แนวคิดเกี่ยวกับการป้องกันอาชญากรรมการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ตด้วยเทคโนโลยีปัญญาประดิษฐ์

A Concept of Crime Prevention on Applications of Artificial Intelligence for Combatting Online Child Sexual Exploitation and Abuse

ภิญโญ มีเปี่ยม[1] และ อัศว์ณุต แสงทองดี[2]
[1] คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
[2] คณะคอมพิวเตอร์ วิศวกรรม และเทคโนโลยีดิจิทัล มหาวิทยาลัยทีซไซด์

Pinyo Meephiam[1] and Usanut Sangtongdee[2]
[1] Faculty of Forensic Science, Royal Police Cadet Academy
[2] School of Computing, Engineering and Digital Technology, Teesside University

Received July 3, 2021 | Revised August 20, 2021 | Accepted September 28, 2021

บทความวิชาการ (Academic Article)

บทคัดย่อ

บทความวิชาการนี้มีวัตถุประสงค์เพื่อนำเสนอแนวคิดเกี่ยวกับการป้องกันอาชญากรรมการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ตด้วยเทคโนโลยีปัญญาประดิษฐ์ โดยมุ่งเน้นความสำคัญของการป้องกันแก้ไขปัญหาการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต บทบาทของเทคโนโลยีปัญญาประดิษฐ์ในการป้องกันการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต และการประยุกต์แนวคิดเกี่ยวกับการป้องกันอาชญากรรมเชิงสภาพแวดล้อม ซึ่งได้แก่ ระดับการป้องกันอาชญากรรมตามรูปแบบการป้องกันและควบคุมโรคทางสาธารณสุขและแนวคิดการป้องกันอาชญากรรมตามสถานการณ์ เพื่อนำมาวิเคราะห์และอธิบายหลักการทำงานของเทคโนโลยีปัญญาประดิษฐ์ในการป้องกันการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต โดยเปรียบเทียบกับการป้องกันและควบคุมการแพร่ระบาดของเชื้อไวรัสโคโรนา 2019 (COVID-19) ซึ่งแบ่งระดับการป้องกันเป็น 3 ระดับ ได้แก่ ระดับปฐมภูมิ ทุติยภูมิ และตติยภูมิ อันจะนำไปสู่การลดโอกาสในการประกอบอาชญากรรมและการตกเป็นผู้เสียหายจากการล่วงละเมิดทางเพศของเด็ก รวมถึงการเพิ่มช่องทางการเข้าถึงกระบวนการยุติธรรมของเด็กและเยาวชนสำหรับการแจ้งเหตุหรือเบาะแสการกระทำความผิด และการลบทำลายสื่อแสดงการล่วงละเมิดทางเพศต่อเด็ก โดยสภาพแวดล้อมที่มีการป้องกันการล่วงละเมิดทางเพศต่อเด็กด้วยเครื่องมือซึ่งพัฒนามาจากเทคโนโลยีปัญญาประดิษฐ์

คำสำคัญ: การป้องกันอาชญากรรม, ปัญญาประดิษฐ์, การล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต

Abstract

This review paper aims to present a concept of crime prevention on various applications of artificial intelligence (AI) for combatting online child sexual abuse and exploitation. It primarily focuses on the importance of online child sexual abuse prevention

and the role of artificial intelligence in child protection. Importantly, the concept of environmental crime prevention strategies including public health model of crime prevention and situational crime prevention has been employed to elaborate the concept of online child sexual abuse prevention by the application of AI-based tools. The proposed crime prevention strategy has been analysed in comparison with the COVID-19 prevention and control strategy which includes three levels of prevention: primary, secondary, and tertiary prevention. This crime prevention concept is expected to reduce the opportunities for offending and child victimisation, improve access to justice for children by AI-enabled hotlines for reporting suspected online child abuse, and accelerate the removals of child sexual abuse material by the application of AI-based tools in the online environment.

Keywords: Crime Prevention, Artificial Intelligence, Online Child Sexual Exploitation and Abuse

บทนำ

การล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต (Online Child Sexual Exploitation and Abuse: OCSEA) เป็นอาชญากรรมประเภทหนึ่งซึ่งใช้ประโยชน์จากคุณสมบัติของอินเทอร์เน็ตที่มีความรวดเร็วและเข้าถึงได้ง่ายจากทุกมุมโลกในการเพิ่มโอกาสสำหรับการแสวงหาประโยชน์ทางเพศจากเด็กในรูปแบบที่หลากหลาย โดยเฉพาะอย่างยิ่ง สื่อลามกอนาจารที่มีเด็กเข้ามาเกี่ยวข้อง ซึ่งจากรายงานของศูนย์เพื่อเด็กหายและถูกแสวงหาผลประโยชน์แห่งชาติสหรัฐอเมริกา (U.S. National Centre for Missing and Exploited Children: NCMEC) พบว่า จำนวนการรายงานเหตุการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ตมีแนวโน้มเพิ่มขึ้นอย่างมีนัยสำคัญจาก 4.4 ล้านครั้งในปี ค.ศ. 2015 เป็น 21.7 ล้านครั้งในปี ค.ศ. 2020 โดยภายในปี ค.ศ. 2020 ปีเดียว มีการรายงานจำนวนสื่อแสดงการล่วงละเมิดทางเพศต่อเด็กมากกว่า 65.4 ล้านไฟล์บนโลกออนไลน์ (National Centre for Missing and Exploited Children, 2021)

นอกจากนั้นยังพบว่า ช่วงสถานการณ์การแพร่ระบาดของเชื้อไวรัสโคโรนา 2019 (COVID-19) มีจำนวนสื่อแสดงการล่วงละเมิดทางเพศต่อเด็กทั่วโลกเพิ่มสูงขึ้น เนื่องมาจากการที่ทั้งเด็กและอาชญากรต้องถูกจำกัดบริเวณอยู่ภายในบ้านและใช้อินเทอร์เน็ตหรือสื่อสังคมออนไลน์มากขึ้นกว่าปกติ จึงทำให้มีโอกาสเสี่ยงในการพบปะพูดคุยและมีปฏิสัมพันธ์กันบนโลกออนไลน์เพื่อการแสวงหาประโยชน์ทางเพศเพิ่มมากขึ้น รวมถึงการบริโภคสื่อลามกอนาจารเด็กทั้งการครอบครองและเผยแพร่ก็เพิ่มมากขึ้นด้วยเช่นกัน (ECPAT, 2020; EUROPOL, 2020b) โดยจะเห็นได้ชัดเจนจากสถิติของ EUROPOL (2020a) ที่มีจำนวนการรายงานสื่อแสดงการล่วงละเมิดทางเพศต่อเด็กภายในประเทศสมาชิกของสหภาพยุโรปเพิ่มขึ้นจากประมาณ 200,000 ครั้งในช่วงปลายปี ค.ศ. 2019 ถึงต้นปี ค.ศ. 2020 เป็นประมาณ 1 ล้านครั้งในช่วงเดือนมีนาคมของปี ค.ศ. 2020 นอกจากนี้ การบันทึกและเผยแพร่สื่อลามกอนาจารเด็กด้วยตัวเด็กเอง (Self-Generated Child Sexual Abuse Material) ก็มีแนวโน้มเพิ่มขึ้น ไม่ว่าจะด้วยเหตุที่รู้เท่าไม่ถึงการณ์หรือความต้องการผลประโยชน์ใดเป็นการส่วนตัวก็ตาม (Internet Watch Foundation, 2020) ดังนี้จะเห็นได้ว่าปัญหาการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ตเป็นปัญหาสำคัญที่จำเป็นต้องได้รับ

การป้องกันแก้ไข เพื่อลดความเสียหายทั้งทางร่างกาย จิตใจ และอารมณ์ ซึ่งจะเกิดแก่เด็กผู้ตกเป็นผู้เสียหายจากการกระทำดังกล่าว

โลกไซเบอร์และอินเทอร์เน็ตเป็นสภาพแวดล้อมที่อาชญากรสามารถใช้ประโยชน์ในทางที่ผิด โดยอาศัยการพัฒนาของเทคโนโลยีในการพัฒนารูปแบบการกระทำความผิดเพื่อหลีกเลี่ยงการถูกจับกุมและดำเนินคดี เช่น การใช้มัลแวร์ (Malware) เพื่อดักรับข้อมูลการเข้าสู่ระบบของผู้อื่นและปลอมแปลงตนเป็นผู้อื่นในการหลอกลวงผู้เสียหาย การเข้ารหัสแบบ End-to-End (End-to-End Encryption: E2EE) ในการสนทนา การใช้เว็บไซต์มืด (Dark Web) และเงินสกุลดิจิทัล (Cryptocurrency) ในการทำธุรกรรมทางการเงิน การถ่ายทอดสดการล่วงละเมิดทางเพศต่อเด็ก (Livestreaming) หรือการใช้เทคโนโลยีตัดต่อภาพและเสียงโดยปัญญาประดิษฐ์ (Deepfake) ในการหลอกลวงผู้เสียหายหรือทำให้ผู้อื่นอับอายหรือเสียชื่อเสียงจากสื่อลามกอนาจาร เป็นต้น ในขณะที่การหลอกลวงด้วยการโน้มน้าวชักจูงหรือตระเตรียมเด็กสำหรับการล่วงละเมิดทางเพศ (Grooming) หรือข่มขู่กรรโชกเพื่อประโยชน์ทางเพศ (Sextortion) ซึ่งใช้วิธีการเชิงจิตวิทยาหรือวิศวกรรมสังคม (Social Engineering) ยังคงมีอยู่ควบคู่ไปกับการพัฒนารูปแบบการกระทำความผิดตามเทคโนโลยี เพื่อแสวงหาประโยชน์ทางเพศต่อเด็กผู้ซึ่งมีโอกาสตกเป็นผู้เสียหายสูงกว่าผู้ใหญ่ด้วยวุฒิภาวะและการตัดสินใจที่อาจจะไม่เพียงพอต่อการป้องกันตนเองจากภัยคุกคามบนโลกออนไลน์

