

มาตรการทางกฎหมายเกี่ยวกับการควบคุมการฉ้อโกงผ่านระบบออนไลน์ จากอาชญากรรมข้ามชาติ

Legal Measures to Contract Online Fraud from Transnational Crimes

¹สุทธศิลป์ สิงหวิโรจน์ และ ²รัฐชฎา ฤาแรง

¹Suthasin Singhaviroj, and ²Radchada Lurang

นิติศาสตร์ดุษฎีบัณฑิต มหาวิทยาลัยเวสเทิร์น

Doctor of Laws Western University, Thailand

E-mail: ¹suthasin673@gmail.com, ²Radchada.ji@western.ac.th

Received October 17, 2025; Revised November 24, 2025; Accepted November 30, 2025

บทคัดย่อ

บทความวิจัยนี้มีวัตถุประสงค์ 1) เพื่อศึกษาแนวความคิด ทฤษฎี คำพิพากษา มาตรการทางกฎหมาย และงานวิจัยที่เกี่ยวข้องกับการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติของไทยและต่างประเทศ 2) เพื่อศึกษาปัญหาข้อเท็จจริงและปัญหาทางกฎหมายเกี่ยวกับการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติของไทย 3) เพื่อวิเคราะห์และเปรียบเทียบกฎหมายของไทยกับกฎหมายต่างประเทศเกี่ยวกับการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติ และ 4) เพื่อนำมาตรการทางกฎหมายว่าด้วยการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติของประเทศที่มีความเหมาะสมมาปรับใช้กับกฎหมายไทย เป็นการวิจัยเชิงคุณภาพ ใช้แนวคิดทฤษฎีมาตรการทางกฎหมายสำหรับการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติ ผู้ให้ข้อมูล คือ นักวิชาการ นักกฎหมาย เจ้าหน้าที่ตำรวจ และประชาชน จำนวน 10 คน ใช้วิธีเฉพาะเจาะจง เครื่องมือ 3 ชนิด คือ 1) การสนทนากลุ่ม 2) แบบสัมภาษณ์เชิงลึก 3) อุปกรณ์ในการบันทึกข้อมูล และการสัมภาษณ์เชิงลึก ใช้การวิเคราะห์เนื้อหาแล้วเขียนบรรยายเชิงพรรณนา

ผลการวิจัยพบว่า 1. ควรมีการกำหนดให้มีบทบัญญัติที่ชัดเจนในการควบคุมการฉ้อโกงผ่านระบบออนไลน์โดยอาศัยความร่วมมือระหว่างประเทศ ตามแนวทางของกฎหมายระหว่างประเทศ 2. ควรมีการกำหนดให้มีการออกมาตรการหรือกำหนดนโยบายในการส่งเสริม สนับสนุน กำหนดกรอบการฝึกอบรมและการพัฒนาศักยภาพของบุคลากร 3. ควรให้มีการกำหนดกำหนดบทลงโทษขององค์กรอาชญากรรมข้ามชาติสำหรับคดีฉ้อโกงผ่านระบบออนไลน์ให้เหมาะสมกับความเสียหาย

ที่เกิดขึ้น ตามแนวทางของกฎหมายต่างประเทศ และ 4. ควรให้มีการกำหนดมาตรการขดเซยเยียวยา
ผู้เสียหายทางแพ่งจากการฉ้อโกงผ่านระบบออนไลน์ของกลุ่มองค์กรอาชญากรรมข้ามชาติ

คำสำคัญ: การฉ้อโกง; ระบบออนไลน์; อาชญากรรมข้ามชาติ

Abstract

This article aimed to (1) study concepts, theories, court judgments, legal measures, and related research on the control of online fraud from transnational crime in Thailand and abroad; (2) examine the factual and legal issues concerning the control of online fraud in Thailand; (3) analyze and compare Thai law with foreign laws; and (4) apply suitable international legal measures to Thai law. This was qualitative research that used theoretical concepts of legal measures for controlling online fraud. The informants included 10 individuals: academics, legal experts, police officers, and members of the public. The study used purposive sampling, and research instruments consisted of focus groups and in-depth interviews. The analysis was conducted through content analysis and descriptive narration.

The research findings revealed that: 1. Clear provisions should be established to control online fraud through international cooperation, following international law guidelines. 2. Measures or policies should be implemented to promote and set frameworks for personnel training and capacity building. 3. Penalties for transnational criminal organizations should be appropriately determined according to the damage caused, in line with international standards. 4. Measures should be set to compensate and provide remedies to victims of online fraud by transnational criminal organizations. These findings highlight the necessity for Thailand to modernize its legal framework and strengthen cross-border collaboration to effectively combat the evolving nature of transnational online fraud.

Keywords: Fraud; Online Systems; Transnational Crime

บทนำ

อาชญากรรมทางเทคโนโลยีในรูปแบบการฉ้อโกงผ่านระบบออนไลน์มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องและมีรูปแบบที่ซับซ้อนมากยิ่งขึ้น การพัฒนาอย่างรวดเร็วของเทคโนโลยีทางการเงินส่งผลให้การทำธุรกรรมทางอิเล็กทรอนิกส์มีความสะดวกสบายมากขึ้น แต่ความสะดวกสบายดังกล่าวมาพร้อมกับความเสี่ยงในหลายมิติ ทั้งในด้านการเข้าถึงบริการทางการเงิน การจัดการทางการเงินส่วนบุคคล และการลงทุน เทคโนโลยีทางการเงินช่วยอำนวยความสะดวกให้ประชาชนสามารถเข้าถึงบริการทางการเงินได้อย่างรวดเร็ว ไม่ว่าจะเป็นการโอนเงิน การชำระค่าสินค้าและบริการ หรือการลงทุน

นอกจากนี้ ยังช่วยให้ประชาชนสามารถจัดการการเงินส่วนบุคคลได้อย่างมีประสิทธิภาพผ่านแอปพลิเคชันและแพลตฟอร์มต่าง ๆ (คำว่า "แพลตฟอร์ม (Platform)" หมายถึง รากฐานหรือกรอบการทำงาน ที่สร้างขึ้นเพื่อเชื่อมโยงกลุ่มผู้ใช้งานที่แตกต่างกันให้โต้ตอบ แลกเปลี่ยน หรือใช้บริการร่วมกันได้ ทำหน้าที่เป็นตัวกลาง ในการสร้าง แลกเปลี่ยนสินค้า บริการ หรือข้อมูล ทำให้เทคโนโลยีหรือแอปพลิเคชันอื่น ๆ สามารถพัฒนาและทำงานร่วมกันได้) แพลตฟอร์มต่าง ๆ นี้จะช่วยสนับสนุนการติดตามงบประมาณ และการลงทุน อย่างไรก็ตาม การใช้จ่ายเงินทางออนไลน์ที่สะดวกสบายยิ่งขึ้นกลับเปิดโอกาสให้ผู้ไม่หวังดีสามารถเข้าถึงทรัพย์สินของประชาชนได้ง่ายขึ้นเช่นกัน

