Intermediary Liability

Child Protection’s Study in Thailand

Aua-aree Engehanit

Abstract

The dissemination of information can be conducted through various channels such as printing media, radio, or television. In fact, the dissemination by internet has become widespread worldwide. In particular, we have found that a lot of contents shown on the internet affect the rights of children, for instance, child pornography or children’s privacy. The government should have a duty to provide preventive measures. In Thailand, besides Penal Code and Child Protection Act, there is the Computer-related Offense Act of 2007, which defines the duties and liabilities of the offender who commit Computer-related crimes and the others who involved in perpetrating the crime. Sometimes, Internet Service Providers (ISP) are included as entities who should take responsibility like an intermediary liability as well.

Born as human beings, children have their right to enjoy human dignity and fundamental rights as well as adults. Children’s rights are basically defined under Universal Declaration of Human Right of 1948 and other laws. The children’s human rights require particular attention during their childhood. The government should be responsible for providing a lawful protection to children in accordance with Convention on the Right of Child (CRC), organized by the UN.

Thailand, a member of United Nation, has ratified the above Convention which indicates that the ratifying country has agreed to follow the proceedings in terms of child

---

1 Assistant Professor at Faculty of Law, Chulalongkorn University, Docteur en Droit, Aix-Marseille Université
protection. As a result, there are many Thai laws associated with children, such as the Constitution of the Kingdom of Thailand from 2007, the Children Protection Act 2003, and the Penal Code, which is guarantees fundamental righteous treatment of children by all means necessary.

Though Thailand has provided various child protection acts, many children face daily violations, mostly in terms of physical abuse or sexual harassment. A growing problem nowadays is the violation of children’s rights over the internet, principally found on pornographic websites or social networks.

Considering the porno media warning focusing on sexual harassment contents or people under 18 years old, we found that child pornographic contents mostly have been transmitted to the website and file drive. With these increasing instances of transmission via social media, it makes sense with evidence found in Thailand databases. The Internet Foundation for the Development of Thailand found more than 528 reports of child sex content last year (2014) and that number is likely to increase. The production and distribution of child pornography breaches each child’s fundamental rights. Collecting and accessing child pornographic media might also cause sexual abuses to them.

Recently, regulations for child pornography have not been implemented yet in Thailand. We only take pornographic media seriously in the Penal Code and the Computer-related Offense Act of 2007. The definition of pornographic media in both laws is includes all kinds of “child and adult pornography”. However, we are trying to create legislation that criminalizes any actions involving child pornography and makes the punishment more severe than adult pornography. Through the amendment process, the Legislature has approved these changes to the Thai Penal Code related to child pornography and they will be enacted soon.

---


[3] มูลนิธิอินเทอร์เน็ตฯ หนุน “กฎหมายคุมสื่อลามกเด็ก”, Thiahotline, 

[4] Id.

[5] The draft of child pornographic provision was voted by the General Assembly last May 2015, Member of National legislative Assembly.
With the limited technology and limited accessibility, the internet in Thailand was only used in education at first\(^6\). Thailand initially obtained internet access in 1987 with the cooperation between Asia Institute of Technology (AIT) and Department of Computer Science, University of Melbourne Australia. Then the rapid growth of the internet expanded to other research institute\(^7\).

The growth of internet usage in Thailand is continuously growing. The fact is that there is the development of Website to Web 2.0 (User Generated Content- UCG), which internet users can easily create and share data one another in textual, visual, vocal, or animated forms. It is expanding the amount of content on the internet rapidly.\(^8\)

Considering the government’s regime in controlling internet, we can divide into 3 periods since the arrival of the internet in Thailand from 1987 to present as follows\(^9\):


   As the small internet usages (mostly public officers) in this time, there is unnecessary to control internet data. Internet societies have become the regime of internet content regulation. They had the agreement based on freedom of expression in surfing internet. The “limitation of internet accessibility” had never existed. It is the idealistic communication which is everyone’s accessible and unidentified usage.

2. **Internet under the government’s control via Ministry of Information and Communication Technology (ICT) (2000-2007)**

   The internet users have massive expanded in this era, which brought too much creation and consumption on the internet. Therefore, some explicit content should be suspended or banned for some kinds of user, especially children. For example, obscene websites, online gaming, and political conflict contents, which affects national security or defamation of the Thai monarchy.

---

6 The usage of internet initially required basic computer knowledge and used only English language. Pirongrong Ramasoota, การกํากับดูแลเนื้อหาอินเทอร์เน็ต (ฉบับที่ ...), พ.ศ... (ความผิดที่เกี่ยวกับสื่อคอมมูนิเคชั่นยุคดิจิตอล), n. 17/2558 (2015), http://library2.parliament.go.th/giventake/content_nla2557/apnla2558-012.pdf

7 Id. at 251.

8 Id. at 267.

9 Id. at 279.
For this reason, the Ministry of Information and Communication Technology (ICT) was established in 2002. Control of the internet is the vital role of the Ministry of ICT. Originally, no legislation existed to control internet content. The relevant regulation had been applied to punish abusers, such as the Control of Business Relating to Tape Cassette and Television Material Act 1987.

In 2003, The Ministry of ICT appointed “the Investigative Committee to Protect and Eliminate Computer Crime” or Cyber Inspector to block inappropriate content, like pornographic websites or threats to national security. In 2006, the Government issued a policy relating to the elimination of obscene websites or other negatively influencing websites. Also they control explicit content on the internet via www.thaicybercop.com, which is open for people who need to report inappropriate public content. If officer’s investigations can prove guilt, they will transfer website domain name to the Ministry of ICT in process. Meanwhile, they will send the cooperation letters to Internet Service Provider (ISP) and server owner of that website. The reported website must then be deactivated within 3 days, or the ISP will charge under the section 287 of Penal Code10.

Thailand did not apply any regulations to block websites in that time. Neither the investigators nor the courts had any authority to ban websites. They only asked for internet usage data from ISP. The Council of State discussed the jurisdiction of authorities with Royal Thai Police. They referred to football gambling website, which had Asia Info Net Co., Ltd. as an ISP case that blocked transmission of pornography or other illegal websites that could not be done by police officers or the courts because no acts or regulations exist that could be applied. The most relevant legislation was the Printing Act of 1941, but this act mostly

---


1. For the purpose of trade or by trade, for public distribution or exhibition, makes, produces, processes, brings or causes to be brought into the Kingdom, sends or causes to be sent out of the Kingdom, taken away, or circulates by any means whatever, any document, drawing, print, painting, printed matter, picture, poster, symbol, photograph, cinematograph film, noise tape, picture tape or any other thing which is obscene;

2. Carries on trade, or takes part or participates in the trade concerning the aforesaid obscene material or thing, or distributes or exhibits to the public, or hires out such material or thing;

3. In order to assist in the circulation or trading of the aforesaid obscene material or thing, propagates or spreads the news by any means whatever that there is a person committing the act which is an Offense according to this Section, or propagates or spreads the news that the aforesaid obscene material or thing may be obtained from any person or by any means, shall be punished with imprisonment not exceeding three years or fined not exceeding six thousand Baht, or both”
stressed on printing materials not websites. Nevertheless, police officers could report the Office of National Telecommunications Commission to revoke the ISP’s license.