เนื่องด้วยความรวดเร็วของอินเทอร์เน็ต ทำให้เนื้อหาที่เกี่ยวกับการล่วงละเมิดทางเพศต่อเด็กแพร่กระจายได้อย่างรวดเร็วและเกิดอุปสรรคในการลบทำลายแบบถาวร ซึ่งข้อจำกัดนี้ส่งผลให้เกิดบาดแผลทางจิตใจแก่เด็กอย่างไม่มีที่สิ้นสุด แม้ผู้กระทำความผิดจะถูกจับกุมดำเนินคดีแล้วก็ตาม ดังนี้ การป้องกันการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ตจึงมีความสำคัญมากกว่าการปราบปรามหรือดำเนินคดีกับผู้กระทำความผิด ทั้งนี้ การป้องกันการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ตไม่เพียงแต่เป็นหน้าที่ของรัฐหรือผู้บังคับใช้กฎหมายเท่านั้น แต่รวมถึงภาคเอกชนและผู้ใช้งานอินเทอร์เน็ตอีกด้วย โดยเฉพาะอย่างยิ่งผู้ให้บริการอินเทอร์เน็ตและบริการสื่อสังคมออนไลน์ (Electronic Service Providers) ซึ่งต่างก็มีบทบาทสำคัญในการช่วยเหลือเจ้าหน้าที่ของรัฐในการป้องกันการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ตด้วยการใช้เทคโนโลยีมาช่วยในการตรวจจับเนื้อหาหรือสื่อที่ไม่เหมาะสมบนโลกออนไลน์ รวมไปถึงการระบุตัวตนของผู้เสียหายและผู้กระทำความผิด การรายงานเหตุไปยังเจ้าหน้าที่บังคับใช้กฎหมาย และการลบทำลายเนื้อหาหรือสื่อแสดงการล่วงละเมิดทางเพศต่อเด็ก เพื่อหยุดวงจรการเผยแพร่สื่อดังกล่าวไม่ให้มีการขยายกว้างต่อไปด้วยความรวดเร็วของการสื่อสารทางอินเทอร์เน็ต ดังนั้น เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) จึงได้ถูกนำมาใช้เป็นเครื่องมือในการป้องกันการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต เพื่อลดระยะเวลาและความเหนื่อยล้าของมนุษย์ในการป้องกันและตรวจจับสื่อแสดงการล่วงละเมิดทางเพศต่อเด็กที่มีจำนวนมหาศาลบนโลกออนไลน์ โดยอาจมีการใช้งานประกอบกับเทคโนโลยีอื่นเพื่อเพิ่มประสิทธิภาพในการทำงาน (Sangtongdee et al., 2020) เช่น โฟโต้ดีเอ็นเอ (PhotoDNA) การจดจำและวิเคราะห์ใบหน้าและเสียง (Face and Voice Recognition) บอทสำหรับเก็บและวิเคราะห์ข้อมูลบนเว็บไซต์ (Web Crawlers) หรือแชทบอท (Chatbots) เป็นต้น

โดยบทความวิชาการนี้จะนำเสนอมุมมองทางอาชญาวิทยาเชิงสภาพแวดล้อมต่อการใช้เทคโนโลยีปัญญาประดิษฐ์ในการป้องกันการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ตโดยใช้ระดับการป้องกันอาชญากรรมตามรูปแบบการป้องกันและควบคุมโรคและแนวคิดการป้องกันอาชญากรรมตามสถานการณ์เพื่อวิเคราะห์เปรียบเทียบระหว่างการป้องกันและควบคุมโรคติดเชื้อไวรัสโคโรนา 2019 กับการป้องกันการ

ล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต โดยเนื้อหาในบทความประกอบด้วยการอธิบายสภาพแวดล้อมของโลกไซเบอร์ แนวคิดเกี่ยวกับการป้องกันอาชญากรรมเชิงสภาพแวดล้อม รูปแบบการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต บทบาทของเทคโนโลยีปัญญาประดิษฐ์ในการป้องกันการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต และบทวิเคราะห์ บทวิจารณ์ และข้อเสนอแนะตามลำดับ

เนื้อหา

1. สภาพแวดล้อมของโลกไซเบอร์และอาชญาวิทยาเชิงสภาพแวดล้อม (Cyberspace and Environmental Criminology)

อาชญาวิทยาเชิงสภาพแวดล้อมเป็นการศึกษาปรากฏการณ์อาชญากรรมโดยมุ่งเน้นอิทธิพลของสถานที่หรือสภาพแวดล้อมที่ส่งผลต่อโอกาสในการประกอบอาชญากรรมมากกว่าปัจจัยภายในส่วนบุคคล โดยนักอาชญาวิทยาเชิงสภาพแวดล้อมมองว่าทฤษฎีอาชญาวิทยาเชิงสภาพแวดล้อมทางกายภาพแบบเดิม (Physical Space) ยังสามารถนำมาปรับใช้กับสภาพแวดล้อมของโลกไซเบอร์ได้ เนื่องจากสภาพแวดล้อมทางไซเบอร์สามารถส่งผลให้เกิดโอกาสและความเสี่ยงในการประกอบอาชญากรรมได้เช่นเดียวกันกับสภาพแวดล้อมทางกายภาพ เพียงแต่โลกไซเบอร์เป็นสภาพแวดล้อมที่แตกต่างจากสภาพแวดล้อมทางกายภาพเนื่องจากเป็นสภาพแวดล้อมที่ไม่สามารถจับต้องได้ มีความรวดเร็ว และมีการปกปิดตัวตนของผู้ใช้งานสูง (Ekblom, 2017) ซึ่งเปิดโอกาสให้อาชญากรสามารถกระทำความผิดบนสภาพแวดล้อมนี้ได้ง่ายและรวดเร็วกว่าสภาพแวดล้อมทางกายภาพ

การเข้าถึงอินเทอร์เน็ตของกลุ่มเด็กและเยาวชนทำให้บุคคลเหล่านี้มีความเสี่ยงต่อการตกเป็นผู้เสียหายจากการล่วงละเมิดทางเพศได้สูงขึ้น (Quayle & Koukopoulos, 2019) โดยการสื่อสารผ่านอินเทอร์เน็ตไม่ว่าในรูปแบบใดนั้นถือเป็นการเปิดช่องโอกาสให้อาชญากรสามารถเข้าถึงเด็กและเยาวชนได้มากยิ่งขึ้น และเกิดกระบวนการล่วงละเมิดทางเพศต่อเด็กจากการสื่อสารออนไลน์ที่สามารถแลกเปลี่ยนข้อมูลและสื่อมัลติมีเดีย (Multimedia) ได้อย่างรวดเร็ว ดังนั้น ผู้เขียนจึงนำเสนอแนวคิดเกี่ยวกับการป้องกันอาชญากรรมเชิงสภาพแวดล้อมสำหรับการป้องกันการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต ได้แก่ การป้องกันอาชญากรรมตามรูปแบบการป้องกันและควบคุมโรค และการป้องกันอาชญากรรมตามสถานการณ์ โดยมีรายละเอียดดังต่อไปนี้

1.1 การป้องกันอาชญากรรมตามรูปแบบการป้องกันและควบคุมโรค (Public Health Model of Crime Prevention)

Brantingham & Faust (1976) ได้นำเสนอแนวคิดเกี่ยวกับการป้องกันอาชญากรรมตามรูปแบบการป้องกันและควบคุมโรค ซึ่งสอดคล้องกับแนวคิดอาชญาวิทยาเชิงสภาพแวดล้อม โดยรูปแบบการป้องกันและควบคุมโรคเป็นแนวคิดที่มุ่งเน้นการชี้ให้เห็นถึงความสำคัญของการดูแลสุขภาพขั้นปฐมภูมิ ซึ่งเป็นการปรับแนวทางการใช้ชีวิตให้มีสุขภาพดีมากกว่าการรักษาพยาบาลซึ่งเป็นการแก้ไขปัญหาที่ปลายเหตุ เช่นเดียวกันกับการป้องกันอาชญากรรม โดยแบ่งเป็น 3 ระดับ ได้แก่

1) ระดับปฐมภูมิ (Primary Prevention) ได้แก่ การระบุปัจจัยในสภาพแวดล้อมทั้งด้านกายภาพและสังคมที่อาจส่งผลให้เกิดโอกาสในการประกอบอาชญากรรม และทำการปรับแก้หรือยับยั้งเหตุปัจจัยนั้นไม่ให้เกิดขึ้น

2) ระดับทุติยภูมิ (Secondary Prevention) ได้แก่ การป้องกันอาชญากรรมด้วยการตรวจจับแนวโน้มของบุคคลที่มีพฤติกรรมอาชญากรรมและกำหนดมาตรการเพื่อป้องกันไม่ให้บุคคลเหล่านั้นกระทำความผิดในสภาพแวดล้อมหรือสังคม

3) ระดับตติยภูมิ (Tertiary Prevention) ได้แก่ การปราบปรามผู้กระทำความผิดด้วยการดำเนินคดีและการลงโทษ ตลอดจนการบำบัดฟื้นฟูพฤตินิสัย เพื่อป้องกันไม่ให้เกิดการกระทำความผิดซ้ำในอนาคต

1.2 การป้องกันอาชญากรรมตามสถานการณ์ (Situational Crime Prevention)

การป้องกันอาชญากรรมตามสถานการณ์เป็นแนวคิดการป้องกันอาชญากรรมซึ่งมุ่งเน้นการลดโอกาสในการประกอบอาชญากรรมแต่ละประเภท ซึ่งได้แก่ การเพิ่มความเสี่ยงและความยากลำบากสำหรับการกระทำความผิด และการลดผลตอบแทนที่อาชญากรจะได้รับจากการกระทำความผิดนั้น โดยวิธีการป้องกันอาชญากรรมจะต้องคำนึงถึงปัจจัยหรือสาเหตุของการเกิดอาชญากรรมในสภาพแวดล้อมที่แตกต่างกันในอาชญากรรมแต่ละประเภท เพื่อที่จะลดปัจจัยดังกล่าวและโอกาสในการกระทำความผิด โดย Cornish & Clarke (2003) ได้เสนอวิธีการ 25 เทคนิคในการป้องกันอาชญากรรมตามสถานการณ์ (Situational Crime Prevention Techniques) ซึ่งจำแนกเป็น 5 องค์ประกอบหลัก และสามารถนำมาปรับใช้ได้กับการป้องกันการล่วงละเมิดทางเพศต่อเด็ก ดังนี้