ราชอาณาจักรไทยซึ่งเป็นประเทศที่ได้รับความเสียหายจากการฉ้อโกงออนไลน์ในระดับสูง มักใช้กลไกทางตำรวจในการจัดการคดีฉ้อโกงผ่านระบบออนไลน์เป็นหลัก การใช้กลไกทางตำรวจในการดำเนินคดีมักเป็นแนวทางที่มีประสิทธิภาพในการป้องกันการฉ้อโกงได้ต่ำ เนื่องจากเมื่อ ผู้ไม่หวังดีได้รับเงินจากเหยื่อแล้วมักจะกระจายเงินผ่านบัญชีม้า คือ บัญชีที่ลงทะเบียนด้วยชื่อบุคคลอื่นเพื่อการก่ออาชญากรรมหลายชั้นเพื่อหลบเลี่ยงการสำรวจถึงตัวผู้ก่อเหตุ กระบวนการดังกล่าวเกิดขึ้นอย่างรวดเร็วภายในไม่กี่นาที ส่งผลให้เจ้าหน้าที่ตำรวจมักกระอักกระอ่วนไม่ทันกับที่ผู้กระทำผิดจะเอาเงินออกจากระบบ และมีโอกาสน้อยที่จะสามารถนำทรัพย์สินมาคืนให้แก่ผู้เสียหายได้ ด้วยเหตุนี้ การฉ้อโกงผ่านระบบออนไลน์จึงเป็นภัยคุกคามทางเศรษฐกิจและความมั่นคงในระดับโลกที่เติบโตอย่างรวดเร็ว ซึ่งปัจจุบันก่อให้เกิดปัญหาต่าง ๆ ซึ่งปัจจุบันทำให้มี ปัญหาข้อเท็จจริง เช่น

1. ปัญหาความร่วมมือในการควบคุมการฉ้อโกงผ่านระบบออนไลน์ด้วยความร่วมมือระหว่างประเทศ
 2. ปัญหาการขาดการฝึกอบรมและพัฒนาขีดความสามารถของเจ้าหน้าที่ที่เกี่ยวข้องเพื่อยับยั้งองค์กรอาชญากรรมข้ามชาติ
 3. ปัญหาการกำหนดบทลงโทษขององค์กรอาชญากรรมข้ามชาติกรณีฉ้อโกงผ่านระบบออนไลน์ซึ่งมีอัตราโทษน้อยเกินไป
 4. ปัญหาการกำหนดมาตรการโดยให้ผู้กระทำผิดต้องร่วมรับผิดชอบโดยการชดเชยเยียวยาช่วยเหลือผู้เสียหายจากการฉ้อโกงผ่านระบบออนไลน์ขององค์กรอาชญากรรมข้ามชาติ
- ปัญหาข้อกฎหมาย เช่น

1. ในราชอาณาจักรไทยยังขาดบทบัญญัติที่ชัดเจนในการควบคุมการฉ้อโกงผ่านระบบออนไลน์โดยอาศัยความร่วมมือระหว่างประเทศ
2. พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 ยังไม่ได้กำหนดกรอบการฝึกอบรมและการพัฒนาศักยภาพของบุคลากรที่ปฏิบัติหน้าที่ในการป้องกันและปราบปรามองค์กรอาชญากรรมข้ามชาติ
3. พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2)

พ.ศ.2568 ยังไม่ได้กำหนดบทลงโทษขององค์กรอาชญากรรมข้ามชาติสำหรับคดีฉ้อโกงผ่านระบบออนไลน์ให้เหมาะสมกับความเสียหายที่เกิดขึ้น

4. พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ.2568 ยังคงขาดมาตรการชดเชยเยียวยาผู้เสียหายทางแพ่งจากการฉ้อโกงผ่านระบบออนไลน์ของกลุ่มองค์กรอาชญากรรมข้ามชาติ

จากปัญหาดังกล่าวผู้วิจัยจึงมีความสนใจที่จะศึกษาแนวความคิดและหลักการพื้นฐานสำคัญเกี่ยวกับการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติของประเทศที่ใช้ระบบกฎหมายลายลักษณ์อักษร (Civil Law System) ราชอาณาจักรเดนมาร์ก ประเทศที่ใช้ระบบกฎหมายจารีตประเพณี (Common Law System) สหราชอาณาจักร สหรัฐอเมริกา สาธารณรัฐสิงคโปร์ ศึกษาสภาพปัญหาและความเป็นมาของปัญหาเกี่ยวกับการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติในระบบกฎหมายของราชอาณาจักรไทย เพื่อวิเคราะห์เปรียบเทียบการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติของราชอาณาจักรไทยกับต่างประเทศอื่นจะนำไปสู่การพัฒนากฎหมายการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติของราชอาณาจักรไทยในส่วนที่เกี่ยวข้องเพื่อให้เป็นที่ยอมรับ น่าเชื่อถือ และมีความทัดเทียมนานาชาติอารยประเทศมากยิ่งขึ้น ทั้งนี้ ผู้วิจัยคาดหวังว่างานวิจัยนี้จะมีส่วนช่วยส่งเสริมและสามารถนำไปใช้ประโยชน์สำหรับการพัฒนากฎหมายเพื่อต่อต้านภัยคุกคามจากองค์กรอาชญากรรมข้ามชาติ และปกป้องความสงบเรียบร้อยและความมั่นคงของประเทศของราชอาณาจักรไทยในอนาคตต่อไป

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาแนวความคิด ทฤษฎี คำพิพากษา มาตรการทางกฎหมาย และงานวิจัยที่เกี่ยวข้องกับการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติของไทยและต่างประเทศ
2. เพื่อศึกษาปัญหาข้อเท็จจริงและปัญหาทางกฎหมายเกี่ยวกับการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติของไทย รวมทั้งแนวทางในการแก้ไขข้อบกพร่องทางกฎหมาย
3. เพื่อวิเคราะห์และเปรียบเทียบกฎหมายของไทยกับกฎหมายต่างประเทศเกี่ยวกับการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติ เพื่อศึกษาความเหมือนและความแตกต่าง
4. เพื่อนำมาตรการทางกฎหมายว่าด้วยการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติของประเทศที่มีความเหมาะสมมาปรับใช้กับกฎหมายไทย เพื่อให้เกิดการยอมรับและสามารถเทียบเคียงกับมาตรฐานสากลได้

การทบทวนวรรณกรรม

แนวคิด และทฤษฎีที่เกี่ยวกับมาตรการทางกฎหมายเกี่ยวกับการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติของราชอาณาจักรไทยและต่างประเทศ การฉ้อโกงผ่านระบบออนไลน์ประกอบด้วยรูปแบบการกระทำความผิดที่หลากหลาย อันได้แก่ การหลอกลวง การโจรกรรมข้อมูล การละเมิดสิทธิส่วนบุคคล การบุกรุกระบบคอมพิวเตอร์ และการเผยแพร่เนื้อหาที่ไม่เหมาะสม การกระทำผิดกฎหมายดังกล่าวก่อให้เกิดความเสียหายทั้งทางด้านเศรษฐกิจและสังคมในวงกว้าง จากเหตุผลข้างต้น ผู้วิจัยจึงได้ดำเนินการศึกษาแนวคิดและทฤษฎีที่เกี่ยวข้องกับมาตรการทางกฎหมายในการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติในราชอาณาจักรไทยและประเทศต่างๆ โดยครอบคลุมประเด็นศึกษาดังต่อไปนี้