Because no applicable regulations existed, internet surveillance pursued by Royal Thai Police, the Ministry of ICT, and the Office of National Telecommunications Commission achieved success with influential political content. Protests against the government of Thaksin Shinawatra during 2005-2006 caused the government to pursue strict surveillance of media, such as revoked radio and TV stations who extremely criticized government’s capability, took part in holding the share on influential newspaper. Therefore, citizen turned to surfing another media which no interference by government. For example, community radio, local cable TV channel or particular website. Discussion on the righteousness and so-called opposing government’s authorities online initiated interception of political instability website conducted by government.

After the Coup in 2006, more than 2,500 websites have been shut down, including interference database accessibility through Proxy servers and cache, such as Google. Plus, closing down interactive online such as Midnight University website and Rajadamnern Room in Pantip, a famous community webboard, significantly conducted to the content that violated the Coup order.

3. Internet’s supervision under the Computer-related Offense Act of 2007

Since the Coup in September 2006, Thai politics has been divided into two sides: the royalists and the non-royalists. The non-royalists were accused of supporting Thaksin Shinawatra, a former Thai Prime Minister, who was ousted abroad since the staged Coup.

Lèse-majesté websites led to internet surveillance. Besides, the Ministry of ICT appointed inspector to conduct surveillance on lèse-majesté websites. Then, Legislative

---

12 Midnight University is a virtual university for free public education. It contains over 1,500 scholarly articles and has a discussion forum, มหาวิทยาลัยเที่ยงคืน, http://v1.midnightuniv.org/midarticle/newpage33.htm (last visited Sep. 2, 2015)
13 The objective of Rajadamnern Room is the political issue’s discussion, ห้องราชดําเนิน, http://pantip.com/forum/rajdumnern (last visited Sep. 2, 2015)
Assembly selected by Council of National Security (CNS) enacted the Computer-related Offense Act of 2007. This act in general authorizes the Ministry of ICT to apply and cooperate with many organizations such as Department of Special Investigation (DSI)\textsuperscript{16} and Thai Royal Police\textsuperscript{17}.

The Constitution of the Kingdom of Thailand of 2007 has certified the rights and liberties of communication and internet access\textsuperscript{18}. Article 36 provides that:

“A person shall enjoy the liberty of communication by lawful mean.

The censorship, detention or disclosure of communications between persons including any other act disclosing information in the communication between persons shall not be permitted except by virtue of the provisions of the law specifically enacted for maintaining the security of the State or maintaining public order or good morals”

Nevertheless, if we consider deeply in relation to communication law, such as the Computer-related Offense Act of 2007, we may find that the law has already specified the duty and the guilt of persons involved with a computer systems compromising national security and containing computer data that is considered obscene. This article addresses (1) general principal guilt of Intermediary liability under the Computer-related Offense Act of 2007 and (2) the liability of Intermediary Service Providers (ISP) relating to Child Protection in Thailand.

\textsuperscript{16} Department of Special Investigation (DSI) is appointed to investigate on certain “special cases”, including complex criminal cases, national security and organized criminal organizations. \url{https://www.dsi.go.th/view.aspx?tid=T0000011} (last visited Dec. 30, 2015)

\textsuperscript{17} Pirongrong Ramasoota, การกํากับดูแลเนื้อหาอินเทอร์เน็ต, 287 (2013).

\textsuperscript{18} Radthathammanoon (§ 47) <2007>. “Transmission frequencies for radio or television broadcasting and telecommunication are national communication resources for public interests.

There shall be an independent regulatory agency having the duty to allocated the frequencies under paragraph one and exercise supervision over the operation of radio or television broadcasting business and telecommunication business as provided by law.

In carrying out the act under paragraph two, regard shall be had to optimal benefits of the people at national and local levels in education, culture, State security, other public interests and free and fair competition, provides that public participation in the operation of public mass media shall also be encouraged.

In exercising supervision over the operation of businesses under paragraph two, there shall be measures for preventing any merger, cross right-holding or market dominance amongst mass media business or by any other person, which has the effect of impeding the liberty of the public in perceiving information or of obstructing public access to a diversity of information”
1. **Intermediary Liability under the Computer-related Offense Act of 2007**

Generally, disseminating fallacies would be considered equivalent to committing the Offense of defamation (if the message is defamatory). However, the dissemination of information through a service program on a computer or the internet area network differs from other communication methods. Physically, the dissemination through computer system will transmit to the receiver quickly, broadly, and easily. Moreover, to control illegal information online requires special technical measures. Therefore, the legislation against Computer-related Offense is necessary. The relevant law is the Computer-related Offense Act of 2007.

1.1 **Background and objective of the Computer-related Offense Act of 2007**

The Computer-related Offense Act of 2007 is the first law that was enacted to control any inappropriate content on computer systems.

(1) **Background**

The Computer-related Offense Act of 2007 was first drafted in 1998 by The National Information Technology Committee and has used many foreign regulations as guidelines to follow:

- Convention on Cyber Crime 2001 of European Parliament
- Computer Misuse Act of Singapore
- Computer Misuse Act 1997 of Malaysia
- Unauthorized Computer Access Law 2000 of Japan
- The Information Technology Act 2000 of India
- United States Code in section of computer-related law

---

19 Suvichapa Onpueng, วิทยานิพนธ์: ปัญหาการยึดกักใช้ทะเบียนชื่อผู้ใช้วิทยุกระจายเสียงวิทยุกระจายภาพผ่านทางคอมพิวเตอร์ พ.ศ. 2550 : 

20 Council of Europe, Convention on Cybercrime, Nov. 23, 2001, 
The Computer-related Offense Act of 2007 was promulgated in the government gazette on June 16, 2007 and became effective on July 18th of the same year.

(2) Objective

The objective of the Computer-related Offense Act of 2007 is to target computer-related crime, including the abuse of data and networks system. In the past, government officers were unauthorized to prosecute offenses against computer-related crimes, such as hacking into other computer system, gambling online, pornographic websites, as well as ISP’s liability21.

1.2 Introduction of the Computer-related Offense Act of 2007

The offenses in the Computer-related Offense Act of 2007 can be divided into two parts.

Part 1 – Direct offenses to computer systems or computer data (section 5 – 13) Ex. Hacking systems, Spam mail;

Part 2 – Criminal or other related-law offenses committed using a computer (section 14 – 17) Ex: Importation of any false computer data, data affecting national security or terrorism, or considered obscene data.

The example content of the Computer-related Offense Act of 2007 described as following,

(1) The offenses of dissemination of illegal contents

The Computer-related Offense Act of 2007 section 14 describes that:

“A person who commits any of the following offenses shall be subject to imprisonment for a term not exceeding five years or to a fine not exceeding one hundred thousand baht22 or to both:

(1) Importation into a computer system any forged computer data, in whole or in part, in a manner that is likely to cause damage to any person or the public;

(2) Importation into a computer system any false computer data in a manner that is likely to cause damage to national security or public panic;

(3) Importation into a computer system any computer data of which itself is a criminal commission against national security or terrorism prescribed in the Penal Code;

(4) Importation into a computer system any computer data which is considered obscene and such computer data is accessible by the public;

(5) Dissemination or forwarding any computer data with knowledge of being computer data in (1), (2), (3) or (4).”

