
- Laws of Malaysia Act 658 Electronic Commerce Act . (2006).
- Laws of Malaysia Act 708 Strategic Trade . (2010).
- Lim, J. a. (2001, December). Drivers and Impediments to e-Commerce in Malaysia. *Malaysian Journal of Library and Information Science*, Vol. 6( No. 2), Page 1-19.
- Lim, M. (2005). Archipelago Online: The Internet and Political Activism in Indonesia. 61. School of Business, Public Administration and Technology, University of Twente, the Netherlands.
- Magna Charta for Philippine Internet Freedom. (2013). Accessed 2013, from <http://www.senate.gov.ph/lisdata/1446312119!.pdf>.
- Malaysia blogger arrested for posting anti-government comments. (2008). may be take from <http://www.theguardian.com/world/2008/sep/12/malaysia.pressandpublishing>
- Malaysia Internet Exchange. (2013). The Malaysia Internet Exchange (MYIX). Accessed at August 1, 2013, from <http://myix.my/about-myix/>
- Malaysiakini. (2009). Target: Broadband Penetration to Go Up to 50% by Next Year. Accessed at August 1, 2013, from <http://malaysiakini.com/news/117064>
- Malaysian elections: Bloggers arrested after police reports lodged against them. (2013, May 8). may be take from



- <http://news.asiaone.com/News/AsiaOne+News/Malaysia/Story/A1Story20130508-420987.html>
- Malaysian police may arrest sex bloggers. (2013, July 17). may be take from <http://www.todayonline.com/world/asia/malaysian-police-may-arrest-sex-bloggers>
- Mirandilla, M. G. (December 2007). Achieving Universal Access through Liberalization, Regulation, and Deregulation: The Case of the Philippine Telecommunications and ICT Sector. *The Communication Policy Research (CPR) south2 conference*. Chennai. may be take from [http://www.cprsouth.org/wp-content/uploads/drupal/Grace\\_Mirandilla.pdf](http://www.cprsouth.org/wp-content/uploads/drupal/Grace_Mirandilla.pdf).
- Mobile overtakes internet cafes as primary access point. (2013). Accessed at August 1, 2013, from <http://www.emarketer.com/Article/Indonesias-Cities-Mobile-Boosts-Internet-No-2-Media-Spot/1009637>
- Mono, G. I. (2012, April 24). Localizing the Internet in the Philippines. May be take from <http://www.telecomasia.net/>
- National Telecommunication Commissions. (2013). <http://www.ntc.gov.ph/>.
- Nelson, K. A. (2009, Winter). Transnational Wiretaps and the Fourth Amendment. *Hasting Constitutional Law Quarterly*, Vol. 36(No. 2), hal. hal. 340-341.
- New enforcement date of the Personal Data Protection Act 2010 announced. (2010). may be take from <http://www.lexology.com/library/detail.aspx?g=9aa430a4-d841-4cb6-9e2d-911c71a24b17>
- Newmediatrendwatch. (2013). <http://www.newmediatrendwatch.com/markets-by-country/11-long-haul/55-malaysia>. Accessed at August 1, 2013, from <http://www.newmediatrendwatch.com/>.
- Office of The High Commissioner for Human Rights. (2011). Internet should remain as open as possible – UN expert on freedom of expression. accessed 2013, from <http://www2.ohchr.org>: [http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27\\_en.pdf](http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf).
- Official Secrets Act. (1972). may be take from <http://www.agc.gov.my/Akta/Vol.%202/Act%2088.pdf>
- Pabico, A. (1999). Online advocacy. Dalam S.S. Coronel (editor), *From Loren to Marimar: The Philippine media in the 1990s*. Quezon City: Philippine Center for Investigative Journalism.
- Philippines Executive Order No. 125-A Year 1987. (1987). May be take from [http://www.lawphil.net/executive/execord/eo1987/eo\\_125\\_a\\_1987.html](http://www.lawphil.net/executive/execord/eo1987/eo_125_a_1987.html)
- Philippines Executive Order No. 18 Year 2001. (2001). May be take from <http://www.itecc.gov.ph/files/eo%2018.pdf>
- Philippines Executive Order No. 264 Year 2000. (2000). May be take from <http://www.itecc.gov.ph/files/eo%20264.pdf>
- Philippines Executive Order No. 269 Year 2004. (2004). May be take from [http://www.lawphil.net/executive/execord/eo2004/eo\\_269\\_2004.html](http://www.lawphil.net/executive/execord/eo2004/eo_269_2004.html)
- Philippines Executive Order No. 454 Year 2005. (2005). May be take from <http://www.gov.ph/2005/08/16/executive-order-no-454-s-2005/>
- Philippines Executive Order No. 47 Year 2011. (2011). May be take from <http://icto.dost.gov.ph/index.php/home>
- Philippines Executive Order No. 47 Year 2011. (2011). May be take from <http://www.gov.ph/2011/06/23/executive-order-no-47/>
- Philippines Executive Order No. 546 Year 1979 . (1979). May be take from [http://www.lawphil.net/executive/execord/eo1979/eo\\_546\\_1979.html](http://www.lawphil.net/executive/execord/eo1979/eo_546_1979.html).
- Philippines Executive Order No. 648 Year 2007. (2007).
- Philippines Internet eXchange. (2013). <http://www.phix.net.ph/>.
- Philippines Republic Act 9775 of Anti-Child Pornography. (2009).
- Philippines Republic Act 9775. (2009).
- Philippines Republic Act No. 8793 of Electronic Commerce. (2000).