แนวคิดและวิวัฒนาการเกี่ยวกับการกระทำความผิดฐานฉ้อโกง

Yar and Steinmetz (2019) ระบุว่าบริบทสังคมดิจิทัลสร้างรูปแบบการฉ้อโกงใหม่ที่เกิดจากโอกาสทางเทคโนโลยี ซึ่งแตกต่างจากฉ้อโกงออฟไลน์ทั้งในเจตนา วิธีการและผลกระทบ โดย Holt et al. (2015) วิเคราะห์ว่าเจตนาและพฤติกรรมของผู้ก่อเหตุออนไลน์มีลักษณะซ่อนเร้นและใช้เทคโนโลยีเป็นตัวกลาง จึงควรจัดองค์ประกอบความผิดต่างจากการฉ้อโกงทั่วไป อย่างไรก็ตาม UNODC (2022) ยืนยันว่า online fraud เป็น cyber-enabled crime ที่ต้องใช้กฎหมายเฉพาะเพราะข้ามพรมแดน รวดเร็ว และซับซ้อนกว่าการฉ้อโกงแบบเดิม

แนวคิดการชดเชยเยียวยาผู้เสียหาย (Compensation for Victims)

UN (1985) วางหลักสากลว่าสิทธิการชดเชยคือองค์ประกอบสำคัญของความยุติธรรม และรัฐควรมีกองทุนช่วยเหลือผู้เสียหายโดยตรง ด้าน OVC (2020) แสดงให้เห็นว่าเงินกองทุนชดเชยผู้เสียหายสหรัฐฯ ช่วยลดภาระผู้เสียหายและเพิ่มความเชื่อมั่นต่อกระบวนการยุติธรรม ทั้งนี้ Singapore Ministry of Law (2021) ระบุว่ารัฐจัดให้มีการชดเชยแก่ผู้เสียหายเพื่อสร้างความเป็นธรรมและลดภาระความเสียหายที่เกิดจากอาชญากรรม เช่นเดียวกับ Wemmers (2017) ที่เน้นย้ำว่าการชดเชยผู้เสียหายเป็นสิทธิพื้นฐานและเป็นการฟื้นฟูความเชื่อมั่นต่อรัฐและกระบวนการยุติธรรม

แนวคิดการควบคุมอาชญากรรม (Crime Control Theory)

นำมาใช้ในการกำหนดแนวทางการบังคับใช้กฎหมายและการสร้างกลไกป้องกันเชิงรุก เช่น การบังคับใช้พระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และการสร้างความร่วมมือระหว่างประเทศในการสืบสวนคดีอาชญากรรมข้ามชาติ (Wilson & Kelling, 1982)

ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory)

อธิบายโครงสร้างของอาชญากรรมออนไลน์ประกอบด้วย “ผู้กระทำความผิด –เหยื่อ – โอกาส” โดยเสนอว่าการลดโอกาสในการก่อเหตุผ่านมาตรการด้านเทคโนโลยี กฎหมาย และการเฝ้าระวังธุรกรรมออนไลน์สามารถลดอาชญากรรมได้ (Clarke, 1997; Cornish & Clarke, 2003)

ทฤษฎีหน้าต่างแตก (Broken Windows Theory)

ใช้วิเคราะห์เชิงนโยบายสาธารณะ โดยเสนอว่าการไม่จัดการกับพฤติกรรมเล็กน้อย เช่น การหลอกลวงหรือสแปม อาจนำไปสู่การก่ออาชญากรรมรุนแรงขึ้น ดังนั้นควรมีมาตรการควบคุมตั้งแต่ระดับเบื้องต้นเพื่อสร้างความยำเกรงต่อกฎหมายดิจิทัล (Wilson & Kelling, 1982)

ทฤษฎีการเรียนรู้ทางสังคม (Social Learning Theory)

อธิบายพฤติกรรมและการเลียนแบบของผู้กระทำผิดในสังคมออนไลน์ และเสนอแนวทางสร้างวัฒนธรรมดิจิทัลปลอดภัยผ่านการให้ความรู้และสร้างจิตสำนึกแก่ประชาชนในครอบครัว ชุมชน และสถานศึกษา (Bandura, 1977; Akers, 1998)

จากการทบทวนวรรณกรรมและแนวคิดทางทฤษฎีที่เกี่ยวข้อง ผู้วิจัยได้นำแนวคิดเกี่ยวกับการฉ้อโกงออนไลน์ การชดเชยเยียวยาผู้เสียหาย และทฤษฎีการควบคุมอาชญากรรม สามเหลี่ยมอาชญากรรม หน้าต่างแตก และการเรียนรู้ทางสังคม มาประยุกต์ใช้เพื่อสร้างกรอบแนวคิดของการวิจัยอย่างครบถ้วน ทั้งในด้านการทำความเข้าใจลักษณะและเจตนาของผู้กระทำผิด การป้องกันและลดโอกาสเกิดอาชญากรรม การคุ้มครองสิทธิผู้เสียหาย และการสร้างวัฒนธรรมดิจิทัลปลอดภัย การประยุกต์ใช้ทฤษฎีเหล่านี้ช่วยให้การวิจัยมีความรอบด้านและเป็นระบบ พร้อมเสนอแนวทางในการปรับปรุงมาตรการทางกฎหมายและนโยบายการป้องกันการฉ้อโกงผ่านระบบออนไลน์อย่างมีประสิทธิภาพ

ระเบียบวิธีวิจัย

การศึกษานี้เป็นงานวิจัยเชิงคุณภาพ (Qualitative Research) มุ่งวิเคราะห์มาตรการทางกฎหมายในการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติของประเทศไทย โดยใช้การวิเคราะห์เชิงพรรณนา (Descriptive Analysis) และการสังเคราะห์เนื้อหา (Content Synthesis) เพื่อเสนอแนวทางเชิงนโยบายที่เหมาะสมกับบริบทปัจจุบัน

กลุ่มตัวอย่างและการเก็บข้อมูล

ผู้ให้ข้อมูลหลักจำนวน 10 คน ได้รับการคัดเลือกแบบเฉพาะเจาะจง (Purposive Sampling) ครอบคลุม 4 กลุ่ม ได้แก่ (1) นักวิชาการด้านกฎหมายและสังคมศาสตร์ (2) นักกฎหมายและผู้เชี่ยวชาญด้านนิติศาสตร์ (3) เจ้าหน้าที่ตำรวจผู้บังคับใช้กฎหมาย และ (4) ประชาชนผู้มีประสบการณ์เกี่ยวกับอาชญากรรมทางเทคโนโลยี เพื่อให้ได้มุมมองที่หลากหลายและสะท้อนปัญหาเชิงระบบได้อย่างครอบคลุม

การเก็บรวบรวมข้อมูลดำเนินการโดยใช้การสัมภาษณ์เชิงลึก (In-depth Interview) และการสนทนากลุ่ม (Focus Group Discussion) เป็นเครื่องมือหลัก ครอบคลุมประเด็นสำคัญ 5 ด้าน ได้แก่ ข้อมูลทั่วไป ความรู้ความเข้าใจในกฎหมาย สภาพปัญหาและข้อจำกัด ความร่วมมือระหว่างหน่วยงาน และข้อเสนอแนะเชิงนโยบาย