This provision is influenced from Penal Code, but focuses on using computers or internet systems to commit the offenses\textsuperscript{23} by dissemination, distribution or forward false computer data.\textsuperscript{24}

Therefore, the violation of this provision is the importation of electronic data in form of messaging, visually, vocally, verbally or any other means of transferring files to a computer system or electronic devices which spontaneously processing data.\textsuperscript{25}

Under section 14 of the Computer-related Offense Act of 2007, the data imported from another computer must have fall in one of the content or meaning categories below:

\textsuperscript{23} Pornpetch Wichitcholchai, คำอธิบายว่าด้วยการกระทําผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, 21, (2007)
\textsuperscript{24} <The Computer-related Offense Act > < § 3> [B.E. 2550. “Computer data” Means data, a message, an instruction, a set of instructions or any other things within a computer system which can be processed by a computer system. Computer data shall also include electronic data under the law on electronic transaction”
A. Importation in part or whole of untrue data (or false data) might cause damage to any person. Thailand National Electronics and Computer Technology Center (NECTEC)\textsuperscript{26} explained that untrue or false computer data can compare to the offense of counterfeiting documents under the Penal Code. Counterfeiting may be accomplished by importing incorrect or correct data, but later forging new content, including erase data by transfer data from recorded devices in a manner likely to fabricate authentic documents. These laws also apply to false data. Importing false data causes damage or is likely to cause damage to any person or to public. The wrongdoer must do know the facts constituting the elements of the offense that imported data is the types of untrue or false information. Such as the applicable one is opening forged website aiming to disguise themselves to public.

B. False data, Ex. any rumors that have not been proved, imported into a computer system that is accessible to other users. That content might cause damage to national security, such as politics, military, economics and society. If it can be proved that the content might not cause real damage, but it affects panic within the citizenry in connection with an ordinary standard of that society, it also may be determined to have caused damage to national security.

C. Computer data is itself an offense against national security or terrorism described in the Penal Code.

D. Any computer data containing obscene content that is accessible by public.

Besides the offenses of the doer, any person who disseminates or forwards the data must be punished by the same penalty if that person knew that the data constituted an offense in section 14 (1)-(4). Nonetheless, disseminating or forwarding data in violation of this act

\textsuperscript{26} NECTEC is an organization which is responsible for the development of Information Technology in Thailand. Its mission is to ensure Thailand's competitiveness in Electronics and Computer and the use of IT to stimulate economic and social impact, ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, \url{http://www.nectec.or.th/en/}. (last visited Dec. 30, 2015)
means commission through computer system, not necessarily physically or face-to-face, which might be punished by other regulations.

Section 14 of the Computer-related Offense Act of 2007 imposes sentences not exceeding five years of imprisonment or fine no more than 100,000 baht. In some instances, sentences include both imprisonment and fines.

**2) Liability of Internet Service Provider (ISP)**

In general, Internet Service Providers are able to control their own internet connecting system. Service provider should have a duty to observe and prevent the crime including cooperating with government officers in the discovery of any beneficial evidence leading to wrongdoer getting punished. The Computer-related Offense Act of 2007 defines “Service Provider” in section 3

“1. A person who, either under his own name or other persons’ names or for the benefits of other persons, provides any person internet access service or any other services which allow persons to communicate via computer systems;

2. A person who provides any person computer data storage service.”

According to this Act, the Service Provider has two duties;

**Firstly**, Service Providers have a duty to verify computer data transmitted through computer system and under their own monitoring obligation.

**Secondly**, Service Providers have a duty to Traffic Data Preservation for at least 90 days after the date that data has been transmitted to the computer system. The preservation period is so officers can identify wrongdoers or conduct an investigation if there is reasonable cause to believe that there is the perpetration of an offense under this act. Ex: data storage which can identify users, serial numbers, IP addresses, chat conversations, etc.

The definition of “Service Provider” under this act is broadly interpreted and includes many types of service providers. Section 15 applies to Service Providers whose actions may constitute contributing to violations of the act:

---

“A service provider, who intentionally provides support to or allows a commission of an offense prescribed in section 14 within a computer system under his supervision, shall be subject to the same punishment as those who commit an offense prescribed in section 14.”

Section 15 of the Computer-related Offense Act of 2007 provides obligation and responsibility to Service Providers to supervise their service, and empowers the government officer to charge ISPs. Intentionally providing support or allowing a commission of an offense means that “Service Providers knew that there had been an offense in their system but did not block or delete data whenever they can or whenever government officers inform Service Provider to do that”29. It may allow internet users to commit an offense in section 14 which implies that ISPs support or provide facility to internet users in committing an offense. Therefore, that ISP deemed to be supporter in committing such an offense within section 86 under Penal Code30.

Section 15 of The Computer-related Offense Act of 2007 provides an option for the government to charge an ISP or computer system accused of contain data in section 14.

(3) The power of government officers in requesting for a Court’s order to cease the dissemination of computer data

The Computer-related Offense Act of 2007’s section 20 describes that:

“In case that the commission of an offense prescribed in this Act causes dissemination of computer data which is likely to affect national security as specified in Book II Title I or Title I/I of the Penal Code, or which is against public order or public policy, a competent authority, by approval of the Minister, shall file an application to the Court within its jurisdiction along with relevant evidence in order to obtain a court order to cease the dissemination of such computer data.

28 Id. at § 15.
30 ประมวลกฎหมายอาญา [Penal Code § 86] B.E. 2499. “Whoever for any reason whatsoever assists or facilitates any other person committing an Offense before or during the commission of the Offense, even though such assistance or facility is not known by the offender, is deemed to be a supporter in committing such Offense and shall be punished by two-thirds of the punishment provided for such Offense”
In case that court order in the previous paragraph was obtained, a competent authority shall be the person who proceeds to cease such dissemination or order the service provider to cease the dissemination of such computer data³¹. 

Section 20 describes how to obtain an order to cease the dissemination of computer data or block a website. Before Section 20, no entity had the authority to grant an order to cease. An officer has a duty to file a complaint to the court by approval of the Minister of ICT³².

Another offense in the Computer-related Offense Act of 2007 is the dissemination of material or data that is likely to affect national security or that is contradictory to the peace or good morals of people, including obscene content.

The offenses relating to the security of the kingdom under the Penal Code are divided into four chapters:

- The offenses against the King, the Queen, the Hier-Apparent and the Regent³³
- The offenses against the Internal Security of the Kingdom³⁴
- The offenses against the External Security of the Kingdom³⁵

---

³² Id. at § 20. According to the provision of Section 20, prior to that authority, 3 processes consequently must be done 1. Competent Officer 2. Minister of ICT and 3. Court.
³³ Ex: Assassination against King <ประมวลกฎหมายอาญา> <มาตรา107> [<Penal Code> <§ 107>] B.E. 2499. "Whoever, assassinating the King to the death, shall be punished by the death. Whoever, attempting to commit the act as aforesaid, shall be punished in the same manner. Whoever, making any act as preparation for assassinating the King or knowing that there is the person who will assassinate the King, having made any act to assist in keeping the secret act, shall be punished by life-imprisonment"
³⁴ <ประมวลกฎหมายอาญา> <มาตรา 113> [<Penal Code> <§ 113>] B.E. 2499. “Whoever, commits an act of violence or threatens to commit an act of violence in order to:
1. Overthrow or change the Constitution;
2. Overthrow the legislative power, the executive power or the judicial power of the Constitution, or nullify such power; or
3. Separate the Kingdom or seize the power of administration in any part of the Kingdom, is said to commit insurrection, and shall be punished with death or imprisonment for life.” Ex: Insurgency
³⁵ <ประมวลกฎหมายอาญา> <มาตรา 121> [<Penal Code> <§ 121>] B.E. 2499. “Whoever, being a Thai, bears the arms in battle against the Country, or participates as an enemy of the Country, shall be punished with death or imprisonment for life” Ex: Thai people join foreign army against country
- The offenses against the Amicable Relation with Foreign States

The Computer-related Offense Act of 2007 addresses offenses already addressed by prior legislation, there have been unforeseen consequences related to the objective of the law. For example, editing pictures in order to damage person is already described in the defamation offense under the Penal Code. The offense relating to national security is already described in Internal Security Act 2008. So, the Computer-related Offense Act of 2007 has increased the existing penalties. For instance, the dissemination of false data that can damage a person is the compoundable offense in defamation under the Criminal Procedure Code. On the contrary, if false data is disseminated through a computer system and proceed under the Computer-related Offense Act of 2007 as based law on prosecution, it is considered to be the non-compoundable offense even there was a compromise between victim and alleged offender.

