Available online at www.iseec2018.kbu.ac.th
I-SEEC 2018
Area: Social Sciences, May 2018, page 574-583
Proceeding
Social Science
www.iseec2018.kbu.ac.th
The 9th International Science, Social Science, Engineering and Energy Conference's e-Proceeding

The Application of the Computer-related Crime Act (No.2) B.E. 2560 (2017) to Protect Children in the Digital Age from Being a Victim of Cyber-grooming

Kanathip Thongraweewong[1]
Associate Professor of law, Director of Digital law Institute , Kasam Bundit University, E-mail: kanathip@yahoo.com

ABSTRACT

This paper examines cyber-grooming from a legal perspective by analyzing its process resulting in the division of behavior into three main stages: 1) assessing risk and selecting a victim, 2) building a relationship to gain trust, and 3) committing sexual activities. Consequently, the paper analyzes the application of Thai's computer crime laws to behaviors in each stage. In addition, the comparative analysis between Thai's and related foreign laws, including the U.K., the U.S., and South Africa, is conducted in each stage. The results of analysis indicate that although the newly amended Computer-related Crime Act (No.2) B.E. 2560 (2017) provides the specific section of sexual content in section 14 (4), this section has limitations in applying to cover the activities of cyber-grooming, e.g., the "publicly accessible" elements, which make this law inapplicable to sexual communication to a child through a private online chat. In contrast, several countries have enacted a specific offence relating to cyber-grooming, which can be applied to both physical and computer-related channels of communication. Consequently, the author suggests the amendment of this section to efficiently protect a child from being a victim of cyber-grooming.

Keywords: *Cyber-grooming, Online-grooming Law, Cyber Law, Child Protection Online*

1. Introduction

Cyber-grooming is described as activities involving the communication with a child to create an emotional connection to gain his or her trust for the purposes of sexual abuse. This activity expands comprehensively through the use of social media and chat applications in the digital age. It is a fact that there is no universally accepted definition of cyber-

grooming and laws relating to this crime; they vary depending on domestic law which is different in scope and element. As for Thai law, there is no specific law on cyber-grooming. The relevant law which can be applied is the Computer-related Crime Act. (The analysis of other laws in Thailand, such as the criminal code, is beyond the scope of this paper.) However, this law is not enacted exclusively for this behavior leading to the problems of application in terms of scope and element. However, several countries have enacted specific offence to cover this behavior. Thus, this paper will start with examining the general meaning of cyber-grooming. Then, related foreign laws will be discussed. Next, the paper will classify cyber-grooming into stages or steps in order to analyze the application of laws to each stage with comparative analysis to the related foreign laws.

2. General meaning and characteristics of "cyber grooming"

There is still no universally accepted term of "cyber or online-grooming." However, the term "cyber-enticement, solicitation, and online grooming" are commonly used collectively or interchangeably to describe "communications made by adults through the use of ICT's for the purpose of sexually abusing or exploiting minors" [1].

Sexual solicitation may also refer to a "request to engage in sexual activities or sexual talk or give personal sexual information that is unwanted, whether wanted or not, made by an adult" [2].

Grooming can be considered as conduct that takes place as part of cyber-enticement or prior to solicitation. It refers to a series of actions that facilitate cyber-enticement or solicitation deliberately undertaken with the aim of befriending and establishment of an emotional connection with and gaining the trust of a child in order to lower the child's inhibitions in preparation for sexual activity with the child [3].

INHOPE Association defines online-grooming as "actions deliberately undertaken with the aim of befriending and establishing an emotional connection with a child in order to lower the child's inhibitions in preparation for sexual activity with the child" [4].

Then, cyber-grooming can be generally described as a series of actions through the use of computer-related communication with the intention of sexually abusing a victim who is a minor.

3. Legal approach to criminalize cyber-grooming

From a legal perspective, there is still no universally accepted term of "cyber- or online-grooming." The element of laws is different depending on the approach of each country. This part will examine relevant foreign laws in order to make a comparative analysis to Thai laws.

U.S. Laws: In the U.S., there is no federal law regulating or criminalizing "cyber-grooming." However, several states have enacted laws to criminalize this behavior. Although the names of offence and element of such laws vary depending on the laws of each state, they cover behavior which can be generally described as "electronic solicitation or use of a computer for the purpose of luring children for sexually exploitive purposes." Examples of state laws are as follows:

Kentucky law provides offence referred to as "Unlawful use of electronic means originating or received within the Commonwealth to induce a minor to engage in sexual or other prohibited activities." The main element is "... knowingly use a communications system, including computers, computer networks, ...or any other electronic means, for the purpose of procuring or promoting the use of a minor, ... for any activity..." (Kentucky Revised Statute, Section 510.155) (activities in violation of state's law, such as engaging in sexual activities, producing child pornography, etc.).