นอกจากนี้ ผู้วิจัยได้ศึกษาข้อมูลจากเอกสารทางกฎหมายและงานวิจัยที่เกี่ยวข้อง ทั้งกฎหมายระหว่างประเทศ กฎหมายของประเทศคู่เทียบ (เช่น สหรัฐอเมริกา สหภาพยุโรป และสิงคโปร์) และกฎหมายไทย อาทิ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2568 รวมถึงรายงานทางสถิติ บทความวิชาการ และเอกสารจากหน่วยงานรัฐที่เกี่ยวข้อง

การวิเคราะห์ข้อมูล

ข้อมูลเชิงคุณภาพทั้งหมดถูกวิเคราะห์ด้วยวิธีการวิเคราะห์เชิงเนื้อหา (Content Analysis) และการสังเคราะห์เชิงเปรียบเทียบ (Comparative Synthesis) ระหว่างข้อมูลจากผู้ให้สัมภาษณ์และเอกสารทางวิชาการ เพื่อหาความเชื่อมโยงระหว่างมาตรการทางกฎหมายของไทยกับแนวทางของต่างประเทศ ทั้งนี้ ผู้วิจัยได้ตรวจสอบความน่าเชื่อถือของข้อมูลด้วยการตรวจสอบสามเส้า (Triangulation) จากหลายแหล่งข้อมูล ก่อนสรุปผลในเชิงพรรณนาและจัดทำข้อเสนอเชิงนโยบายเพื่อปรับปรุงระบบกฎหมายไทยให้เท่าทันอาชญากรรมทางเทคโนโลยี

ผลการวิจัย

การวิจัยครั้งนี้มุ่งทำความเข้าใจ “มาตรการทางกฎหมายในการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติ” โดยอาศัยข้อมูลจากการวิเคราะห์เอกสารกฎหมายและมาตรการระหว่างประเทศควบคู่กับการสัมภาษณ์เชิงลึกผู้เชี่ยวชาญด้านกระบวนการยุติธรรมจำนวน 10 คน ผลการศึกษาที่ได้สะท้อนภาพรวมทั้งในเชิงแนวคิด ทฤษฎี กฎหมายเปรียบเทียบ และข้อเท็จจริงเชิงปฏิบัติ นำไปสู่ข้อค้นพบตามวัตถุประสงค์ของการวิจัยทั้งสี่ประการอย่างสอดคล้องต่อเนื่องกัน

1. แนวความคิด ทฤษฎี คำพิพากษา มาตรการทางกฎหมายกับการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติของไทยและต่างประเทศ ผลการวิจัยพบว่า การทบทวนองค์ความรู้ชี้ให้เห็นว่า ประเทศต่าง ๆ ที่รับมือกับการฉ้อโกงออนไลน์อย่างได้ผลล้วนตั้งอยู่บนฐานคิดทางอาชญาวิทยาที่เน้น “การควบคุมเชิงรุก” มากกว่า “การลงโทษภายหลัง” โดยเฉพาะแนวคิดการควบคุมอาชญากรรมในฐานะกระบวนการทางสังคมที่ต้องอาศัยการทำงานร่วมกันของสถาบันรัฐและผู้มีส่วนเกี่ยวข้อง (Reiss, 1983) การลด “โอกาส” ตามสามเหลี่ยมอาชญากรรมผ่านมาตรการทางเทคโนโลยีและกฎเกณฑ์ที่เข้มงวด (Eck, 2003) การบังคับใช้กฎหมายอย่างสม่ำเสมอแต่ต่อความผิดเล็กน้อยเพื่อไม่ให้ปัญหาลุกลาม (Wilson & Kelling, 1982) และการสร้างภูมิคุ้มกันทางสังคมเพื่อลดการเลียนแบบรูปแบบการกระทำผิดในพื้นที่ออนไลน์ (Bandura, 1977) เมื่อนำกรอบคิดเหล่านี้ไปพิจารณาพร้อมข้อกฎหมายเฉพาะของต่างประเทศเช่น CFAA ของสหรัฐอเมริกา, Cybersecurity Act ของสิงคโปร์ และกรอบกำกับความยืดหยุ่นเชิงปฏิบัติการด้านดิจิทัลจะเห็นภาพของระบบกฎหมายที่ผสมผสานกลไกป้องกัน สอดส่อง และบังคับใช้เข้าด้วยกันอย่างเป็นระบบ ขณะที่บริบทไทยแม้มีกฎหมายเกี่ยวข้องหลายฉบับ แต่ยังขาดกลไกบูรณาการระหว่างประเทศและมาตรการเยียวยาผู้เสียหายที่เป็นรูปธรรม

จึงเกิด “ช่องว่างเชิงโครงสร้าง” ในการควบคุมการฉ้อโกงออนไลน์ (สำนักงานป้องกันและปราบปรามการฟอกเงิน, 2566)

2. ปัญหาข้อเท็จจริงและปัญหาทางกฎหมายเกี่ยวกับการควบคุมการฉ้อโกงผ่านระบบออนไลน์ จากอาชญากรรมข้ามชาติของไทย ผลการวิจัยพบว่า การวิเคราะห์ข้อมูลจากการสัมภาษณ์ผู้เชี่ยวชาญสะท้อนข้อจำกัดสำคัญของการบังคับใช้กฎหมายไทยในลัทธิที่เกี่ยวพันกัน ได้แก่ การขาดกลไกความร่วมมือระหว่างประเทศและช่องทางแลกเปลี่ยนข้อมูลต่อเนื่อง ทำให้การติดตามอาชญากรข้ามแดนและเส้นทางการเงินเป็นไปได้ยากลำบาก (UNODC, 2022) ความเหลื่อมล้ำด้านสมรรถนะบุคลากร โดยเฉพาะทักษะสืบสวนดิจิทัลเชิงลึก เช่น การติดตามธุรกรรมบนบล็อกเชนหรือการพิสูจน์หลักฐานข้อมูลขนาดใหญ่ ซึ่งเป็นจุดอ่อนของกระบวนการยุติธรรมดิจิทัล กรอบทฤษฎีที่ไม่สอดคล้องกับความเสียหายจำนวนมาก จึงไม่ก่อแรงยับยั้งเพียงพอ (ศปอส.ตร., 2567) และการขาดกลไกเยียวยาผู้เสียหายในระดับระบบ ส่งผลให้เหยื่อจำนวนมากไม่สามารถเข้าถึงความเป็นธรรมได้ทันเวลาที่จำเป็นต้องมีเครื่องมือทางกฎหมายเฉพาะเพื่อจัดตั้งกองทุนเยียวยาหรือมาตรการชดเชยที่มีประสิทธิภาพ

3. วิเคราะห์และเปรียบเทียบกฎหมายของไทยกับกฎหมายต่างประเทศเกี่ยวกับการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติ เพื่อศึกษาความเหมือนและความแตกต่าง

ตารางที่ 1 การวิเคราะห์และเปรียบเทียบกฎหมายไทยกับกฎหมายต่างประเทศเกี่ยวกับการควบคุมการฉ้อโกงออนไลน์จากอาชญากรรมข้ามชาติ