1) เพิ่มความยากลำบากในการประกอบอาชญากรรม (Increase the Effort) ได้แก่ การกระทำซึ่งเป็นการขัดขวางให้อาชญากรล่วงละเมิดทางเพศต่อเด็กได้ยากขึ้น เช่น การควบคุมการเข้าถึงพื้นที่ที่เด็กอาศัยหรือช่องทางการสื่อสารที่ใช้งานอยู่ตามหลักการป้องกันอาชญากรรมโดยการออกแบบสภาพแวดล้อม (Crime Prevention Through Environmental Design) ตลอดจนการเสริมความแข็งแกร่งให้กับเด็กผู้ที่มีความเสี่ยงต่อการตกเป็นเป้าหมาย (Target Hardening) ได้แก่ การให้ความรู้และความตระหนักถึงภัยคุกคามทางเพศแก่เด็ก หรือการฝึกให้เด็กรู้จักปฏิเสธการพูดคุยกับบุคคลแปลกหน้า เป็นต้น

2) เพิ่มความเสี่ยงในการประกอบอาชญากรรม (Increase the Risks) ได้แก่ การเพิ่มความเสี่ยงต่อการถูกตรวจพบการกระทำความผิดและการจับกุมอาชญากรที่ล่วงละเมิดทางเพศต่อเด็ก โดยใช้กลไกการดูแลปกป้องและคุ้มครองเด็ก (Guardianship) เช่น การส่งเสริมให้ผู้ปกครองและชุมชนเข้าร่วมการฝึกอบรมการคุ้มครองบุตรหลานจากภัยคุกคามทางเพศ หรือการบังคับใช้กฎหมายของเจ้าหน้าที่รัฐ หรือการคัดกรอง ปิดกั้นการเข้าถึง และลบทำลายเนื้อหาที่ไม่เหมาะสมโดยผู้ให้บริการอินเทอร์เน็ต (Internet Service Providers) ซึ่งเป็นปัจจัยสำคัญที่จะสามารถช่วยทำให้การตัดสินใจกระทำความผิดของอาชญากรมีแนวโน้มลดลง (Quayle & Koukopoulos, 2019)

3) ลดผลตอบแทนที่จะได้รับจากการประกอบอาชญากรรม (Reduce the Rewards) ได้แก่ การลดผลประโยชน์ทางเพศหรือเชิงพาณิชย์ที่อาชญากรจะได้รับจากการล่วงละเมิดทางเพศ เช่น การปิดกั้นการเข้าถึงเว็บไซต์หรือการลบทำลายบัญชีสื่อสังคมออนไลน์ของอาชญากรที่ใช้ในการประกอบอาชญากรรมไม่ให้สามารถใช้บัญชีดังกล่าวในการแสวงหาประโยชน์จากผู้ติดตามหรือผู้สนับสนุนต่อไปได้

4) ลดแรงกระตุ้นหรือสิ่งยั่วยุที่มีอิทธิพลต่อการประกอบอาชญากรรม (Reduce Provocations) ได้แก่ การระบุและกำจัดสิ่งยั่วยุที่จะกระตุ้นให้บุคคลล่วงละเมิดทางเพศต่อเด็ก เช่น การลบทำลายสื่อลามกอนาจารเด็กไม่ว่าจะเป็นสื่อที่มีบุคคลจริงหรือสื่อเสมือนจริง (Virtual Child Sexual Abuse Material) หรือการบำบัดรักษาโรคใคร่เด็ก (Paedophilia) เพื่อป้องกันไม่ให้บุคคลที่มีแนวโน้มเป็นโรคดังกล่าวกระทำการล่วงละเมิดทางเพศต่อเด็ก

5) ขจัดข้อแก้ตัวสำหรับการประกอบอาชญากรรม (Remove Excuses) ได้แก่ การกำหนดกฎหมาย ประมวลจริยธรรม และนโยบายการให้บริการให้ชัดเจนว่าสิ่งใดสามารถกระทำได้หรือไม่ได้ พร้อมกำหนดบทลงโทษและผลกระทบที่จะได้รับตามมาอย่างชัดเจนหากมีการล่วงละเมิดทางเพศต่อเด็ก

การป้องกันอาชญากรรมตามสถานการณ์ได้ถูกนำมาเป็นกรอบแนวคิดสำหรับการป้องกันอาชญากรรมทางเทคโนโลยี โดย Ekblom (2017, p.355) ได้อธิบายว่า เหตุอาชญากรรมเกิดขึ้นก็ต่อเมื่ออาชญากรซึ่งมีความพร้อมและมีเจตนาในการกระทำความผิดโดยปราศจากทรัพยากรที่จะทำให้ตนหลีกเลี่ยงหรืองดเว้นการกระทำความผิดนั้น ทำการคัดเลือกเหยื่อซึ่งมีความเปราะบางและเสี่ยงต่อการตกเป็นเหยื่ออาชญากรรมในสภาพแวดล้อมซึ่งไม่มีความมั่นคงปลอดภัยและเอื้ออำนวยต่อการกระทำความผิดโดยปราศจากผู้ดูแลคุ้มครองที่เหมาะสม ซึ่งหมายถึงสภาพแวดล้อมของโลกออนไลน์หรืออินเทอร์เน็ต ในทางกลับกัน หากมีมาตรการในการป้องกันคุ้มครองที่เหมาะสมแล้ว อาชญากรก็จะไม่เลือกกระทำความผิด เนื่องจากผลตอบแทนที่จะได้รับนั้นไม่คุ้มค่ากับความพยายามและความเสี่ยง อาชญากรรมจึงไม่เกิดขึ้น ดังนั้น การใช้เทคโนโลยีในการป้องกันยับยั้งปัจจัยและโอกาสในการเกิดอาชญากรรมบนโลกอินเทอร์เน็ตจึงมีความสำคัญ ด้วยเหตุปัจจัยด้านการเปลี่ยนแปลงของสภาพแวดล้อมทางกายภาพเป็นสภาพแวดล้อมแห่งข้อมูลข่าวสารและระบบความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

2. รูปแบบการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ตที่สำคัญ

สำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (United Nations Office on Drugs and Crime: UNODC) ได้แบ่งประเภทของการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต ซึ่งจำแนกตามการบัญญัติกฎหมายของประเทศส่วนใหญ่ในโลกที่กำหนดให้การกระทำต่อไปนี้เป็นความผิดเกี่ยวกับการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต (UNODC, 2020) ได้แก่

2.1 การตระเตรียมเด็กสำหรับการล่วงละเมิดทางเพศออนไลน์ (Online Grooming)

การตระเตรียมเด็กสำหรับการล่วงละเมิดทางเพศออนไลน์ หมายถึง การกระทำของผู้ใหญ่ซึ่งเป็นการสร้างปฏิสัมพันธ์และความไว้เนื้อเชื่อใจกับเด็กผ่านการสื่อสารทางอินเทอร์เน็ต โดยมีวัตถุประสงค์เพื่อการล่วงละเมิดทางเพศ ไม่ว่าจะในรูปแบบออนไลน์หรือออฟไลน์ก็ตาม โดยผู้กระทำความผิดอาจเริ่มจากการคัดเลือกเหยื่อซึ่งเป็นเด็กตามสื่อสังคมออนไลน์ ซึ่งบุคคลเหล่านี้ถือเป็นกลุ่มเปราะบาง ง่ายต่อการเข้าถึง และเป็นผู้ที่มีโอกาสจะหลงเชื่อบุคคลได้ง่าย เช่น บัญชีสื่อสังคมออนไลน์ของเด็กที่อนุญาตให้ทุกคนสามารถเข้าถึงข้อมูลส่วนตัวและความเคลื่อนไหวได้ (Visible to the Public) เป็นต้น จากนั้นก็จะทำการติดต่อไปยังเด็กเพื่อพูดคุยสร้างปฏิสัมพันธ์และความไว้เนื้อเชื่อใจในห้องสนทนา (Chatroom) จนเกิดการล่วงละเมิดทางเพศในที่สุด

พฤติกรรมการก่อเหตุมักเริ่มจากการศึกษาข้อมูลส่วนตัวของเด็กเพื่อเริ่มต้นการสนทนาด้วยการนำเข้าสู่เรื่องที่เด็กสนใจ เช่น งานอดิเรก เกมที่ชื่นชอบ ดาราที่ชื่นชอบ หรือสถานภาพทางเศรษฐกิจ เป็นต้น หลังจากนั้นจะเป็นการใช้ถ้อยคำหรือข้อความเพื่อสานความสัมพันธ์ในเชิงฉันท์ชู้สาวจนนำไปสู่การร้องขอให้มีกิจกรรมทางเพศ เช่น การส่งภาพหรือวิดีโออันมีลักษณะลามกอนาจาร เป็นต้น (Winters & Jeglic, 2017) ซึ่งในเวลาต่อมาอาชญากรก็จะข่มขู่และควบคุมให้เด็กซึ่งตกเป็นผู้เสียหายส่งสื่ออิเล็กทรอนิกส์ในลักษณะดังกล่าวเพิ่มขึ้นอย่างต่อเนื่อง โดยอาจข่มขู่ว่าจะเผยแพร่ส่งต่อสื่อนั้นไปยังพื้นที่สาธารณะหรือบุคคลในครอบครัวหากเด็กไม่ยินยอมส่งให้แก่ตน หรืออาจจะนำไปสู่การข่มขู่ให้เด็กมีเพศสัมพันธ์กับตนในทางกายภาพได้ อย่างไรก็ตาม ในปัจจุบันประเทศไทยยังไม่มีกฎหมายที่กำหนดให้

การตระเตรียมเด็กสำหรับการล่วงละเมิดทางเพศออนไลน์เป็นความผิด แต่ได้มีการนำเสนอให้มีการบัญญัติให้การกระทำดังกล่าวเป็นความผิดตามกฎหมายป้องกันและปราบปรามการกระทำผิดต่อเด็กและเยาวชนโดยใช้สื่อออนไลน์ ซึ่งอยู่ในระหว่างการพิจารณายกร่างกฎหมายเพื่อแทรกบทบัญญัติดังกล่าวเพิ่มเติมเข้าไปในประมวลกฎหมายอาญา

2.2 การผลิต ครอบครอง และเผยแพร่สื่อลามกอนาจารเด็ก (Production, Possession, and Distribution of Child Sexual Abuse Material)

