

มาตรการทางกฎหมายในการป้องกันอาชญากรรมคอมพิวเตอร์ในมิติของเด็กและเยาวชน

Legal Measures to Protect Juveniles Involved in Computer Crimes

อมรรัตน์ อริยะชัยประดิษฐ์ นิมหนู¹, นพดล นิมหนู²

Amornrat Ariyachaipradit Nimnool¹, Noppadon Nimnool²

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ 1) เพื่อศึกษาสภาพปัญหาอาชญากรรมคอมพิวเตอร์ในมิติของเด็กและเยาวชนในปัจจุบัน 2) เพื่อศึกษาถึงแนวคิดทฤษฎีว่าด้วยอาชญากรรมคอมพิวเตอร์ในมิติของเด็กและเยาวชน 3) เพื่อศึกษาถึงมาตรการทางกฎหมายของต่างประเทศในการป้องกันอาชญากรรมคอมพิวเตอร์ในมิติของเด็กและเยาวชน และ 4) เพื่อเสนอมาตรการทางกฎหมายในการป้องกันอาชญากรรมคอมพิวเตอร์ในมิติของเด็กและเยาวชนไทย ซึ่งวิธีการวิจัยในเรื่องนี้เป็นการศึกษาวิจัยเชิงคุณภาพ (Qualitative Research) ใช้วิธีวิเคราะห์เชิงพรรณนา (Descriptive Analysis) โดยทำการศึกษาจากแนวคิดทฤษฎีและวรรณกรรมที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ มาตรการทางกฎหมายในการป้องกันอาชญากรรมคอมพิวเตอร์ของต่างประเทศ รวมถึงการกระทำความผิดของเด็กและเยาวชนตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เพื่อวิเคราะห์หาบทสรุปและเสนอมาตรการทางกฎหมายในการป้องกันอาชญากรรมคอมพิวเตอร์ของในมิติเด็กและเยาวชนของไทย โดยการรวบรวมข้อมูลจากเอกสารต่างๆ ที่เกี่ยวข้องทั้งที่เป็นภาษาไทยและภาษาต่างประเทศ และใช้วิธีการสัมภาษณ์ (Interview) ด้วยวิธีการสัมภาษณ์แบบเชิงลึก (In-depth Interview) จากผู้ทรงคุณวุฒิ

ผลการวิจัยพบว่าแม้ประเทศไทยจะมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เป็นกฎหมายหลักในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ประกอบกับกฎหมายอื่นๆ ในการคุ้มครองเด็กและเยาวชน ทั้งยังมีการดำเนินกระบวนการพิจารณาคดีอาญาเด็กและเยาวชนเฉพาะตามพระราชบัญญัติศาลเยาวชนและครอบครัวและวิธีพิจารณาคดีเยาวชนและครอบครัว พ.ศ. 2553 ที่แตกต่างไปจากผู้ใหญ่ แต่ประเทศไทยก็ยังไม่มีความมาตรการทางกฎหมายที่เป็นรูปแบบเฉพาะในการป้องกันอาชญากรรมคอมพิวเตอร์ในมิติของเด็กและเยาวชน ทั้งนี้เกิดจาก 1) การที่กฎหมายยังบัญญัติไม่ครอบคลุมเพียงพอที่จะตีความถึงข้อมูลที่ไม่เหมาะสมสำหรับเด็กและเยาวชน 2) สภาพสังคมและเทคโนโลยีมีการเปลี่ยนแปลงรวดเร็ว ส่งผลให้กฎหมายไม่สามารถตามได้ทัน ทำให้เกิดปัญหาในการบังคับใช้กฎหมายและปัญหาในการตีความ ประกอบกับความสามารถของผู้บังคับใช้กฎหมาย ทำให้การบังคับใช้

¹ ผู้ช่วยศาสตราจารย์, คณะนิติศาสตร์ มหาวิทยาลัยมหาสารคาม

² อาจารย์ประจำ, คณะนิติศาสตร์ มหาวิทยาลัยมหาสารคาม

¹ Assistant Professor, Faculty of Law, Mahasarakham University

² Lecturer, Faculty of Law, Mahasarakham University

กฎหมายไม่สามารถที่จะแก้ปัญหาได้ 3) ปัญหาความไม่ชัดเจนและซ้ำซ้อนในเรื่องอำนาจหน้าที่ เช่น เจ้าหน้าที่ตามพระราชบัญญัติคุ้มครองเด็กจะต้องร้องขอความร่วมมือจากเจ้าหน้าที่ตำรวจเพื่อปฏิบัติงานส่งผลให้การปฏิบัติหน้าที่ของเจ้าหน้าที่เป็นไปอย่างล่าช้าและไม่มีอำนาจในการกำกับดูแลที่แท้จริง

ดังนั้น การที่หน่วยงานภาครัฐและหน่วยงานอื่นๆ ที่เกี่ยวข้อง ไม่ว่าจะเป็นครอบครัว สถาบันการศึกษา ชุมชน เด็กและเยาวชน ต่างร่วมมือกันในการกำกับดูแลการเข้าถึงข้อมูลทางคอมพิวเตอร์ (self – regulation) ร่วมกัน ไม่ว่าการจัดระดับความเหมาะสมของข้อมูล การกำหนดห้ามข้อมูลที่ไม่เหมาะสมต่างๆ โดยมีการจัดอบรมให้ความรู้ทางกฎหมายอาชญากรรมคอมพิวเตอร์ และจัดตั้งหน่วยงานเฉพาะด้านในการป้องกันอาชญากรรมคอมพิวเตอร์ในมิติของเด็กและเยาวชน รวมถึงการกำหนดบทลงโทษในทางกฎหมายให้ครอบคลุมไปถึงผู้ปกครองที่ปล่อยปละละเลยเด็กและเยาวชนด้วย นับว่าเป็นมาตรการทางกฎหมายที่มีประสิทธิภาพในการป้องกันปัญหาดังกล่าวที่อาจเกิดขึ้น

คำสำคัญ : อาชญากรรมคอมพิวเตอร์, เด็ก, เยาวชน

Abstract

This research aimed to study 1) the current problems related to juvenile computer crime 2) the theory of juvenile computer crime 3) an evaluation of the laws of comparable countries and their solutions for juvenile computer crime 4) recommendations to resolve problems related to juvenile computer crime in Thailand. This research is qualitative research employing descriptive analysis for data analysis. The researcher conducted literature reviews pertaining to computer crime, measurements for dealing with computer crime from different countries, and the juvenile delinquency rate according to the Thai Cyber Crime Act B.E.2550. This research seeks to conclude and propose a legal measurement for addressing the problems of juvenile computer crime in Thailand. Data were collected through a review of related literatures both in Thai and foreign languages and also through in-depth interviews of experts.

The research found that Thailand has a number of laws that should enable the country to adequately address the problem of juvenile computer crime Those laws include the Thai Cyber Crime Act B.E. 2550, the Juvenile and Family Court, the Juvenile and Family Case Procedure Act, B.E. 2553, and other related laws aimed at protecting juveniles in computer crime. Thailand remains without a legal model for dealing with juvenile computer crimes. This is a problem at three levels 1) the content of related laws not being comprehensive enough to reasonably interpret the terms of “unsuitable information from juvenile” 2) the dramatically changing social and technological environment in concert with the limited capacity of law enforcers significantly inhibit effective law enforcement and legal interpretation for addressing the problem of juvenile computer crimes in an effective manner. 3) the ambiguity and the complexity of authority of the various related officials, for example, even though officials are already empowered by the juvenile computer crime laws, they still have to ask for cooperation from the police before exercising their power. This implies

that the officials lack exclusive power, which considerably constrains them. Therefore, the relevant organizations including governmental authorities and other related organizations such as the family, the educational institution, community, and the juvenile should collaborate for self-regulation. This encompasses an information control method, dissemination about the knowledge of computer crime laws, establishing an authority specifically for juvenile computer crime control. Also, the role of parents or custodians to prevent juvenile computer crime control should be considered by law makers.

Keywords : Computer Crime, Child, Juvenile

บทนำ

อาชญากรรมนั้นนับเป็นประเด็นสำคัญที่ก่อให้เกิดปัญหาในสังคมและเศรษฐกิจของประเทศ ก่อให้เกิดความหวาดกลัว และมีผลกระทบต่อการดำเนินชีวิตประจำวัน สถานที่สาธารณะขาดความปลอดภัยและทำให้สภาพสังคมโดยทั่วไปขาดความสงบสุข โดยเฉพาะอย่างยิ่งในปัจจุบันอาชญากรรมได้มีการพัฒนาควบคู่ไปกับความเจริญของสังคมและเทคโนโลยี กล่าวคือสังคมยังมีความเจริญมากเท่าใด อาชญากรรมก็จะเจริญเติบโตมากขึ้นเป็นเงาตามตัว ซึ่งสิ่งที่ไม่อาจหลีกเลี่ยงได้ ในปัจจุบันมีแนวโน้มของความรุนแรงของอาชญากรรมมากขึ้นและสลับซับซ้อนมากขึ้นตามความเจริญของเทคโนโลยีและความทันสมัยของการสื่อสารแขนงต่าง ๆ โดยเฉพาะเทคโนโลยีทางคอมพิวเตอร์และอินเทอร์เน็ตได้ก่อให้เกิดความเปลี่ยนแปลงอย่างมากในการดำรงชีวิตของมนุษย์ ทำให้บางครั้งกฎหมายและกระบวนการทางสังคมไม่สามารถปรับตัวให้ทันกับความเปลี่ยนแปลงที่เกิดขึ้น

ด้วยพัฒนาการในข้างต้น จึงทำให้เกิดรูปแบบใหม่ของอาชญากรรมที่เกิดจากการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำผิด ทำให้แต่ละรัฐจำเป็นต้องมีการพัฒนา กฎหมายอาชญากรรมทางคอมพิวเตอร์ (Computer Crime Law) ขึ้น บางรัฐ เรียกว่ากฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางมิชอบ (Computer Misuse

Law) หรือในบางรัฐก็มีการปรับปรุงแก้ไขประมวลกฎหมายอาญาเพื่อให้รองรับกับความผิดในรูปแบบใหม่ๆ ด้วยการกำหนดฐานความผิดและบทลงโทษสำหรับการก่ออาชญากรรมคอมพิวเตอร์ขึ้นเพื่อให้เหมาะสมและมีประสิทธิภาพ