ประเด็นเปรียบเทียบ	ประเทศพัฒนาแล้ว (ตัวอย่าง: สหรัฐอเมริกา, สหราชอาณาจักร)	ประเทศในระบบกฎหมาย ลายลักษณ์อักษร (ตัวอย่าง: เคนยา, สิงคโปร์)	ประเทศไทย	การอ้างอิงหลัก
โครงสร้างระบบกฎหมาย	ระบบกฎหมายจารีตประเพณี (Common Law) – ยึดหยุ่นสูง ใช้คดีตัวอย่างเป็นบรรทัดฐาน	ระบบกฎหมายลายลักษณ์อักษร (Civil Law) – ยึดบทบัญญัติกฎหมายที่ชัดเจน	ระบบลายลักษณ์อักษรแบบผสม แต่มีข้อจำกัดในการตีความและบังคับใช้	Council of Europe (2021); UNODC (2022)
กลไกกำหนดความรับผิดชอบ	ใช้ทั้งความรับผิดชอบทางอาญาและแพ่งร่วมกัน เพื่อให้สามารถลงโทษและชดเชยความเสียหาย	เน้นความรับผิดชอบทางอาญา และมาตรการทางปกครอง โดยมีการคืนทรัพย์สินผ่านกระบวนการยุติธรรม	เน้นทางอาญาเป็นหลัก ขาดความเชื่อมโยงกับความรับผิดชอบทางแพ่งและการเยียวยาผู้เสียหาย	Council of Europe (2021)
กระบวนการคืนทรัพย์สิน	มีระบบศาลเฉพาะทางและกลไกยึดทรัพย์ได้รวดเร็ว (asset recovery)	ใช้ระบบการประสานงานข้ามชาติและฐานข้อมูลร่วมระหว่างหน่วยงาน	กระบวนการคืนทรัพย์สินยังช้าและซับซ้อน ขาดความร่วมมือข้ามหน่วยงาน	UNODC (2022)
โครงสร้างสถาบันและการประสานข้อมูล	มีศูนย์ข้อมูลกลางระดับชาติ เช่น FBI Cyber Division, NCA Cybercrime Unit	มีระบบ centralized database ที่เชื่อมโยงกับสถาบันการเงินและหน่วยข่าวกรองไซเบอร์	ขาดกลไกเชื่อมโยงข้อมูลข้ามหน่วยงานและข้ามพรมแดน	Council of Europe (2021); UNODC (2022)

ประเด็น เปรียบเทียบ	ประเทศพัฒนาแล้ว (ตัวอย่าง: สหรัฐอเมริกา, สหราชอาณาจักร)	ประเทศในระบบกฎหมาย ลายลักษณ์อักษร (ตัวอย่าง: เดนมาร์ก, สิงคโปร์)	ประเทศไทย	การอ้างอิงหลัก
การฝึกอบรมและ ศักยภาพ เจ้าหน้าที่	มีหลักสูตรเฉพาะด้าน digital forensics และ cyber investigation ที่ต่อเนื่อง	มีการฝึกอบรมเชิงเทคนิค ภายใต้กฎหมายความมั่นคง ไซเบอร์ (Cybersecurity Act)	มีการอบรมไม่ต่อเนื่อง ขาดมาตรฐานกลางและ การประเมินสมรรถนะ ระยะยาว	UNODC (2022)
มาตรการเยียวยา ผู้เสียหาย	ศาลสามารถมีคำสั่งชดใช้ ค่าเสียหายและคืนทรัพย์สิน อัตโนมัติ	มีกองทุนช่วยเหลือผู้เสียหาย และกลไกฟ้องแบบรวม (class action)	ไม่มีระบบเยียวยาโดยรัฐ หรือกองทุนเฉพาะทาง	Council of Europe (2021)
มาตรฐานความ ร่วมมือระหว่าง ประเทศ	มีสนธิสัญญาและข้อตกลง ร่วม (MLATs, Budapest Convention)	มีการขอความร่วมมือภายใต้ สหภาพยุโรปและอาเซียน	เข้าร่วมอนุสัญญาบาง ฉบับแต่ยังไม่มีการอบรม ระดับภูมิภาคที่ชัดเจน	Council of Europe (2021); UNODC (2022)

ผลการวิจัยพบว่า ภาพที่ปรากฏชัดคือ ความแตกต่างเชิงระบบกฎหมายกับสถาปัตยกรรมสถาบันของประเทศพัฒนาแล้วกับไทย ประเทศในระบบจารีตประเพณี เช่น สหรัฐอเมริกาและสหราชอาณาจักร ใช้การกำหนดความรับผิดชอบทั้งอาญาและแพ่งควบคู่ พร้อมกลไกยึดและคืนทรัพย์สินแก่ผู้เสียหายผ่านศาลอย่างคล่องตัว ขณะที่ประเทศในระบบลายลักษณ์อักษร เช่น เดนมาร์กและสิงคโปร์ เน้นสถาปนาระบบข้อมูลรวมศูนย์และการยกระดับทักษะเจ้าหน้าที่อย่างต่อเนื่อง กรอบเปรียบเทียบนี้ยืนยันว่า ไทยยังขาดองค์ประกอบหลักสามประการ ได้แก่ กลไกเชื่อมโยงข้อมูลข้ามแดน ระบบฝึกอบรมระดับปฏิบัติการที่ยั่งยืน และมาตรการเยียวยาโดยรัฐ ส่งผลให้ประสิทธิภาพการควบคุมอาชญากรรมออนไลน์ยังไม่อาจเทียบมาตรฐานสากล (Council of Europe, 2021; UNODC, 2022)

4. มาตรการทางกฎหมายว่าด้วยการควบคุมการร้องไต่ถามผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติของประเทศที่มีความเหมาะสมมาปรับใช้กับกฎหมายไทย เพื่อให้เกิดการยอมรับและสามารถเทียบเคียงกับมาตรฐานสากลได้ ผลการวิจัยพบว่า การสังเคราะห์มาตรการที่เหมาะสมเพื่อนำมาปรับใช้ในไทยนำไปสู่ข้อเสนอเชิงระบบ 4 ประการที่เชื่อมโยงกับข้อค้นพบก่อนหน้าอย่างเป็นเหตุเป็นผล ประการที่ 1 การเสริมสร้างความร่วมมือระหว่างประเทศผ่านศูนย์ประสานงานกลางด้านอาชญากรรมไซเบอร์ที่ทำหน้าที่รวบรวม แลกเปลี่ยน และวิเคราะห์ข้อมูล เทียบเคียงบทบาทของศูนย์ระดับภูมิภาคในต่างประเทศ ประการที่ 2 การพัฒนาสมรรถนะบุคลากรด้วยสถาบันฝึกอบรมเฉพาะทางด้านสืบสวนดิจิทัล เพื่อเติมเต็มจุดอ่อนด้านทักษะเชิงเทคนิค ประการที่ 3 การปรับปรุงกรอบโทษและขยายความรับผิดชอบทางแพ่งให้สอดคล้องกับความร้ายแรงและความเสียหายจริง เพิ่มแรงยับยั้งและความรับผิดชอบในองค์กรอาชญากรรม และประการที่ 4 การจัดตั้งกองทุนเยียวยาผู้เสียหายจากอาชญากรรมออนไลน์ เพื่อให้ความช่วยเหลือทางการเงินเบื้องต้นโดยไม่ต้องรอผลคดีถึงที่สุด มาตรการทั้ง 4 ด้านนี้ทำหน้าที่เกาะเกี่ยวกันเป็น “แพ็คเกจนโยบาย” ที่ปรับสมดุลระหว่างการป้องกันปราบปราม และเยียวยา สอดรับกับข้อเท็จจริงเชิงปฏิบัติและแนวโน้มสากล (UNODC, 2022)