Ohio provides offence referred to as "Importuning." The main element of this law is "... No person shall solicit a person who is less than thirteen years of age to engage in sexual activity with the offender, whether or not the offender knows the age of such person ..." (Ohio Revised Code, Section 2907.07).

Washington provides offence referred to as "Communication with a minor for immoral purposes." The main element is "... a person who communicates with a minor for immoral purposes, or a person who communicates with someone whom the person believes to be a minor for immoral purposes is guilty of a gross misdemeanor ..." (Revised Code, Section 9.68A.090).

Texas law provides offence referred to as "Online Solicitation of a minor." The main element is "A person commits an offence if the person, over the Internet, by electronic mail or text message or other electronic message service or system, or through a commercial online service, knowingly solicits a minor to meet another person, including the actor, with

the intent that the minor will engage in sexual contact, sexual intercourse, or deviate sexual intercourse with the actor or another person" (Texas Penal Code, Section 33.021).

Although the name and element of state laws come in a variety of forms, there are three common elements [5] consisting of: 1) to use a computer or similar device, 2) to contact a person whom he knows or believers to be a minor, 3) to solicit, encourage, entice, or lure him or her, 4) for the purpose of engaging in sexual activity in violation of a state laws. Consequently, "cyber-grooming" in the U.S. law can be studied by considering the common elements as mentioned.

The EU laws: According to the EU law, cyber-grooming is referred to as "solicitation of children for sexual purposes" (Article 6 of Directive 2011/92/EU). This behavior means "solicitation of children for sexual purposes" and refers to the intentional proposal, through information and communication technologies, by an adult, to meet a child who has not reached the age of majority under domestic law, for the purpose of committing sexual abuse of producing child pornography where this proposal has been followed by material acts leading to such a meeting.

The U.K. law provides the specific offence of "sexual communication with a child," stating that "A person aged 18 or over ("A") commits an offence if (a) for the purpose of obtaining sexual gratification, "A" intentionally communicates with another person ("B"), (b) the communication is sexual or is intended to encourage "B" to make (whether to "A" or to another) a communication that is sexual, and (c) "B" is under 16 and "A" does not reasonably believe that "B" is 16 or over. (Sexual Offences Act 2003, Section 15 A (1)).

In addition, this law provides a separate offence for meeting a child following sexual grooming. The element is "A person aged 18 or over ("A") commits an offence if -- (a) "A" has met or communicated with another person ("B") on one or more occasions and subsequently-- (i) "A" intentionally meets "B", (ii) "A" travels with the intention of meeting "B" in any part of the world or arranges to meet "B" in any part of the world, or (iii) "B" travels with the intention of meeting "A" in any part of the world, (b) "A" intends to do anything to or in respect of "B", during or after the meeting mentioned in paragraph (a) (i) to (iii) and in any part of the world, which if done will involve the commission by "A" of a relevant offence, (c) "B" is under 16, and (d) "A" does not reasonably believe that "B" is 16 or over (Sexual Offences Act 2003, Section 15).

South Africa has also enacted laws to explicitly cover "online-grooming" by criminalizing a person who (Article 18, Sexual Offences and Related Matters Amendment Act of 2007)

- ... commits any act with or in the presence of "B" with the intention to encourage or persuade "B"... to (i) perform a sexual act with "A" or a third person (''C'') (ii) perform an act of self-masturbation in the presence of "A" or "C" or while "A" or "C" is watching (iii) be in the presence of or watch "A" or "C" while "A" or "C" performs a sexual act or an act of self-masturbation (iv) be exposed to child pornography or pornography...

- ... arranges or facilitates a meeting or communication with "B" by any means from, to, or in any part of the world, with the intention that A will commit a sexual act with "B"

- ... having met or communicated with "B" by any means from ... with the intention of committing a sexual act with.

Contrary to foreign law which enacted specific laws on cyber-grooming, there is recently no specific offence of cyber-grooming in Thailand. The relevant law which can be applied is the **Computer-related Crime Act (No.2) B.E. 2560 (2017)** of Thailand which provides content-related offence including "pornographic content" with a broader scope covering both adult and child pornography (Section 14 (4)). Although there is no specific offence of cyber-grooming in this Act, Section 14 (4) could be a relevant offence leading to the main question whether such Section could be applied in the case of cyber-grooming, which will be discussed in the next topic.