สำหรับในมิติของเด็กและเยาวชนนั้น ก็ยิ่งจะเริ่มเรียนรู้เทคโนโลยีเร็วขึ้นเรื่อย ๆ ซึ่งข้อมูลทางคอมพิวเตอร์และอินเทอร์เน็ต มีทั้งที่เป็นประโยชน์เป็นแหล่งเรียนรู้และศึกษาค้นคว้าที่สำคัญ แต่ในขณะเดียวกันก็เป็นแหล่งรวมข้อมูลที่ไม่เหมาะสมต่างๆ มากมาย ไม่ว่าจะเป็นข้อมูลที่ผิดกฎหมายอย่างชัดเจน เช่น ภาพลามกอนาจาร ข้อความหมิ่นประมาท หรือการละเมิดลิขสิทธิ์ หรืออาจจะเป็นข้อมูลที่ไม่เหมาะสมในด้านต่างๆ เช่น ภาพที่สื่อไปในทางลามก อนาจาร การกระทำที่ก้าวร้าวรุนแรง การเผยแพร่วิธีการทำระเบิด การสอนวิธีฆ่าตัวตาย ฯลฯ เป็นต้น ซึ่งข้อมูลเหล่านี้ล้วนแล้วแต่เป็นข้อมูลที่ไม่เหมาะสมสำหรับเด็กที่จะรับรู้ทั้งสิ้น ดังนั้น การจำกัดการเข้าถึงข้อมูลเช่นนี้ เป็นแนวทางหนึ่งที่จะลดการเกิดอาชญากรรมคอมพิวเตอร์ในมิติของเด็กและเยาวชนได้ ซึ่งขณะนี้ประเทศไทยยังไม่มีกฎหมายที่มีความครอบคลุมเพียงพอที่จะควบคุมการเข้าถึงหรือรับรู้ข้อมูลเหล่านี้ของเด็กและเยาวชน ทำให้เด็กและเยาวชนได้รับผลกระทบจากข้อมูลที่ไม่เหมาะสมนี้ทั้งทางด้านการพัฒนาการรวมถึงพฤติกรรม และโดยเฉพาะอย่างยิ่งเด็กและเยาวชนนั้นถือเป็นกลุ่มบุคคลที่อ่อนด้วย

ประสบการณ์ ความรู้สึกผิดชอบชั่วดีต่าง ๆ และขาดความรู้เท่าทันในด้านต่าง ๆ ทำให้มักปรากฏข่าวเกี่ยวกับความประพฤติของเด็กและเยาวชนในทางที่เสียหาย ไม่สมควรและผิดกฎหมายอยู่เสมอ

จึงกล่าวได้ว่า ปัจจุบันเด็กและเยาวชนมีแนวโน้มในการกระทำความผิดทางอาญา รวมไปถึงตกเป็นเหยื่อจากการกระทำความผิดอาญาจากอาชญากรรมประเภทนี้มากขึ้น ซึ่งเป็นเรื่องยากที่จะค้นหาตัวผู้กระทำผิด และยากต่อการที่จะป้องกันและแก้ไข ประกอบกับเรื่องสิทธิและเสรีภาพเป็นหลักสากลของโลกที่ต้องเป็นหลักประกันให้แก่เด็กและเยาวชน การคุ้มครองสิทธิของเด็กและเยาวชนในประเทศไทยจึงเป็นมาตรฐานสากลมากขึ้น จนบางครั้งอาจมองว่าเป็นการคุ้มครองสิทธิเสรีภาพเกินควร จนลืมนึกถึงการควบคุมอาชญากรรม (Crime Control) ไป ปัญหาสำคัญที่จะต้องพิจารณาคือ เรื่องของมาตรการที่จะนำมาใช้ดำเนินการเกี่ยวกับข้อมูลทางคอมพิวเตอร์บนอินเทอร์เน็ตที่ไม่เหมาะสมเหล่านั้น โดยเฉพาะในกรณีที่ข้อมูลนั้นเป็นข้อมูลที่ไม่ได้ผิดกฎหมายอย่างชัดเจน แต่เป็นข้อมูลที่ไม่เหมาะสมสำหรับเด็กอันอาจส่งผลร้ายต่อเด็กได้หากได้รับรู้ ที่แม้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทย จะมีมาตรา 14 วางหลักกำหนดฐานความผิดในการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลที่ไม่มีความเหมาะสมในเรื่องต่าง ๆ เอาไว้ เช่น ข้อมูลคอมพิวเตอร์ปลอมหรือเท็จโดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคงของราชอาณาจักรหรือเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา ข้อมูลอันมีลักษณะลามกซึ่งประชาชนสามารถเข้าถึงได้ เป็นต้น อีกทั้งยังกำหนดให้การเผยแพร่หรือส่งต่อข้อมูลดังกล่าวเป็นความผิดด้วยแล้วก็ตาม แต่กฎหมายฉบับนี้ก็ยังไม่ได้มีการกำหนดขอบเขตหรือให้คำนิยามศัพท์ที่ชัดเจนและครอบคลุมเพียงพอที่จะสามารถคุ้มครองเด็กได้ เพราะยังมีข้อมูลอีกหลายประเภทที่ไม่เหมาะสม

สำหรับเด็กเป็นการเฉพาะ ซึ่งกฎหมายฉบับนี้ยังไม่ได้มีการบัญญัติไว้ ทำให้ยังคงมีข้อมูลที่ไม่เหมาะสมสำหรับเด็กอีกมากที่กฎหมายยังไม่สามารถเข้าไปควบคุมดูแลได้

ในส่วนของกฎหมายอื่น ๆ นอกจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ยังมีกฎหมายที่เกี่ยวกับการคุ้มครองเด็กและเยาวชนที่สมควรนำมาพิจารณาดู ซึ่งจากการศึกษาพบว่า กฎหมายดังกล่าวก็ยังไม่สามารถที่จะนำมาปรับใช้เพื่อกำกับดูแลการเข้าถึงข้อมูลบนอินเทอร์เน็ตที่ไม่เหมาะสมสำหรับเด็กได้หรือยังไม่มีความชัดเจนเพียงพอ คือพระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546 มีมาตรา 26 (3) กำหนดห้ามมิให้ผู้ใดบังคับ ชุ่เชิญ ชักจูง ส่งเสริมหรือยินยอมให้เด็กประพฤติตนไม่สมควรหรือนำจะทำให้เด็กมีความประพฤติเสี่ยงต่อการกระทำความผิด ซึ่งยังไม่มีความชัดเจนถึงขอบเขตของการปรับใช้ ต้องอาศัยการตีความซึ่งอาจจะไม่ครอบคลุมเพียงพอ อีกทั้งข้อมูลทางคอมพิวเตอร์บนเครือข่ายอินเทอร์เน็ตก็เปลี่ยนแปลงอย่างรวดเร็วและตลอดเวลา จึงเป็นการยากที่กฎหมายที่มีอยู่จะสามารถตามไปควบคุมดูแลได้เท่าทัน ทำให้ข้อมูลที่ไม่เหมาะสมสำหรับเด็กยังคงอยู่และสามารถที่จะเข้าถึงได้ ส่งผลให้ผู้ที่ใช้บริการอินเทอร์เน็ตได้รับข้อมูลข่าวสารที่ไม่เหมาะสมเหล่านั้นไป ไม่ว่าจะเป็นโดยตั้งใจหรือโดยบังเอิญก็ตาม ทั้งนี้เพราะบางเว็บไซต์นั้นใช้ชื่อของเว็บไซต์ที่ไม่ได้บ่งบอกลักษณะของเนื้อหาความด้านในหรือไม่ตรงกับเนื้อหาความในเว็บไซต์ ทำให้ในบางครั้งการเข้าเว็บไซต์โดยผ่านทาง Search Engines อาจจะมีเว็บไซต์ที่ไม่เหมาะสมปรากฏขึ้นมาด้วยและอาจจะทำให้เกิดการเข้าถึงข้อมูลที่ไม่เหมาะสมต่าง ๆ โดยไม่ตั้งใจได้ ซึ่งในเรื่องของการรับรู้ข้อมูลที่ไม่เหมาะสมเหล่านี้เป็นเรื่องที่เป็นปัญหาอย่างมากในปัจจุบัน เพราะอาจส่งผลกระทบในทางลบแก่เด็กซึ่งเป็นผู้ที่ยังต้องประสบการณ์และวุฒิภาวะได้

ในรัฐต่างประเทศอย่างเช่น ประเทศสหรัฐอเมริกา ก็ประสบปัญหาเกี่ยวกับการใช้คอมพิวเตอร์และอินเทอร์เน็ตของเด็กและเยาวชนเช่นกัน โดยเฉพาะในเรื่องของการเข้าถึงเว็บไซต์ลามกของเด็ก ทำให้ประเทศสหรัฐอเมริกาเป็นหนึ่งในเรื่องของศีลธรรมอันดีเป็นอย่างมากจนกระทั่งมีความพยายามที่จะออกกฎหมายมาควบคุมการเข้าถึงสื่อที่ไม่เหมาะสมสำหรับเด็กเหล่านี้ เช่น Children's Internet Protection Act ที่ออกมากำหนดให้ห้องสมุดหรือโรงเรียนที่รับทุนสนับสนุนจากรัฐบาลจะต้องจัดให้มีระบบซอฟต์แวร์ เพื่อคัดกรองเว็บไซต์ที่มีเนื้อหาที่ไม่เหมาะสมสำหรับเด็กและเยาวชน โดยกำหนดให้ต้องทำเพื่อเป็นเงื่อนไขของการได้รับทุนสนับสนุนการดำเนินการจากรัฐบาล ซึ่งกฎหมายของสหรัฐอเมริกานับนี้ศาลสูงของประเทศสหรัฐอเมริกาได้ให้การรับรองแล้วว่าไม่ขัดต่อรัฐธรรมนูญ อันแสดงให้เห็นได้อย่างชัดเจนว่า ปัญหาการที่เด็กเข้าถึงข้อมูลบนอินเทอร์เน็ตที่ไม่เหมาะสมสำหรับเด็กเป็นปัญหาสำคัญที่แม้กระทั่งประเทศที่ยึดมั่นในสิทธิเสรีภาพของปัจเจกชนอย่างมากเช่นประเทศสหรัฐอเมริกาเอง ก็ยังต้องมีการออกกฎหมายมากำกับดูแลการเข้าถึงสิ่งที่ไม่เหมาะสมดังกล่าวเพื่อเป็นฐานในการป้องกันอาชญากรรมคอมพิวเตอร์ในมิติของเด็กและเยาวชน

สำหรับประเทศไทยเอง รัฐของเราไม่สามารถที่จะไปปิดกั้นการเผยแพร่และการรับรู้ข้อมูลข่าวสารของบุคคลทุกคนได้โดยเพียงอ้างว่าข้อมูลข่าวสารที่ไม่เหมาะสมสำหรับเด็กเท่านั้น ประเทศไทยจึงควรที่จะมองถึงปัญหาที่อาจจะเกิดกับเด็กและเยาวชนผู้ที่เป็นอนาคตของชาติ อันเกิดจากการที่เด็กและเยาวชนรับรู้ข้อมูลบนอินเทอร์เน็ตที่ไม่เหมาะสมสำหรับเด็กและเยาวชน เราควรที่จะหามาตรการที่เหมาะสมที่จะนำมาดำเนินการเกี่ยวกับการเข้าถึงข้อมูลทางคอมพิวเตอร์บนอินเทอร์เน็ตที่ไม่เหมาะสมสำหรับเด็กและเยาวชน โดยในขณะเดียวกันมาตรการดัง

