การศึกษาเพื่อพัฒนากฎหมายเกี่ยวกับมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ให้รองรับอาชญากรรมทางเทคโนโลยีในอนาคต

A Study on the Development of Legal Measures for the Prevention and Suppression of Cybercrime to Address Future Technological Crimes

ส.ต.อ.ภัทรพงษ์ จันทร์พรหม [1*]

Pattarapong Chanprom, Police Sergeant [1*]

คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย [1]

School of Law. The University of the Thai Chamber of Commerce. [1]

Corresponding author E-mail: Batzasodasing@gmail.com *

Received: 13 August 2025**; Revised:** 13 November 2025**; Accepted:** 6 December 2025

บทคัดย่อ

ในยุคดิจิทัลปัจจุบัน เทคโนโลยีเข้ามามีบทบาทอย่างมากในชีวิตประจำวัน ส่งผลให้เกิดอาชญากรรมทางเทคโนโลยี (Cybercrime) ที่มีความซับซ้อนและหลากหลายมากขึ้น เช่น การหลอกลวงออนไลน์ การขโมยข้อมูล และการใช้ปัญญาประดิษฐ์ (AI) หรือ Deepfake เป็นเครื่องมือในการกระทำผิด แม้ประเทศไทยจะมีการตรากฎหมายพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และกฎหมายพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีฉบับแก้ไข พ.ศ. 2568แล้ว แต่ยังคงพบปัญหาช่องว่างทางกฎหมายที่ไม่สามารถรองรับการเปลี่ยนแปลงของเทคโนโลยีได้อย่างมีประสิทธิภาพ งานวิจัยนี้จึงมีวัตถุประสงค์เพื่อศึกษา ศึกษาช่องโหว่ทางกฎหมาย วิเคราะห์ข้อจำกัดของกฎหมายที่มีอยู่ และศึกษากฎหมายของต่างประเทศ เช่น สหรัฐอเมริกา สหภาพยุโรป และสิงคโปร์ เพื่อเสนอแนวทางเชิงกฎหมายที่ทันสมัยและเหมาะสมกับบริบทของประเทศไทย งานวิจัยใช้วิธีการศึกษาเอกสารเชิงคุณภาพ โดยวิเคราะห์จากแนวคิด ทฤษฎี และบทความวิชาการที่เกี่ยวข้อง /จากการศึกษาแนวทางกฎหมายไซเบอร์ในต่างประเทศ พบว่าประเทศพัฒนาแล้วมีการออกแบบระบบกฎหมายที่เน้นการปรับตัวต่อเทคโนโลยีใหม่อย่างต่อเนื่อง ใช้กลไกเชิงรุกผ่านการกำหนดบทบาทของแพลตฟอร์มเอกชนในการแจ้งเตือนและจัดการความเสี่ยงไซเบอร์ พร้อมทั้งส่งเสริมความร่วมมือระหว่างรัฐกับภาคเอกชนในรูปแบบพันธมิตรด้านความมั่นคงไซเบอร์ รวมถึงการจัดตั้งหน่วยงานกลางที่มีอำนาจเต็มในการกำกับ ดูแล สืบสวน และประสานงานระดับระหว่างประเทศ บทเรียนสำคัญที่ประเทศไทย

สามารถนำมาประยุกต์ได้คือการยกระดับกรอบกฎหมายให้มีความยืดหยุ่นและตอบสนองต่อความเปลี่ยนแปลงของเทคโนโลยีอย่างทันท่วงที พร้อมส่งเสริมกลไกการทำงานเชิงรุกทั้งในระดับนโยบาย แพลตฟอร์ม และความร่วมมือระหว่างประเทศ เพื่อให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพและยั่งยืนในระยะยาว จึงควรมีการปรับปรุงและพัฒนานโยบายในหลายมิติอย่างเป็นระบบ เริ่มจากการปรับแก้บทบัญญัติของกฎหมายให้ครอบคลุมและชัดเจนยิ่งขึ้น โดยเฉพาะการกำหนดนิยามของอาชญากรรมที่เกี่ยวข้องกับ AI และ Deepfake ให้เป็นที่รับรู้ทางกฎหมาย อาทิ การปลอมแปลงบุคคลโดยใช้เทคโนโลยี Deepfake หรือการสร้างเนื้อหาหลอกลวงผ่านระบบอัตโนมัติ ซึ่งการบัญญัตินิยามและฐานความผิดเหล่านี้อย่างชัดเจนจะช่วยป้องกันความคลุมเครือในการบังคับใช้กฎหมาย และเปิดทางให้กระบวนการยุติธรรมสามารถดำเนินการได้อย่างทันการณ์

นอกจากนี้ ควรมีการจัดตั้งหน่วยงานเฉพาะทางด้านอาชญากรรม AI ภายใต้สำนักงานตำรวจแห่งชาติ คือการพัฒนาศักยภาพของบุคลากรที่เกี่ยวข้องกับกระบวนการยุติธรรม ไม่ว่าจะเป็นเจ้าหน้าที่ตำรวจ พนักงานสอบสวน หรือผู้เชี่ยวชาญด้านนิติวิทยาศาสตร์ดิจิทัล ประเทศไทยควรผลักดันให้เกิดการจัดตั้ง “คณะกรรมการความร่วมมืออาเซียนว่าด้วยการปราบปรามอาชญากรรมไซเบอร์”

คำสำคัญ :ปัญญาประดิษฐ์, เสียงและเนื้อหาปลอมที่สร้างขึ้นเพื่อหลอกลวงหรือบิดเบือนความจริง โดยเฉพาะเมื่อใช้ในทางที่ก่อให้เกิดความเสียหาย, อาชญากรรมทางไซเบอร์

Abstract

In the current digital era, technology plays a significant role in daily life, leading to increasingly complex and diverse forms of cybercrime such as online fraud, data theft, and the misuse of artificial intelligence (AI) and deepfake technologies for criminal purposes. Although Thailand has enacted the Royal Decree on Measures for the Prevention and Suppression of Technology Crime B.E. 2566 (2023) and its amendment in B.E. 2568 (2025), there remain legal gaps that hinder the law’s ability to effectively keep pace with rapid technological advancements. This research aims to explore these legal loopholes, analyze the limitations of existing laws, and study international legal frameworks such as those in the United States, the European Union, and Singapore. The objective is to propose modern and context-appropriate legal approaches for Thailand. This study employs qualitative document analysis, drawing on relevant theories, academic articles, and legal concepts. The findings are expected to offer recommendations for enhancing Thai legislation to be more flexible and up-to-date, capable of addressing future

cybercrimes, and fostering public and business confidence in using technology safely and sustainably/ From the study of international approaches to cyber law, it has been found that developed countries design their legal systems to continuously adapt to new technologies. They employ proactive mechanisms by defining the roles of private platforms in alerting and managing cyber risks, while also promoting collaboration between the public and private sectors through cyber security partnerships. In addition, these countries have established central agencies with full authority to regulate, supervise, investigate, and coordinate at the international level.