1.3 Enforcement of Computer-related Offense Act of 2007

The offense of the Computer-related Offense Act of 2007 can be divided into two categories: real computer-related offenses against data or computer systems and offenses involving the dissemination of content by computer system. Real computer-related crime or the offense against “data” or computer system following section 5-13 includes illegal or

---

36 <ประกาศกฎหมายอาญา>  มาตรา 130  B.E. 2499. “Whoever, committing bodily harm, or committing any act of violence against the liberty of the Sovereign, his Queen or her Consort, Heir-apparent or Head of a amicable foreign State, shall be punished with imprisonment of one to fifteen years” Ex: Harming against Sovereign’s Liberty

37 <ประกาศกฎหมายอาญา>  มาตรา 328  B.E. 2499. “If the offense of defamation be committed by means of publication of a document, drawing, painting, cinematography film, picture or letters made visible by any means, gramophone record or any other picture, or by propagation by any other means, the offender shall be punished with imprisonment not exceeding two years and fined not exceeding two hundred thousand baht”

38 Compoundable offense means an offense in which the victim of crime plays an important role in determining of prosecution. In compoundable offense, an offender can be prosecuted only if there is a complaint of the victim. Moreover, during prosecution or trial, compoundable offense can be compromise; the offender is acquitted without any trial.

39 Sawatree Suksri, อาชญากรรมคอมพิวเตอร์  งานวิจัยหัวข้อ "ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทําความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐเกี่ยวกับสิทธิเสรีภาพในการแสดงความคิดเห็น", 74 (2012).
unauthorized accessibility, computer sabotage by distribution malicious program (e.g. a virus, worm, logic bomb or Trojan horse). Offenses involving the dissemination of “content” through a computer system following section 14-16 includes the dissemination of pornographic content, data compromising national security or defamation by editing picture online.

It is noticed that there are a disproportionate amount of Offenses in the second portion, including sections 14-16, as opposed to the first portion, including sections 5-13.

Enforcement of the Computer-related Offense Act of 2007 has been noted in some provisions below.

(1)  Applying section 14 against the defamation

Since the Computer-related Offense Act of 2007 has come into effective, section 14, especially 14(1), has been applied on prosecution to people involved in lawsuit at most. Section 14 of the Computer-related Offense Act of 2007 states that “A person who commits any of the following offenses shall be subject to imprisonment for a term not exceeding five years or to a fine not exceeding one hundred thousand baht or to both:

(1) Importation into a computer system any forged computer data, in whole or in part, in a manner that is likely to cause damage to any person or the public”

A lot of defamation cases have been used as a political tool for several years. For example, politicians will press charges against each other. Nevertheless, by using and interpreting legal code for the offense of defamation case even it occurs in online media, we can apply the existing Civil and Commercial Code section 423⁴⁰ related to the infraction by defamation or Penal Code section 326 and 328 together with. There is no more need to apply any provision from the Computer-related Offense Act of 2007. But, in fact, we have found that many defamation online cases were litigated as computer crime cases too. The people involved allege the Offense under Civil or Penal Code attached to section 14(1) the

⁴⁰<ประมวลกฎหมายแพ่งและพาณิชย์> <มาตรา 423> [<The Civil and Commercial Code> <§ 423>] B.E. 2535. “A person who, contrary to the truth, asserts or circulates as a fact that which injurious to the reputation or the credit of another or his earnings or prosperity in any other manner, shall compensate the other for any damage arising therefrom, even if he does not know of its untruth, provided he ought to know it…”
Computer-related Offense Act of 2007. Even though if we interpret from the spirit of legislator with the context of section 14(1), we will find that importing untrue data into a computer system which may cause damage to the other is not relevant to the definition of defamation.

The true purpose of section 14(1) is to fill the gap of Penal Code in covering “counterfeit documents” or making “false documents.” At first, the term “document” means only “any paper or other objects with take shape and tangible.” Thus, the Penal Code cannot be interpreted to cover the counterfeiting of electronic data which really caused a gap in the law. So, the meaning of section 14(1) doesn’t mean importation to a computer system with the content that may cause any person dishonor, disrespect, or detested which composed of the similar component with the offense of “defamation” under Civil or Penal Code. The section 14(1) does not comport with aspects of the defamation law under the civil or Penal Code but, it is rather likely means the “importation [of unreal, forged data] to [a] computer system made by a “person who is not in authority to make it,” which should be the same meaning as the offense of “counterfeit document” under Penal Code.

The interpretation of section 14(1) into a section dealing with the offense of defamation not only causes a legal error, but also a duplication of the law. This would bring the confusion to both accused person and public.

For instance, most of the cases in 2013 were under defamation and because the messages were published online, there was prosecution under section 14(1) for the dissemination of false messages or “illegal” messages applied together. This result is probably because the Computer-related Offense Act of 2007 provides more severe penalties than the offense of defamation under Penal Code does.

41 <ประมวลกฎหมายอาญา> <มาตรา 1 (7)> [Penal Code § 1 (7)] B.E. 2499. “Document means any paper or other material for expressing the meaning by letters, figures, plan or an other design, whether it be by way of printing, photographing or any other means, which is evidence of such meaning”

42 Sawatree Sukshi, อาชญากรรมคอมพิวเตอร์?: แนวปฏิบัติวัตถุ ผลการทบทวนพระราชบัญญัติการกระทําความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐเกี่ยวกับสิทธิเสรีภาพในการแสดงความคิดเห็น, 82-83 (2012).

43 <ประมวลกฎหมายอาญา> <มาตรา 326> [Penal Code § 326] B.E. 2499. The defamation under the section 326 of Penal Code is subject to imprisonment for a term not exceeding one year or to a fine not exceeding twenty thousand baht or to both, while the defamation under the Computer-related Offense Act determines the imprisonment for a term not exceeding one year or to a fine not exceeding one hundred thousand baht or to both.
Moreover, government officers often intimidate internet users with repeated news stories related to the so-called offenses on computer systems. For example, the Minister of ICT\(^{44}\) stated that clicking the “like” or “share” button might be considered as illegal conduct similar to downloading pirated file. This clicking might be charged under the Computer-related Offense Act of 2007. It is noticeable that these conducts cannot be charged under the Computer-related Offense Act because it contains no provision authorizing the power to do so\(^{45}\).