กล่าวก็จะต้องไม่ไปลดทอนสิทธิเสรีภาพของผู้มีวุฒิภาวะเพียงพอในการที่จะเข้าถึงและรับรู้ข้อมูลข่าวสาร อันจะเป็นการช่วยวางแนวทางป้องกันไว้ก่อนที่ปัญหาเกี่ยวกับอาชญากรรมคอมพิวเตอร์ในมิติของเด็กและเยาวชนจะเกิดขึ้น

ดังนั้น อาชญากรรมคอมพิวเตอร์ในมิติของเด็กและเยาวชน ไม่ว่าจะเป็นในฐานะผู้กระทำความผิด หรือเป็นผู้รับผลหรือเหยื่อจากการกระทำความผิด จึงนับว่าเป็นปัญหาสำคัญที่รัฐบาลหรือหน่วยงานต่างๆ ที่เกี่ยวข้องจะต้องระดมสรรพกำลังต่างๆ เข้าดำเนินการแก้ไขอย่างจริงจัง ไม่ว่าจะเป็นการปรับปรุงแก้ไขกฎหมาย พัฒนาระบบการยุติธรรมให้มีระบบการอำนวยความยุติธรรมที่มีประสิทธิภาพ โปร่งใสและเป็นธรรม ตลอดจนพัฒนาระบบและวิธีการปฏิบัติในการแก้ไขฟื้นฟูผู้กระทำความผิดที่ รวมถึงกระบวนการป้องกัน หรือแม้กระทั่งการเยียวยาเหยื่อเป็นเด็กหรือเยาวชนให้มีความหลากหลายและเหมาะสมยิ่งขึ้น

ความมุ่งหมายของการวิจัย

1. เพื่อศึกษาสภาพปัญหาอาชญากรรมคอมพิวเตอร์ของเด็กและเยาวชนในปัจจุบัน
2. เพื่อศึกษาถึงแนวคิดทฤษฎีว่าด้วยอาชญากรรมคอมพิวเตอร์ของเด็กและเยาวชน
3. เพื่อศึกษาถึงมาตรการทางกฎหมายของต่างประเทศในการป้องกันอาชญากรรมคอมพิวเตอร์ของเด็กและเยาวชน
4. เพื่อหามาตรการทางกฎหมายในการป้องกันอาชญากรรมคอมพิวเตอร์ของเด็กและเยาวชนของไทย

วิธีวิจัย

เป็นการศึกษาวิจัยเชิงคุณภาพ (Qualitative Research) และการสัมภาษณ์ (Interview) โดยใช้วิธีวิเคราะห์พรรณนา (Descriptive Analysis) ซึ่ง

ศึกษาถึงแนวคิดทฤษฎีและวรรณกรรมที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ มาตรการทางกฎหมายในการป้องกันอาชญากรรมคอมพิวเตอร์ของต่างประเทศ การกระทำความผิดของเด็กและเยาวชนตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เพื่อวิเคราะห์หาบทสรุปและเสนอมาตรการทางกฎหมายในการป้องกันอาชญากรรมคอมพิวเตอร์ของเด็กและเยาวชนของไทย

ผลการวิจัย

แนวโน้มของความรุนแรงของอาชญากรรมมีซับซ้อนมากขึ้นตามความเจริญของเทคโนโลยีและความทันสมัยของการสื่อสารแขนงต่าง ๆ โดยเฉพาะเทคโนโลยีทางคอมพิวเตอร์และอินเทอร์เน็ตได้ก่อให้เกิดความเปลี่ยนแปลงอย่างมากในการดำรงชีวิตของมนุษย์ โดยเหตุที่สังคมและกฎหมายยังวางอยู่บนข้อสมมติฐานที่มนุษย์และสังคมกายภาพ (Physical being) แยกกันอยู่เป็นหมวดหมู่ตามอาณาเขตทางกายภาพ กฎหมายจึงเป็นส่วนประกอบและข้ออ้างอิง (Reference) ของสังคมที่สมาชิกเกาะเกี่ยวกันอยู่ จึงไม่แปลกที่ปัจจุบันจะปรากฏกฎหมายที่หลากหลายรูปแบบทฤษฎี หลักการ แนวทาง และการประยุกต์ใช้ แต่โดยที่วิทยาการและเทคโนโลยีสมัยใหม่ได้พัฒนาไปรวดเร็วมาก ทำให้บางครั้งกฎหมายและกระบวนการทางสังคมก็ต้องปรับตัวให้ทันกับความเปลี่ยนแปลงที่เกิดขึ้น และเมื่อความแตกต่าง (disparity) ระหว่างสังคมเกิดขึ้น ประเทศไทยจึงต้องปรับตัวเข้ากับกระแสความเปลี่ยนแปลงของโลกที่พัฒนาไปด้วย โดยเฉพาะอย่างยิ่งสื่อคอมพิวเตอร์และอินเทอร์เน็ตซึ่งเป็นเครือข่ายระดับโลก (global network) โดยที่ประเทศไทยไม่มีทางเลือกเลย กระแสนี้ได้ (เลอสรุภ ธนสุกาญจน์ และคณะ, 2541)

จากข้อมูลของสำนักงานสถิติแห่งชาติทำให้พบว่าเด็กและเยาวชนเข้าถึงข้อมูลที่ไม่เหมาะสม

จากคอมพิวเตอร์อินเทอร์เน็ตมากขึ้นในอัตราก้าวกระโดดและมีชั่วโมงของการใช้คอมพิวเตอร์อินเทอร์เน็ตสูงขึ้น ในขณะที่ข้อมูลจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทยแสดงให้เห็นว่าประเทศไทยมีภัยคุกคามบนโลกอินเทอร์เน็ตในลักษณะที่เป็นอาชญากรรมคอมพิวเตอร์เพิ่มมากขึ้นทุกปี จึงสะท้อนภาพปัญหาว่าเด็กและเยาวชนไทยอาจเข้าไปมีส่วนในฐานะผู้กระทำความผิด หรืออาจตกเป็นเหยื่อจากอาชญากรรมคอมพิวเตอร์ได้

ปัญหาเกี่ยวกับการกระทำความผิดของเด็ก อันถือเป็นการก่ออาชญากรรมคอมพิวเตอร์ในขณะนี้ ส่วนหนึ่งเป็นผลจากการที่เด็กได้รับข้อมูลที่ไมเหมาะสมสำหรับเด็กจากอินเทอร์เน็ต (สันติชัย สนิทไชย, 2551) ดังนั้น การที่จะป้องกันอาชญากรรมคอมพิวเตอร์ในมิติของเด็กและเยาวชนได้อย่างมีประสิทธิภาพนั้น จำเป็นต้องมีมาตรการที่ดีที่สามารถดูแลการเข้าถึงข้อมูลทางคอมพิวเตอร์ของเด็กและเยาวชนได้ ซึ่งจะมีความสอดคล้องกับหลักทฤษฎีทางอาชญาวิทยาที่ได้ให้ความสำคัญต่อกระบวนการเรียนรู้ การจดจำและการปฏิบัติตามของเด็กและเยาวชน ประกอบกับแนวคิดในการสื่อสาร การจัดการและการกำกับดูแลตนเองทางคอมพิวเตอร์ที่ว่า การเรียนรู้และจดจำส่งผลพฤติกรรมและการปฏิบัติตามของเด็กและเยาวชน หากการเรียนรู้เทคโนโลยีทางคอมพิวเตอร์ของเด็กและเยาวชนขาดการชี้แนะแนวทางที่เหมาะสมหรือการขาดมาตรการที่ดีในการดูแลพฤติกรรมของเด็กและเยาวชนที่มีประสิทธิภาพ อาจนำไปสู่พฤติกรรมเบี่ยงเบนซึ่งจะกลายเป็นปัญหาอาชญากรรมคอมพิวเตอร์ของเด็กและเยาวชน

นี่เป็นประเด็นสำคัญที่รัฐจะต้องให้ความสำคัญกับการบริหารจัดการอินเทอร์เน็ต (Internet Governance) อันเป็นการประสานงานร่วมกันระหว่างภาครัฐบาล ภาคเอกชน และภาคประชาสังคมในการแสวงหาหลักการ บรรทัดฐาน กติกา กฎระเบียบ และกระบวนการตัดสินใจ เพื่อกำหนด

แนวทางการพัฒนา และการใช้อินเทอร์เน็ต (Johannes M. Bauer, 2005)

สำหรับในต่างประเทศ ได้มีการกำหนด มาตรการทางกฎหมายในการป้องกันอาชญากรรม คอมพิวเตอร์ในมิติของเด็กและเยาวชนไว้ดังนี้คือ

1. อนุสัญญาว่าด้วยอาชญากรรม คอมพิวเตอร์

อนุสัญญานี้เป็นผลสำเร็จจากความพยายาม ระหว่างประเทศ ในการสร้างกฎเกณฑ์ร่วมกันเพื่อ ปรามปรามการกระทำความผิดอาชญากรรม คอมพิวเตอร์ และถือเป็นสนธิสัญญาระหว่าง ประเทศฉบับแรกที่ได้บัญญัติขึ้นเกี่ยวกับการกระ ทำความผิดเกี่ยวกับคอมพิวเตอร์ในทางระหว่าง ประเทศ มีวัตถุประสงค์ที่สำคัญ 3 ประการ คือ

1. เพื่อให้กฎหมายสารบัญญัติของรัฐต่างๆ มีความเป็นเอกภาพ เพราะได้กำหนดฐานความผิด ฐานจำนวน 9 ประเภท คือ การเข้าถึงระบบ คอมพิวเตอร์โดยมิชอบ การดักจับข้อมูลการรบกวน การทำงานของข้อมูล การรบกวนการทำงานของ ระบบคอมพิวเตอร์ การใช้อุปกรณ์ในทางมิชอบ การ ปลอมแปลงข้อมูลคอมพิวเตอร์ การฉ้อโกงทาง คอมพิวเตอร์ การเผยแพร่ภาพลามกอนาจารเด็ก และการละเมิดลิขสิทธิ์และสิทธิข้างเคียง ให้รัฐ สมาชิกนำไปบัญญัติเป็นกฎหมายภายในของรัฐ ตลอดจนเป็นแบบอย่างให้แก่อื่นๆ นำไปศึกษา เป็นตัวอย่างของการกำหนดฐานความผิด อาชญากรรมคอมพิวเตอร์ภายในประเทศของตน

2. เพื่อกำหนดกฎหมายวิธีพิจารณาความ อาญาภายในของรัฐ ให้มีอำนาจที่จำเป็นเพียงพอ ต่อการสืบสวนสอบสวนและการฟ้องร้องดำเนินคดี ในความผิดที่ได้กระทำโดยอาศัยระบบคอมพิวเตอร์ ตลอดจนการรวบรวมพยานหลักฐานทาง อิเล็กทรอนิกส์ เช่น การกำหนดให้รัฐต้องมี กฎหมายกำหนดให้อำนาจในการสั่งให้ผู้ครอบครอง ข้อมูลคอมพิวเตอร์มีการเก็บรักษาข้อมูลนั้นไว้ไม่ เกิน 90 วัน การกำหนดให้มีอำนาจในการสั่งยึดอายัดข้อมูลทางคอมพิวเตอร์ หรือมีอำนาจในการ