The key lesson that Thailand can apply is to enhance its legal framework to be more flexible and responsive to technological changes in a timely manner, as well as to promote proactive mechanisms at the policy, platform, and international cooperation levels. This would enable the country to effectively and sustainably address cyber threats in the long term.

Therefore, Thailand should systematically revise and develop policies across multiple dimensions, beginning with the amendment of legal provisions to make them more comprehensive and explicit — particularly by defining crimes related to AI and Deepfake technologies in legal terms. For example, acts such as impersonation through Deepfake technology or the creation of deceptive content using automated systems should be clearly defined as offenses. Establishing clear definitions and legal bases for such crimes will help prevent ambiguity in law enforcement and allow the justice system to respond promptly.

Furthermore, a specialized AI Crime Unit should be established under the Royal Thai Police It refers to the development of the potential and capabilities of personnel involved in the justice process, including police officers, investigators, and digital forensic experts Thailand should promote the establishment of an “ASEAN Committee on Cooperation for Combating Cybercrime.”

Keywords: AI (Artificial Intelligence), Deepfake, Cybercrime

บทนำ

ในยุคดิจิทัลปัจจุบัน เทคโนโลยีมีบทบาทสำคัญและแทรกซึมอยู่ในทุกมิติของชีวิตมนุษย์ ตั้งแต่การทำงาน การศึกษา การสื่อสาร ตลอดจนการดำเนินชีวิตประจำวัน ความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology: ICT) ได้เปลี่ยนแปลงวิถีชีวิตของผู้คนทั่วโลกอย่างรวดเร็ว ทำให้โลกเชื่อมโยงถึงกันได้อย่างไร้พรมแดน อย่างไรก็ตาม ความเจริญก้าวหน้าดังกล่าวย่อมนำมาซึ่งความท้าทาย โดยเฉพาะในด้านความมั่นคงและความปลอดภัยทางไซเบอร์ ซึ่งนำไปสู่การเกิดอาชญากรรมทางเทคโนโลยีหรืออาชญากรรมไซเบอร์(Cybercrime)อาชญากรรมไซเบอร์เป็นการกระทำผิดโดยใช้เทคโนโลยีดิจิทัล เช่น คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ในการก่อให้เกิดความเสียหาย หรือแสวงหาผลประโยชน์โดยมิชอบ ซึ่งปรากฏในหลายรูปแบบ เช่น การหลอกลวงทางออนไลน์ การโจมตีระบบคอมพิวเตอร์ การขโมยข้อมูลส่วนบุคคล และการเผยแพร่เนื้อหาที่ไม่เหมาะสม “สภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ (สศช.)”สถิติจากสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ (สศช.) ระบุว่า ในปี พ.ศ. 2565 มีชาวไทยกว่า 50% เคยถูกหลอกลวงทางออนไลน์ และในช่วงปี พ.ศ. 2565–2567 มีการแจ้งความคดีอาชญากรรมทางเทคโนโลยีมากกว่า 575,000 คดี รวมมูลค่าความเสียหายกว่า 65,000 ล้านบาทแม้ว่าประเทศไทยจะมีพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และฉบับแก้ไข พ.ศ. 2568 แล้วก็ตาม แต่กฎหมายดังกล่าวยังประสบข้อจำกัดในการรับมือกับภัยคุกคามที่มีความซับซ้อนและพัฒนาอย่างต่อเนื่อง โดยเฉพาะอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยีใหม่ เช่น ปัญญาประดิษฐ์ (AI) การสร้างสื่อปลอมด้วยเทคนิค Deepfake และการกระทำความผิดในโลกเสมือนจริง (Metaverse) กฎหมายปัจจุบันยังขาดความยืดหยุ่นเพียงพอในการรองรับสถานการณ์ที่เปลี่ยนแปลงอย่างรวดเร็วนอกจากนี้ ปัญหาด้านการบังคับใช้กฎหมายยังคงเป็นอุปสรรคสำคัญ เช่น การขาดบุคลากรผู้เชี่ยวชาญด้านเทคโนโลยี กระบวนการรวบรวมพยานหลักฐานที่ไม่ทันสมัย และข้อจำกัดในการดำเนินคดีในกรณีที่ผู้กระทำผิดอยู่ต่างประเทศ ส่งผลให้การรับมือกับอาชญากรรมไซเบอร์ยังไม่มีประสิทธิภาพเท่าที่ควร ด้วยเหตุนี้ ผู้วิจัยจึงเห็นความสำคัญของการศึกษากฎหมายที่มีอยู่ เพื่อประเมินประสิทธิภาพและระบุช่องว่างทางกฎหมาย ตลอดจนศึกษาแนวทางปฏิบัติของประเทศที่มีการจัดการอาชญากรรมไซเบอร์อย่างมีประสิทธิภาพ เช่น สหรัฐอเมริกา สหภาพยุโรป และสิงคโปร์ เพื่อนำมาใช้เป็นแนวทางในการพัฒนากฎหมายไทยให้สามารถรับมือกับอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิผลในอนาคต

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาช่องว่างทางกฎหมายในการรับมืออาชญากรรมทางเทคโนโลยีในรูปแบบใหม่ โดยเฉพาะอาชญากรรมที่ใช้เครื่องมือปัญญาประดิษฐ์ (AI) และการสังเคราะห์ภาพหรือเสียง Deepfake เพื่อกระทำความผิด

2. เพื่อวิเคราะห์พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และฉบับแก้ไข 2568 และระบุช่องโหว่ทางกฎหมายที่ต้องการการพัฒนา

3. เพื่อศึกษากฎหมายของ สหภาพยุโรป ประเทศสหรัฐอเมริกา และ ประเทศสิงคโปร์

กรอบแนวคิดและสมมติฐานในการวิจัย

กฎหมายเทคโนโลยีที่มีอยู่ในปัจจุบันไม่สามารถรองรับอาชญากรรมทางเทคโนโลยีที่เกิดขึ้นใหม่ได้อย่างมีประสิทธิภาพ เนื่องจากการพัฒนาและการใช้งานเทคโนโลยีที่เพิ่มขึ้นอย่างรวดเร็วทำให้เกิดอาชญากรรมทางเทคโนโลยีรูปแบบใหม่ที่ซับซ้อนและหลากหลาย ซึ่งกฎหมายที่มีอยู่ในปัจจุบันไม่สามารถปรับตัวได้ทันต่อสถานการณ์ดังกล่าว การพัฒนากฎหมายเทคโนโลยีให้ทันสมัยและสอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงจะเป็นกลไกสำคัญในการลดอัตราการเกิดอาชญากรรมทางเทคโนโลยีในอนาคต โดยเฉพาะอย่างยิ่งในกรณีที่มีการร่วมมือระหว่างภาครัฐและภาคเอกชนในการพัฒนากฎหมายที่สามารถตอบสนองได้อย่างทันท่วงทีและมีประสิทธิภาพ ซึ่งจะช่วยป้องกันและควบคุมการเกิดอาชญากรรมทางเทคโนโลยีในระยะยาวได้อย่างมีประสิทธิผล