(2) Internet Service Provider’s liability under the section 15

Because the internet relies on “intermediaries” to connect and display the data. The announcement of the Ministry of ICT in “The Computer Traffic Data Preservation of Internet Service Provider”\(^{46}\) categorized ISP types, but not for the purposes of liability. The definitions of “Internet Service Provider” under the Computer-related Offense Act of 2007 and the announcement of the Ministry of ICT are too broad and cover many kinds of service providers, regardless of the duties and responsibilities of Internet Service Provider as appeared in section 15.

A. Types of Internet Service Provider

The Ministerial Regulation of the Ministry of ICT – The Computer Traffic Data Preservation of Internet Service Provider has categorized the types of ISPs as follows:

- “Basic Telecommunication Service Provider” is the Telecommunication and Broadcast Carrier such as Telephone Organization of Thailand (TOT) and Mobile Service Provider (AIS, DTAC, True) etc.

- “Access Service Provider” is the internet connection service providers. Their duty is to supply gateway to connect computer to internet network. So Access Service Provider includes both ISP and companies, schools, universities or most of private and public organizations.

\(^{44}\) ติดต่อให้ระวังกล้อค แชร์ปลุกระดมการเมือง, Dailynews online, http://m.dailynews.co.th/News.do?contentId=73009 (Last visited Sep 5, 2015)

\(^{45}\) Thai Netizen’s Report 2013, Thai Netizen Network, 32 (2014)

\(^{46}\) [ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ ฯ 2550]

[<The Ministry of information and communication technology’s Regulation on Criteria for the Computer Traffic Data Preservation for Internet Service Provider >] B.E. 2550
“Host Service Provider or various applications rental business” Ex. Web Hosting

“Internet Station-Service Provider” Ex. Internet Café

Requiring the above service providers to a commit to liability under section 15 of the Computer-related Offense Act of 2007 regarding the dissemination of illegal data by internet users is unreasonable. These ISPs assume too much responsibility in providing the observation or prevention of offenses, which is difficult to technically prove for intermediary Service Provider in data transmission (Mere Conduit). In other words, Service Providers should not take any liabilities for the data they have passed in their telecommunication networks’ accessibility or temporary storage during the automatic transmission process.

B. Liability in Computer Traffic Data Storage

Section 26 of the Computer-related Offense Act of 2007 on Traffic Data Preservation:

“A service provider shall have to store computer traffic data for a term not less than ninety days after the date that such data is transmitted into its computer system. When it becomes necessary, a competent authority shall order a service provider, on a case-by-case basis, to store such data for a term exceeding ninety days, but the entire duration shall not exceed one year.

As from the beginning of a service utilized by a user until not exceeding ninety days after the service terminated, a service provider shall have to store any user’s data which is necessary to identify such user.

The provision prescribed in the first paragraph shall only be applied to a category of service provider and in a time frame required by a declaration of the minister as published in the Government Gazette.

47 Id.
A service provider, who does not comply with the provision in this Section, shall be subject to a fine not exceeding five hundred thousand baht.\(^{48}\)

This provision states that service providers must have reserved computer traffic data for at least 90 days after the date that the data is accessed by a given computer system. Because the prosecution process under this Computer Crime Act normally takes time and data to investigate the source, including some valuable evidences, in order to confirm the allegation of accused person.

(3) **Internet Service Provider’s penalty**

Section 15 of the Computer-related Offense Act of 2007 set the penalties for ISPs who are willingly to support or consent to an offense under section 14 within a computer system under their control. The penalty for ISPs shall be the same penalty as if a person committed the offense.

As the prosecution under the Computer-related Offense Act of 2007 pursues the Criminal proceedings, to prove intention of ISP whether they willingly support or consent to an offense within computer system under their control. ISPs are subject to the same criminal investigation or proceedings in order to prove their intent under the Act. They must be subject to the provisions under Penal Code and Criminal Procedure Code since there is no specification in the Computer-related Offense Act of 2007. At the trial level, strategies for proving intent include various pieces of evidence. In the case of refusal by ISP, considerations include following the competent authority’s order to remove or delete illegal data out of the computer system.

Ambiguity in section 14 and section 15 can even lead ISPs to arrests for violations of competent authority’s orders. The first prosecution in Thailand concerned intermediary surveillance. The Director of Prachatai online newspapers\(^ {49}\) was charged with allegedly

\(^{48}\)咚ThanOrEqualToบัญญัติการกระทําผิดเกี่ยวกับคอมพิวเตอร์ ๒๖ ประมวลกฎหมายว่าด้วยการกระทําผิดเกี่ยวกับคอมพิวเตอร์ <มาตรา ๒๖> [The Computer-related Offense Act §26] B.E. 2550.

\(^{49}\) The main content of Prachatai online newspapers focus on news from and commentary on NGOs, social movements, and human rights issues, the website became an alternative source for social and political news.
violating section 15 and section 14(3) of the Computer-related Offense Act of 2007 through intentionally support or consent to leave comments deemed offensive to monarchy (section 112 of Penal Code) on Prachatai webboard in 2012. The court found her guilty and she was sentenced to one year in prison and a 30,000 baht fine. Because of her cooperation with the court and the fact that this was her first offense, her sentence was immediately reduced to a suspended sentence of eight months and a 20,000 baht fine.

Throughout this case, defining what kinds of acts or commitments can be deemed as “intentional support of consent” was of crucial importance in determining the ISP’s liability under sections 14 and 15 of the Computer-related Offense Act of 2007. Especially when considering a specifically appropriate length of time for questionable comments must be removed. The verdict stated that the defendant removed nine out of ten alleged lèse-majesté comments within one to eleven days. It showed that the Director of Prachatai did not intentionally support of consent to leave those removed comments. But, the tenth comment was suspended on the web board for twenty days before it was removed. The court adjudicated that this conduct was “tacit consent”. For that reason, the court judged that the Director of Prachatai was convicted for violating the Computer-related Offense Act of 2007.

1.4 The Impact of Computer-related Offense Act of 2007

Since the Computer-related Offense Act of 2007 has come into effect, the overview of impact from law enforcement can be concluded as follows:

(1) **Blocking websites has become a legal issue**

At first, blocking websites could not be done because there were no applicable regulations. But, now that the Computer-related Offense Act of 2007 can into effect, it has brought rapid blocking of illegal content on the internet by court order under section 20. It is noticeable that this computer-related offense Act applies more to managing “content” in online media than solving computer-related crime under section 5 to 13, which was the initial intention of the Act\(^5\).

---

\(^5\) Sawatree Sukri, อาชญากรรมคอมพิวเตอร์?: อนาคตทางกฎหมายระบายปัญญาภูมิพลอดิเรก การกระทําความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐบาลเพื่อรักษาสิทธิในอิสระในการแสดงความคิดเห็น, 90 (2012).
The rationale for blocking websites can be described via ranking:\(^{51}\):

1. The content and photograph that insults or defames the King, the Queen, the Heir-apparent, or the Regent (79% of all blocked URL);
2. The obscene content and pornography (19% of all blocked URL);
3. The other reasons (2% of all blocked URL)

Even the Computer-related Offense Act of 2007 gives officers, who have been nominated by the Minister of ICT,\(^{52}\) the authority to block websites. Real computer-related crimes were rarely found go against the conflict and political change after 2007 which brought to more strictly enforce the Computer-related Offense Act of 2007 on national security cases.