ความผิดเกี่ยวกับการผลิต ครอบครอง และเผยแพร่สื่อลามกอนาจารเด็กได้ถูกบัญญัติให้เป็นความผิดในกฎหมายของหลายประเทศทั่วโลก โดยได้ถูกบัญญัติไว้ในประมวลกฎหมายอาญาของไทยตั้งแต่ปี พ.ศ. 2558 ตามพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 24) พ.ศ. 2558 ซึ่งได้บัญญัติความผิดเกี่ยวกับการครอบครองและส่งต่อสื่อลามกอนาจารเด็ก เพื่อแสวงหาประโยชน์ในทางเพศสำหรับตนเองหรือผู้อื่นไว้ในมาตรา 287/1 และความผิดเกี่ยวกับการทำ ผลิต มีไว้ นำเข้า หรือส่งออกนอกราชอาณาจักร หรือทำให้แพร่หลายซึ่งสื่อลามกอนาจารเด็ก เพื่อความประสงค์ทางการค้าหรือแจกจ่ายแก่ประชาชนไว้ในมาตรา 287/2 อนุมาตรา (1) ถึง (3) โดยกำหนดโทษจำคุกสูงสุดไม่เกิน 10 ปี และปรับสูงสุดไม่เกิน 200,000 บาท นอกจากนี้ยังมีการบัญญัติความผิดเกี่ยวกับการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้ไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

การผลิตสื่อลามกอนาจารเด็ก หมายถึง การผลิตสื่อแสดงการล่วงละเมิดทางเพศด้วยวิธีการทางดิจิทัลหรืออิเล็กทรอนิกส์ ซึ่งรวมถึงสื่ออื่นที่เกี่ยวข้องกับเด็กซึ่งมีลักษณะลามกอนาจารไม่ว่าทั้งหมดหรือบางส่วน (UNODC, 2020) ส่วนการครอบครองและเผยแพร่สื่อลามกอนาจารเด็กมักเกิดขึ้นบนช่องทางการสื่อสารต่าง ๆ เช่น อีเมล (Email) แอปพลิเคชันรับส่งข้อความ (Instant Messaging Applications) สื่อสังคมออนไลน์ (Social Media Platforms) หรือเครือข่ายเพียร์ทูเพียร์ (Peer-to-Peer Network) ซึ่งเปิดให้มีการแบ่งปันและดาวน์โหลดไฟล์อย่างกว้างขวางและรวดเร็ว ตลอดจนเว็บไซต์มืด (Dark Web) ซึ่งมีการปกปิดตัวตนของผู้ใช้งานสูงกว่าการใช้งานเว็บไซต์ทั่วไป (Surface Web)

2.3 การถ่ายทอดสดการล่วงละเมิดทางเพศต่อเด็กออนไลน์ (Livestreaming of Child Sexual Abuse)

การถ่ายทอดสดการล่วงละเมิดทางเพศต่อเด็กออนไลน์ หมายถึง การเผยแพร่การล่วงละเมิดทางเพศต่อเด็กแบบทันที (Real Time) ให้แก่ผู้ชมซึ่งอยู่ระยะไกลจากพื้นที่ที่มีการล่วงละเมิดทางเพศต่อเด็ก โดยมักเกิดขึ้นบนช่องทางการสื่อสารที่มีคุณลักษณะการใช้งานที่สามารถส่งสัญญาณภาพและเสียงพร้อมกันหรือวิดีโอคอล (Video Call) หรือการถ่ายทอดสด (Live) ได้ เช่น ไลน์ (Line) ติ๊กต็อก (TikTok) เอ็มไลฟ์ (MLive) หรือสไกป์ (Skype) เป็นต้น โดยผู้เข้าชมอาจต้องสมัครสมาชิกหรือมีค่าใช้จ่ายในการรับชมการล่วงละเมิดทางเพศต่อเด็กในกลุ่มลับ และสามารถบังคับหรือขอให้เด็กกระทำอนาจารตามสั่งการได้ในลักษณะคล้ายกับการท่องเที่ยวทางเพศในรูปแบบออนไลน์ (Webcam Child Sex Tourism) ซึ่งมักมีนายหน้าหรือผู้รับประโยชน์ซึ่งมิใช่เด็กอยู่เบื้องหลังในการจัดการให้เด็กถ่ายทอดสด โดยอาจมีการบันทึกการถ่ายทอดสดดังกล่าวไว้และนำไปแสวงหาประโยชน์จากการค้าหรือเผยแพร่สื่อดังกล่าวได้อีกทอดหนึ่ง ซึ่งผู้รับผลประโยชน์ที่บังคับให้เด็กถ่ายทอดสดอาจเป็นบุคคลในครอบครัวของเด็กเองด้วยเหตุผลทางด้านการเงิน โดยเฉพาะอย่างยิ่งในประเทศกำลังพัฒนาในภูมิภาคเอเชียตะวันออกเฉียงใต้ ซึ่งรวมถึงประเทศไทยด้วย (Internet Watch Foundation, 2020)

3. เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence)

เทคโนโลยีปัญญาประดิษฐ์เกิดขึ้นครั้งแรกเมื่อปี ค.ศ. 1950 โดยมีแนวคิดที่ว่าคอมพิวเตอร์จะสามารถเลียนแบบตรรกะเหมือนสมองของมนุษย์ได้ (Turing, 1950 as cited in Perrot, 2017) ซึ่งต่อมาก็ได้มีการพัฒนาซอฟต์แวร์และภาษาโปรแกรมคอมพิวเตอร์เพื่อแปลงตรรกะการวิเคราะห์เชิงเหตุผลของมนุษย์เป็นการเรียนรู้ของระบบคอมพิวเตอร์ โดยมีหลักการเรียนรู้ที่สำคัญ เช่น การเรียนรู้ของเครื่อง (Machine Learning) การเรียนรู้เชิงลึก (Deep Learning) ซึ่งพัฒนาเครือข่ายการเรียนรู้ในรูปแบบที่คล้ายกับระบบประสาทของมนุษย์ (Neural Networks) การประมวลผลภาษาธรรมชาติ (Natural Language Processing) และการเรียนรู้แบบเสริมกำลัง (Reinforcement Learning) โดยแนวทางการพัฒนาเทคโนโลยีสมัยใหม่ทำให้ระบบคอมพิวเตอร์สามารถเรียนรู้และจดจำข้อมูลจำนวนมหาศาลได้ในระยะเวลาอันสั้น ทั้งนี้ ธรรมชาติของปัญญาประดิษฐ์เกิดจากการลองผิดลองถูกกับโจทย์ปัญหาที่มนุษย์ป้อนข้อมูลนำเข้ามา หลังจากนั้นจึงเข้าสู่กระบวนการฝึกฝน เมื่อคอมพิวเตอร์ประมวลผลได้อย่างแม่นยำกับปัญหาทางคณิตศาสตร์ที่เคยมีการเรียนรู้มาแล้ว ขั้นตอนต่อไปคือการป้อนข้อมูลที่เต็มไปด้วยโจทย์ใหม่ที่คอมพิวเตอร์ยังไม่เคยประมวลผลมาก่อน เมื่อคอมพิวเตอร์เรียนรู้ข้อมูลใหม่จากฐานความรู้ที่ฝึกฝนกับชุดข้อมูลเก่ามาอย่างดี ขั้นตอนนี้จึงก่อให้เกิดการเรียนรู้ว่าการกระทำใดดีหรือไม่ดี คล้ายกับการจำแนกคำตอบถูกหรือผิดแบบไบนารี (Binary) ซึ่งตัวอย่างนี้เรียกว่าหลักการเรียนรู้จำแนก (Classification Technique) และกระบวนการสุดท้ายจะเป็นการตัดสินใจเลือกกระทำในสิ่งที่เกิดประโยชน์สูงสุดต่อกิจกรรมนั้น จนกระทั่งสามารถพัฒนาตนเองให้เหนือกว่ามนุษย์ได้ เช่นกรณีของบอท AlphaGo ซึ่งสามารถเอาชนะเกมหมากล้อมในการแข่งขันกับแชมป์โลกได้ เป็นต้น (Perrot, 2017)

เทคโนโลยีปัญญาประดิษฐ์ได้ถูกนำมาใช้ในการป้องกันปราบปรามอาชญากรรมในหลากหลายรูปแบบ เช่น การตรวจจับพฤติกรรมของบุคคลต้องสงสัยผ่านกล้องวงจรปิด รวมถึงการระบุตัวตนของบุคคลที่ปรากฏในกล้องวงจรปิดด้วยระบบจดจำใบหน้า (Facial Recognition) นอกจากนี้ยังมีการใช้ปัญญาประดิษฐ์ในการตรวจจับและวิเคราะห์เสียงปืน (Gunshot Detection and Analysis) ซึ่งสามารถช่วยระบุตำแหน่งของจุดที่มีการยิงปืนและชนิดของอาวุธปืนได้ ยิ่งไปกว่านั้นยังรวมถึงการพยากรณ์การเกิดอาชญากรรมในพื้นที่ (Crime Prediction) โดยวิเคราะห์ความสัมพันธ์ระหว่างจำนวนเหตุอาชญากรรมกับช่วงเวลาและสถานที่ด้วยการวิเคราะห์ข้อมูลจากหลายแหล่ง และการพยากรณ์อัตราการกระทำความผิดซ้ำของบุคคลพ้นโทษ ซึ่งตัวอย่างดังกล่าวนี้ทำให้การนำปัญญาประดิษฐ์ไปใช้ในงานรักษาความปลอดภัยสาธารณะได้รับความนิยมมากขึ้นอย่างต่อเนื่อง ในขณะเดียวกัน เทคโนโลยีปัญญาประดิษฐ์ก็ได้ถูกนำมาใช้ในการตรวจจับสื่อหรือเนื้อหาซึ่งเกี่ยวข้องกับการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ตด้วยเช่นกัน เพื่อจำแนกว่าสื่อหรือเนื้อหาใดไม่เหมาะสมและก่อให้เกิดความเสี่ยงต่อการล่วงละเมิดทางเพศต่อเด็ก

3.1 การนำปัญญาประดิษฐ์มาใช้ในการป้องกันการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต

Bracket Foundation (2019) ได้จำแนกเทคโนโลยีที่ใช้ในการป้องกันปราบปรามการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ตไว้ 3 ประเภท ซึ่งทำหน้าที่เป็นเครื่องมือในการช่วยเหลือเจ้าหน้าที่ผู้บังคับใช้กฎหมาย รวมถึงผู้ให้บริการอินเทอร์เน็ตและช่องทางการสื่อสารออนไลน์ในการคัดกรองและตรวจจับเนื้อหาหรือสื่อที่มีความเสี่ยงต่อการล่วงละเมิดทางเพศต่อเด็กบนโลกออนไลน์แบบอัตโนมัติ โดยอาศัยการพัฒนาการเรียนรู้ด้วยเทคโนโลยีปัญญาประดิษฐ์เพื่อเพิ่มประสิทธิภาพในการทำงานและประมวลผลอย่างรวดเร็ว ได้แก่