4. A comparative analysis of applying the Computer-related Crime Act and foreign laws to "cyber-grooming"

Due to the fact that "grooming" has different meaning and scope without universally-accepted definition, several researchers studied this behavior as a process by classifying into sub-behavior or series of stages [6]. However, it is difficult to make a model for describing the process of this behavior [7], especially for online-grooming due to the high level of variance in the process [8]. In addition, the classifying of this behavior into process could have limitations due to the difficulties in defining the beginning and the end of each stage [9]. In a legal perspective, the classification of grooming into relevant stages is necessary for analyzing the application of relevant law to each stage, especially in the case of Thailand, where there is no specific law on grooming. Hence, this part of the paper will classify "cyber-

grooming" into stages and conduct an analysis of applying the Computer Crime Act to each stage.

Stage 1: The risk assessment and selection of a victim. In this stage, the perpetrator uses several factors to select a victim; for example, physical characteristics, the appearance or attractiveness [10], family situation such as living without adult supervision or family with problems such as marital discord or violence, psychological characteristics, e.g., low confidence which implies vulnerabilities [11]. In addition, the perpetrator will assess the risk for being arrested [12].

According to the Computer Crime Act, risk assessment by analyzing relevant factors is not an offence. With regard to the selection of a victim, the information searching process is not illegal provided that there is no "illegal access" of computer data. For example, searching the profile of a victim via social media, which is accessible to public or other public available data. This stage could violate the Act when the perpetrator gains access to data that need specific authorization. Comparing to foreign laws, specific offence on grooming does not have element to cover this stage.

Stage 2: Relationship building or befriending. This can be regarded as the central role in the grooming process because the perpetrator will gain trust and confidence from the victim [13] which can be accomplished by several ways in order to "befriend," e.g., as giving gifts or sharing secrets [14]. Some scholars have referred to this stage as the "exclusivity stage" [12]. However, these steps can be subdivided into "gaining access" to the child involving communication between perpetrator to victim in order to separate them from other adults or environment, e.g., offering a ride, invitation to a party, or offering drugs or alcohol [9]. However, this is not limited to physical separation but also include isolating a victim emotionally from those around them [15].

Based on the Computer Crime Act, the communication to build relationship can be divided into two types. Firstly, communication via telephone or a physical channel shall not be deemed as computer crime. Secondly, communication through computer channels could be regarded as "input data" according to Section 14. However, illegal computer data in Section 14 shall be limited to "false or fake computer data." Thus, general conversation to befriend the other may not be illegal. Despite the fact that such content is fake or false, Section 14 (1) requires that the data could potentially harm the public. Thus, building a

personal relationship between perpetrator and victim could not be deemed as causing harm to the general public.

Comparing to foreign laws, specific laws on grooming can be applied to the communication stage. However, mere relationship-related content could not be sufficient due to the element of offence in some countries that requires that content shall relate to "sexual communication," such as the law of the U.K. Under the U.S. law, the content should involve inviting to sexual activities. Similarly, South Africa law requires that grooming content should include the invitation to meet or pornography. Although Australian law is broader including "indecency content," which is not limited to sexual content, mere relationship building could not be deemed as "indecency." Furthermore, intention to have sexual activity with the victim is a critical element in foreign laws.

Stage 3: Sexual stage [12] which is evident in the escalation of physical contact in order to prepare the child for the sexual contact later. The perpetrator may start with accidental touch or other methods, such inviting the victim to play games, swim in the nude, or show pornography [14]. Some scholars have referred to this stage as "desensitizing the child to touch" [16].

According to the Computer Crime Act, this stage can be divided into two types. Firstly, the physical act of sexual exploitation such as rape or sexual assault which is irrelevant to the Computer Crime Act. Secondly, sexual activities relating to computer-related communication will be under the scope of this Act. In principle, section 14 (4) covers the input of "pornographic computer data;" hence, communicating data which is pornographic will be covered by this section. However, the main limitation of this section is that the pornography must be "publicly available," e.g., posting a video on YouTube which can be accessed by the general public but does not include posting images or video via chat applications between two persons. Thus, this Section cannot be applied to cyber-grooming, which is commonly related to the targeted victim by personal communication, e.g., the perpetrator induces a child to send his or her nude image via chat applications or private communication which is not publicly accessible.

In addition, the Computer-related Crime Act does not cover "cyber extortion" where the perpetrator coerces someone to do something online provided that the content of coercion does not relate to "false, fake, or distortive content." Thus, this law cannot be applied to the case of cyber-grooming where the perpetrator coerces a child to engage in or

demonstrate sexually related activities online, e.g., coercing a child to perform sexual activities, masturbation, or to submit them to a nude image, etc.