(2) Intermediary Surveillance

The Computer-related Offense Act of 2007 requires ISPs to comply with “Intermediary Liability” in a similar way as the offender. As a result, ISPs are likely to pay more attention to their contents online so as not to break the law. Starting from identification of users’ sign-up and sign-in processes which could be different depending on each website and application’s terms & conditions, such as, the authentication for log-in by username and password or authentication for subscription by email, ID number or name & address and so on.

The Computer-related Offense Act of 2007 also resulted in the creation of new regulatory measures to internet surveillance.\(^{53}\)

- ISPs must store computer traffic data for at least 90 days after the date that the data is accessed by computer system;
- ISPs must provide identification and verification for the users and institution’s server level including member of webboard level

---

\(^{51}\) Pirongrong Ramasoota, การกํากับดูแลเนื้อหาอินเทอร์เน็ต, 291 (2013).

\(^{52}\) In nomination the officer under this Act, the Minister of ICT nominates persons who have knowledges and skills of computer system and meet qualifications imposed by the Minister of ICT. พระราชบัญญัติว่าด้วยการกระทําผิดเกี่ยวกับคอมพิวเตอร์ (มาตรา 28)  B.E. 2550.

\(^{53}\) Id. at § 26.
- ISPs must provide efficient content filtering of their websites;

- ISPs need to keep an eye on illegal comments at all the times.

(3) Censorship and Surveillance of Data Service Provider

ISP have launched various measures relating to internet data surveillance since the Computer-related Offense Act of 2007 has come into effect and in consideration of the political climate at that time. Obviously, the censorship by ISP as section 15 stipulates, ISPs shall be subject to the same penalty as internet users if they allow offenses under the Act to occur on their website. The censorship of websites is to protect the ISPs themselves first.

Instead of first filing a petitions to the court in order to block websites, the government required cooperation from ISPs to restrain the dissemination of “inappropriate” content, which some may not have qualified as an illegal websites to begin with. The ways by which the government and these ISPs coordinated the blocking of websites were found in formal issues, such as official letters and officially electronic mails that failed to identify what is the exactly of the illegal message.

1.5 Overview and Suggestion from Enforcement of the Computer-related Offense Act of 2007

Since the Computer-related Offense Act of 2007 has come into effect, government officers have been given the authority to block websites, but only by subpoena. Apart from legal measures, the government also has another issue regarding ISPs’ cooperation which is not truly conducive to freedom of data acknowledgement and freedom of speech. However, several State projects have been opposed by the public to such an extent that, the ICT Ministry was forced to cancel certain projects. For instance, there was the concept of installing program that used to capture data being transmitted on a network (sniffer) by ICT Ministry. Internet users and ISPs gathered the group called “Thailand No Sniffer” on

54 Id. at § 20. “…a competent authority, by approval of the Minister, shall file an application to the court within its jurisdiction along with relevant evidence in order to obtain a court order to cease the dissemination of such computer data…”

55 Pirongrong Ramasoota, การกํากับดูแลเนื้อหาอินเทอร์เน็ต, 300 (2013).


57 Id. at 239.
Twitter and Facebook in order to retaliate against prohibition of express by using the ‘Comment’ or ‘Like’ functions on Facebook. The group retaliated by releasing the campaign ‘Press Like is not a Crime,’ which was run by Thai Netizen Network (TNN)\textsuperscript{58}. Therefore, ICT was forced to terminate these projects.

In addition, this act also resulted in changes to the computer traffic data provided to the government. The Act allows ISPs to refuse reference to “Personal Information” of their clients. The Computer-related Offense Act of 2007 stipulates ISPs must store computer traffic data which might be useful in the investigation of the potential offenses and provide it to competent officers. Failure to provide said data would result in their own violations under the Act.

However, the Computer-related Offense Act of 2007 causes ISPs, especially in webmaster and administrative roles, to adjust practices within organization, such as filtering users’ contents before it is published online. ISPs must now require users to register before posting content, or potentially add more personnel and tools to review and monitor the messages.

This notice from the Computer-related Offense Act of 2007 effects ISPs as follows:

1. The interpretation of section 15 which requires ISPs who “intentionally support or consent” to disseminating offense-related messages (under section 14) must be subject to the same penalty as a person who post the same messages. This truly makes ISPs worried because they are unconfident in what are the government’s criteria to prove “intentional support or consent” by an ISP in dissemination illegal content.

2. There is a problem in the cooperation between ISPs and the government with regard to the blocking of websites. Even though ISPs take it seriously and act quickly, the informed data is sometimes unclear. It brings ISPs into trouble and exposes them to potential prosecution.

3. When the Computer-related Offense Act of 2007 has imposed a punishment on an intermediary, the government officers emphasize prosecution of ISP in order to find someone responsible for an offense more than finding a real wrongdoer. This lends too much burden on ISPs in terms of budget, personnel, and liability risk. It might not be a big deal for

\textsuperscript{58} Id. at 239.
large media, but it is for kinds of user-generated content and small websites. The result is self-censorship or some other means to avoid a lawsuit, which includes moving server out of the country.

(4) If government needs ISPs to be responsible for their content, classification of liability should be clearer than it is now. The government should realize that some ISPs are just “an intermediary” in transmitting content. They should not have any duties in monitoring directly.

The Computer-related Offense Act of 2007 has been criticized very often because the act should be a criminal law which regulates only an offense and penalty for crimes against computer systems or computer data, such as data theft. However, the Act is more applied in national security offenses than computer crime offenses. It also creates ISP liability which is too wide by subjecting them to the “equal” penalties of the wrongdoer. This broad liability window results in self-censorship of ISPs. Moreover, the interpretation of section 14(1) for use with defamation online is against spirit of law. That is why amendment of this act must be made. The Act currently is in the consideration of legislative process. Some suggested draft amendment could be described as follows:

- Amend section 14(1) to manage and punish fraud, such as the creation of websites that deceive internet users (Phishing) and the use of forged files to disguise themselves in order to destroy computer systems. But the defamation online should be removed.

- Since the Computer-related Offense Act of 2007 did not make mention of pornography involving people under the age of 18 years, an amendment of this act will specify an offense for any person who possesses child pornography in computer data.

- ISP liability was not mentioned in the petition and should to be amended from the Computer-related Offense Act of 2007 completely.

2. Liability of Intermediary Service Providers relating to Child Protection in Thailand

Although Thailand has ratified in the Convention on the Rights of the Child of UN, but regulations related to child pornography in Thailand as it appears in section 34 (C) that:
“States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent:

(c) The exploitative use of children in pornographic performances and materials".59

Thailand still has not applied any regulation relating to child pornography as appear under the Convention on the Rights of the Child, while the issues of child pornography on internet or media have been continuously increasing.

Apart from child pornography, there are other issues about the dangers of inappropriate internet use by children. The technology surveillance center (IT Watch) has estimated technology disaster that threaten Thai children in 200860.

1. Conversations through internet (Chat Line) are often published in many cases. The offender uses chat program to seduce children into sexual abuse by using deceitful means, such as giving expensive gifts and tempting the child to have sexual intercourse with them. This conduct can continue between the offender and the child for a while until the child trusts the offender.

2. Contact through social networks such as the most popular one, ‘Facebook’. The frightening threat is that some people would abuse Facebook as a sexual conduct.

The research in 2009 found that more than half of parents (71.8 %) have never informed themselves about how to prevent improper internet usage by their children and remain behind their children in internet understanding61.