โดยภาพรวม ผลการวิจัยจึงชี้ว่าการยกระดับประสิทธิภาพกฎหมายไทยในการควบคุมการฉ้อโกงออนไลน์ต้องเปลี่ยนจากแนวทางเชิงรับไปสู่แนวทางเชิงรุก ผ่านโครงสร้างความร่วมมือระหว่างประเทศที่ชัดเจน การพัฒนาศักยภาพบุคลากรตามโจทย์เทคโนโลยีสมัยใหม่ กรอบโทษและความรับผิดชอบที่สมส่วน และระบบเยียวยาที่เข้าถึงได้จริง เมื่อองค์ประกอบเหล่านี้ถูกออกแบบและขับเคลื่อนร่วมกันอย่างเป็นระบบ ไทยก็จะสามารถยกระดับการคุ้มครองประชาชนและความเชื่อมั่นในระบบเศรษฐกิจดิจิทัลได้อย่างยั่งยืนบนมาตรฐานสากล

อภิปรายผลการวิจัย

ผลจากการวิจัยวัตถุประสงค์ที่ 1 พบว่า การควบคุมการฉ้อโกงผ่านระบบออนไลน์ในประเทศไทยยังอยู่ในระดับที่ไม่สมบูรณ์และไม่สอดคล้องกับมาตรฐานสากล แม้ว่ารัฐบาลจะมีการตรากฎหมายที่เกี่ยวข้องหลายฉบับ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (แก้ไขเพิ่มเติม พ.ศ.2560 และ 2566) และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2568 แต่กฎหมายเหล่านี้ยังไม่สามารถรองรับลักษณะของ “อาชญากรรมข้ามชาติ” ที่มีการเคลื่อนย้ายข้อมูล การเงิน และเครือข่ายผู้กระทำความผิดข้ามพรมแดนได้อย่างมีประสิทธิภาพ ทั้งนี้อาจเป็นเพราะ โครงสร้างการบริหารจัดการทางกฎหมายของประเทศไทยยังขาด “กลไกบูรณาการ” ระหว่างหน่วยงานหลัก เช่น สำนักงานตำรวจแห่งชาติ สำนักงานอัยการสูงสุด ธนาคารแห่งประเทศไทย และสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ซึ่งทำให้เกิดความซ้ำซ้อนในการดำเนินงานและขาดศูนย์กลางข้อมูลกลางที่ใช้ในการติดตามการกระทำความผิดทางเทคโนโลยี นอกจากนี้ การศึกษาเชิงเอกสารยังพบว่า กฎหมายไทยยังขาดมาตรการด้าน “การป้องกันล่วงหน้า” (Preventive Legal Measures) ที่มีอยู่ในต่างประเทศ เช่น สหรัฐอเมริกาและสหราชอาณาจักร ซึ่งใช้กลไกการเฝ้าระวังเชิงรุก (Proactive Surveillance) และระบบการแบ่งปันข้อมูลระหว่างหน่วยงาน (Data Sharing) เพื่อป้องกันอาชญากรรมไซเบอร์ตั้งแต่ต้นทาง (Council of Europe, 2021)

ผลการวิจัยข้อนี้จึงสอดคล้องกับแนวคิดของ Reiss (1983) ที่เสนอว่า “การควบคุมอาชญากรรมที่มีประสิทธิภาพต้องอาศัยกระบวนการทางสังคมร่วมกับกลไกทางกฎหมาย” ซึ่งในกรณีของประเทศไทยยังคงมีช่องว่างระหว่าง “ตัวบทกฎหมาย” กับ “การบังคับใช้จริง” อันเป็นสาเหตุหลักที่ทำให้การควบคุมการฉ้อโกงออนไลน์ยังไม่เกิดผลชัดเจน

ผลจากการวิจัยวัตถุประสงค์ที่ 2 พบว่า ปัญหาการควบคุมการฉ้อโกงผ่านระบบออนไลน์ในประเทศไทยมีลักษณะเชิงโครงสร้างมากกว่าปัญหาทางกฎหมาย กล่าวคือ แม้กฏหมายจะมีอยู่เพียงพอ แต่การบังคับใช้กลับไม่ต่อเนื่องและไม่สามารถปรับตัวให้เท่าทันเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว (ศปอส.ตร., 2567) ผู้เชี่ยวชาญที่ให้ข้อมูลส่วนใหญ่เห็นตรงกันว่า ปัญหาหลักเกิดจาก “ขีดความสามารถของบุคลากร” โดยเฉพาะเจ้าหน้าที่ตำรวจและอัยการที่ยังขาดความเชี่ยวชาญในการสืบสวนคดีไซเบอร์ เช่น การตรวจสอบธุรกรรมในระบบบล็อกเชน การวิเคราะห์เส้นทางการเงินดิจิทัล

หรือการสกัดข้อมูลจากโทรศัพท์มือถือ ทั้งนี้อาจเป็นเพราะระบบการฝึกอบรมและพัฒนาบุคลากรด้านเทคโนโลยีในหน่วยงานรัฐยังมีข้อจำกัด และไม่มีหลักสูตรเฉพาะทางด้าน “นิติวิทยาศาสตร์ดิจิทัล” (Digital Forensics) ซึ่งประเทศพัฒนาแล้วให้ความสำคัญมาก ตัวอย่างเช่น สิงคโปร์มีการจัดตั้ง Cybersecurity Agency (CSA) และศูนย์ฝึกอบรมเฉพาะด้าน (Cybercrime Academy) เพื่อพัฒนาทักษะของเจ้าหน้าที่รัฐให้เท่าทันภัยคุกคามใหม่ ๆ (UNODC, 2022)

เอกสารสนับสนุน จากรายงานของ OECD (2022) ระบุว่า ประเทศที่มีอัตราการเกิดอาชญากรรมไซเบอร์ต่ำมักมีนโยบายลงทุนด้านการพัฒนาบุคลากรอย่างต่อเนื่อง ซึ่งช่วยให้เจ้าหน้าที่สามารถตรวจจับและวิเคราะห์พฤติกรรมอาชญากรรมได้อย่างรวดเร็ว ตรงกันข้ามกับประเทศไทยซึ่งยังเน้นการลงโทษภายหลังเกิดเหตุ มากกว่าการสร้างขีดความสามารถในการป้องกันล่วงหน้า