สั่งการให้ผู้ประกอบการ หรือผู้ที่เกี่ยวข้องกับระบบ คอมพิวเตอร์ เช่น ผู้ให้บริการเข้าถึงอินเทอร์เน็ต (Internet Service Provider / ISP) ทำการเก็บข้อมูล จราจรทางคอมพิวเตอร์ทันทีเมื่อพนักงานเจ้าหน้าที่ ร้องขอ เป็นต้น การกำหนดเช่นนี้ย่อมทำให้ มาตรฐานการดำเนินกระบวนการยุติธรรมของ แต่ละรัฐเป็นไปในมาตรฐานเดียวกัน ไม่ลำเอียงหรือ มีวิธีการที่แตกต่างออกไป อันจะทำให้เกิดความ สะดวกรวดเร็วในการติดตามจับกุมผู้กระทำความ ผิด และทำให้การปรามปรามเป็นไปอย่างมี ประสิทธิภาพ

3. เพื่อสร้างความร่วมมือระหว่างประเทศ ให้เกิดขึ้นด้วยความรวดเร็วและเป็นไปอย่างมี ประสิทธิภาพ อนุสัญญาจึงได้กำหนดหลักเกณฑ์ใน การส่งผู้ร้ายข้ามแดน การให้ความช่วยเหลือซึ่งกัน และกันในการดำเนินกระบวนการยุติธรรมทางอาญา นอกจากนี้อนุสัญญายังเปิดโอกาสให้ประเทศนอก กลุ่มคณะมนตรีแห่งยุโรปเข้าร่วมเป็นภาคีใน อนุสัญญาได้ ซึ่งจะช่วยขยายขอบเขตความร่วมมือ ระหว่างรัฐในการปรามปรามการกระทำความผิด อาชญากรรมทางคอมพิวเตอร์ออกไปทั่วโลก และ ทำให้อนุสัญญาใกล้เคียงความเป็นสากล

2. EU Safer Internet Action Plan

สภายุโรปและคณะมนตรีแห่งสหภาพยุโรป (The European Parliament and the Council of the European Union) วางแผนการสร้าง อินเทอร์เน็ตที่ปลอดภัยกว่าเพื่อบังคับใช้ในสหภาพ ยุโรป เพื่อเป็นแนวทางให้ประเทศสมาชิกได้นำไป ใช้วางมาตรการสำหรับประเทศของตนเอง ทั้งนี้ โดยมีจุดประสงค์หลักก็คือ การป้องกันเด็กและ เยาวชนจากเนื้อหาบนอินเทอร์เน็ตที่เป็นอันตราย ต่างๆ ก็มาพร้อมกับการเจริญเติบโตนี้ โดยเฉพาะ อันตรายกับเด็กและเยาวชนและการละเมิดทางด้าน เทคโนโลยีที่ปรากฏให้เห็นอยู่เนืองๆ ทำให้แผนการ รับมือก็ต้องมีการเปลี่ยนแปลงเพื่อให้เท่าทันตลอด เวลา เพื่อที่จะสามารถจัดการกับทั้งข้อมูลที่เป็น อันตรายกับเด็กและเยาวชน ข้อมูลที่ผู้ใช้ไม่ต้องการ

และรวมไปถึงข้อมูลที่ผิดกฎหมาย แผนการสร้างอินเทอร์เน็ตที่ปลอดภัยกว่าในสหภาพยุโรปที่ผ่านมาจึงวัตถุประสงค์ คือ

1. เพื่อให้การใช้งานอินเทอร์เน็ตมีความปลอดภัยมากขึ้น โดยเฉพาะสำหรับเด็กและเยาวชน และเพื่อที่จะจัดการกับข้อมูลหรือเนื้อหาที่ผิดกฎหมายหรือที่ผู้ใช้อินเทอร์เน็ตไม่ต้องการ

2. ในการที่จะบรรลุวัตถุประสงค์ดังกล่าวในข้อ 1 จะต้องมีการดำเนินการในเรื่องต่างๆ คือ

(1) ต่อกับเนื้อหาที่ผิดกฎหมาย โดยมีการตั้งสายด่วนรายงานเกี่ยวกับเนื้อหาที่ผิดกฎหมาย ซึ่งช่องทางของการรายงานจะต้องสะดวกและพร้อมที่จะรับข้อมูล และเพื่อความมีประสิทธิภาพก็อาจจะมีการตั้งตัวที่จะบ่งชี้ว่าข้อมูลแบบใดที่ถือว่าเป็นข้อมูลที่จะต้องแจ้งและดำเนินไปได้ทุกข้อมูลที่ถูกแจ้งมาและตรวจสอบแล้วว่าเป็นข้อมูลที่ผิดกฎหมายควรจะถูกประกาศให้สาธารณชนรับรู้อย่าง

(2) จัดการกับเนื้อหาที่ไม่เป็นที่ต้องการและที่เป็นอันตราย ซึ่งอาจต้องอาศัยเครื่องมือทางเทคนิคเพื่อให้ผู้ที่เป็แหล่งข้อมูล ผู้ที่ใช้อินเทอร์เน็ตและผู้ที่ต้องรับผิดชอบต่อเด็กและเยาวชนใช้เป็นเครื่องมือในการจัดการดูแลควบคุมซึ่งถือเป็นการสร้างอำนาจให้แก่ผู้ใช้อินเทอร์เน็ต ซึ่งระบบของการจัดระดับความเหมาะสมของข้อมูลและการให้สัญลักษณ์แก่ข้อมูลแต่ละประเภทก็ควรจะนำมาใช้ควบคู่กัน เพื่อจะเป็นตัวช่วยในการตัดสินใจรับหรือปิดกั้นข้อมูล

(3) ส่งเสริมให้มีสภาพแวดล้อมที่ปลอดภัย ระบบที่สมบูรณ์ของการควบคุมดูแลตนเองเป็นเครื่องมือที่มีประสิทธิภาพในการหยุดการแพร่กระจายของข้อมูลที่ไม่เป็นที่ต้องการ เป็นอันตรายและข้อมูลที่ผิดกฎหมาย ซึ่งการควบคุมดูแลตนเองนี้ประกอบไปด้วยส่วนสำคัญต่างๆ มากมาย อาทิ การให้คำปรึกษาและการแสดงออกซึ่งหน้าที่อย่างเหมาะสมของหน่วยงานที่เกี่ยวข้องกฎหมายที่จะออกมาวางแนวทางพฤติกรรม การส่งเสริม

ความร่วมมือในระดับชุมชน และการประเมินผลระดับชาติในรายงานควบคุมดูแลตนเอง อีกทั้งยังมีความพยายามที่ให้การประสานงานระดับชุมชนนี้เป็นตัวกระตุ้นให้อุตสาหกรรมเทคโนโลยีใหม่ๆ และอินเทอร์เน็ตในยุโรปนำกฎหมายเกี่ยวกับแนวทางการประพฤติปฏิบัติมาปรับใช้ด้วย

(4) การเพิ่มความตระหนักและระมัดระวัง โดยจะมีการระบุถึงประเภทหรือชนิดของข้อมูลที่ผิดกฎหมาย ไม่เป็นที่ต้องการหรือเป็นอันตราย ซึ่งก็รวมถึงข้อมูลที่ไม่เหมาะสมสำหรับเด็ก การเหยียดสีผิวหรือเชื้อชาติด้วย และบูรณาการเข้ากับเรื่องของการคุ้มครองผู้บริโภค การคุ้มครองข้อมูลและความปลอดภัยของเครือข่ายและข้อมูล โดยมีความจำเป็นที่จะต้องหาจัดการกับข้อมูลที่เผยแพร่อยู่บนอินเทอร์เน็ต ซึ่งการจัดการนั้นก็ต้องเท่าทันกับข้อมูลข่าวสารและการพัฒนาที่รวดเร็วของเทคโนโลยีอินเทอร์เน็ตและโทรศัพท์มือถือด้วย เช่น บริการรับส่งข้อมูลระหว่างผู้ใช้อินเทอร์เน็ต ระบบเครือข่ายวิดีโอ การสนทนาผ่านอินเทอร์เน็ต เป็นต้น

โดยในการดำเนินการเพื่อให้เป็นไปตามแผนงานดังกล่าวเป็นหน้าที่ของสมาชิกที่จะบัญญัติกฎหมายภายในเพื่อรองรับการดำเนินการนั้น โดยที่ทางแผนงานจะมีเงินสนับสนุนให้แก่แต่ละประเทศ และจากความสำเร็จของแผนงานที่ผ่านๆ มาจึงได้มีการคิดวางแผนการดำเนินการต่อเนื่องกับแผนที่กำลังจะสิ้นสุดลงในปี 2008 โดยได้มีการเริ่มวางแผนการดำเนินงานสำหรับปี 2009-2013 ซึ่งแผนการดำเนินงานใหม่จะต่อสู้ไม่ใช้กับเฉพาะเนื้อหาที่ผิดกฎหมายเท่านั้น แต่จะรวมไปถึงพฤติกรรมที่เป็นอันตรายอย่างเช่น การหลอกลวงเพื่อวัตถุประสงค์ในการล่วงละเมิดทางเพศ (Grooming) และการคุกคามทางอินเทอร์เน็ต (Cyber Bullying) ด้วย

3. มาตรการทางกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของประเทศต่างๆ

3.1 ประเทศสหรัฐอเมริกา

- Children's internet Protection Act, 2000 (CIPA)

CIPA เป็นกฎหมายที่รัฐสภาออกมาเพื่อที่จะจำกัดขอบเขตการรับรู้ข้อมูลของเด็กที่อายุต่ำกว่า 17 ปี เกี่ยวกับสิ่งลามกอนาจารที่มีอย่างโจ่งแจ้งในสังคมออนไลน์ โดยจะใช้บังคับกับโรงเรียนและห้องสมุดที่ได้รับเงินทุนจากโครงการ E-Rate ของกองทุน LSTA (The Library Services and Technology Act) เท่านั้น โดยมี The Federal Communications Commission (FCC) ทำหน้าที่ดูแลรับผิดชอบให้เป็นไปตามกฎหมายฉบับนี้ซึ่งประธานาธิบดีบิล คลินตัน ได้ลงนามในกฎหมายนี้เมื่อวันที่ 21 ธันวาคม ค.ศ. 2000 และได้รับการรับรองว่าไม่ขัดต่อรัฐธรรมนูญโดยศาลสูงของประเทศสหรัฐอเมริกา (The U.S. Supreme Court) เมื่อวันที่ 23 มิถุนายน ค.ศ. 2003