1) การวิเคราะห์ภาพด้วยปัญญาประดิษฐ์ (Computer Vision AI)

Computer Vision AI เป็นเทคโนโลยีปัญญาประดิษฐ์ที่ทำการฝึกระบบคอมพิวเตอร์ให้สามารถวิเคราะห์และจำแนกภาพและวิดีโอได้อย่างรวดเร็ว โดยมีพื้นฐานการเรียนรู้แบบ Deep Learning ซึ่งถือเป็นวิวัฒนาการของการคัดแยกสื่อแสดงการล่วงละเมิดทางเพศต่อเด็กแบบเดิม ซึ่งใช้วิธีการวิเคราะห์ภาพ (Image Analytics) ด้วยข้อมูลเมตาดาต้า (Metadata) ของไฟล์และการคำนวณค่าแฮช (Hashes) ที่แสดงความเป็นอัตลักษณ์ของไฟล์ (Sangtongdee et al., 2020) ซึ่งอาจจำเป็นต้องอาศัยมนุษย์ในการช่วยวิเคราะห์ในบางขั้นตอน แต่ Computer Vision AI เป็นระบบที่ทำงานโดยอัตโนมัติซึ่งมีขั้นตอนวิธี (Algorithm) ในการเรียนรู้และประมวลผลผ่านฐานข้อมูลสื่อแสดงการล่วงละเมิดทางเพศต่อเด็ก โดยจะสามารถคัดแยกประเภทของสื่อรูปภาพและวิดีโอได้ (Image Classification) แบบเรียลไทม์ (Real Time) ด้วยการจำแนกว่าเป็นสื่อแสดงการล่วงละเมิดทางเพศต่อเด็กหรือไม่ และจำแนกช่วงอายุของเด็กที่ปรากฏอยู่ในสื่อนั้น ตลอดจนเชื่อมโยงการทำงานกับเทคโนโลยีการวิเคราะห์ภาพแบบโฟโต้ดีเอ็นเอ (PhotoDNA) ซึ่งมีประสิทธิภาพในการจับคู่ค่าแฮชที่ตรงกันระหว่างไฟล์สื่อที่ต้องสงสัยกับฐานข้อมูลสื่อแสดงการล่วงละเมิดทางเพศต่อเด็กของหน่วยงานบังคับใช้กฎหมาย (Sangtongdee et al., 2020; Council of Europe, 2021) นอกจากนี้ยังมีระบบการจดจำและวิเคราะห์ภาพใบหน้า ข้อมูลทางชีวภาพ หรือวัตถุ (Facial, Biometric, and Object Recognition) เพื่อเปรียบเทียบสื่อที่ต้องสงสัยกับสื่อที่มีอยู่ในฐานข้อมูล เช่น การเปรียบเทียบภาพใบหน้าของคนร้ายหรือผู้เสียหาย ตลอดจนการเปรียบเทียบสถานที่ที่ปรากฏอยู่ในสื่อ เช่น สภาพแวดล้อมภายในห้อง ซึ่งอาจนำไปสู่การระบุสถานที่เกิดเหตุหรือแหล่งที่อยู่ของคนร้ายหรือผู้เสียหายได้ เป็นต้น

2) การประมวลผลภาษาธรรมชาติและการวิเคราะห์เสียงด้วยปัญญาประดิษฐ์ (Natural Language Processing and Voice AI)

Natural Language Processing (NLP) เป็นเทคโนโลยีปัญญาประดิษฐ์ที่ทำการฝึกระบบคอมพิวเตอร์ให้สามารถเข้าใจและตีความภาษาปกติที่มนุษย์ใช้ในการสื่อสารได้ ซึ่งเป็นวิวัฒนาการที่พัฒนามาจากการวิเคราะห์ข้อมูลเชิงอักษรและจินตภาพ (Text and Visual Analytics) เช่น การวิเคราะห์รายการคำสำคัญหรือศัพท์เฉพาะกลุ่ม (Keywords) ที่ใช้ในการค้นหาสื่อลามกอนาจารเด็ก รวมถึงการสร้างความสัมพันธ์ของข้อมูลด้วยแผนผังความเชื่อมโยง (Data Visualisation and Mapping) เพื่อหาความเชื่อมโยงระหว่างบุคคลและสถานที่ โดยเทคโนโลยี NLP นี้จะเริ่มจากการใช้ Algorithm ในการสกัดคำสำคัญ (Keywords) รูปแบบโครงสร้างประโยค (Syntax) และการตีความหมาย (Semantics) เพื่อทำความเข้าใจและจำแนกข้อมูลเชิงอักษร ตลอดจนแจ้งเตือนการตรวจพบเนื้อหาข้อความที่มีลักษณะการใช้ภาษาส่อไปในทางลามกอนาจาร นอกจากนั้น NLP ยังมีการเรียนรู้และฝึกฝนเพื่อโต้ตอบหรือสนทนากับมนุษย์ด้วยการเลียนแบบลักษณะการพูดคุยกันผ่านข้อความของมนุษย์ โดยแชทบอท (Chatbot) เป็นเครื่องมือหนึ่งซึ่งใช้เทคโนโลยี NLP เข้าไปแฝงตัวและมีปฏิสัมพันธ์กับผู้กระทำความผิดในห้องสนทนาหรือกลุ่มลับตามช่องทางการสื่อสารออนไลน์ เพื่อรวบรวมพยานหลักฐานหรือแจ้งเตือนป้องปรามไม่ให้มีการกระทำความผิดเกิดขึ้น

นอกจากนี้ เทคโนโลยีการจดจำและวิเคราะห์เสียงและคำพูด (Speech Recognition and Voice Analytics) ก็ได้ถูกนำมาใช้ในการป้องกันปราบปรามการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต โดยทำการประมวลผลและระบุอัตลักษณ์ของบุคคลจากเสียงพูด เพื่อช่วยระบุตัวตนของบุคคลที่ปรากฏอยู่

ภายในสื่อ ได้แก่ ผู้เสียหายซึ่งรอรับการคุ้มครองช่วยเหลือ และผู้กระทำความผิดสำหรับการติดตามจับกุมและดำเนินคดีตามกฎหมาย

3) ปัญญาประดิษฐ์เชิงทำนายสำหรับการคาดการณ์หรือพยากรณ์ (Predictive AI)

เทคโนโลยีนี้มีวิวัฒนาการมาจากการวิเคราะห์เชิงทำนายโดยใช้เครื่องข่ายความเชื่อมโยงของข้อมูล (Network and Predictive Analytics) ซึ่งปัญญาประดิษฐ์เชิงทำนายจะใช้ Algorithm ในการสร้างรูปแบบจำลองเพื่อคาดการณ์เหตุการณ์ในอนาคต (Predictive Modelling) โดยการอนุมานจากข้อมูลหรือเหตุการณ์ที่เกิดขึ้นในอดีตด้วยการวิเคราะห์เชิงสถิติเพื่อหารูปแบบและแนวโน้มของเหตุการณ์ที่จะเกิดขึ้นในอนาคต ทั้งนี้ อาจมีการทำเหมืองข้อมูล (Data Mining) เพื่อวิเคราะห์ข้อมูลจำนวนมากหรือบิ๊กดาต้า (Big Data) สำหรับการทำนายรูปแบบและแนวโน้มของข้อมูลที่มีความสัมพันธ์เชื่อมโยงกัน ซึ่งในการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ตอาจเป็นการวิเคราะห์รูปแบบและแนวโน้มของพฤติกรรมหรือการสนทนาที่นำไปสู่การล่วงละเมิดทางเพศต่อเด็ก โดยวิเคราะห์ปฏิสัมพันธ์ที่เกิดขึ้นระหว่างบัญชีสื่อสังคมออนไลน์และข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ทั้งในเว็บไซต์ทั่วไปและเว็บไซต์มืด (Dark Web)

นอกจากการวิเคราะห์รูปแบบและแนวโน้มของเหตุการณ์ในอนาคตแล้ว ปัญญาประดิษฐ์เชิงทำนายยังทำหน้าที่แจ้งเตือนถึงความเสี่ยงของข้อมูลที่อาจจะนำไปสู่การล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ตได้ โดยการฝึกระบุระดับความเสี่ยงของเนื้อหาหรือข้อมูลที่ปรากฏอยู่ในช่องทางการสื่อสารออนไลน์ และมีการปรับปรุงความแม่นยำของการทำนายอย่างต่อเนื่องโดยอัตโนมัติจากการวิเคราะห์ข้อมูลที่เข้ามาใหม่ตลอดเวลา ซึ่งถือเป็นหนึ่งในเครื่องมือพยากรณ์อาชญากรรมสำหรับการบังคับใช้กฎหมาย (Predictive Policing Tools) เพื่อช่วยระบุบุคคลที่มีแนวโน้มจะล่วงละเมิดทางเพศต่อเด็กหรือบุคคลที่มีความเสี่ยงต่อการตกเป็นผู้เสียหาย ตลอดจนช่องทางการสื่อสารออนไลน์ซึ่งถือเป็นสถานที่เกิดเหตุที่มีความเสี่ยงต่อการล่วงละเมิดทางเพศต่อเด็กอีกด้วย

3.2 ตัวอย่างการนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ในการป้องกันปราบปรามการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต

1) โครงการอะราคนิด (Project Arachnid) ซึ่งเกิดขึ้นในปี ค.ศ. 2016 โดยศูนย์คุ้มครองป้องกันเด็กแห่งแคนาดา (Canadian Centre for Child Protection) โดยการนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ในการสำรวจเว็บไซต์ (Crawling) ที่มีเนื้อหาเสี่ยงต่อการล่วงละเมิดทางเพศต่อเด็กและทำการประมวลผลสื่อออนไลน์ด้วยความรวดเร็ว เพื่อจับคู่สื่อที่ต้องสงสัยกับฐานข้อมูลสื่อแสดงการล่วงละเมิดทางเพศต่อเด็กที่มีอยู่ ซึ่งหากตรวจพบก็จะทำการรายงานไปยังผู้ให้บริการเพื่อลบทำลายอย่างรวดเร็ว โดยพบว่า นับตั้งแต่ปี 2016 จนถึงปัจจุบัน โครงการดังกล่าวได้ทำการประมวลผลสื่อออนไลน์ไปแล้วมากกว่า 129 พันล้านสื่อ และตรวจพบสื่อต้องสงสัยใหม่เป็นจำนวนมากกว่า 100,000 สื่อต่อเดือน (Council of Europe, 2021)