ดังนั้น ผลการศึกษาข้อนี้สะท้อนให้เห็นว่า การปรับปรุงกฎหมายเพียงอย่างเดียวไม่เพียงพอ จำเป็นต้องยกระดับ “ทรัพยากรมนุษย์” และ “โครงสร้างการบริหารจัดการคดีไซเบอร์” ให้สอดคล้องกับพลวัตของเทคโนโลยี

ผลจากการวิจัยวัตถุประสงค์ที่ 3 พบว่า การเปรียบเทียบกฎหมายไทยกับกฎหมายต่างประเทศแสดงให้เห็นถึง “ความแตกต่างเชิงระบบ” (Systemic Difference) อย่างชัดเจน โดยประเทศที่มีกฎหมายไซเบอร์ที่เข้มแข็ง เช่น สหรัฐอเมริกา อังกฤษ และสิงคโปร์ มักใช้หลักการ “ความรับผิดชอบร่วม” (Joint Liability) และ “ความโปร่งใสของข้อมูล” (Transparency) เป็นแกนหลักในการดำเนินการ ซึ่งต่างจากประเทศไทยที่ยังเน้นการดำเนินคดีเฉพาะบุคคล

ในสหรัฐอเมริกา Computer Fraud and Abuse Act (CFAA) กำหนดให้ผู้ให้บริการเครือข่าย (Service Provider) ต้องร่วมรับผิดชอบหากละเลยต่อการตรวจสอบความผิดปกติของระบบ ซึ่งสร้างแรงกดดันให้ภาคเอกชนมีส่วนร่วมในกระบวนการป้องกันอาชญากรรม (Council of Europe, 2021) ขณะที่ในสิงคโปร์ Cybersecurity Act (2018) บังคับให้หน่วยงานรัฐและเอกชนร่วมกันรายงานเหตุโจมตีทางไซเบอร์ภายใน 72 ชั่วโมง เพื่อให้เกิดการตอบสนองเชิงระบบอย่างรวดเร็ว ทั้งนี้อาจเป็นเพราะประเทศเหล่านี้ให้ความสำคัญกับ “ความรับผิดชอบร่วม” และ “การแจ้งเตือนภัยทางไซเบอร์” (Cyber Incident Notification) ซึ่งยังไม่ปรากฏชัดในกฎหมายไทย ผู้ให้บริการเครือข่ายส่วนใหญ่ในประเทศไทยไม่ได้ถูกกำหนดให้มีหน้าที่แจ้งเหตุความผิดปกติ ทำให้ข้อมูลไม่ถูกส่งต่อถึงหน่วยงานรัฐในเวลาที่เหมาะสม

เมื่อเปรียบเทียบกับทฤษฎีสามเหลียมอาชญากรรมของ Eck (2003) ผลการวิจัยสอดคล้องกับแนวคิดที่ว่า การลด “โอกาสในการเกิดอาชญากรรม” ต้องอาศัยการร่วมมือจากทุกฝ่าย โดยเฉพาะผู้ควบคุมสภาพแวดล้อม (Place Managers) ซึ่งในกรณีนี้หมายถึงผู้ให้บริการอินเทอร์เน็ตและสถาบันการเงิน หากภาครัฐสามารถกำหนดให้เอกชนร่วมรับผิดชอบ จะช่วยลดโอกาสการฉ้อโกงออนไลน์ได้อย่างมีนัยสำคัญ

ผลจากการวิจัยวัตถุประสงค์ที่ 4 พบว่า ประเทศไทยควรปรับปรุงมาตรการทางกฎหมายโดยบูรณาการแนวทางจากต่างประเทศเข้ากับบริบทภายใน โดยเฉพาะใน 4 ด้านหลัก ได้แก่ (1) การจัดตั้งศูนย์ประสานงานอาชญากรรมทางเทคโนโลยีระหว่างประเทศ, (2) การฝึกอบรมบุคลากรเฉพาะทาง, (3) การเพิ่มโทษและขยายความรับผิดชอบทางแพ่ง, และ (4) การจัดตั้งกองทุนเยียวยาผู้เสียหาย ทั้งนี้อาจเป็นเพราะประเทศไทยยังขาดระบบการจัดการเชิงบูรณาการ (Integrated Legal Mechanism) ที่เชื่อมโยงระหว่างภาครัฐ เอกชน และองค์กรระหว่างประเทศ ซึ่งเป็นหัวใจสำคัญของการจัดการอาชญากรรมไซเบอร์ในประเทศพัฒนาแล้ว เช่น *Europol Cybercrime Centre (EC3)* ของสหภาพยุโรป ซึ่งทำหน้าที่เป็นศูนย์กลางข้อมูลกลาง (Data Hub) และศูนย์แลกเปลี่ยนข่าวกรองระหว่างประเทศ (Intelligence Sharing Center) (Council of Europe, 2021; UNODC, 2022) จากรายงานของ UNODC (2022) ระบุว่า ประเทศที่มีศูนย์ประสานงานระดับชาติและนานาชาติสามารถลดระยะเวลาการสืบสวนคดีข้ามชาติได้มากกว่า 60% และเพิ่มอัตราการจับกุมผู้กระทำผิดได้ถึงสองเท่าเมื่อเทียบกับประเทศที่ไม่มีศูนย์กลางดังกล่าว

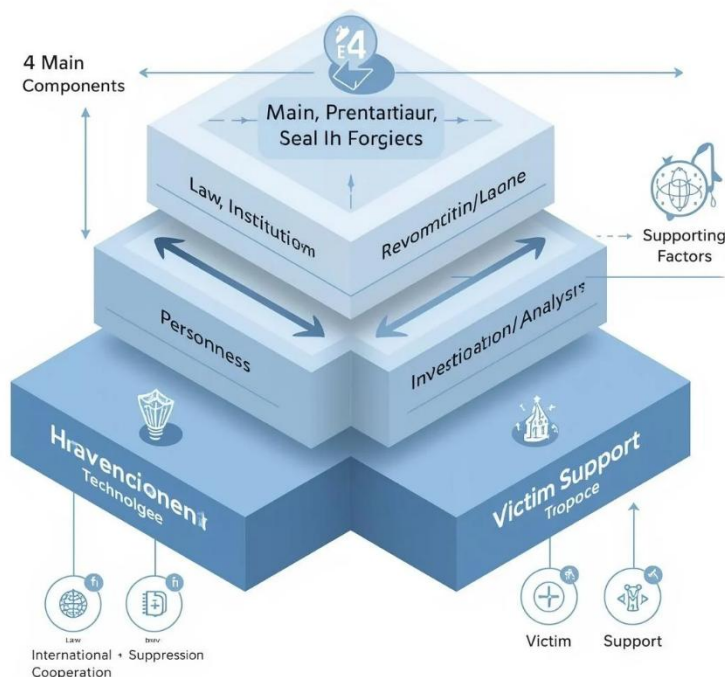
ดังนั้น ผลการวิจัยข้อนี้สะท้อนแนวคิดของ Wilson and Kelling (1982) ที่ว่า “การบังคับใช้กฎหมายอย่างต่อเนื่องและเข้มงวด” จะช่วยยับยั้งการขยายตัวของอาชญากรรม ซึ่งในกรณีของประเทศไทยหมายถึงการสร้างโครงสร้างพื้นฐานทางกฎหมายที่ต่อเนื่อง มีระบบสนับสนุน และมีการฝึกอบรมบุคลากรอย่างสม่ำเสมอ เพื่อให้การควบคุมอาชญากรรมออนไลน์เกิดผลจริงในระยะยาว