2.1 The law related to children, obscene media, and internet in Thailand

In general, there are several laws related to children, obscene media, and internet in Thailand:

59 Convention on the Rights of the Child § 34. 1990
61 Id. at 229.
- Penal Code
- Computer-related Offense Act of 2007
- Child Protection Act of 1999

The details are as below:

(1) **Penal Code**

A provision on pornography appeared in offenses relating to sexuality in section 287:

“Whoever

(1) for the purpose of trade or by trade, for public distribution or exhibition, makes, produces, possesses, brings or causes to be brought into the Kingdom, sends or causes to be sent out of the Kingdom, takes away or causes to be taken away, or circulates by any means whatever, any document, drawing print, painting, printed matter, picture, poster, symbol, photograph, cinematograph film, noise tape or any other thing which is obscene,

(2) carries on trade, or take part or participates in the trade concerning the aforesaid obscene material or thing, or distributes or exhibits to the public, or hires out such material or thing,

(3) in order to assist the circulation or trading of the aforesaid obscene material or thing, propagates or spreads the news by any means whatever that there is a person committing the act which is an Offense according to this Section, or propagates or spread the news that the aforesaid obscene material or thing may be obtained from any person or by any means

Imprisonment not exceeding three years or fine not exceeding six thousand baht, or both.62

---

This section shows that the liability of pornography under Penal Code includes all types of adult and child pornography. There are not any provisions prohibiting the trade, dissemination, or possession of child pornography explicitly. Therefore, there are not any provisions individually specifying the penalties of offenses relating to child pornography.

The lack of provisions pertaining to child pornography offenses has been discussed and it has been proposed for addition to the Penal Code by amendment for more than ten years. As recently as May of 2015, the General Assembly approved a draft amendment to the Penal Code, which prescribed child pornography as a specific offense. This legislation has been awaiting the King’s signature before announced on the Government Gazette.\(^{63}\)

The contents of proposed amendment related to child pornography in Penal Code are as follows:

Section 287/1

“Whoever, for the purpose of sexual exploitation for themselves or others, possesses child pornography shall be punished with imprisonment not exceeding 5 years and fined not exceeding 100,000 baht, or both

In order to distribute child pornography to the others, shall be punished with imprisonment not exceeding 7 years and fined not exceeding 140,000 baht, or both.\(^{64}\)

Section 287/2

“Whoever

(1) For the purpose of trade or by trade, for public distribution or exhibition, makes, produces, possesses, brings or causes to be brought into the Kingdom, sends or causes to be sent out of the Kingdom, take away or causes to be taken away, or circulates by any means of any child pornography,

---

\(^{63}\) Information on 1 September 2015

(2) Carries on trade, or takes part or participates in the trade concerning the aforesaid child pornography, or distributes or exhibits to the public, or hires out such materials or things

(3) In order to assist in the circulation or trading of the aforesaid child pornography, propagates or spreads the news by any means whatever there is a person committing the act which is an offense according to this section,

Shall be punished with imprisonment from 3-10 years and fined from 60,000-200,000 baht.  

As a result, the person who commits or participates in the offense related to child pornography is deemed to take liability according to the proposed amendment of Penal Code. However, the amendment awaits an announcement and the King’s signature in order to go into effect. There is no clearly defined period until now.

(2) Computer-related Offense Act of 2007

The provisions of the Computer-related Offense Act of 2007 relating to the offense against dissemination obscene data,

“A person who commits any of the following offenses shall be subject to imprisonment for a term not exceeding five years or to a fine not exceeding one hundred thousand baht or to both...

(4) importation into a computer system any computer data which is considered obscene, and such computer data is accessible by the public.  

Though the offense of disseminating pornographic images has already appeared in Penal Code section 287, the drafting committee of the Computer-related Offense Act of 2007

---

65 Id. at § 287/2.
66 พระราชบัญญัติว่าด้วยการกระทําผิดเกี่ยวกับคอมพิวเตอร์ มาตรา 14}
suggested that this matter should be more clearly specified in computer-relate law\textsuperscript{67} in order to avoid confusion when interpreting, section 14(4). The intention of this section of 14(4) is to punish the person who imports obscene data into computer systems accessible by public, for instance, posting child and adult pornography on various web board forums.

There are two Acts controlling obscene media in Thailand. Section 287\textsuperscript{68} under Penal Code prohibits the production, the possession, the distribution, the exhibition and the trade of obscene media, while section 14(4)\textsuperscript{69} of the Computer-related Offense Act of 2007 prohibits the importation of obscene data into computer systems which are accessible by the public. The Supreme Court reasoned that the necessity to control obscene media is to maintain good morals and prevent sexual offenses, especially rape.\textsuperscript{70}

The results of enforcing these two laws (Penal Code and the Computer-related Offense Act of 2007) can make the offenders subject to the penalties. Nonetheless, without clearly classifying obscene media in any Thai laws, it brings to

1. Rate of penalty for the offenders in child pornography is the same as common obscene media.

2. The person who possesses child pornography has no liability at all.

The basic idea of obscene media in Thailand is totally different from international ideas, which aim to control child pornography, but not adult pornography. Because Thailand does not aim to regulate the “material or thing” but rather the “the behavior of the owners of the pornography” If their behavior is to possess not to distribute or to sell to another person whether it is an adult pornography or child pornography, it is considered as a lawful act. But, if their behavior is to distribute or to sell, it is definitely an unlawful act, whether it is under

\textsuperscript{67}รายงานการประชุมคณะกรรมาธิการวิสามัญเพื่อพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทําความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ....ครั้งที่ 9/2550 วันที่ 10 กุมภาพันธ์ 2550> [Report of the committee relating to the draft Computer-related Offense Act B.E..., No. 9/2550] B.E. 2550

\textsuperscript{68}ประมวลกฎหมายอาญา [Penal Code] § 287 B.E. 2499

\textsuperscript{69}พระราชบัญญัติว่าด้วยการกระทําผิดเกี่ยวกับคอมพิวเตอร์ [The Computer-related Offense Act] § 14 (4) B.E. 2550.

\textsuperscript{70}The Supreme Court of Justice <2136/2531> ; <The Supreme Court f Justice> <9634/2542> <1999>.
section 287 of Penal Code\textsuperscript{71} or under the Computer-related Offense Act of 2007\textsuperscript{72}. It is seen that Thai law does not classify “material or thing” between child and adult of obscene media.

“The Service Provider” according to the Computer-related Offense Act of 2007 related to obscene media still refers to the same term “Service Provider” under section 3\textsuperscript{73}. It also includes Service Provider as defined in ICT Ministry’s regulation, ‘The Computer Traffic Data Preservation of Internet Service Provider.’ ISPs who are aware that there is obscene material on a computer system under their control and still ignore or refuse to delete it shall be punished with imprisonment not exceeding five years or fined not exceeding 100,000 baht, or both\textsuperscript{74}.

However, section 14(4) has mostly been applied in cases requiring a court order to block websites and interestingly enough, all those cases are the result of confession. These lawsuits were initiated by both government officers and by the victims whose images were published online. The allegations in these lawsuits regularly apply section 14(4) in conjunction with section 287 of Penal Code\textsuperscript{75}.

(3)\textsuperscript{76} Child Protection Act of 2003

The Child Protection Act of 2003 aims to protect the children’s right to be raised well, to be taught well and to develop appropriately, which is encouraging the stability of family. The definition of “child” in this act is “a person who is under 18 years of age but does not include those who have attained majority through marriage.”