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาช่องว่างทางกฎหมายในการรับมือกับอาชญากรรมทางเทคโนโลยีสมัยใหม่ โดยเฉพาะในกรณีที่มีการใช้ AI และ Deepfake เป็นเครื่องมือในการกระทำความผิด นอกจากนี้ยังมุ่งวิเคราะห์พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และฉบับแก้ไข พ.ศ. 2568 เพื่อระบุข้อจำกัดและประเด็นที่ควรได้รับการพัฒนาให้สอดคล้องกับบริบททางเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

เพื่อให้ได้แนวทางการพัฒนากฎหมายที่มีประสิทธิภาพ งานวิจัยนี้ยังได้ศึกษาเปรียบเทียบกฎหมายจากต่างประเทศ ได้แก่ สหภาพยุโรป สหรัฐอเมริกา และสิงคโปร์ ซึ่งถือเป็นประเทศหรือเขตเศรษฐกิจที่มีความก้าวหน้าในการจัดการกับอาชญากรรมทางเทคโนโลยี การศึกษาเปรียบเทียบนี้มีเป้าหมายเพื่อเสนอแนวทางเชิงกฎหมายที่เหมาะสมสำหรับประเทศไทยในการเสริมสร้างกฎหมายให้ทันสมัยและสามารถรับมือกับภัยคุกคามใหม่ๆ ได้อย่างมีประสิทธิภาพ

แนวคิดทฤษฎีเกี่ยวกับอาชญากรรมทางเทคโนโลยี

ความหมายของอาชญากรรมทางเทคโนโลยี อาชญากรรมทางเทคโนโลยี หมายถึง การกระทำความผิดที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ คอมพิวเตอร์ หรือเครือข่ายอินเทอร์เน็ต ซึ่งก่อให้เกิดความเสียหายต่อบุคคล องค์กร หรือสังคมในหลากหลายมิติ เช่น เศรษฐกิจ ความมั่นคง สิทธิส่วนบุคคล และจริยธรรมในสังคม

ดิจิทัลโดยผู้เชี่ยวชาญหลายคนได้ให้คำจำกัดความไว้ อาทิ Shelly และ Vermaat: ได้เน้นความผิดที่ใช้ความรู้ด้านเทคโนโลยี เช่น การขโมยข้อมูล การฟอกเงิน การละเมิดลิขสิทธิ์ซอฟต์แวร์

สำหรับHalder Jaishankar: ได้เน้นการกระทำที่มีผลกระทบต่อร่างกาย จิตใจ และชื่อเสียงของเหยื่อผ่านช่องทางดิจิทัล นอกจากนี้วาสิน มีธรรม และบัณฑิต ขวาโยธา: ได้เน้นความเสียหายเชิงเศรษฐกิจ และเทคนิคการหลอกลวงที่ซับซ้อนผ่านเทคโนโลยี ลักษณะเฉพาะของอาชญากรรมทางเทคโนโลยี อาชญากรรมทางเทคโนโลยีในยุคดิจิทัลมีลักษณะเฉพาะ 3 ประการหลัก

1. การกระทำผ่านระบบดิจิทัล (Digital Modality)

ใช้เทคโนโลยี เช่น อินเทอร์เน็ต โทรศัพท์มือถือ โซเชียลมีเดีย ผู้กระทำผิดสามารถเข้าถึงเหยื่อได้โดยไร้ขอบเขตด้านภูมิศาสตร์และเวลา

2. การกระทำโดยไม่มีปฏิสัมพันธ์โดยตรง (Non-Physical Interaction)

อาชญากรไม่จำเป็นต้องพบเหยื่อ เช่น การส่ง SMS, อีเมลหลอก, โทรศัพท์ปลอมตัวยากต่อการติดตามและจับกุมตัวผู้กระทำผิด

3. การกระทำเป็นเครือข่ายที่มีการจัดการ (Organized Cybercrime)

แบ่งหน้าที่เป็นระบบ เช่น ผู้สร้างเว็บไซต์ปลอม, ผู้เปิดบัญชีม้า, ผู้ลบหลักฐาน สะท้อนความเป็น “องค์กรอาชญากรรมยุคใหม่”

รูปแบบของอาชญากรรมทางเทคโนโลยีที่พบในปัจจุบัน

Synthetic Media Crimes (ใช้ AI/Deepfake สร้างเนื้อหาปลอมที่สมจริงสูง) วิธีการใช้ สร้างข้อความ ภาพ หรือวิดีโอที่สมจริง (นอกจาก deepfake) เพื่อนำไปใช้ในแคมเปญหลอกลวง ปั่นกระแสข่าวปลอม กระทำการชิงทรัพย์ทางจิตวิทยา หรือฟอกเงิน ตัวอย่าง สร้างเอกสารรับรองปลอม, สร้างโพสต์โซเชียลมีเดียปลอมที่สร้าง panic, ผลิตบันทึกเสียงของบุคคลสำคัญเพื่อออกคำสั่งทางการเงินผลกระทบ ข้อมูลบิดเบือนระดับใหญ่, การทำลายความเชื่อมั่นสาธารณะ, การฉ้อโกงระดับองค์กรหรือรัฐสัญญาณเตือนเนื้อหาที่ “สมบูรณ์แบบเกินจริง” หรือขัดแย้งกับแหล่งข้อมูลเชื่อถือได้, ข้อความหรือไฟล์ที่ส่งมาจากแหล่งไม่คาดคิด ป้องกันพัฒนาและใช้เครื่องมือพิสูจน์ความแท้ (authentication), ตรวจสอบแหล่งที่มา, ส่งเสริมความรู้ด้านสื่อสารมวลชน (media literacy)

ปัจจัยที่เอื้อต่อการเกิดอาชญากรรมทางเทคโนโลยี ช่องโหว่ของระบบความปลอดภัยไซเบอร์ เช่น ซอฟต์แวร์ไม่อัปเดต ขาดระบบสำรองข้อมูล ภาวะ **“ความไม่รู้เท่าทันดิจิทัล”** (Digital Illiteracy) ของประชาชน เช่น ขาดทักษะในการแยกแยะข่าวจริง-เท็จ หรือเว็บไซต์หลอกลวง

กฎหมายเกี่ยวกับอาชญากรรมทางเทคโนโลยีในต่างประเทศ 3 ประเทศ

1. สิงคโปร์: Protection from Scams Act 2025

กฎหมายฉบับนี้เป็นความพยายามของรัฐบาลสิงคโปร์ในการปรับปรุงกฎหมายให้เท่าทันกับภัยคุกคามจากอาชญากรรมไซเบอร์ โดยเฉพาะการหลอกลวงออนไลน์ที่พุ่งสูงขึ้นในช่วงหลายปีที่ผ่านมา