- Philippines Republic Act 10175 of Cyber Crime Law. (2012). Accessed at August 1, 2013, from <http://www.gov.ph/2012/09/12/republic-act-no-10175/>.
- Philippines Republic Act 7925 of Public Telecommunications Policy. (1995). May be take from <http://ntc.gov.ph/laws/laws/LAW%207925.pdf>
- Pinoy netizens welcome Miriam's online rights bill. (2013). Accessed at August 1, 2013, from <http://www.abs-cbnnews.com/nation/07/03/13/pinoy-netizens-welcome-miriam-online-rights-bill>
- PKPS Bappenas. (1999). [http://pkps.bappenas.go.id/dokumen/uu/Uu%20Sektor/Telekomunikasi/20.%20uu\\_36\\_1999.pdf](http://pkps.bappenas.go.id/dokumen/uu/Uu%20Sektor/Telekomunikasi/20.%20uu_36_1999.pdf). Accessed at August 1, 2013
- Republic Act 10173 Data Privacy Act. (2012).
- Republic Act 4200 The Anti-wiretapping Law. (1965).
- Republic Act 8484 Access Devices Regulation. (1998). May be take from <http://www.pctc.gov.ph/initiatv/RA8484.htm>
- Rue, F. L. (2010). *A/HRC/14/23 Paragraf 59*.
- Saptaningrum, I. D.; Wahyudi Djafar (2013). *Tata kelola internet yang berbasis hak: Studi tentang permasalahan umum tata kelola internet dan dampaknya terhadap perlindungan hak asasi manusia*. Jakarta: ELSAM.
- Sejarah Perkembangan Internet di Indonesia. (2010). Accessed at August 1, 2013, from <http://id.shvoong.com/internet-and-technologies/commercial-companies/2040621-sejarah-perkembangan-internet-di-indonesia/#ixzz1O8XRNW00>
- Socialmemos. (2013). Social Media Statistics for Indonesia. Accessed at August 1, 2013, from <http://socialmemos.com/social-media-statistics-for-indonesia/>
- Solons defend blogger sued by DSWD for libel. (2010). May be take from <http://newsinfo.inquirer.net/breakingnews/nation/view/20100125-249403/Solons-defend-blogger-sued-by-DSWD-for-libel>
- Soriano, C. R. (December 2007). Universal Access in the Philippines: A Review of Policies and Strategies. *The CPRsouth2 2007: Research of Improving ICT governance in the Asia Pacific*. Chennai. Diambil kembali dari [http://www.cprsouth.org/wp-content/uploads/drupal/Cheryll\\_Soriano.pdf](http://www.cprsouth.org/wp-content/uploads/drupal/Cheryll_Soriano.pdf).
- Soriano, E. C. (2007). *Towards Universal Internet Access in the Philippines*. Manila: Ideacorp and Intel Technology Philippines, Inc. May be take from <http://www.unapcict.org/ecohub/resources/towards-universal-internet-access>
- Sosa, G. C. (2009, Desember). Country Report on Cybercrime: The Philippines. *The Criminal Justice Response to Cybercrime Course*. Tokyo. May be take from [http://www.unafei.or.jp/english/pdf/RS\\_No79/No79\\_00All.pdf](http://www.unafei.or.jp/english/pdf/RS_No79/No79_00All.pdf).
- Supreme Court of the Philippines. (2012). <http://sc.judiciary.gov.ph/microsite/cybercrime/203469.php>.
- The Constitution of the Philippines. (1987).
- The National Computer Center. (2013). <http://www.ncc.gov.ph/default.php?a1=2&a2=5&a3=1&a4=PQRS&a5=37>. May be take from <http://www.ncc.gov.ph/>.
- United Nations. (1966). International Covenant on Civil and Political Rights. Accessed at 2013, from <http://treaties.un.org/>
- United Nations. (2013). [http://treaties.un.org/Pages/ViewDetails.aspx?mtdsg\\_no=IV-4&chapter=4&lang=en%23EndDec#EndDec](http://treaties.un.org/Pages/ViewDetails.aspx?mtdsg_no=IV-4&chapter=4&lang=en%23EndDec#EndDec).
- United Nations Human Rights Council. (2010). A/HRC/14/23.
- United Nations Human Rights Council. (2012). A/HRC/20/L.13. May be take from <http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement>.