\textsuperscript{71} \langle ประมวลกฎหมายอาญา \rangle \langle มาตรา 287 \rangle \langle Penal Code \rangle \langle § 287 \rangle B.E. 2499

\textsuperscript{72} \langle พระราชบัญญัติว่าด้วยการกระทําผิดเกี่ยวกับคอมพิวเตอร์ \rangle \langle มาตรา 14 (4) \rangle \langle The Computer-related Offense Act \rangle \langle § 14 (4) \rangle B.E. 2550.

\textsuperscript{73} Id. at § 3. “Service provider” means :

(1) A person who. Either under his own name or other persons’ names or for the benefits of other persons provides any person internet access service or any other services which allow persons to communicate via computer systems.

(2) A person who provides any person computer data storage service”

\textsuperscript{74} Id. at § 15. “A service provider, who intentionally provides support to or allows a commission of an offence prescribed in section 14 within a computer system under his supervision shall be subject to the same punishment as those who commit an offence prescribed in section 14”

\textsuperscript{75} \langle พระราชบัญญัติคุ้มครองเด็ก \rangle \langle มาตรา 287 \rangle \langle Penal Code \rangle \langle § 287 \rangle B.E. 2499

\textsuperscript{76} \langle พระราชบัญญัติคุ้มครองเด็ก \rangle \langle มาตรา 4 \rangle \langle The Child protection Act \rangle \langle § 4 \rangle B.E. 2546
This act also imposes a duty on parents to take care of their children appropriately from moral and ethical aspects\(^ {77}\). However, if parents fail to reach such criteria, there are no penalties for this failure.\(^ {78}\)

In the part of child and the use of online communication devices such as internet, Child Protection Act of 2003 has not specifically mentioned to the child pornography’s punishment. Only section 26(9) mentioned pornographic offenses when it details that forcing, threatening, using, encouraging, or allowing a child to perform or act in a pornographic manner, regardless of whether the intention is to obtain remuneration or anything else, shall the offender to punishment by imprisonment not exceeding three months and fines not exceeding 30,000 baht, or both\(^ {79}\). The same section also prohibits the advertising or broadcasting a child’s information with the intention of causing damage to that child or seeking benefits for oneself or others in an unlawful manner\(^ {80}\). If a person breaches this law, they shall be punished by imprisonment not exceeding six months and a fine not exceeding 60,000 baht, or both\(^ {81}\).

However, there is an announcement from National Commission for Child Protection related to the protection of personal data for children who use the internet, but it requires ISP cooperation in not disclosing personal data of internet users below the age of 18 years old that could result in others contacting that child. For instance, a child’s photograph, age, sex, telephone number, email or address are all personal data points that must not be disclosed. Such notification is just asks for cooperation, but lends no legal enforcement mechanism at all.

### 2.2 Analysis of ISP liability and Child Protection in Thailand

Despite provisions controlling the dissemination of obscene media within Penal Code and the Computer-related Offense Act of 2007, these penalties in the case of disseminating of child pornography have not been truly set. A latest amendment of Penal Code regarding child

\(^{77}\) Id. at § 23.

\(^{78}\) พระราชบัญญัติคุ้มครองเด็ก บทที่ 27 [\textit{The Child protection Act} § 27] B.E. 2546

\(^{79}\) พระราชบัญญัติคุ้มครองเด็ก บทที่ 78 [\textit{The Child protection Act} § 78] B.E. 2546

\(^{80}\) Id. at § 27.

\(^{81}\) Id. at § 79.
pornography has improved child protection in Thailand to be more accordance with the
Convention on the Rights of the Child.\footnote{82}

The specification of penalties for child pornography under Penal Code results in the
case of possession, trade, or disseminate child pornography of persons under 18 years of age
be subject to imprisonment and fine penalties. At the beginning, the liability of a child
pornographer under Penal Code would apply to the offender only and not include ISP liability
in any way.

Nevertheless, liability and duties for ISPs can develop when victims alleged failures
under the Computer-related Offense Act of 2007. This act requires ISPs to “watch” the data
delineated in section 14, which includes obscene data. If ISPs leave or ignore such data
visible in a computer system, they might become liable for their “intentional support or
consent” of an offense prohibited in section 14. Moreover, when considering the Computer-
related Offense Act of 2007, we found that ISPs shall have to store computer traffic data for a
term not less than 90 days after the date that such data is imported or transmitted into their
computer system. ISPs also need to keep their users’ necessary data in order to identify
internet users from the beginning of their usage and store data for no less than 90 days after
the completion of their usage. However, there are not any provisions in the Computer-related
Offense Act of 2007 that specifically relate to a duty of ISPs with regard to children. So, ISPs
need to be cautious of their liability under the Act that they share the same criminal liability
as the offender who imports obscene data, whether it is child or adult pornography into
computer system. ISPs are liable if they intentionally support or consent to obscene data of
their users by ignoring, deleting, or destroying such pornographic data.

Apart from that, many kinds of businesses, such as internet cafés or online gaming
cafés should not be classified as ISPs.\footnote{83} This business group deems to have a duty and

\footnote{82} Convention on the Rights of the Child § 34. 1990
undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States
Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent:
(a) The inducement or coercion of a child to engage in any unlawful sexual activity;
(b) The exploitative use of children in prostitution or other unlawful sexual practices;
(c) The exploitative use of children in pornographic performances and materials”.

\footnote{83} [ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550]
[The Ministry of information and communication technology’s Regulation on Criteria for the Computer
Traffic Data Preservation for Internet Service Provider ] B.E. 2550
liability described within the Computer-related Offense Act of 2007 as well as other larger ISPs.

Conclusion

The Computer-related Offense Act of 2007 in Thailand has not yet classified the liabilities of the people who import obscene data into a computer system, whether it is child or adult pornography. Thus, the liabilities among those offenses are not so different. The liabilities might actually include ISPs. If ISPs realize that there is obscene data in computer system under their control, but still ignore to delete said data from computer system, the ISP need to take liability as well as the offender. An amendment of the Penal Code relating to child pornography is in progress and will come into effect soon. The amendment would affect guilt onto the person who trades, disseminates, or possesses child pornography of persons under 18 years old. By the way, the punishment to the person who trades, disseminates, or possesses child pornography according to the proposed amendment will not include ISPs at all, unless an ISP is the entity that disseminates the obscene data directly. According to the amendment of Penal Code, if ISPs realizes that there is child pornography on their computer system but ignore to perform any action to delete such data out of their computer system, there are no any liabilities in terms of child pornography in anyway.

Author’s Biography

Assistant Professor Dr. Aua-aree Engchanil earned her LL.B. from Thammasat University in Thailand before receiving her LL.M. in Public Law and Ph.D. in Public

84 On 8th September 2015, the provision of child pornography under Penal Code had been announced by the government gazette, it will become effective in next 90 days after this announcement.

http://library2.parliament.go.th/giventake/content_nla2557/law86-080958-84.pdf
Finances from University of Aix-Marseille III, France. Her academic interests include public finance, rights and equality, and public health law. At Chulalongkorn University, she teaches courses in public law, for example Public Finances Law, Economic Public Law, Election Law, and Seminar on Constitutional Law. Miss Engchanil also has been appointed a legal consultant of Tobacco Control Bureau, Ministry of Public Health.