ลักษณะสำคัญของกฎหมาย

Shared Liability Framework: ยึดหลัก "ความรับผิดร่วม" ซึ่งหมายถึงการวางภาระความรับผิดชอบทางกฎหมายต่อทั้งผู้ให้บริการทางการเงิน ผู้ให้บริการโทรคมนาคม และแพลตฟอร์มออนไลน์ หากมีส่วนในการเอื้อให้เกิดการหลอกลวง

แนวคิดเชิงป้องกัน (Preventive-Oriented): ให้ความสำคัญกับการสกัดกลโกงตั้งแต่ต้นทาง มากกว่าการลงโทษภายหลัง และ เพิ่มอำนาจรัฐ หน่วยงานรัฐสามารถสั่งระงับบัญชี บล็อกเว็บไซต์ และข้อความหลอกลวงได้ทันทีโดยไม่ต้องรอคำสั่งศาล โดยมีการบูรณาการหลายภาคส่วนภาครัฐ เอกชน และผู้ใช้งานต้องร่วมมือกันในระบบการป้องกันภัยไซเบอร์ ให้ครอบคลุมหลายรูปแบบของการหลอกลวง: เช่น phishing, identity fraud, scam ads, fake investment platforms ฯลฯ และทั้งเชิงนโยบายมากกว่าการลงโทษ เป็นเครื่องมือกำกับดูแลความเสี่ยง มากกว่าการดำเนินคดีแบบเฉพาะราย

ผู้บังคับใช้หลัก (Ministry of Home Affairs – กระทรวงมหาดไทยสิงคโปร์ MHA),(Singapore Police Force – สำนักงานตำรวจแห่งชาติสิงคโปร์ : SPF),(Monetary Authority of Singapore – ธนาคารกลางและหน่วยงานกำกับดูแลทางการเงินของสิงคโปร์ : MAS),(Infocomm Media Development Authority – สำนักงานพัฒนาสื่อและสารสนเทศสิงคโปร์ : IMDA), โครงการ ScamShield และภาคเอกชน (ธนาคาร แพลตฟอร์ม และผู้ให้บริการโทรคมนาคม)

2. สหรัฐอเมริกา: การรับมือกับ AI และ Deepfake

กฎหมายสหรัฐอเมริกา USA

สหรัฐอเมริกายังไม่มี “กฎหมายกลางระดับกลาง” (Federal Laws) ที่ควบคุมการใช้ AI และ Deepfake เพื่อกระทำความผิดโดยตรงแบบครอบคลุมทั้งหมด แต่มีกฎหมายเฉพาะระดับรัฐ (State Laws)และ การใช้กฎหมายเดิมร่วมกับเทคโนโลยีใหม่ ตลอดจนร่างกฎหมายที่กำลังดำเนินการ ซึ่งสามารถสรุปการป้องกันและปราบปรามอาชญากรรมที่ใช้ AI และ Deepfake ได้เป็น 3 แนวทางหลัก

การใช้กฎหมายอาญาเดิมปรับใช้กับอาชญากรรมที่ใช้ AI หรือ Deepfake

แม้จะยังไม่มี Federal Law เฉพาะ AI แต่รัฐบาลกลางและรัฐต่างๆ ใช้กฎหมายที่มีอยู่แล้วมาปรับใช้กับกรณีที่อาชญากรรมเกี่ยวข้องกับ AIหรือDeepfake เช่น

การหลอกลวงด้วยเสียงหรือภาพปลอม (AI Fraud, Voice Scam) Wire Fraud (18 U.S.C. § 1343), Identity Theft (18 U.S.C. § 1028)

การเผยแพร่สื่อลามก Deepfake โดยไม่ได้รับความยินยอม Cyberstalking (18 U.S.C. § 2261A), Revenge Porn Laws (บางรัฐ) การปลอมแปลงเสียงหรือภาพนักการเมืองเพื่อบิดเบือนข้อมูล Election Law Violations, Defamation (รัฐกฎหมายแพ่ง)การแฮ็กหรือฝัง AI เพื่อโจมตีระบบ Computer Fraud and Abuse Act (CFAA)

กฎหมายระดับรัฐที่ควบคุม Deepfake และ AI โดยตรง

รัฐหลายแห่งในสหรัฐอเมริกาออกกฎหมายเฉพาะที่เกี่ยวกับการใช้ Deepfake ในการกระทำความผิด ได้แก่

รัฐแคลิฟอรเนีย (California)

- AB 602 (2020) – ห้ามเผยแพร่ Deepfake สื่อลามก ที่สร้างโดยไม่ได้รับความยินยอม
- AB 730 (2020) – ห้ามเผยแพร่ สื่อ Deepfake ที่บิดเบือนคำพูดนักการเมือง ภายใน 60 วัน ก่อนการเลือกตั้ง

รัฐเท็กซัส (Texas) SB 751 (2019) – กำหนดความผิดทางอาญาสำหรับการใช้ “deep fake video” ที่มีเจตนาโน้มน้าวหรือบิดเบือนผลการเลือกตั้ง

Virginia / New York / Illinois มีกฎหมายเฉพาะที่ ห้าม Deepfake ลามก และคุ้มครองภาพลักษณ์ของบุคคล (Right of Publicity) ดังนี้

กฎหมายของรัฐที่ห้าม Deepfake เนื้อหาลามก และคุ้มครองภาพลักษณ์ของบุคคล

1. Virginia Code of Virginia § 8.01-42.6 (2019) เป็นหนึ่งในรัฐแรกที่ออกกฎหมายห้ามการเผยแพร่สื่อ Deepfake ที่ลามกอนาจาร โดยเฉพาะที่เกี่ยวข้องกับภาพของบุคคลจริงโดยไม่ได้รับความยินยอมห้ามสร้าง แจกจ่าย หรือเผยแพร่ภาพหรือวิดีโอที่ตัดต่อให้ดูเหมือนว่าบุคคลอยู่ในสถานการณ์ทางเพศให้สิทธิผู้เสียหายในการฟ้องร้องทางแพ่งเป็นกฎหมายที่เน้น “การคุ้มครองศักดิ์ศรีของบุคคล”

2. New York Civil Rights Law §§ 50-f (2020) มีการแก้ไขกฎหมายสิทธิส่วนบุคคลเพื่อห้ามการใช้เทคโนโลยีเช่น Deepfake เพื่อสร้าง ภาพลามกอนาจารหรือภาพที่ล่วงละเมิดศักดิ์ศรี ห้ามการใช้เทคโนโลยีสร้างภาพ/วิดีโอลักษณะลามกอนาจารของบุคคลที่ยังมีชีวิตยังขยายการคุ้มครอง “Right of Publicity” โดยให้บุคคลมีสิทธิในการควบคุมภาพลักษณ์ของตนแม้หลังเสียชีวิต (post-mortem right) มีข้อยกเว้นสำหรับงานเสียดสีวิจารณ์ หรืองานที่อยู่ภายใต้การคุ้มครองตามรัฐธรรมนูญ