York, J. C. (2013). *A Brief Analysis of the Magna Carta for Philippine Internet Freedom*. May be take from <https://www.eff.org/deeplinks/2013/07/brief-analysis-magna-carta-philippine-internet-freedom>



Institute for Policy Research and Advocacy (ELSAM), established in August 1993 in Jakarta, is a policy advocacy organisation with limited association as its legal entity. To actively participate in the efforts to develop, promote and protect civil and political rights and other human rights, as mandated by the 1945 Constitution and Universal Declaration of Human Rights (UDHR), has become ELSAM's 'driving' objective. From the outset, ELSAM has committed itself to developing a democratic political order in Indonesia by empowering civil society through advocacy and promoting human rights.

### **VISION**

Indonesia as a democratic and just society and country that respect for human rights.

### **MISSION**

As a non-governmental organisation, ELSAM strives for all human rights, including civil and political rights and economic, social and cultural rights.

### **MAIN PROGRAMMES:**

1. Policy and law research and their impacts on human rights
2. Human rights advocacy in various forms
3. Human rights education and training
4. Publication and human rights information dissemination

### **PROGRAMME OF WORK:**

1. The Integration of Human Rights Principles and Norms in State Law and Policy
2. The Integration of Human Rights Principles and Norms in Corporate Operation Policy in Relation with Local Communities
3. Strengthening Civil Society's Capacity in Promoting Human Rights

### **Board (period 2010-2014)**

Chairperson: Ihdhal Kasim, S.H. (Chairperson of National Commission on Human Rights 2007-2012)

Vice: Sandra Moniaga, S.H. (Environment and Indigenous People Activist)

Secretary: Roichatul Aswidah, S.Sos, M.A. (Researcher on Democracy and Human Rights issues)

Treasurer 1 : Suraiya Kamaruzzaman, S.T., LL.M (Women Activist in Aceh)