2) มูลนิธิเฝ้าระวังทางอินเทอร์เน็ต (Internet Watch Foundation: IWF) ได้มีการใช้เทคโนโลยีปัญญาประดิษฐ์ในการเพิ่มศักยภาพการประมวลผลสำหรับการคัดกรองสื่อออนไลน์ที่มีการล่วงละเมิดทางเพศต่อเด็กบนเว็บไซต์และกลุ่มสนทนา (Newsgroups) โดยสามารถจำแนกได้ว่าสื่อใดเป็นสื่อแสดงการล่วงละเมิดทางเพศต่อเด็กหรือไม่ และจัดอยู่ในประเภทใด ซึ่งได้แก่ ประเภท (Category) A, B, และ C ตามลำดับ ซึ่งจำแนกตามระดับความรุนแรงของการกระทำในสื่อแสดงการล่วงละเมิดทางเพศต่อเด็ก (Internet Watch Foundation, 2020) นอกจากนี้ยังได้มีการพัฒนาแชทบอท (IWF Rethink Chatbot) เพื่อช่วยหยุดยั้งกระบวนการล่วงละเมิดทางเพศต่อเด็กด้วยการแจ้งเตือนผู้ใช้งานที่มีความสนใจในสื่อลามกอนาจารเด็กหรือมีแนวโน้มในการใช้ข้อความที่สื่อไปในลักษณะการตระเตรียมเด็กเพื่อประโยชน์ทางเพศ

(Grooming) ในแอปพลิเคชันที่ให้บริการห้องสนทนา โดยมีระบบโต้ตอบด้วยข้อความอัตโนมัติกับผู้ใช้งาน เพื่อเสนอแนวทางการให้ความช่วยเหลือไม่ให้กลายเป็นผู้กระทำความผิดเกี่ยวกับการล่วงละเมิดทางเพศต่อเด็กออนไลน์ ซึ่งแชทบอทลักษณะนี้ถือเป็นเครื่องมือหนึ่งในการต่อต้านการตระเตรียมเด็กออนไลน์สำหรับการล่วงละเมิดทางเพศ (Anti-Grooming Tool)

3) สปอตไลท์ (Spotlight) เป็นเครื่องมือที่ถูกพัฒนาขึ้นโดยองค์กรไม่แสวงหาผลกำไรธอร์น (Thorn) ซึ่งมีจุดมุ่งหมายในการร่วมมือกับหน่วยงานบังคับใช้กฎหมายในการป้องกันปราบปรามการค้ามนุษย์ (Human Trafficking) โดยเฉพาะอย่างยิ่งในรูปแบบของการแสวงหาประโยชน์จากสื่อลามกอนาจารเด็ก ซึ่งเริ่มต้นจากการพัฒนาการเรียนรู้ของระบบโดยเทคโนโลยีปัญญาประดิษฐ์ในการตรวจจับโฆษณาที่เกี่ยวข้องกับการล่วงละเมิดทางเพศต่อเด็ก และพัฒนาระบบการระบุตัวตนของผู้เสียหาย (Victim Identification) ด้วยการเรียนรู้แบบ Deep Learning ร่วมกับแอมะซอนดอทคอม (Amazon.com) เพื่อช่วยติดตามและให้ความช่วยเหลือแก่เด็กได้อย่างรวดเร็ว

4) มายซิส (MySis) เป็นแชทบอทของไทยซึ่งถูกพัฒนาร่วมกันโดยหน่วยงานหลายภาคส่วน โดยทำงานอยู่บนเฟซบุ๊กเมสเซ็นเจอร์ (Facebook Messenger) ซึ่งทำหน้าที่สื่อสารโต้ตอบกับผู้ใช้งานแบบอัตโนมัติ เพื่อให้ความช่วยเหลือผู้เสียหายที่อยู่ในกลุ่มเปราะบาง เช่น เด็กและสตรี ในการแจ้งเหตุเบาะแส หรือการดำเนินการทางกฎหมาย โดยเฉพาะอย่างยิ่งในคดีเกี่ยวกับความรุนแรงในครอบครัว ตลอดจนคดีเกี่ยวกับเด็กและสตรี เพื่อเปิดช่องทางให้ผู้เสียหายได้รับการดูแลคุ้มครองอย่างเหมาะสม ทั้งนี้ MySis จะช่วยลดการถูกกระทำหรือการตกเป็นเหยื่อซ้ำ (Revictimisation) จากการดำเนินการของเจ้าหน้าที่ในกระบวนการยุติธรรมที่อาจจะไม่เหมาะสมกับกลุ่มเปราะบาง และเปิดโอกาสให้ผู้เสียหายบอกเล่าประสบการณ์หรือข้อเท็จจริงในคดีได้อย่างสบายใจมากขึ้น ซึ่งในอนาคตแชทบอทดังกล่าวนี้จะมีการพัฒนาการเรียนรู้โดยอาศัยการประมวลผลแบบ NLP และการจดจำและวิเคราะห์เสียง (Voice Recognition) เพื่อทำให้แชทบอทสามารถสื่อสารกับมนุษย์ได้อย่างชาญฉลาดและเป็นธรรมชาติยิ่งขึ้น ซึ่งจะทำให้ผู้เสียหายสามารถเข้าถึงกระบวนการยุติธรรมได้มากขึ้นเช่นกัน (Kongsuwan, 2021)

บทวิเคราะห์

จากทฤษฎีการป้องกันอาชญากรรมเชิงสภาพแวดล้อมและการนำเทคโนโลยีปัญญาประดิษฐ์มาใช้ในการป้องกันการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต สามารถวิเคราะห์ได้ตามระดับการป้องกันอาชญากรรมตามรูปแบบการป้องกันและควบคุมโรคทางสาธารณสุข ซึ่งผู้เขียนจะอธิบายโดยเปรียบเทียบอย่างง่ายระหว่างระดับการป้องกันการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ตกับการป้องกันการแพร่ระบาดของเชื้อไวรัสโคโรนา 2019 (COVID-19) ในปัจจุบัน ซึ่งองค์การอนามัยโลก (World Health Organisation: WHO) ได้วางแนวทางไว้ 3 ระดับ (Hassad, 2020) โดยมีรายละเอียดดังนี้

1) การป้องกันโรคระดับปฐมภูมิ ซึ่งมีความสำคัญที่สุด ได้แก่ การให้ความรู้ความเข้าใจด้านการป้องกันตนเองจากโรคติดต่ออันตราย เช่น การสวมหน้ากากอนามัย การเว้นระยะห่างทางสังคม (Social Distancing) รวมถึงการเสริมสร้างความตระหนักรู้ถึงความร้ายแรงจากการติดเชื้อ COVID-19 นอกจากนี้ การให้วัคซีนแก่ประชาชนเพื่อเสริมสร้างภูมิคุ้มกันต่อโรคยังถือเป็นการป้องกันโรคระดับปฐมภูมิที่สำคัญไม่น้อยไปกว่าการให้ความรู้ความเข้าใจในการป้องกันโรค ซึ่งจำเป็นต้องดำเนินการควบคู่กันไป

ดังนั้น การป้องกันอาชญากรรมระดับปฐมภูมิ (Primary Crime Prevention) จึงหมายถึงการป้องกันอาชญากรรมก่อนเกิดเหตุโดยคำนึงถึงปัจจัยและสาเหตุของโอกาสที่จะส่งผลต่อการเกิด

อาชญากรรม และใช้มาตรการในการป้องกันไม่ให้เกิดปัจจัยดังกล่าวขึ้น ซึ่งก็จะทำให้ไม่มีโอกาสในการเกิดอาชญากรรม เช่น การออกแบบการให้บริการระบบที่มีความปลอดภัยต่อการใช้งาน รวมถึงการให้ความรู้ความเข้าใจและทักษะเกี่ยวกับการใช้งานเทคโนโลยีดิจิทัล (Digital Literacy) แก่ผู้ปกครอง ตลอดจนเด็กและเยาวชนที่ใช้งานอินเทอร์เน็ตให้มีความตระหนักรู้ถึงภัยคุกคามออนไลน์และการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต รวมถึงการสร้างเครือข่ายเฝ้าระวังภัยจากการล่วงละเมิดทางเพศต่อเด็กในสภาพแวดล้อมไซเบอร์ (Quayle & Koukopoulos, 2019) ซึ่งถือเป็นวัคซีนสำคัญที่จะป้องกันไม่ให้เด็กตกเป็นเหยื่อการล่วงละเมิดทางเพศ และเป็นการป้องกันอาชญากรรมโดยการเพิ่มความยากลำบากและความเสี่ยงในการประกอบอาชญากรรมด้วยการเพิ่มภูมิคุ้มกันของเป้าหมาย (Target Hardening) โดยมีตัวอย่างการเผยแพร่ความรู้ที่น่าสนใจ ได้แก่ คู่มือการป้องกันตนเองจากการล่วงละเมิดทางเพศแบบโต้ตอบออนไลน์ได้ (Interactive Handbook) ซึ่งจัดทำขึ้นโดยโครงการฮัก ภายใต้มูลนิธิสานสัมพันธ์ครอบครัว (Hug Project Thailand) ที่มีการใช้งานในรูปแบบที่เป็นมิตรกับเด็ก (Child Friendly) และเปิดโอกาสให้ผู้ใช้งานโต้ตอบหรือเลือกสถานการณ์ได้ ตลอดจนแชทบอท MySis ที่ใช้ปัญญาประดิษฐ์ในการสนทนากับผู้ใช้งานซึ่งสามารถขอคำปรึกษาและแจ้งเหตุได้อย่างเหมาะสม