CIPA ได้วางข้อกำหนดต่างๆ ให้โรงเรียนและห้องสมุดที่ได้รับเงินทุนจากโครงการ E-Rate ต้องดำเนินการ คือ

- โรงเรียนและห้องสมุดที่อยู่ภายใต้กฎหมายฉบับนี้จะไม่ได้รับความช่วยเหลือจากโครงการ E-Rate เว้นเสียแต่จะทำให้การรับรองว่า มีนโยบายเกี่ยวกับความปลอดภัยบนอินเทอร์เน็ต และมีมาตรการป้องกันทางเทคโนโลยีพร้อมใช้ซึ่งนโยบายการใช้อินเทอร์เน็ตเกี่ยวกับความปลอดภัยบนอินเทอร์เน็ต ดังกล่าวจะต้องรวมถึงมาตรการป้องกันทางเทคโนโลยีที่จะใช้เพื่อปิดกั้นหรือกั้นกรองการเข้าถึงอินเทอร์เน็ตซึ่งรูปภาพที่ลามกอนาจาร ภาพโป๊เปลือยของเด็ก หรือสิ่งที่เป็นอันตรายต่อเด็ก ซึ่งเทคโนโลยีดังกล่าวจะต้องใช้ตลอดเวลาที่เด็กเป็นผู้ที่ใช้อินเทอร์เน็ต

- โรงเรียนที่อยู่ภายใต้กฎหมายฉบับนี้ จะต้องรับเอาและนำไปบังคับใช้ซึ่งนโยบายการกำกับดูแลกิจกรรมบนโลกออนไลน์ของเด็ก

- โรงเรียนและห้องสมุดที่อยู่ภายใต้กฎหมายฉบับนี้ จะต้องรับเอาและนำไปปรับใช้ซึ่ง

นโยบายที่สามารถระบุให้เห็นถึงการเข้าถึงสิ่งที่ไม่เหมาะสมบนอินเทอร์เน็ตของเด็ก ความมั่นคงและปลอดภัยของเด็กขณะใช้อินเทอร์เน็ตเพื่อหลีกเลี่ยงอันตราย และการติดต่อสื่อสารโดยตรงผ่านทางอิเล็กทรอนิกส์วิธีอื่นๆ การเข้าถึงโดยไม่มีอำนาจ (hacker) และกิจกรรมที่ผิดกฎหมายอื่นๆ ที่กระทำโดยเด็ก การเปิดเผย ใช้ หรือทำให้แพร่หลายซึ่งข้อมูลส่วนบุคคลของเด็ก และการจำกัดการเข้าถึงของเด็กต่อข้อมูลที่เป็นอันตรายต่อเด็ก

อย่างไรก็ตาม กฎหมายยังได้ให้เป็นดุลพินิจของผู้ที่มีอำนาจในการที่จะปิดเทคโนโลยีปิดกั้นหรือกั้นกรองนี้ในกรณีที่ผู้ใช้เป็นใหญ่ เพื่อประโยชน์ในการทำวิจัยหรือเพื่อวัตถุประสงค์ที่สุจริตและไม่ต้องห้ามตามกฎหมาย ทั้งนี้ CIPA ไม่ได้กำหนดให้ต้องมีการติดตามร่องรอยการใช้อินเทอร์เน็ตแต่อย่างใด

3.2 ประเทศออสเตรเลีย

- The Broadcasting Services Act 1992

กฎหมายฉบับนี้ได้กำหนดนิยามของ “เนื้อหาที่ต้องห้าม” (Prohibited Content) คือ เนื้อหาที่ถูกจัดลำดับชั้นหรือแบ่งประเภทอย่างใดอย่างหนึ่งต่อไปนี้

1. MA 15+ คือ ข้อมูลที่ไม่เหมาะสมสำหรับผู้ที่ยังต่ำกว่า 15 ปี ซึ่งการเข้าถึงข้อมูลดังกล่าวไม่มีการควบคุมหรือการเข้าถึงอยู่ในรูปของบริการที่แสวงหากำไรหรือต้องจ่ายค่าธรรมเนียม และเนื้อหาไม่ปรากฏรูปภาพที่ชัดเจน

2. R18+ คือ ข้อมูลที่อาจจะรบกวนหรือเป็นอันตรายแก่บุคคลที่ยังต่ำกว่า 18 ปี ซึ่งข้อมูลระดับนี้จะต้องห้ามก็ต่อเมื่อเป็นเครือข่ายอินเทอร์เน็ตในประเทศออสเตรเลียและการเข้าถึงข้อมูลดังกล่าวไม่มีระบบตรวจสอบอายุที่กำหนดขึ้นโดย ACMA

3. X18+ คือ สิ่งที่แสดงให้เห็นอย่างชัดแจ้งเกี่ยวกับความสัมพันธ์ทางเพศด้วยความเต็มใจของผู้ใหญ่ โดยไม่มีการใช้ความรุนแรงทางเพศ

4. RC (Refused Classification)

คือ สิ่งที่ถูกปฏิเสธการจัดระดับชั้น

ซึ่งเนื้อหาต่าง ๆ บนอินเทอร์เน็ตจะเป็นเนื้อหาที่ต้องห้ามก็ต่อเมื่อ พบว่า ส่วนใดส่วนหนึ่งของเนื้อหาเข้าตามลักษณะดังกล่าวข้างต้น ทั้งนี้ การจัดการกับเนื้อหาที่ต้องห้ามมีความแตกต่างกันในการใช้บังคับกฎหมายขึ้นอยู่กับว่าเนื้อหา มีแหล่งที่มาอยู่ในประเทศออสเตรเลียหรือไม่และขึ้นอยู่กับการจัดระดับของข้อมูลนั้นกล่าวคือ

1. ถ้าเนื้อหาที่มีแหล่งที่มาจากในประเทศออสเตรเลีย ก็จะมีการแจ้งถึงผู้ให้บริการอินเทอร์เน็ตและผู้ที่ได้รับฝากเนื้อหานั้นจัดการลบเนื้อหาที่ต้องห้ามหรือที่อาจจะต้องห้ามออกไปจากระบบของตน ซึ่งรวมถึงเนื้อหาในระดับ X18, RC และระดับ R18 ที่ไม่มีการติดตั้งระบบการตรวจสอบอายุ

2. ถ้าเนื้อหาที่มีแหล่งที่มาจากภายนอกประเทศ ก็จะมีการแจ้งให้ผู้จัดทำโปรแกรมในการปิดกั้นและกั้นกรองข้อมูลเพิ่มเนื้อหาที่ต้องห้ามหรืออาจจะต้องห้ามดังกล่าวลงไป ในบัญชีรายชื่อที่ควรถูกปิดกั้นหรือกั้นกรอง แต่ทั้งนี้จะไม่รวมถึงเนื้อหาที่ถูกจัดอยู่ในระดับ R18 โดยไม่ต้องคำนึงว่ามีการวางระบบการตรวจสอบอายุสำหรับเนื้อหาในระดับ R18 นั้นหรือไม่

- Classification (Publications, Films and Computer Games) Act 1995

การจัดระดับหรือการตรวจสอบเนื้อหาบนอินเทอร์เน็ตเป็นไปตามแนวปฏิบัติในการจัดระดับซึ่งตราขึ้นภายใต้ มาตรา 12 แห่งกฎหมายฉบับนี้ ซึ่งในการจัดระดับก็มีหลักเกณฑ์ที่แตกต่างกันไปตามสิ่งที่ต้องการจัดระดับ โดยในการจัดระดับหรือตรวจสอบเนื้อหาบนอินเทอร์เน็ตเป็นไปตามแนวปฏิบัติในการจัดระดับสำหรับภาพยนตร์และคอมพิวเตอร์เกม (Guidelines for the Classification of Films and Computer Games) ซึ่งในแนวปฏิบัติฉบับนี้ได้ให้ความหมายของคำว่า “ภาพยนตร์” ให้รวมถึงข้อมูลที่สามารถแสดงให้ปรากฏบนคอมพิวเตอร์ (computer generated

image) ด้วยโดยในการจัดระดับนั้นสิ่งที่ต้องคำนึงถึงในการพิจารณาข้อมูลต่าง ๆ คือ

1. มาตรฐานทางด้านศีลธรรม ความถูกต้องเหมาะสมที่ได้รับการยอมรับในวิญญูชนผู้ที่มีวุฒิภาวะ

2. คุณค่าทางด้านวรรณกรรม ศิลปะและการศึกษาในข้อมูลเหล่านั้น

3. ลักษณะโดยทั่วไปของข้อมูลแต่ละประเภท รวมถึงลักษณะทางการแพทย์ กฎหมายและวิทยาศาสตร์

4. บุคคลหรือกลุ่มประเภทของบุคคลที่เป็นผู้ได้รับหรือมีแนวโน้มว่าจะได้รับข้อมูลข่าวสารดังกล่าว

ทั้งนี้ โดยประเทศออสเตรเลียได้วางกรอบของการพิจารณาข้อมูลออกเป็น 6 เรื่องหลัก ๆ คือ เรื่องของเนื้อหาหลัก เรื่องเกี่ยวกับความรุนแรง เรื่องทางเพศ เรื่องการใช้ภาษา เรื่องการใช้ยา และเรื่องของการไปเปลือย โดยวัตถุประสงค์หลักก็เพื่อให้ผู้ใหญ่สามารถรับรู้ในสิ่งที่เขาต้องการรับรู้ ในขณะที่เด็กก็ควรที่จะได้รับการปกป้องคุ้มครองจากสิ่งที่มีอาจจะเป็นอันตรายหรือรบกวนเด็ก อีกทั้งสังคมโดยรวมจะต้องได้รับการคุ้มครองจากภัยที่อาจจะเกิดจากข้อมูลที่เป็นอันตราย โดยเฉพาะข้อมูลที่กระตุ้นอารมณ์ทางเพศ แสดงความรุนแรงทางเพศหรือข้อมูลที่สามารถทำให้พฤติกรรมของคนในสังคมตกต่ำลง โดยได้มีการจัดระดับของข้อมูลสำหรับภาพยนตร์เป็น 7 ระดับ โดยในส่วนที่เกี่ยวกับการห้ามการเข้าถึงของเด็กมีอยู่ใน 4 ระดับ กล่าวคือ

1. MA 15+(Mature Accompanied)

คือ เนื้อหาที่ได้รับการพิจารณาแล้วว่าไม่เหมาะสมกับผู้ที่ยังต่ำกว่า 15 ปี อาจจะมีการใช้ภาษาที่รุนแรงแต่คำพูดที่ก้าวร้าวอย่างมากจะต้องมีไม่มากนัก และอาจจะประกอบไปด้วยสิ่งที่สื่อถึงกิจกรรมทางเพศ โดยข้อมูลด้านอื่นๆ จะพิจารณาตามบริบทของข้อมูลนั้น