3. Illinois Right of Publicity Act (765 ILCS 1075) คุ้มครองภาพลักษณ์ ชื่อเสียง เสียง หรือเอกลักษณ์ของบุคคลจากการนำไปใช้ในเชิงพาณิชย์โดยไม่ได้รับความยินยอมถึงแม้ไม่ได้ระบุคำว่า “Deepfake” อย่างชัดเจน

แต่สามารถตีความได้ว่าเทคโนโลยี Deepfake เข้าข่ายละเมิดหากใช้ภาพหรือเสียงของบุคคลในเชิงพาณิชย์โดยไม่ได้รับอนุญาตให้สิทธิฟ้องร้องเรียกค่าเสียหายทางแพ่งคุ้มครองสิทธิภาพลักษณ์หลังเสียชีวิตได้นานถึง 50 ปี

3. สหภาพยุโรป (EU): European Union Artificial Intelligence Act

AI ที่ห้าม (Prohibited AI) – Article 5

• กล่าวถึง AI บางประเภทที่ถือว่าฝ่าฝืนสิทธิมนุษยชน เช่น Social Scoring หรือ Deepfake ที่หลอกลวงโดยไม่แจ้ง

AI เสี่ยงสูง (High-Risk AI) – Article 6–10

• ครอบคลุมระบบ AI ที่ใช้ในงานสำคัญต่อความปลอดภัย สิทธิขั้นพื้นฐาน หรือความโปร่งใส เช่น ระบบคัดกรองใบสมัครงาน, วิเคราะห์เครดิต, ระบบควบคุมโครงสร้างพื้นฐาน

• มีข้อกำหนดเข้มงวดเรื่อง data governance, documentation, transparency, human oversight

AI เสี่ยงจำกัด (Limited-Risk AI) – Article 52–53

• ตัวอย่างเช่น Chatbot หรือระบบแนะนำสินค้า

• ต้องมีการแจ้งเตือนผู้ใช้เมื่อโต้ตอบกับ AI เพื่อความโปร่งใส

AI เสี่ยงต่ำ (Minimal-Risk AI) – ไม่มีบทความเฉพาะเจาะจง

• ระบบทั่วไปที่แทบไม่มีผลกระทบต่อสิทธิหรือความปลอดภัย เช่น ระบบกรองสแปม, เกม AI

• ไม่มีข้อกำหนดเฉพาะมากนัก แต่ยังคงอยู่ภายใต้ข้อกำหนดทั่วไป

แนวทางควบคุม Deepfake และ AI Fraud ต้องระบุชัดเจนว่าเนื้อหา Deepfake “ไม่ใช่ของจริง”หากใช้ Deepfake เพื่อการหลอกลวงอาจเข้าข่าย “ระบบต้องห้าม”หรือ“เสี่ยงสูง”และแพลตฟอร์มต้องมีระบบตรวจจับและลบเนื้อหาผิดกฎหมาย

ประเด็นในการวิเคราะห์ปัญหา

ข้อจำกัดของกฎหมายไทยในปัจจุบัน

1. ความไม่เพียงพอของบทบัญญัติ นิยามของเทคโนโลยีสมัยใหม่ยังไม่ชัดเจน พระราชกำหนดมาตรการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี ปี 2566 และฉบับแก้ไข 2568 ยังไม่มีนิยามที่ครอบคลุมเทคโนโลยีใหม่ เช่น Deepfake, AI fraud, synthetic content และ Hybrid Scam และบัญชีม้า ยังไม่ถูกบัญญัติหรือจัดประเภทอย่างชัดเจนในเชิงกฎหมาย แม้จะมีบทบาทสำคัญในอาชญากรรมไซเบอร์ยุคใหม่

2. ช่องว่างทางกฎหมายกับเทคโนโลยีเกิดใหม่ การปลอมแปลงเสียงหรือภาพด้วย AI ยังไม่มีกฎหมายเฉพาะในการควบคุม แม้จะเริ่มมีกรอบแนวทางใน พ.ร.ก.ฯ แต่ยังขาดรายละเอียดทางเทคนิคและข้อบังคับทางกฎหมายที่ชัดเจน

3. ข้อจำกัดด้านกฎหมายข้ามพรมแดน ขาดกลไกความร่วมมือระหว่างประเทศ เช่น การไม่เข้าร่วม Budapest Convention หรือไม่มี MLAT ที่มีผลผูกพัน กฎหมายไทยไม่มีบทบัญญัติรองรับการปฏิบัติข้ามเขตแดนอย่างมีประสิทธิภาพ ทำให้ไม่สามารถขอข้อมูลจากรัฐต่างประเทศได้ทันต่อเวลา หรือดำเนินคดีข้ามเขตอำนาจได้ ประมวลกฎหมายอาญา มาตรา 4–11 ไม่ครอบคลุม คือกรณีที่ การกระทำความผิด เกิดขึ้นนอกราชอาณาจักร, ไม่เข้าหลักเกณฑ์ในมาตรา 6–11, และ ไม่มีผลกระทบมาถึงในราชอาณาจักร ตัวอย่าง

1. คนไทยทำผิดในต่างประเทศ แต่ไม่เข้าเงื่อนไขมาตรา 6–11

• ตัวอย่างเช่น นาย ก. (สัญชาติไทย) ทำร้ายร่างกายนาย ข. ที่ประเทศลาว แล้วหนีกลับประเทศไทย

⟶ ความผิดนี้เกิดขึ้นนอกราชอาณาจักร และไม่ใช่ความผิดต่อรัฐหรือความมั่นคง

⟶ศาลไทยไม่มีอำนาจฟ้องนาย ก. ได้ เว้นแต่ลาวร้องขอส่งตัวผู้ร้ายข้ามแดนไปดำเนินคดีตามสนธิสัญญา

2. คนต่างด้าวทำผิดต่อต่างด้าวนอกราชอาณาจักร

• เช่น นาย A (คนต่างด้าว) ฆ่านาย B (คนต่างด้าว) ที่สิงคโปร์ แล้วเดินทางเข้ามาในไทย