นอกจากนี้ เทคโนโลยีปัญญาประดิษฐ์ยังมีบทบาทในการตรวจจับเนื้อหาหรือข้อความที่มีความเสี่ยงต่อการล่วงละเมิดทางเพศต่อเด็ก เช่น การวิเคราะห์ข้อความสนทนาในแอปพลิเคชันสนทนาเพื่อตรวจจับถ้อยคำที่มีแนวโน้มเป็นการชักจูงหรือเชิญชวนให้มีกิจกรรมทางเพศ เพื่อป้องกันการตระเตรียมเด็กเพื่อล่วงละเมิดทางเพศ (Grooming) นอกจากนี้ การพยากรณ์ด้วย Predictive AI จะสามารถช่วยวิเคราะห์ช่องทางการสื่อสารที่มีความเสี่ยงต่อการล่วงละเมิดทางเพศต่อเด็ก เพื่อที่จะได้เฝ้าระวังและประกาศแจ้งเตือนหรือป้องปรามไม่ให้มีการเกิดเหตุขึ้น เช่น แอปพลิเคชันหาคู่รัก (Dating Applications) หรือสื่อสังคมออนไลน์ประเภทอื่น รวมถึงการตรวจจับพฤติกรรมการเข้าถึงเว็บไซต์สื่อลามกอนาจารเด็กของผู้ใช้งานที่อาจเป็นโรคใคร่เด็ก (Paedophilia) เพื่อเสนอการให้ความช่วยเหลือและแนะแนวทางการบำบัดรักษาโรคก่อนที่จะมีการกระทำความผิดต่อเด็กเกิดขึ้น ดังเช่นโครงการ Dunkelfeld ในประเทศเยอรมนี ซึ่งเปิดโอกาสให้บุคคลที่มีโรคใคร่เด็กเข้ารับการรักษาหากมีพฤติกรรมการบริโภคสื่อลามกอนาจารเด็กเป็นจำนวนมากแต่ยังไม่มีการล่วงละเมิดเด็ก โดยไม่ต้องเข้าสู่กระบวนการยุติธรรม (Beier, 2016) อันเป็นการลดแรงกระตุ้นหรือความต้องการทางเพศซึ่งเป็นปัจจัยในการล่วงละเมิดทางเพศต่อเด็ก

2) การป้องกันโรคระดับทุติยภูมิ ได้แก่ การตรวจคัดกรองโรค (Screening) หรือการตรวจค้นหาผู้ป่วยเชิงรุก (Proactive Case Finding) เพื่อระบุบุคคลที่ติดเชื้อและจำกัดพื้นที่การแพร่กระจายของเชื้อไม่ให้เกิดวงกว้าง รวมถึงการกักตัว (Self-Quarantine) เพื่อเฝ้าระวังอาการ สำหรับบุคคลกลุ่มเสี่ยงที่มีประวัติการสัมผัสกับบุคคลที่ติดเชื้อ กล่าวคือ การป้องกันโรคระดับทุติยภูมินี้เป็นการลดพื้นที่ในการแพร่กระจายของเชื้อ ซึ่งเปรียบเสมือนกับการลดการแพร่กระจายของเนื้อหาที่ไม่เหมาะสมที่จะนำไปสู่การล่วงละเมิดทางเพศต่อเด็กบนโลกออนไลน์

ดังนั้น การป้องกันอาชญากรรมระดับทุติยภูมิ (Secondary Crime Prevention) จึงหมายถึงความสามารถในการตรวจจับหรือระบุได้อย่างรวดเร็วว่ามีพฤติการณ์ที่มีแนวโน้มต่อการเกิดอาชญากรรมในสภาพแวดล้อม ซึ่งในกรณีของการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต อาจเป็นการตรวจค้นหาพฤติการณ์ที่มีความเสี่ยงต่อการตกเป็นผู้เสียหายของเด็กผู้ใช้งานอินเทอร์เน็ตให้ได้อย่างรวดเร็ว (Early Detection) (Quayle & Koukopoulos, 2019) ได้แก่ การใช้เทคโนโลยีปัญญาประดิษฐ์ในการตรวจจับเนื้อหาที่ไม่เหมาะสมหรือมีความเสี่ยงต่อการล่วงละเมิดทางเพศต่อเด็ก เช่น การโพสต์รูปภาพเด็กที่มี

ลักษณะยั่วยุให้เกิดกามารมณ์บนสื่อสังคมออนไลน์ พร้อมข้อความเชิญชวนให้เข้ากลุ่มลับซึ่งต้องชำระค่าสมาชิก (Membership Fee) เพื่อบริโภคสื่อลามกอนาจารเด็กหรือร้องขอให้เด็กใช้สื่อสังคมออนไลน์ในการถ่ายทอดสด (Livestreaming) เพื่อแสดงกิจกรรมทางเพศแลกกับการได้รับผลประโยชน์จากการเข้าชม ซึ่งปัญญาประดิษฐ์จำเป็นต้องเรียนรู้การวิเคราะห์สื่อภาพและวิดีโอเพื่อคัดกรองเนื้อหาที่เหมาะสม ตลอดจนเรียนรู้ด้านนิติภาษาศาสตร์ (Forensic Linguistics) ในการวิเคราะห์ข้อความที่มีคำสำคัญ (Keywords) ที่เกี่ยวข้องกับการล่วงละเมิดทางเพศต่อเด็กซึ่งอาจเป็นกลุ่มคำศัพท์เฉพาะกลุ่มหรือสแลง เพื่อจะได้ทำการลบเนื้อหาที่ไม่เหมาะสมเหล่านั้น รวมถึงระงับบัญชีที่มีความเสี่ยงหรือลิงก์โฆษณา เพื่อลดการเข้าถึงสื่อแสดงการล่วงละเมิดทางเพศต่อเด็ก ซึ่งถือเป็นการลดแรงกระตุ้นหรือสิ่งยั่วยุที่มีอิทธิพลต่อการประกอบอาชญากรรม ตลอดจนลดผลตอบแทนที่จะได้รับจากการประกอบอาชญากรรมของผู้กระทำความผิดที่จะได้รับจากการใช้บัญชีสื่อสังคมออนไลน์ในการรับผลประโยชน์จากการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต

3) การป้องกันโรคระดับตติยภูมิ ได้แก่ การป้องกันไม่ให้ผู้ติดเชื้อมีอาการแย่ลงหรือเสียชีวิต ได้แก่ การรักษาโรคด้วยวิธีทางการแพทย์ รวมถึงการกักแยกตัวเพื่อรักษาอาการป่วยที่บ้านหรือชุมชน (Home/Community Isolation) สำหรับผู้ป่วยที่ไม่แสดงอาการหรือไม่มีอาการรุนแรง

การป้องกันอาชญากรรมระดับตติยภูมิ (Tertiary Crime Prevention) หมายถึง การดำเนินการหลังจากที่มีการกระทำความผิดเกิดขึ้นแล้ว ซึ่งได้แก่ การบังคับใช้กฎหมายเพื่อติดตาม จับกุม ดำเนินคดี และลงโทษแก่ผู้กระทำความผิด เพื่อป้องกันไม่ให้บุคคลนั้นกระทำความผิดซ้ำหรือสร้างความเสียหายต่อเหยื่อหรือบุคคลอื่นอีก ซึ่งมักจะมีความเกี่ยวข้องกับหน่วยงานในกระบวนการยุติธรรมทางอาญา ได้แก่ ตำรวจ อัยการ ศาล ราชทัณฑ์ รวมตลอดจนสถานบำบัดฟื้นฟูพฤตินิสัยและหน่วยงานที่ดำเนินมาตรการทางการเงิน เพื่อตรวจยึดผลประโยชน์ซึ่งได้มาจากการกระทำความผิด ซึ่งถือเป็นการลดผลตอบแทนที่ได้รับจากการประกอบอาชญากรรมและขจัดข้อแก้ตัวสำหรับการกระทำความผิด โดยปัญญาประดิษฐ์จะมีส่วนช่วยในด้านการระบุตัวตนของผู้กระทำความผิดและรายงานไปยังผู้บังคับใช้กฎหมาย นอกจากนี้จะต้องมีการบำบัดรักษาเด็กซึ่งเป็นผู้เสียหาย เพื่อช่วยเหลือคุ้มครองเด็กไม่ให้ตกเป็นเหยื่ออาชญากรรมซ้ำอีก และป้องกันไม่ให้กลายเป็นผู้กระทำความผิดเสียเองในอนาคตจากบาดแผลและความผิดปกติภายในจิตใจ โดยปัญญาประดิษฐ์สามารถช่วยตรวจวิเคราะห์สื่อทั้งจากใบหน้า เสียง หรือสภาพแวดล้อมของสถานที่เกิดเหตุเพื่อระบุตัวตนของผู้เสียหาย (Victim Identification) สำหรับการให้ความช่วยเหลืออย่างทันท่วงที ตลอดจนการลบทำลายสื่อแสดงการล่วงละเมิดทางเพศต่อเด็กเพื่อลดบาดแผลทางจิตใจของผู้เสียหาย (Završnik, 2020)

บทวิจารณ์

แม้เทคโนโลยีปัญญาประดิษฐ์จะมีส่วนช่วยในการป้องกันการล่วงละเมิดทางเพศต่อเด็กในหลากหลายมิติ แต่ผู้บังคับใช้กฎหมายจำเป็นต้องคำนึงถึงความสมดุลระหว่างการบังคับใช้กฎหมายและสิทธิส่วนบุคคล รวมถึงเสรีภาพในการแสดงความคิดเห็น (Freedom of Speech) ของผู้ใช้งานอินเทอร์เน็ต ซึ่งการใช้เทคโนโลยีปัญญาประดิษฐ์ในการตรวจจับเนื้อหาหรือข้อมูลโดยอัตโนมัตินั้นอาจส่งผลกระทบต่อความเป็นส่วนตัวหรือสิทธิส่วนบุคคลของผู้ใช้งานอินเทอร์เน็ตอย่างหลีกเลี่ยงไม่ได้ อย่างไรก็ตาม คณะกรรมการด้านสิทธิมนุษยชนแห่งสภาสหภาพยุโรปได้วางแนวทางการคุ้มครองสิทธิส่วนบุคคลของผู้ให้บริการอินเทอร์เน็ตและสื่อสังคมออนไลน์ไว้ แต่ไม่ได้จำกัดห้ามการใช้ปัญญาประดิษฐ์ในการตรวจจับ

เนื้อหาที่เกี่ยวข้องกับการล่วงละเมิดทางเพศต่อเด็กในสภาพแวดล้อมทางไซเบอร์ (Council of Europe, 2021) เนื่องจากเป็นประเด็นปัญหาสำคัญสำหรับทุกประเทศทั่วโลกที่ต้องให้การคุ้มครองและช่วยเหลือเด็ก ในขณะที่ยังต้องให้ความเคารพในสิทธิและข้อมูลส่วนบุคคลในระดับที่เหมาะสมตามหลักนิติธรรม (The Rule of Law)