2. R 18+ (Restricted) คือ เนื้อหาที่ได้รับการพิจารณาแล้วว่าไม่เหมาะกับผู้ที่อายุต่ำกว่า 18 ปี ประกอบไปด้วยความรุนแรง เมื่อดูตามบริบทแล้วแสดงเป็นภัยถึงความรุนแรงทางเพศ อาจจะมีการจำลองภาพของกิจกรรมทางเพศที่ไม่ใช่ของจริง การเปลือยกายหรือการใช้ยา

3. X 18+ (Restricted) คือ เนื้อหาที่ได้รับการพิจารณาแล้วว่าไม่เหมาะกับผู้ที่อายุต่ำกว่า 18 ปี เป็นระดับพิเศษที่ต้องได้รับการควบคุมเพราะประกอบไปด้วยเรื่องเกี่ยวกับทางเพศอย่างโจ่งแจ้ง มีการแสดงถึงการร่วมเพศหรือกิจกรรมทางเพศอย่างเต็มที่ของผู้ใหญ่ แต่ทั้งนี้ต้องไม่ปรากฏถึงความรุนแรงทางเพศ ภาษาที่แสดงถึงการล่วงละเมิดทางเพศ วัตถุที่แสดงถึงความคลั่งไคล้ทางเพศหรือผู้แสดงที่ไม่ใช่ผู้ใหญ่หรือผู้ที่ดูแล้วยังไม่เป็นผู้ใหญ่หรือการแต่งกายผู้ใหญ่ให้มีลักษณะคล้ายกับเด็ก

4. RC (Refused Classification) คือ สิ่งที่รุนแรงหรือมากเกินไปกว่าที่ระบุไว้ใน R 18+ และ X 18+ จะถูกปฏิเสธในการจัดระดับของข้อมูล กล่าวคือ เป็นข้อมูลที่แสดงถึงส่งเสริมการประกอบอาชญากรรมหรือความรุนแรง แสดงถึงการร่วมเพศหรือการล่วงละเมิดทางเพศหรือการขายบริการทางเพศของเด็กหรือของผู้ที่มีลักษณะอายุไม่เกิน 18 ปี แสดงถึงการร่วมเพศโดยมีอุปกรณ์ที่แสดงความคลั่งไคล้ทางเพศ การร่วมเพศของบุคคลภายในครอบครัว หรือแสดงถึงการร่วมเพศโดยมีอุปกรณ์ที่แสดงความคลั่งไคล้ทางเพศ การร่วมเพศของบุคคลภายในครอบครัว หรือแสดงถึงวิธีการหรือรายละเอียดของการใช้ยาที่ต้องห้ามตามกฎหมาย

3.3 ประเทศสิงคโปร์

- The Broadcasting (Class Licence) Notification 1996

ตามกฎหมายฉบับนี้กำหนดให้ผู้ให้บริการอินเทอร์เน็ต (ISPs) และผู้จัดทำเนื้อหาบนอินเทอร์เน็ต (ICPs) จะต้องได้รับใบอนุญาตตามกฎหมายประเภทของใบอนุญาตที่กฎหมายกำหนดขึ้น โดย

ผู้ให้บริการอินเทอร์เน็ตหมายความว่ารวมถึง ผู้ให้บริการการเข้าถึงอินเทอร์เน็ต (IASPs) (ซึ่งเป็นผู้ที่ได้รับการเข้าถึงอินเทอร์เน็ตจาก IASPs และทำการขายการเข้าถึงอินเทอร์เน็ตนั้นให้แก่สาธารณะ) โดยในปัจจุบันนี้ผู้ให้บริการการเข้าถึงอินเทอร์เน็ตที่เป็นหลักในประเทศสิงคโปร์ได้แก่ SingNet, Pacific Internet และ Starhub Internet ซึ่งผู้ขายบริการการเข้าถึงอินเทอร์เน็ตหมายความว่ารวมถึง โรงเรียน ห้องสมุดสาธารณะและร้านอินเทอร์เน็ต และผู้ให้บริการอย่างเช่น the Singapore Network Services Pte Ltd และ National Computer Services Pte Ltd ซึ่ง ISPs ต้องลงทะเบียนต่อ MDA ภายใน 14 วันนับแต่ที่เกิดให้บริการ ทั้งนี้ยกเว้นให้กับ IASPs ที่ให้บริการการเข้าถึงอินเทอร์เน็ตแก่สาธารณะเป็นการชั่วคราว หรือเพื่อวัตถุประสงค์ในการสาธิตหรือจัดแสดง

ผู้จัดทำเนื้อหาบนอินเทอร์เน็ต (ICPs) คือ ผู้ที่จัดหาข้อมูลต่าง ๆ บนเครือข่ายอินเทอร์เน็ต ซึ่งรวมถึงผู้สร้างและบรรณาธิการของเว็บไซต์ ผู้โฆษณาทางเว็บไซต์และผู้ควบคุมดูแลเซิร์ฟเวอร์ ซึ่งผู้จัดทำเนื้อหาบนอินเทอร์เน็ตไม่จำเป็นต้องขึ้นทะเบียนกับ MDA เว้นแต่ว่าเว็บเพจนั้นมีขึ้นเพื่อวัตถุประสงค์ทางการเมืองและศาสนา แต่ทั้งนี้การขึ้นทะเบียนดังกล่าวก็มีได้หมายความว่าห้ามมิให้มีการโฆษณาในเรื่องดังกล่าว เพียงแต่มีขึ้นเพื่อให้ผู้ที่ลงทะเบียนต้องมีความรับผิดชอบต่อสิ่งที่เขาเหล่านั้นได้พูดหรือโฆษณากออกไป ซึ่งสิ่งนี้เป็นสิ่งที่สำคัญมากสำหรับประเทศที่ประกอบไปด้วยประชากรหลายเชื้อชาติและหลายศาสนาอย่างประเทศสิงคโปร์

บุคคลทั่วไปที่จัดทำหน้าเว็บเพจของตนเองขึ้นได้รับการยกเว้นจากการขึ้นทะเบียนใบอนุญาต เว้นแต่การจัดทำนั้นมีวัตถุประสงค์ทางธุรกิจ และเพื่อการสนับสนุนทางการเมืองหรือศาสนา หรือผู้ที่จัดหาข้อมูลหรือข่าวในเบื้องต้นเกี่ยวกับทางการเงิน ผู้ที่ปรับปรุงระบบซอฟต์แวร์และบริษัทที่จัดให้มีการเข้าถึงอินเทอร์เน็ตสำหรับ

ลูกจ้างของตนเองก็ไม่จำเป็นต้องอยู่ภายใต้ระบบใบอนุญาตนี้เช่นกัน

ทั้งนี้ ผู้ที่ได้รับใบอนุญาตตามกฎหมายฉบับนี้จะต้องลบหรือห้ามการเผยแพร่เนื้อหาหรือโปรแกรม ไม่ว่าจะทั้งหมดหรือบางส่วน ตามที่ได้รับการร้องขอจากหน่วยงานที่รับผิดชอบว่าเนื้อหา นั้นขัดกับหลักเกณฑ์ที่กฎหมายกำหนดไว้ใน Code of Practice หรือเป็นสิ่งที่ขัดต่อประโยชน์สาธารณะ ความสงบเรียบร้อยหรือความเป็นหนึ่งเดียวของ ชนชาติ หรือเป็นสิ่งที่ขัดต่อสิ่งที่พึงงามหรือเป็นสิ่งที่ ไม่เหมาะสม อีกทั้งการปฏิบัติตามการร้องขอดังกล่าวยังใช้เป็นองค์ประกอบในการพิจารณาต่อใบอนุญาตให้ประกอบกิจการอีกด้วย

- Internet Code of Practice 1997

ข้อกำหนดภายใต้กฎหมายฉบับนี้มีดังนี้คือ

1. ผู้ให้บริการการเข้าถึงอินเทอร์เน็ต (IASPs) และผู้ขายบริการการเข้าถึงอินเทอร์เน็ต (Internet Service Resellers) จะพ้นจากภาระหน้าที่ตามที่กฎหมายฉบับนี้ในส่วนที่เกี่ยวข้องกับ โปรแกรมบนเครือข่ายอินเทอร์เน็ต ก็ต่อเมื่อได้มีการปฏิเสธการเข้าถึงเว็บไซต์ที่ได้รับแจ้งจากผู้ควบคุมดูแลว่าเป็นเว็บไซต์ที่มีสิ่งที่ต้องห้ามเผยแพร่อยู่ภายใน

2. ผู้ให้บริการการเข้าถึงอินเทอร์เน็ต (IASPs) และผู้ขายบริการการเข้าถึงอินเทอร์เน็ต (Internet Service Resellers) จะพ้นจากภาระหน้าที่ตามที่กฎหมายฉบับนี้ในส่วนที่เกี่ยวข้องกับกลุ่ม ข่าวนอนอินเทอร์เน็ตต่อเมื่อ

1) งดเว้นการเข้าเป็นสมาชิกของกลุ่มข่าวสารทางอินเทอร์เน็ตใด ๆ ที่เห็นว่าน่าจะมี สิ่งที่ต้องห้ามเผยแพร่อยู่

2) ระวังการเป็นสมาชิกของกลุ่ม ข่าวสารทางอินเทอร์เน็ตที่ได้รับแจ้งจากผู้ควบคุมดูแล

3. ผู้จัดทำเนื้อหาบนอินเทอร์เน็ต (ICPs) จะพ้นจากภาระหน้าที่ตามที่กฎหมายฉบับนี้ต่อเมื่อ

1) ในส่วนที่เกี่ยวกับการรวมกลุ่ม วิพากษ์วิจารณ์แบบเป็นส่วนตัวที่ใช้บริการอยู่บน เว็บไซต์ของตน เมื่อผู้ที่ได้รับใบอนุญาตมีการเลือก หัวข้อการสนทนาที่ไม่ต้องห้ามตามกฎหมาย

2) ในส่วนที่เกี่ยวกับโปรแกรมที่อยู่ บนเว็บไซต์ของตนที่บุคคลอื่นซึ่งเป็นผู้ที่ได้รับการ เชื้อเชิญให้กระทำการดังกล่าวบนบริการของผู้ที่ได้รับใบอนุญาตเพื่อให้ปรากฏแก่สาธารณชน เป็น ผู้นำมาเผยแพร่ เมื่อผู้ที่ได้รับใบอนุญาตปฏิเสธการ เข้าถึงการแจกจ่ายโปรแกรมดังกล่าวที่มีสิ่งที่ต้อง ห้ามซึ่งปรากฏแก่บุคคลดังกล่าวเองหรือได้รับการ แจ้งถึงสิ่งนั้น

3) ในส่วนที่เกี่ยวกับโปรแกรม อื่นๆ บนบริการของตน ถ้าผู้ที่ได้รับใบอนุญาตมีความมั่นใจว่า โปรแกรมต่าง ๆ เหล่านี้ไม่มีสิ่งที่อาจ ถูกจัดว่าเป็นสิ่งที่ต้องห้าม บรรลุอยู่