⟶ ไม่ใช่ความผิดในไทย, ไม่ใช่ผลเกิดในไทย, ไม่เข้าเงื่อนไขมาตรา 6–11

⟶ ไทยไม่มีอำนาจดำเนินคดี

3. คดีหมิ่นประมาทหรือโพสต์ข้อความในต่างประเทศ

• ถ้าการโพสต์กระทำในต่างประเทศ และ ไม่มีผู้เสียหายหรือผลกระทบในไทย

⟶ ศาลไทยจะไม่มีอำนาจรับฟ้อง เพราะไม่ถือว่า “ผลเกิดในราชอาณาจักร” ตามมาตรา 5

การเปรียบเทียบกับกฎหมายต่างประเทศ

1. สหภาพยุโรป (European Union) – EU AI Act แนวทาง Risk-based: แบ่งระดับความเสี่ยง AI เป็น 4 ระดับ ตั้งแต่ Unacceptable Risk ถึง Minimal Risk มาตรการควบคุม Deepfake และ GPAI อย่างเข้มงวด ต้องเปิดเผยเนื้อหาที่สร้างโดย AI และทำ Impact Assessment European AI Office และ National AI Regulators ทำหน้าที่ควบคุม บังคับใช้ และประสานงานภายในภูมิภาค

2. สหรัฐอเมริกา CFAA (1986) และ USA Patriot Act (2001) มุ่งควบคุมการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบและการป้องกันภัยก่อการร้าย CISA (2015) ส่งเสริมความร่วมมือภาครัฐ-เอกชน มีระบบแจ้งเตือนภัยไซเบอร์แบบเรียลไทม์

3. สิงคโปร์ Cybersecurity Act 2018 เน้นการควบคุม Critical Information Infrastructure (CII) และให้หน่วยงานรัฐมีอำนาจสอบสวน แนวทาง Whole-of-Nation และความร่วมมือกับภาคเอกชน ผ่าน CSA, CLS และ SG Cyber Safe

แนวทางการพัฒนากฎหมายไทยในอนาคต

เพื่อให้กฎหมายไทยสามารถรับมือกับภัยไซเบอร์ยุคใหม่ได้อย่างมีประสิทธิภาพ จำเป็นต้องดำเนินการดังนี้:

1. ปรับปรุงนิยามและขอบเขตกฎหมาย บัญญัตินิยามของ เนื้อหาสังเคราะห์โดย AI, Deepfake, AI fraud, Hybrid Scam, และ บัญชีม้า อีกทั้งพัฒนาบทบัญญัติเพื่อ รองรับเทคโนโลยีเกิดใหม่ โดยอิงตามแนวทาง “technology-neutral” และ “future-proof” หมายความว่า ข้อความ ภาพ เสียง วิดีโอ หรือสื่อรูปแบบอื่นใดที่สร้างขึ้นทั้งหมดหรือบางส่วนโดยกระบวนการประมวลผลอัตโนมัติของระบบปัญญาประดิษฐ์ (Artificial Intelligence) หรืออัลกอริทึมคอมพิวเตอร์ ซึ่งมีผลให้สื่อนั้นมีลักษณะเป็นของจริงหรือมีความน่าเชื่อถือเทียบเท่ากับผลงานของมนุษย์ “Deepfake” หมายความว่า เนื้อหาดิจิทัลใด ๆ ที่ถูกสร้าง แก้ไข หรือดัดแปลงด้วยเทคโนโลยีปัญญาประดิษฐ์ หรือเทคนิคการเรียนรู้เชิงลึก (Deep Learning) เพื่อทำให้บุคคลหรือเหตุการณ์ปรากฏในลักษณะที่ไม่ตรงกับความเป็นจริง โดยมีเจตนาให้เกิดความเข้าใจผิด หลอกลวง หรือทำให้เสียชื่อเสียง การฉ้อโกงโดย AI” หมายความว่า การใช้ระบบปัญญาประดิษฐ์ หรืออัลกอริทึมอัตโนมัติ เพื่อกระทำการหลอกลวงหรือสร้างความเสียหายแก่บุคคลอื่น เช่น การปลอมเสียง ปลอมตัวตน หรือสร้างข้อมูลเท็จเพื่อประโยชน์ทางการเงินหรือชื่อเสียง

2. จัดตั้งกลไกความร่วมมือระหว่างประเทศ ไทยควรเข้าร่วมใน อนุสัญญานานาชาติ เช่น Budapest Convention และ พัฒนา MLAT, Cybersecurity Treaty, หรือกรอบความร่วมมือด้านข้อมูลไซเบอร์ร่วมกับประเทศพันธมิตร

3. จัดตั้งหน่วยงานกลางด้านความมั่นคงไซเบอร์ สร้าง Cybersecurity Response Center ระดับชาติ มีอำนาจบังคับใช้กฎหมาย, วิเคราะห์ความเสี่ยง, และตอบสนองภัยคุกคามแบบเรียลไทม์ มีลักษณะ บูรณาการระหว่างภาครัฐ-เอกชน คล้าย ENISA (EU) หรือ CISA (US) ตามมาตรา 8/5 แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับ ที 2) พ.ศ. 2568 กำหนดให้มีการจัดตังและให้อำนาจ แก่ “ศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี” (ศปอท.) ซึ่งสังกัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (DE) หรือ บทบัญญัติมาตรา 8/6 มีการให้อำนาจสำนักงานตำรวจแห่งชาติ กรมสอบสวนคดี

พิเศษ ธนาคารแห่งประเทศไทย หรือหน่วยงานอื่น ของรัฐหรือเอกชนที่รัฐมนตรีประกาศกำหนดแต่งตังผู้แทนเข้าร่วม ปฏิบัติงานในส่วนดังกล่าว

ศปอท. ยังอยู่ภายใต้กระทรวงดิจิทัลฯ ซึ่งเป็น “หน่วยงานนโยบาย” มากกว่า “หน่วยงานปฏิบัติการด้านความมั่นคง”ขาดอำนาจ “บังคับใช้กฎหมาย” โดยตรงเหมือน CISA (สหรัฐฯ) หรือ ENISA (สหภาพยุโรป) ซึ่งมีอำนาจกำหนดมาตรฐาน บังคับใช้ และตรวจสอบความมั่นคงของระบบสารสนเทศของหน่วยงานรัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) มาตรา 8/6 เปิดช่องให้หลายหน่วยงานเข้าร่วม แต่ไม่ได้กำหนด “กลไกบังคับบัญชาร่วม” หรือ “โครงสร้างอำนาจการตัดสินใจ” ที่ชัดเจนส่งผลให้ในภาวะวิกฤติไซเบอร์ อาจเกิดการซ้ำซ้อนหรือความล่าช้าในการตัดสินใจ เช่น ระหว่าง ศปอท., ตำรวจไซเบอร์, DSI, และหน่วย CERT ต่างๆ ทั้งยังขาดงบประมาณ บุคลากร และความต่อเนื่องทางเทคนิคโครงสร้างภายใต้กระทรวง DE ไม่มีงบประมาณและบุคลากรเชี่ยวชาญเทียบเท่าหน่วยงานด้านความมั่นคงหรือหน่วยข่าวกรอง

4. ควรมีการแก้ไขและเพิ่มบทบัญญัติของคำนิยาม พระราชกำหนดการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีพ.ศ.2566 (ฉบับแก้ไข) มาตรา 3 ควรแก้ไขหรือเพิ่มนิยามใน มาตรา 3 พระราชกำหนดการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีพ.ศ.2566 ให้ความหมายของคำสำคัญ เช่น “ระบบคอมพิวเตอร์”, “ข้อมูลคอมพิวเตอร์”, “การเข้าถึงโดยมิชอบ”