นอกจากนี้ ความท้าทายด้านนิติภาษาศาสตร์ในการวิเคราะห์ข้อความบนสื่อสังคมออนไลน์ในการพัฒนาเครื่องมือในการตรวจจับข้อมูลที่มีความเสี่ยงต่อการล่วงละเมิดทางเพศต่อเด็กยังเป็นประเด็นที่สำคัญ โดยเฉพาะอย่างยิ่งภาษาไทย ซึ่งมีวิวัฒนาการทางภาษาอย่างรวดเร็วและเกิดคำศัพท์ใหม่ขึ้นตลอดเวลา จึงมีความจำเป็นที่จะต้องให้ปัญญาประดิษฐ์เรียนรู้ภาษาอย่างต่อเนื่องและสามารถตรวจจับการเลี่ยงใช้คำของผู้กระทำความผิดในรูปแบบที่ซับซ้อนได้ ตลอดจนการพัฒนาเทคโนโลยีการเข้ารหัส (Encryption Technologies) อาจทำให้เกิดความท้าทายในการวิเคราะห์ข้อมูลของปัญญาประดิษฐ์ด้วยเช่นกัน

ประการสุดท้าย ได้แก่ การนำข้อมูลที่ได้รับจากเทคโนโลยีปัญญาประดิษฐ์มาใช้เป็นพยานหลักฐานในคดีอาญา ควรคำนึงถึงหลักการรับฟังพยานหลักฐานเป็นสำคัญ โดยมีกรณีศึกษาที่น่าสนใจ ได้แก่ สวีทตี้ (Sweetie) ซึ่งเป็นแชทบอทในรูปร่างของเด็กหญิงชาวฟิลิปปินส์วัย 10 ขวบ ซึ่งสามารถรวบรวมข้อมูลที่เป็นพยานหลักฐานสำคัญซึ่งนำไปสู่ปฏิบัติการจับกุมผู้กระทำความผิด (Završnik, 2020) แต่มีข้อมูลบางส่วนที่ไม่สามารถรับฟังเป็นพยานหลักฐานในชั้นศาลได้ เนื่องจากเป็นพยานหลักฐานที่เกิดขึ้นหรือได้มาจากการล่อให้กระทำความผิด อันเป็นเหตุให้แชทบอทดังกล่าวถูกระงับการใช้งานไปในที่สุด

บทสรุปและข้อเสนอแนะ

เทคโนโลยีปัญญาประดิษฐ์มีบทบาทสำคัญในการป้องกันการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต เนื่องจากสามารถประมวลผลข้อมูลอย่างอัตโนมัติและสามารถเรียนรู้ได้รวดเร็วกว่ามนุษย์ตามพัฒนาการของเทคโนโลยี โดยบทความวิชาการนี้ได้นำเสนอแนวคิดเกี่ยวกับการป้องกันอาชญากรรมเชิงสภาพแวดล้อมซึ่งสามารถอธิบายหลักการทำงานของเทคโนโลยีปัญญาประดิษฐ์ในการป้องกันการล่วงละเมิดทางเพศต่อเด็กได้ โดยแบ่งระดับการป้องกันอาชญากรรมเป็น 3 ระดับ ได้แก่ 1) ระดับปฐมภูมิ ซึ่งเน้นการสร้างภูมิคุ้มกันแก่เด็กและเยาวชนไม่ให้ตกเป็นเหยื่ออาชญากรรม 2) ระดับทุติยภูมิ ซึ่งมุ่งเน้นการตอบสนองอย่างรวดเร็วของการตรวจจับและป้องกันพฤติกรรมที่มีความเสี่ยง และ 3) ระดับตติยภูมิ ซึ่งเป็นการดำเนินการกับผู้กระทำความผิดไม่ให้สร้างความเสียหายมากยิ่งขึ้นและป้องกันการกระทำความผิดซ้ำ ตลอดจนการฟื้นฟูเยียวยาความเสียหายที่เกิดขึ้นกับผู้เสียหายทั้งทางร่างกายและจิตใจ ซึ่งรวมถึงการใช้เทคโนโลยีปัญญาประดิษฐ์ในการตรวจค้นหาและลบทำลายสื่อแสดงการล่วงละเมิดทางเพศต่อเด็กอย่างทันท่วงที

อย่างไรก็ตาม การพัฒนาปัญญาประดิษฐ์ยังคงมีความจำเป็นอย่างต่อเนื่อง เพื่อให้ก้าวทันการพัฒนาไปอย่างรวดเร็วของเทคโนโลยีซึ่งอาจถูกนำไปใช้ประโยชน์ในทางที่ผิด เช่น การพัฒนาการเรียนรู้ของปัญญาประดิษฐ์ต่อรูปแบบของข้อความ ซึ่งต้องใช้หลักการทางนิติภาษาศาสตร์ รวมถึงความท้าทายในการวิเคราะห์รูปแบบการเข้ารหัสของข้อมูลและเทคโนโลยีใหม่ในอนาคต ซึ่งจะต้องคำนึงถึงความสมดุลระหว่างการบังคับใช้กฎหมายกับการเคารพในสิทธิและข้อมูลส่วนบุคคลของผู้ใช้งานอินเทอร์เน็ต ตลอดจนหลักการรับฟังพยานหลักฐาน ควบคู่ไปกับการสร้างความตระหนักรู้และทักษะการใช้สื่อดิจิทัลเพื่อสร้าง

ภูมิคุ้มกันให้แก่เด็กและเยาวชน เพื่อสร้างสภาพแวดล้อมในโลกออนไลน์ให้มีความปลอดภัยจากการล่วงละเมิดทางเพศต่อเด็กมากยิ่งขึ้นต่อไป

เอกสารอ้างอิง

Beier, K.M. (2016). **Proactive Strategies to Prevent Child Sexual Abuse and the Use of Child Abuse Images: The German Dunkelfeld-Project for Adults (PPD) and Juveniles (PPJ).** Cham: Springer. 249-272.

Bracket Foundation. (2019). **Artificial Intelligence: Combatting Online Sexual Abuse of Children.** Retrieved June 30, 2021 from https://respect.international/ai-combating-online-sexual-abuse-of-children.

Brantingham, P.J. and Faust, F.L. (1976). A Conceptual Model of Crime Prevention. **Crime and Delinquency**, 22(3), 284–296. Retrieved June 21, 2021 from https://doi.org/10.1177/001112877602200302.

Cornish, D.B. and Clarke, R.V. (2003). Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention. **Crime Prevention Studies**, 16, 41-96.

Council of Europe. (2021). **Respecting Human Rights and the Rule of Law When Using Automated Technology to Detect Online Child Sexual Exploitation and Abuse.**

ECPAT. (2020). **Why Children Are at Risk of Sexual Abuse and Exploitation During COVID-19.** Retrieved June 10, 2021 from https://www.ecpat.org/news/covid-19-sexual-abuse.

Ekblom, P. (2017). Crime, Situational Prevention and Technology. **The Routledge Handbook of Technology, Crime and Justice**. 353–374.

EUROPOL. (2020a). **Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse During the COVID-19 Pandemic.** European Union Agency for Law Enforcement Cooperation.

EUROPOL. (2020b). **Internet Organised Crime Threat Assessment (IOCTA) 2020**. Retrieved July 1, 2021, from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

Hassad, R.A. (2020). **COVID-19: A Pandemic Preparedness Mindset - Primary, Secondary, and Tertiary Prevention Strategies All Play a Role.** Retrieved June 5, 2021 from https://www.medpagetoday.com/infectiousdisease/covid19/85200.

Internet Watch Foundation. (2020). **IWF Annual Report 2020.** Retrieved June 30, 2021 from https://annualreport2020.iwf.org.uk.

Kongsuwan, S. (2021). **MySis: A Chatbot Working as a 'Sister' Who Supports Children and Women Facing Violence.** Thailand Institute of Justice (TIJ) and The101.world. Retrieved July 3, 2021 from https://www.the101.world/mysis-chatbot/. (In Thai).

National Centre for Missing and Exploited Children. (2021). **Reduce Child Sexual Exploitation.** Retrieve July 3, 2021 from https://www.missingkids.org/content/ncmec/en/ourwork/impact.html.

Perrot, P. (2017). What about AI in Criminal Intelligence: From Predictive Policing to AI Perspectives. **European Police Science and Research Bulletin,** 16, 65-76.

Quayle, E. and Koukopoulos, N. (2019). Deterrence of Online Child Sexual Abuse and Exploitation. **Policing: A Journal of Policy and Practice**. 13(3), 345-362.

Sangtongdee, U., Poengranai, K., and Meephiam, P. (2020). Hashing Technology and PhotoDNA Database in Multimedia Forensics. **Journal of Criminology and Forensic Science,** 6(2), 181-196. Retrieved June 3, 2021 from https://so02.tci-thaijo.org/index.php/forensic/article/view/244801. (In Thai).

UNODC. (2020). Online Child Sexual Exploitation and Abuse. **E4J University Module Series on Cybercrime.** Retrieved June 1, 2021 from https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html.

Winters, G.M. and Jeglic, E.L. (2017). I Knew It All Along: The Sexual Grooming Behaviours of Child Molesters and the Hindsight Bias. **Journal of Child Sexual Abuse**, 25(1), 20-36.

Završnik, A. (2020). Criminal Justice, Artificial Intelligence Systems, and Human Rights. **ERA Forum**, 20(4), 567-583. Retrieved July 1, 2021 from https://doi.org/10.1007/s12027-020-00602-0.

ประวัติผู้เขียน

คำนำหน้า ชื่อ-สกุล **ว่าที่พันตำรวจตรี ภิญโญ มีเปี่ยม ***
ตำแหน่ง/สถานะ อาจารย์ (สัญญาบัตร 2)
ที่อยู่หน่วยงาน/สังกัด กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
90 หมู่ 7 ตำบลสามพราน อำเภอสามพราน จังหวัดนครปฐม 73110
ไปรษณีย์อิเล็กทรอนิกส์ pinyo@rpca.ac.th

คำนำหน้า ชื่อ-สกุล **พันตำรวจโท ดร.อัศว์ณุต แสงทองดี**
ตำแหน่ง/สถานะ นักศึกษาปริญญาเอกและอาจารย์ผู้ช่วยสอน
ที่อยู่หน่วยงาน/สังกัด School of Computing, Engineering and Digital Technology,
Teesside University Campus Heart, Southfield Rd,
Middlesbrough, UK TS1 3BX
ไปรษณีย์อิเล็กทรอนิกส์ U.Sangtongdee@tees.ac.uk

* ผู้ประพันธ์บรรณกิจ (Corresponding Author)