4. ผู้จัดทำให้มีเนื้อหาบนอินเทอร์เน็ตจะต้องปฏิเสธการเข้าถึงสิ่งซึ่งถูกพิจารณาแล้วว่าเป็น สิ่งที่ต้องห้ามถ้าได้รับการร้องขอจากผู้ควบคุมดูแล

5. ในข้อที่ 3 ไม่นำไปปรับใช้กับผู้โฆษณาผ่านเว็บไซต์หรือผู้ควบคุมเซิร์ฟเวอร์ที่ไม่มี อำนาจในการควบคุมดูแลโปรแกรมที่อยู่บนบริการ ของบุคคลดังกล่าว

“สิ่งที่ต้องห้าม” (Prohibited Material) ตามระเบียบการปฏิบัติเกี่ยวกับการใช้อินเทอร์เน็ต (Internet Code of Practice) คือ สิ่งซึ่งตามหลักของ ประโยชน์สาธารณะ ศีลธรรม อันดีของประชาชน ความสงบเรียบร้อย ความปลอดภัยสาธารณะ ความเป็นหนึ่งเดียวของชนชาติ เป็นสิ่งที่ควรจะถูก ปฏิเสธหรือไม่ควรยอมรับ หรือเป็นสิ่งที่ต้องห้าม ตามกฎหมายของประเทศสิงคโปร์โดยในการ พิจารณาส่งใดจะเป็นสิ่งที่ต้องห้ามหรือไม่นั้น ปัจจัยต่างๆ ต่อไปนี้ควรได้รับการนำไปพิจารณาคือ สิ่งนั้นมีลักษณะดังต่อไปนี้

1) แสดงถึงร่างกายที่โป๊เปลือย หรือเห็นอวัยวะเพศ หรือในลักษณะที่ชวนไปใน ทางนั้น

2) ส่งเสริมความรุนแรงทางเพศหรือกิจกรรมทางเพศที่แสดงถึงการบีบบังคับหรือความไม่สมัครใจในทุกรูปแบบ

3) แสดงให้เห็นถึงการร่วมเพศหรือกิจกรรมทางเพศอย่างโจ่งแจ้ง

4) แสดงให้เห็นบุคคลที่อายุต่ำกว่า 16 ปี ในกิจกรรมทางเพศหรือในลักษณะแสดงออกทางเพศอย่างโจ่งแจ้ง

5) แสดงให้เห็นหรือส่งเสริมร่วมเพศ การมีเพศสัมพันธ์ในครอบครัว การมีความสัมพันธ์ทางเพศกับเด็ก

6) แสดงให้เห็นถึงกิจกรรมที่มีลักษณะรุนแรงหรือโหดเหี้ยมอย่างมาก

7) ยกย่อง ยั่วยุ หรือให้การสนับสนุนความเกลียดชัง ความขัดแย้งหรือการไม่ยอมรับในเรื่องของมนุษยชาติ เชื้อชาติหรือศาสนา

สำหรับประเทศไทย แม้ในปัจจุบันจะมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายหลักในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ประกอบกับมีพระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546 ในการคุ้มครองประโยชน์สูงสุดของเด็ก และการปฏิบัติต่อเด็กอย่างเสมอภาคเป็นธรรม อีกทั้งยังวางบทบัญญัติกำหนดให้โรงเรียนและสถานศึกษาต้องจัดให้มีระบบงานและกิจกรรมเพื่อส่งเสริมความประพฤติที่เหมาะสม ความรับผิดชอบ ต่อสังคม และความปลอดภัยแก่นักเรียนและนักศึกษา นอกจากนี้ยังมีการดำเนินกระบวนการพิจารณาคดีอาญาเด็กและเยาวชนเฉพาะตามพระราชบัญญัติศาลเยาวชนและครอบครัวและวิธีพิจารณาคดีเยาวชนและครอบครัว พ.ศ. 2553 ที่มีมาตรการพิเศษแทนการดำเนินคดีอาญ่อีกด้วย แต่ประเทศไทยยังไม่มีมาตรการทางกฎหมายที่เป็นรูปแบบในการป้องกันอาชญากรรมคอมพิวเตอร์ในมิติของเด็กและเยาวชน ซึ่งเกิดจากปัญหาดังต่อไปนี้ กล่าวคือ

1. ปัญหาความไม่ครอบคลุมและความไม่เท่าทันของกฎหมาย เนื่องจากข้อมูลทางคอมพิวเตอร์มีลักษณะที่สามารถเข้าถึงได้ง่ายและสะดวกรวดเร็ว อีกทั้งมีความหลากหลายทำให้เป็นการยากต่อการควบคุมหรือกำกับดูแล เป็นผลทำให้การบังคับใช้กฎหมายที่มีอยู่จึงไม่มีประสิทธิภาพมากเท่าใด เพราะยังไม่สามารถที่จะทำการกลั่นกรองหรือดำเนินการกับข้อมูลที่ไม่เหมาะสมสำหรับเด็กทางคอมพิวเตอร์ได้ ทั้งนี้เนื่องจาก การที่กฎหมายยังบัญญัติไม่ครอบคลุมเพียงพอที่จะตีความถึงข้อมูลที่ไม่เหมาะสมสำหรับเด็กได้ เช่น ลักษณะของข้อมูลที่ห้ามนำเข้า เผยแพร่หรือส่งต่อตามที่บัญญัติไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 14 ซึ่งกำหนดไว้เพียงไม่กี่ประเภทเท่านั้น ซึ่งเราต้องคำนึงถึงสิทธิเสรีภาพของเด็กและเยาวชนด้วยเช่นกัน

2. ด้วยสังคมที่มีการเปลี่ยนแปลงไปอย่างรวดเร็วและเทคโนโลยีที่พัฒนาอย่างมาก ส่งผลให้กฎหมายที่มีอยู่ไม่สามารถนำมาปรับใช้กับปัญหาที่เกิดขึ้นได้ ทำให้เกิดปัญหาในการบังคับใช้กฎหมายและปัญหาในการตีความกฎหมาย ประกอบกับเจ้าหน้าที่ผู้บังคับใช้กฎหมายยังไม่เข้าใจถึงสถานการณ์ และความสำคัญของปัญหาที่ต้องการการบังคับใช้กฎหมายที่เด็ดขาดและจริงจัง ทำให้การบังคับใช้กฎหมายในขณะนี้ไม่สามารถที่จะแก้ปัญหาต่างๆ ที่เกิดขึ้นให้หมดไปได้

3. ปัญหาความไม่ชัดเจนและซ้ำซ้อนในเรื่องอำนาจหน้าที่ เช่น เจ้าหน้าที่ตามพระราชบัญญัติคุ้มครองเด็กจะต้องร้องขอความร่วมมือจากเจ้าหน้าที่ตำรวจเพื่อปฏิบัติงานส่งผลให้การปฏิบัติหน้าที่ของเจ้าหน้าที่เป็นไปอย่างล่าช้าและไม่มีอำนาจในการกำกับดูแลที่แท้จริง

จากปัญหาดังกล่าวทำให้ขณะนี้เราจึงยังไม่มีมาตรการทางกฎหมายในการป้องกันอาชญากรรมคอมพิวเตอร์ของเด็กและเยาวชน เพื่อคุ้มครองเด็กและเยาวชนจากภัยที่อาจเกิดขึ้นจาก

ข้อมูลที่ไม่เหมาะสมทางคอมพิวเตอร์ ดังนั้น ความร่วมมือของหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้อง (Co-regulation) จึงควรหาแนวทางและมาตรการที่มีประสิทธิภาพมากที่สุดในการกำกับดูแลตนเองของเด็กและเยาวชน (Self-regulation) เพื่อที่เด็กและเยาวชนจะได้รับรู้วิธีการที่จะสามารถใช้คอมพิวเตอร์และอินเทอร์เน็ตได้อย่างปลอดภัย

ข้อเสนอแนะ

มาตรการทางกฎหมายที่มีประสิทธิภาพที่สุดในการป้องกันอาชญากรรมคอมพิวเตอร์ในมิติของเด็กและเยาวชนคือการทำหน้าที่ของหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้องพร้อมทั้งเด็กและเยาวชนในประเทศไทยต้องร่วมมือกันในการกำกับดูแลการเข้าถึงข้อมูลทางคอมพิวเตอร์ (self – regulation) โดยหน่วยงานที่สำคัญ เช่น สถาบันครอบครัว สถาบันการศึกษา ห้างสมุดหรือร้านอินเทอร์เน็ต ซึ่งต้องคำนึงถึงความเหมาะสมของเนื้อหาและการจำกัดการเข้าถึงของข้อมูลทางคอมพิวเตอร์เกี่ยวกับเนื้อหาที่ไม่เหมาะสมสำหรับเด็กและเยาวชนด้วย โดยการให้หน่วยงานภาครัฐที่เกี่ยวข้องกับสื่อคอมพิวเตอร์โดยตรง เช่น กระทรวงเทคโนโลยีสารสนเทศ กระทรวงวัฒนธรรม กระทรวงศึกษาธิการ สำนักงานตำรวจแห่งชาติ เข้ามาทำหน้าที่กำกับดูแลตามกฎหมาย ซึ่งจำต้องอาศัยเจ้าหน้าที่และบุคลากรที่มีความรู้ความสามารถทางเทคโนโลยีกับทั้งงบประมาณเพียงพอในการดำเนินการป้องกันอาชญากรรมทางคอมพิวเตอร์

ดังนั้น เพื่อเป็นการป้องกันอาชญากรรมทางคอมพิวเตอร์ของเด็กและเยาวชนจากภัยทางคอมพิวเตอร์ที่มากับข้อมูลที่ไม่เหมาะสมสำหรับเด็กและเยาวชน เราจึงควรวางมาตรการทางกฎหมายที่เหมาะสมในการเข้าถึงข้อมูลทางคอมพิวเตอร์ของเด็ก กล่าวคือ เราควรมีมาตรการเกี่ยวกับการป้องกันเนื้อหาที่ไม่เหมาะสมต่อเด็ก

และเยาวชนในการเข้าถึงคอมพิวเตอร์มาใช้บังคับหรือลงโทษในกรณีที่มีการฝ่าฝืนรวมถึงต้องกำหนดเรื่องอำนาจหน้าที่ของหน่วยงานที่จะมาทำหน้าที่กำกับดูแลมาตรการด้วยดังต่อไปนี้

1. ควรกำหนดให้เด็กที่อายุไม่เกิน 15 ปี ต้องได้รับความคุ้มครองเป็นพิเศษในเรื่องของข้อมูลที่ไม่เหมาะสมเนื่องด้วยเป็นช่วงอายุที่ยังไม่วุฒิภาวะเพียงพอและมีความเสี่ยงต่อการรับอิทธิพลในทางลบจากข้อมูลที่ไม่เหมาะสม