สภาพปัญหาของมาตรา 3 ปัจจุบัน (ไทย)

พระราชกำหนดฯพ.ศ.2566มิได้ให้นิยามคำสำคัญบางคำอย่างละเอียด ระบบคอมพิวเตอร์ทั้งข้อมูลคอมพิวเตอร์และการเข้าถึงโดยมิชอบ เป็นต้น แต่ยังไม่มีคำใดที่อธิบายหรือครอบคลุมถึง สื่อปลอมที่สร้างโดย AI เช่น Deepfake เพื่อตอบสนองต่อการป้องอาชญากรรมรูปแบบใหม่และเพิ่มประสิทธิภาพต่อการบังคับใช้กฎหมายให้ดียิ่งขึ้นในอนาคต

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดของอุปกรณ์ที่ทำงานร่วมกันโดยอัตโนมัติเพื่อประมวลผล จัดเก็บ ส่ง หรือรับข้อมูล ไม่ว่าจะอยู่ภายในสถานที่เดียวกันหรือเชื่อมโยงกันผ่านระบบเครือข่าย

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อความ ตัวเลข ภาพ เสียง โปรแกรม หรือข้อมูลอื่นใดในรูปแบบที่สามารถประมวลผลโดยระบบคอมพิวเตอร์ได้

“การเข้าถึงโดยมิชอบ” หมายความว่า การเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต หรือเกินขอบเขตของสิทธิที่ได้รับอนุญาต

“ระบบเทคโนโลยีสารสนเทศที่สำคัญทางโครงสร้างพื้นฐาน” หมายความว่า ระบบคอมพิวเตอร์ที่มีผลกระทบต่อความมั่นคงทางเศรษฐกิจ ความปลอดภัยของรัฐ หรือการดำเนินชีวิตประจำวันของประชาชน

สรุปผลการวิจัย

กฎหมายไทยในปัจจุบันยังมีข้อจำกัดอย่างมากในการรองรับอาชญากรรมทางเทคโนโลยีที่มีลักษณะซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว ทั้งในแง่ของนิยามทางกฎหมายที่ไม่ทันสมัย ขาดความชัดเจน และไม่ครอบคลุมพฤติกรรมที่เกี่ยวข้องกับเทคโนโลยีใหม่ เช่น Deepfake หรือการใช้ AI เพื่อหลอกลวง นอกจากนี้ กฎหมายยังไม่สามารถรับมือกับพฤติกรรมอาชญากรรมรูปแบบใหม่ที่ซับซ้อนและข้ามพรมแดนได้อย่างมีประสิทธิภาพ เช่น การฟอกเงินผ่านสกุลเงินดิจิทัล หรือการหลอกลวงแบบ Hybrid Scam ที่ผสมผสานเทคนิคทางจิตวิทยาเข้ากับแพลตฟอร์มออนไลน์

อีกทั้งบทลงโทษในกฎหมายไทยยังไม่ครอบคลุมและไม่สะท้อนความร้ายแรงของอาชญากรรมเทคโนโลยีได้อย่างแท้จริง การสอบสวนยังขาดเครื่องมือด้านนิติวิทยาศาสตร์ดิจิทัลที่สามารถวิเคราะห์ข้อมูลข้ามแพลตฟอร์มได้อย่างทันท่วงที ขณะเดียวกันมาตรการเร่งด่วนบางประการ เช่น การอายัดบัญชีโดยไม่แจ้งล่วงหน้า ก็อาจกระทบต่อสิทธิของประชาชนโดยไม่มีช่องทางทบทวนหรืออุทธรณ์ที่ชัดเจน ในบริบทของอาชญากรรมข้ามชาติ กฎหมายไทยยังเผชิญกับอุปสรรคสำคัญ ทั้งการไม่มีสนธิสัญญาระหว่างประเทศที่เอื้อต่อการแลกเปลี่ยนข้อมูลหรือร่วมมือสอบสวน รวมถึงการไม่สามารถเข้าถึงข้อมูลจากแพลตฟอร์มต่างประเทศได้เนื่องจากข้อจำกัดทางเขตอำนาจศาล และความร่วมมือเชิงกฎหมายที่ยังขาดแคลน ระบบการแจ้งเตือนภัยและแลกเปลี่ยนข้อมูลไซเบอร์ในระดับสากลก็ยังไม่พัฒนาในระดับที่เพียงพอ

ข้อเสนอแนะจากการวิจัย

จากผลการศึกษาวิจัยเชิงคุณภาพและการวิเคราะห์เปรียบเทียบระบบกฎหมายระหว่างประเทศ พบว่า พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และฉบับแก้ไขเพิ่มเติมในปี พ.ศ. 2568 แม้จะเป็นความพยายามของรัฐในการปรับปรุงกลไกทางกฎหมายให้เท่าทันต่อภัยคุกคามยุคดิจิทัล ทว่าในทางปฏิบัติยังคงปรากฏข้อจำกัดหลายประการในการรับมือกับอาชญากรรมรูปแบบใหม่ โดยเฉพาะอย่างยิ่งอาชญากรรมที่อาศัยเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) และการปลอมแปลงเชิงลึก (Deepfake) ซึ่งมีความซับซ้อน ยากต่อการตรวจสอบ และมีผลกระทบรุนแรงต่อความมั่นคงทางไซเบอร์และความเชื่อมั่นของประชาชน เพื่อเสริมสร้างขีดความสามารถของประเทศไทยในการตอบสนองต่ออาชญากรรมรูปแบบใหม่นี้อย่างมีประสิทธิภาพ เพื่อเป็นศูนย์กลางในการตรวจสอบ วิเคราะห์ และให้ความรู้ทางเทคนิคเกี่ยวกับอาชญากรรมที่มีความซับซ้อนสูง ปัจจุบันแม้จะมีหน่วยงานด้านอาชญากรรมไซเบอร์อยู่แล้ว แต่ยังไม่มีโครงสร้างหรือทรัพยากรที่มุ่งเน้นเรื่อง AI โดยตรง ซึ่งส่งผลให้การสืบสวนในกรณีที่เกี่ยวข้องกับ AI และ Deepfake ขาดความชัดเจนและความเชี่ยวชาญที่จำเป็น