Treasurer 2 : Abdul Haris Semendawai, S.H., LL.M. (Chairperson of Victim and Witness Protection Institution, 2008-2013)

### **Members of Association:**

Abdul Hakim G. Nusantara, S.H., LL.M.; I Gusti Agung Putri Astrid Kartika, M.A.; Ir. Agustinus Rumansara, M.Sc.; Hadimulyo; Lies Marcoes, M.A.; Johni Simanjuntak, S.H.; Kamala Chandrakirana, M.A.; Maria Hartiningsih; E. Rini Pratsnawati; Ir. Yosep Adi Prasetyo; Francisia Saveria Sika Ery Seda, Ph.D.; Raharja Waluya Jati; Sentot Setyasiswanto S.Sos.; Tugiran S.Pd.; Herlambang Perdana Wiratraman, S.H., M.A.

**Executives 2013-2015:**

Executive Director: Indriaswati Dyah Saptaningrum, S.H., LL.M.

Deputy Director of Human Rights Advocacy for Justice: Wahyu Wagiman, S.H.

Deputy Director of Human Rights Resource Development (Atty.): Zainal Abidin, S.H.

Head of Research and Institutional Development Bureau: Otto Adi Yulianto, S.E.

**Staffs:** Ahmad Muzani; Andi Muttaqien, S.H.; Ari Yurino, S.Psi.; Daywin Prayogo, S.IP.; Elisabet Maria Sagala, S.E.; Elly F. Pangemanan; Ester Rini Pratsnawati, S.E.; Ikhana Indah Barnasaputri, S.H.; Khumaedy; Kosim; Maria Ririhena, S.E.; Mohamad Zaki Husein, S.H., M. Sos.; Paijo; Rina Erayanti, S.Pd.; Siti Mariatul Qibtiyah; Sukadi; Wahyudi Djafar, S.H.; Yohanna Kuncup S.S.

**Address:**

Jl. Siaga II No. 31, Pejaten Barat, Pasar Minggu, Jakarta 12510 INDONESIA

Tel.: (+62 21) 797 2662; 7919 2519; 7919 2564

Telefax.: (+62 21) 7919 2519

Email: office@elsam.or.id

Website: www.elsam.or.id

Timeline on Twitter: @elsamnews and @ElsamLibrary

Visit us on Facebook : <http://www.facebook.com/perkumpulanelam>

This paper would look on the preliminary initiatives of utilization and development of information and communication technology, especially internet, in the southeast region, taking examples in three countries, Indonesia, Malaysia and Philippines. The paper would also discuss the framework and model adopted by each country in governing use and development of Information and communication technology. Furthermore, as the use and development of ICT had expanded in the last few years, some crucial problem had arisen related with the use of this technology. To emphasize the previous point, besides of delivering various positive benefits for the advance of human life qualities and human rights fulfillment in general, the rapid growth of internet had also spurred negative impacts, putting everyone as potential victim of the impact. These negative impact had triggered the government to issue some regulations the specifically governs the use and control of this technology.

Viewing the situation, the paper would also examine the tendencies of countries to set national rules to limit the user in the use of internet technology. The limitation phenomena gained legitimacy from the raising issue of cyber sovereignty, which often propose nationalism slogan without closely and holistically examining every facet of cyber characteristic that hardly had any apparent territorial borders. The issue of limitation on usage of internet technology seems to complete the problem of internet access that are still primary problem in the third world countries, specially developing countries like Indonesia, Malaysia and Philippines.



The Institute for Policy Research and Advocacy [ELSAM]  
Jl. Siaga II No. 31, Pejaten Barat, Pasar Minggu, Jakarta 12510 INDONESIA  
Tel.: (+62 21) 797 2662; 7919 2519; 7919 2564, Telefax.: (+62 21) 7919 2519  
Email: [office@elsam.or.id](mailto:office@elsam.or.id)  
Website: [www.elsam.or.id](http://www.elsam.or.id) | Timeline on Twitter: @elsamnews | @ElsamLibrary