2. ควรกำหนดให้มีเจ้าหน้าที่หรือหน่วยงานของรัฐที่เกี่ยวข้อง เช่น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงวัฒนธรรม สำนักงานตำรวจแห่งชาติ ในการจัดให้มีการลงทะเบียนการเข้าใช้ทางคอมพิวเตอร์ที่เป็นต้นทาง (Registration) โดยจะต้องมีรายละเอียดเรื่องอายุเป็นสำคัญด้วยหลักฐานการแสดงตนของผู้ใช้คอมพิวเตอร์ หากผู้ใช้คอมพิวเตอร์ปลายทางไม่ให้ความร่วมมือหรือขาดหลักฐานการแสดงตนดังกล่าวจะไม่ได้อนุญาตให้เข้าถึงข้อมูลทางคอมพิวเตอร์

3. เจ้าหน้าที่หรือหน่วยงานของรัฐที่เกี่ยวข้องข้างต้น ต้องมีการวิเคราะห์ความเสี่ยงในการเข้าถึงข้อมูลทางคอมพิวเตอร์ของเด็กและเยาวชน อีกทั้งประชาชนทั่วไปควรให้ความร่วมมือในการแจ้งข้อมูลที่ไม่เหมาะสมแก่เจ้าหน้าที่ และควรมีการติดตั้งโปรแกรมกั้นกรองข้อมูลที่ไม่เหมาะสมสำหรับเด็กและเยาวชนทั้งที่บ้าน สถาบันการศึกษา ห้างสมุดหรือร้านอินเทอร์เน็ต โดยเฉพาะร้านที่ให้บริการอินเทอร์เน็ตเพียงต้องอยู่ภายใต้ระบบของใบอนุญาตตั้งเช่นร้านเกมอินเทอร์เน็ต เพื่อจะได้สามารถควบคุมและตรวจสอบลักษณะการให้บริการได้

4. ควรมีการกำหนดห้ามข้อมูลที่ไม่เหมาะสมสำหรับเด็กและเยาวชนในทางกฎหมายที่ไม่ควรนำมาเปิดเผย เผยแพร่หรือโฆษณา ได้แก่ ข้อมูลที่มีลักษณะลามกอนาจาร หรือข้อมูลที่มีลักษณะเป็นการกระตุ้นให้เด็กหรือเยาวชนเกิดความ

ต้องการทางเพศได้ ข้อมูลที่มีการส่งเสริมเรื่องการรักร่วมเพศ การมีเพศสัมพันธ์ภายในครอบครัว หรือข้อมูลที่ทำให้เด็กมีความคิดที่ผิดจากทำนองคลองธรรมหรือจริยธรรมที่ดี ข้อมูลที่มีลักษณะก้าวร้าวหรือแสดงถึงความรุนแรง อันอาจเป็นเหตุให้เกิดความรุนแรงหรือกระตุ้นให้เด็กกระทำความผิด ข้อมูลที่มีลักษณะให้การสนับสนุนความขัดแย้ง เช่น เรื่องมนุษยชาติ เชื้อชาติ ศาสนา หรือการเมือง อันอาจชักจูงเด็กและเยาวชนไปสู่การต่อต้านสังคมและร่วมกระทำความผิด

5. ควรมีการจัดระดับความเหมาะสม (Rating) ของข้อมูลทางคอมพิวเตอร์ก่อนที่เด็กและเยาวชนจะเข้าสู่ระบบโดยให้มีการแบ่งระดับข้อมูลให้ครอบคลุมข้อมูลทุกประเภท ซึ่งอาจเป็นการติดป้ายหรือแสดงสัญลักษณ์ (Labeling) ที่จะสามารถอธิบายถึงลักษณะของข้อมูลแต่ละระดับ และควรมีมาตรการตรวจสอบอายุ (Age Verification) ของผู้ที่เข้าถึงในส่วนของคุณสมบัติที่ไม่เหมาะสมสำหรับเด็กและเยาวชน

6. ต้องมีการปิดกั้นเว็บไซต์เมื่อมีการแจ้งจากประชาชนต่อเจ้าหน้าที่หรือหน่วยงานของรัฐที่เกี่ยวข้องและที่รับผิดชอบโดยมีการตรวจสอบแล้วว่าข้อมูลที่ไม่เหมาะสมสำหรับเด็กปรากฏอยู่ และควรมีโปรแกรมกลั่นกรองข้อมูลทางคอมพิวเตอร์ (Filtering) โดยจะต้องบอกถึงลักษณะ วิธีใช้และประโยชน์ของโปรแกรมดังกล่าวในการที่จะช่วยป้องกันเด็กจากข้อมูลที่ไม่เหมาะสมสำหรับเด็กและเยาวชน ซึ่งการดำเนินการปิดกั้นการเข้าถึงเว็บไซต์อาจเป็นการกระทำต่อสิทธิเสรีภาพของบุคคลทั่วไปซึ่งไม่ใช่เพียงจำกัดเฉพาะเด็กและเยาวชนแต่รวมถึงผู้ใหญ่ด้วย ดังนั้น กระบวนการในการดำเนินการปิดกั้นจะต้องเหมาะสมและสามารถตรวจสอบได้ ซึ่งควรให้อำนาจแก่เจ้าหน้าที่ตามกฎหมายในการขออนุญาตต่อศาลเพื่อพิจารณาอนุญาตก่อนดำเนินการดังกล่าว โดยศาลควรคำนึงถึงประโยชน์สูงสุดในการคุ้มครองเด็กและเยาวชนจากข้อมูลที่ไม่เหมาะสมกับการจำกัดสิทธิเสรีภาพของเจ้าของ

เว็บไซต์

7. ควรมีการจัดตั้งหน่วยงานที่อยู่ภายใต้การกำกับดูแลโดยองค์กรของรัฐโดยเฉพาะในการรับผิดชอบการเข้าถึงและรับรู้ข้อมูลที่ไม่เหมาะสมสำหรับเด็กและเยาวชน และควรกำหนดให้มีพนักงานเจ้าหน้าที่ของรัฐที่ความรู้ความสามารถในเรื่องของเทคโนโลยีคอมพิวเตอร์ และกฎหมายเพื่อป้องกันการละเมิดสิทธิเสรีภาพของประชาชนและคอยประสานงานระหว่างหน่วยงานที่มีส่วนเกี่ยวข้องต่างๆ

8. ควรมีการจัดอบรมความรู้ทางเทคโนโลยีใหม่ ๆ แก่พนักงานเจ้าหน้าที่อย่าสม่ำเสมอเพื่อการปฏิบัติหน้าที่ที่มีประสิทธิภาพ

9. ควรมีการส่งเสริมการกำกับดูแลตนเองของเด็กและเยาวชน โดยให้ความรู้เกี่ยวกับภัยที่อาจจะมาพร้อมกับข้อมูลข่าวสารที่ไม่เหมาะสมทางคอมพิวเตอร์

10. ควรอาศัยความร่วมมือและมีการประชาสัมพันธ์ให้แก่ประชาชนในการเรียนรู้ถึงภัยอันตรายที่อาจเกิดขึ้นจากข้อมูลที่ไม่เหมาะสมทางคอมพิวเตอร์ อีกทั้งจัดให้มีการรับเรื่องร้องเรียนและการแจ้งเบาะแสโดยสายด่วนแก่หน่วยงานที่รับผิดชอบโดยตรง

11. ในมติของกรณีพิพาทว่าเด็กและเยาวชนเป็นผู้กระทำความผิดอาชญากรรมคอมพิวเตอร์ ภาครัฐควรกำหนดมาตรการทางกฎหมายให้ครอบคลุมไปเอาผิดกับผู้ปกครองที่ปล่อยปละละเลยเด็กและเยาวชนด้วย

12. กระบวนการในการแก้ไขฟื้นฟูเด็กและเยาวชนที่กระทำความผิดหรือก่ออาชญากรรมคอมพิวเตอร์นั้น ภาครัฐควรที่จะกำหนดกฎเกณฑ์ของกระบวนการให้เป็นกฎหมายที่ชัดเจน ทั้งนี้เนื่องจาก พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้นในบางมาตราเป็นความผิดที่ยอมความไม่ได้ การที่เด็กหรือเยาวชนได้กระทำความผิดแล้วภาครัฐใช้วิธีการไม่ดำเนินคดีนั้นย่อมเป็นการละเว้นการปฏิบัติหน้าที่ตาม

กฎหมาย ดังนั้น จึงควรมีการกำหนดบทบัญญัติของกฎหมายให้สามารถเปิดช่องให้สามารถใช้กระบวนการแก้ไขบำบัดฟื้นฟูเด็กหรือเยาวชนที่มีความรู้ความสามารถ เพื่อที่จะได้นำความรู้ความสามารถมาใช้ให้เป็นประโยชน์แก่ทางราชการโดยถูกต้องตามกฎหมายต่อไป

13. สำหรับในมิติของกรณีของเด็กและเยาวชนตกเป็นเหยื่อจากการกระทำความผิดอาชญากรรมคอมพิวเตอร์ภาครัฐเองควรกำหนดมาตรการทางกฎหมายเพื่อคุ้มครองเด็กและเยาวชนเป็นพิเศษ โดยเฉพาะอย่างยิ่งควรเร่งเสนอปรับแก้บทบัญญัติในประมวลกฎหมายอาญาให้ครอบคลุมการครอบครองภาพลามกของเด็ก (Child Porn) โดยหากมีคอมพิวเตอร์เข้าไปเกี่ยวข้อง เช่น การเผยแพร่ผ่าน

สื่ออินเทอร์เน็ต ก็อาจกำหนดระวางโทษให้สูงขึ้นกว่าปกติ เพื่อจะได้สอดคล้องกับพิธีสารเลือกรับของอนุสัญญาว่าด้วยสิทธิเด็กเรื่องการค้าเด็ก การค้าประเวณี และสื่อลามกที่เกี่ยวกับเด็ก ที่ประเทศไทยได้ร่วมทำความตกลงไว้

กิตติกรรมประกาศ

ผู้วิจัยขอขอบพระคุณสำนักงานคณะกรรมการวิจัยแห่งชาติ, วิทยาลัยการเมืองการปกครอง และคณะนิติศาสตร์ มหาวิทยาลัยมหาสารคามได้ช่วยสนับสนุนทุนและอำนวยความสะดวกให้การวิจัยครั้งนี้ลุล่วงสมบูรณ์

เอกสารอ้างอิง

- เลอสรร ธนสุกาญจน์ และคณะ. (2541). *กฎหมายสำหรับบริการอินเทอร์เน็ตในประเทศไทย*. กรุงเทพมหานคร : สำนักพิมพ์นิติธรรม. 94-110.
- สันธิชัย สนิทไชย. (2551). *มาตรการทางอาญาเกี่ยวกับการเข้าถึงข้อมูลบนอินเทอร์เน็ตที่ไม่เหมาะสมสำหรับเด็ก* (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต). กรุงเทพมหานคร : คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.
- Johannes M. Bauer. (2005). "Internet Governance: Theory and First Principle." Available from URL// <http://web.si.umich.edu/tprc/papers/2005/441/Bauer-TPRC-2005-fin.pdf>.