Comparing with foreign laws, the offence of online grooming covers the activities in this stage due to the fact that the main element of laws includes "sexual content" in the communication. This is evident in the U.S law which prohibits content inviting a child to participate in sexual activities, the U.K. law which criminalizes "sexual communication," as well as South Africa law which prohibits content inviting a child to meet with sexual purpose or content involving pornography.

5. Conclusions

Due to the fact that the definition and scope of cyber-grooming vary according to the laws of each country, this paper classifies this behavior into three stages and conducts legal analysis by comparing with foreign laws for each stage. The result of comparative analysis indicates problems relating to the application of the **Computer-related Crime Act (No.2) B.E. 2560 (2017)** to cover the whole process of cyber-grooming which comprises a series of different stages. In certain stages, Thai laws share similarities with foreign laws that cannot be applied, i.e., victim selection and risk assessment. However, in certain stages, Thai laws cannot be applied sufficiently while foreign laws can be applied. Consequently, the author suggests the amendment of this section to efficiently protect a child from being a victim of cyber-grooming by using foreign laws as a model to enact new specific offences without limitation as discussed above.

Acknowledgement

The author would like to thank Kasem Bundit University for the sponsorship of this paper in this conference.

References

[1] United Nations Office on Drugs and Crime (UNODC). (2015). **Study on the effects of new information technologies on the abuse and exploitation of children**. New York: United Nations.

[2] Ethel Quayle, Lars Lööf, Kadri Soo, and Mare Ainsaar. (2011). "Methodological issues". In: **Online behavior related to child sexual abuse**. Mare Ainsaar and Lars Lööf. Literature Report.

[3] Alisdair A. Gillespie. (2002). "Child Protection on the Internet Challenges for Criminal Law". **Child and Family Law Quarterly**. Vol. 14(4): 411-425.

[4] INHOPE Association. (2018). **Online Grooming**. Retrieved: March 25, 2018; URL: http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/online - grooming.aspx.

[5] Julie S. Stanger. (2005). "Salvaging States' Rights to Protect Children from Internet Predation: State Power to Regulate Internet Activity Under the Dormant Commerce Clause". **Birmingham Young University Law Review**. Vol. 2005(1): 190-226.

[6] Benoit Leclerc, Jean Proulx, and Eric Beauregard. (2009). "Examining the Modus Operandi of Sexual Offenders Against Children and Its Practical Implications". **Aggression and Violent Behavior**. Vol. 14(1): 5-12.

[7] Andy Williams. (2015). "Child Sexual Victimisation: Ethnographic Stories of Stranger and Acquaintance Grooming". **Journal of Sexual Aggression**. Vol. 21(1): 28–42.

[8] Helen C. Whittle, Catherine E. Hamilton-Giachritsis, and Anthony R. Beech. (2015). "A Comparison of Victim and Offender Perspectives of Grooming and Sexual Abuse". **Deviant Behavior**. Vol. 36(7): 539–564.

[9] Jamie-Lee Mooney and Suzanne Ost. (2013). "Group Localised Grooming: What Is It and What Challenges Does It Pose for Society and Law?". **Child and Family Law Quarterly**. Vol. 25(4): 1–20.

[10] Michele Elliott, Kevin Browne, and Jennifer Kilcoyne. (1995). "Child Sexual Abuse Prevention: What Offenders Tell Us". **Child Abuse and Neglect**. Vol. 19(5): 579–594.

[11] Loreen N. Olson, Joy L. Daggs, Barbara L. Ellevold, and Teddy K.K. Rogers. (2007). "Entrapping the Innocent: Toward a Theory of Child Sexual Predators' Luring Communication". **Communication Theory**. Vol. 17(3): 231–251.

[12] Jonathan Clough. (2015). **Principles of Cybercrime**. Cambridge University Press.

[13] Carla Van Dam. (2001). **Identifying Child Molesters: Preventing Child Sexual Abuse by Recognizing the Patterns of Offenders**. Binghamton, NY: The Haworth Press.

[14] Anne-Marie McAlinden. (2006). "Setting 'em up': Personal, Familial and Institutional Grooming in the Sexual Abuse of Children". **Social & Legal Studies**. Vol. 15(3): 339–362.

[15] Kenneth V. Lanning. (2010). **Child Molesters: A Behavioral Analysis for Professional Investigating the Sexual Exploitation of Children**. Fifth edition. National Center for Missing and Exploited Children.

[16] Georgia M. Winters and Elizabeth L. Jeglic. (2016). "Stages of Sexual Grooming: Recognizing Potentially Predatory Behaviors of Child Molesters". **Deviant Behavior**. Vol. 38(6): 724-733.