อีกประการหนึ่งที่มีความสำคัญไม่ยิ่งหย่อนไปกว่ากัน โดยควรจัดให้มีหลักสูตรอบรมเฉพาะทาง อาทิ การกู้ข้อมูลจากระบบคลาวด์ การตรวจสอบธุรกรรมผ่านบล็อกเชน และการวิเคราะห์พฤติกรรมผิดปกติด้วย AI ทั้งนี้ การจัดตั้ง “ศูนย์อบรมแห่งชาติด้านอาชญากรรมไซเบอร์และพยานหลักฐานดิจิทัล” ที่มีการรับรองคุณวุฒิในระดับสากล และสามารถเชื่อมโยงกับองค์กรระหว่างประเทศ เช่น International Criminal Police Organization : INTERPOL (องค์การตำรวจสากล) หรือ ASEAN-Japan Cybersecurity Capacity Building Centre จะช่วยยกระดับขีดความสามารถของประเทศไทยได้อย่างเป็นรูปธรรม ในขณะเดียวกัน การเผชิญกับอาชญากรรมไซเบอร์ไม่อาจจำกัดอยู่ในกรอบพรมแดนของประเทศใดประเทศหนึ่ง การจัดตั้งกลไกความร่วมมือระหว่างประเทศในระดับภูมิภาคจึงเป็นสิ่งจำเป็นอย่างยิ่ง เพื่อประสานการแลกเปลี่ยนข้อมูลภัยคุกคามแบบเรียลไทม์ สนับสนุนการสืบสวนคดีข้ามพรมแดนโดยลดขั้นตอนทางการทูต และส่งเสริมการจัดตั้งศูนย์ปฏิบัติการร่วมในระดับภูมิภาค โดยกลไกดังกล่าวควรได้รับการประสานกับองค์กรระหว่างประเทศ เช่น United Nations Office on Drugs and Crime : UNODC, International Criminal Police Organization : INTERPOL (องค์การตำรวจสากล) และ International Telecommunication Union : ITU สหภาพโทรคมนาคมระหว่างประเทศ เพื่อขยายพลังความร่วมมือในระดับโลก

เอกสารอ้างอิง

ชนลดา อินบุตร. (2567). **ปัญหาความมั่นคงไซเบอร์และความร่วมมือในการแก้ปัญหา.** จาก https://so16.tci-thaijo.org/index.php/SJ_SS/article/view/380.

ตำรวจภูธรภาค 9. (2567). **สถิติเหยื่ออาชญากรรมไซเบอร์.** จาก https://www.police9.go.th/สถิติเหยื่ออาชญากรรมไซเบอร์.

ธันย์ธรณ์เทพ แย้มอุทัย. (2568). **การศึกษาปัญหาและอุปสรรคของกฎหมายและนโยบายที่เกี่ยวข้องกับมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี.** จาก https://so06.tci-thaijo.org/index.php/mcjou/article/view/276367.

ธิติรัตน์ สมบูรณ์ (2566). **รู้ เข้าใจและตระหนัก “อาชญากรรมทางไซเบอร์” (Cybercrime) ป้องกันภัยคุกคามใกล้ตัว.** จาก https://www.chula.ac.th/news/138291/.

ธนาคารแห่งประเทศไทย. https://www.bot.or.th/th/satang-story/fraud/call-center.htm.

ปิยอร เปลี่ยผดุง. (2567). **กฎหมายและหน่วยงานที่เกี่ยวข้องกับการบังคับใช้ในการควบคุม ป้องกัน และปราบปรามอาชญากรรมทางการเงินออนไลน์ในประเทศไทย.** จาก https://www.econ.chula.ac.th/download/research/Nualnoi/03-final.pdf.

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566. 20230323_094210_105_13452642.pdf.

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2568 ฉบับที่ 2. https://ratchakitcha.soc.go.th/documents/67320.pdf.

วาสิน มีธรรม และบัณฑิต ขวาโยธา (2564). **ปัญหาการบังคับใช้กฎหมายตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ 2 พ.ศ.2560.** วารสารปัญญาปณิธาน. 6(1) , 135-146.

สถานีโทรทัศน์สำนักงานตำรวจแห่งชาติ. (2566). **สำนักงานตำรวจแห่งชาติ เตือนภัยการฉ้อโกงใน โลกไซเบอร์ อาจส่งผลกระทบ ต่อสาเหตุการเกิดอาชญากรรมที่เกี่ยวข้องกับชีวิต ร่างกายและทรัพย์สินในชีวิตประจำวันได้.** จาก https://policetv.tv/archives/20228.

สรวิศ บุญมี. (2566). **ภัยแก๊งคอลเซ็นเตอร์จากอาชญากรรมทางเศรษฐกิจสู่อาญากรรมทำงเทคโนโลยี.** วารสารวิชาการมหาวิทยาลัยอีสเทิร์นเอเชีย 17(2), 19-26.

สัจจะ โชคบุญส่งสวัสดิ์. (2566). **แนวทางการเพิ่มประสิทธิภาพในการตัดวงจรอาชญากรรมออนไลน์.** จาก https://www.ocsc.go.th/?attachment_id=87343&.

สำนักงานตำรวจแห่งชาติ.(2566). **รายงานสถิติการหลอกลวงทางออนไลน์ 1 มีนาคม 2565- 31 พฤษภาคม 2566.** ออนไลน์. สืบค้นเมื่อ 8 สิงหาคม 2566. แหล่งที่มา http://www.thaipoliceonline.com.

สำนักงานส่งเสริมเศรษฐกิจดิจิทัล. (2566). **เทคโนโลยีที่สำคัญในยุคดิจิทัล: เทคโนโลยีปัญญาประดิษฐ์ Tech Series: Artificial Intelligence (AI).** จาก https://www.depa.or.th/th/article-view/tech-series-artificial-intelligence.

อภิชาติ บวบขม. (2566). **ปัญหาทางกฎหมายในการสอบสวนความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี.** จาก. https://so02.tci-thaijo.org/index.php/JRKSA/article/download/266556/178800/1096195?.

อาริยา สุขโต. (2565). **ภัยอาชญากรรมแก๊งคอลเซ็นเตอร์.** จาก https://library.parliament.go.th/th/radioscript/rr2565-jul7.

Halder, Debarati, Jaishankar, Karuppannan, & Jaishankar, K. (2012). **Cyber crime and the victimization of women: laws, rights and regulations: Information Science** ReferenceIllinois General Assembly. (1999). Illinois Right of Publicity Act (765 ILCS 1075). Retrieved from https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2271&ChapterID=64.

Meland, H.P., Tokas,S., Erdogan, G., Bernsmed,K. & Omerovic,A.(2021) **A Systematic mapping study on cyber security indicator data.** Electronics. 10, e1092. https://doi.org/10.3390/electronics10091092.

New York State Senate. (2020). **Civil Rights Law § 50-f: Prohibited use of a deceased individual's persona for commercial purposes.** Retrieved from https://www.nysenate.gov/legislation/laws/CVR/50-F.

Shelly, G., & Vermaat, M. (2010). **Discovering Computers 2011: Complete: Cengage Learning.Virginia General Assembly.** (2019). § 8.01-42.6. Unauthorized dissemination of sexually explicit images or video. Retrieved from https://law.lis.virginia.gov/vacode/title8.01/chapter3/section8.01-42.6/.