โดยสรุป การอภิปรายผลทั้งหมดสะท้อนให้เห็นว่า ปัญหาการควบคุมการฉ้อโกงออนไลน์ของไทยมิใช่เรื่องของ “การมีกฎหมายหรือไม่” แต่คือ “คุณภาพของระบบการบังคับใช้” ที่ยังไม่สามารถบูรณาการให้สอดคล้องกับความซับซ้อนของอาชญากรรมสมัยใหม่ การวิจัยครั้งนี้จึงเสนอว่า ประเทศไทยควรใช้แนวคิด “การควบคุมอาชญากรรมแบบบูรณาการ” (Integrated Crime Control System) ซึ่งผสมผสานทั้งมาตรการทางกฎหมาย เทคโนโลยี การบริหารจัดการบุคลากร และความร่วมมือระหว่างประเทศ เพื่อยกระดับประสิทธิภาพการป้องกันและปราบปรามอาชญากรรมออนไลน์ให้เทียบเท่ามาตรฐานสากล

องค์ความรู้ใหม่จากการวิจัย

จากผลการศึกษาผู้วิจัยได้สังเคราะห์องค์ความรู้ใหม่ที่เรียกว่า “Legal Enforcement Integration Model (LEIM)” ซึ่งเป็นแนวคิดเชิงบูรณาการในการจัดการอาชญากรรมทางเทคโนโลยีและการฉ้อโกงออนไลน์ในลักษณะข้ามชาติ โดยเชื่อมโยงมิติของกฎหมาย สถาบัน เทคโนโลยี และการคุ้มครองผู้เสียหายให้ทำงานร่วมกันอย่างเป็นระบบ เพื่อให้เกิดกลไกการบังคับใช้กฎหมายที่มีประสิทธิภาพและยั่งยืนในสังคมดิจิทัล

Legal Enforcement Integration- Retention Camel LEIM



โมเดล LEIM อธิบายว่า การบังคับใช้กฎหมายในยุคดิจิทัลไม่อาจดำเนินการในกรอบเดิมที่เน้นเพียงบทบัญญัติหรือการลงโทษ แต่จำเป็นต้องขยายกรอบความคิดไปสู่ “การบังคับใช้แบบบูรณาการ (Integrated Legal Enforcement)” ซึ่งเชื่อมโยงองค์ประกอบหลัก 4 ประการ ได้แก่ มิติทางกฎหมาย มิติทางสถาบัน มิติทางเทคโนโลยี และมิติการคุ้มครองผู้เสียหาย ทั้งหมดนี้ถูกขับเคลื่อนด้วยปัจจัยสนับสนุนสำคัญคือ ความร่วมมือระหว่างประเทศ และการพัฒนาศักยภาพบุคลากรของรัฐให้มีความพร้อมในการรับมือกับอาชญากรรมรูปแบบใหม่

ในมิติทางกฎหมาย (Legal Framework) โมเดลนี้เน้นว่ากฎหมายต้องมีความยืดหยุ่น ทันสมัย และเชื่อมโยงกับมาตรฐานสากล เช่น อนุสัญญา Budapest Convention เพื่อให้เกิดการประสานงานด้านข้อมูลและหลักฐานระหว่างประเทศ ขณะที่มิติทางสถาบัน (Institutional Mechanism) มุ่งให้เกิดการจัดตั้งศูนย์กลางบูรณาการข้อมูลและการประสานงานระหว่างหน่วยงาน เช่น ตำรวจ อัยการ ปปง. และธนาคาร เพื่อให้สามารถติดตาม ตรวจสอบ และตอบสนองต่ออาชญากรรมไซเบอร์ได้อย่างรวดเร็วและเป็นระบบ

ในมิติทางเทคโนโลยี (Technological Enforcement) LEIM เน้นการใช้เทคโนโลยีดิจิทัลเข้ามาสนับสนุนการบังคับใช้กฎหมาย เช่น ระบบตรวจจับธุรกรรมออนไลน์แบบอัตโนมัติ (AI Surveillance) ระบบยืนยันตัวตนดิจิทัล (Digital ID) และฐานข้อมูลกลางที่ใช้สำหรับการตรวจสอบผู้กระทำความผิดทางเทคโนโลยี (Cybercrime Database) การใช้เทคโนโลยีเหล่านี้ช่วยลดความล่าช้าในการสืบสวนคดี และเพิ่มความแม่นยำในการเก็บหลักฐานดิจิทัล

ส่วนมิติการคุ้มครองผู้เสียหาย (Victim Support) ถือเป็นหัวใจของระบบนิติธรรมที่สมบูรณ์ โดยโมเดล LEIM เสนอให้จัดตั้งกองทุนเยียวยาผู้เสียหายจากอาชญากรรมทางเทคโนโลยี และสร้างระบบให้คำปรึกษาทางกฎหมายแก่ประชาชน เพื่อให้เกิดการคุ้มครองสิทธิและความเป็นธรรมอย่างแท้จริงในกระบวนการยุติธรรม ทั้งนี้มิติการคุ้มครองผู้เสียหายยังช่วยสร้างความเชื่อมั่นต่อประชาชนและเสริมสร้างภาพลักษณ์ของรัฐในฐานะผู้ปกป้องผลประโยชน์สาธารณะ

นอกจากนั้น โมเดล LEIM ยังชี้ให้เห็นถึง ปัจจัยสนับสนุน (Supporting Factors) ที่สำคัญ เช่น ความร่วมมือระหว่างประเทศ (International Cooperation) ซึ่งช่วยให้เกิดการแลกเปลี่ยนข้อมูล การสืบสวนข้ามพรมแดน และการยึดทรัพย์สินที่ได้จากอาชญากรรม ตลอดจนการพัฒนาบุคลากร (Capacity Building) เพื่อเสริมสร้างความรู้ ความเข้าใจ และทักษะทางเทคโนโลยีแก่เจ้าหน้าที่ที่ปฏิบัติงานด้านกฎหมายให้สามารถทำงานได้อย่างมีประสิทธิภาพ

จากองค์ประกอบทั้งหมดนี้ ทำให้ LEIM กลายเป็นโมเดลที่สะท้อนถึง “ระบบนิเวศแห่งการบังคับใช้กฎหมาย” ที่ผสมผสานทั้งโครงสร้างทางกฎหมายและการบริหารจัดการอย่างครบวงจร กล่าวคือ หากแต่ละองค์ประกอบทำงานประสานกันอย่างสมดุล จะนำไปสู่ผลลัพธ์หลัก 3 ประการ ได้แก่ (1) ระบบควบคุมอาชญากรรมไซเบอร์ที่เข้มแข็ง (2) การป้องกันอาชญากรรมล่วงหน้าอย่างยั่งยืน และ (3) การคุ้มครองผู้เสียหายอย่างเป็นธรรมและทั่วถึง

กล่าวโดยสรุป องค์ความรู้ใหม่จากการวิจัยนี้มีคุณค่าอย่างยิ่งต่อการพัฒนานโยบายสาธารณะด้านความมั่นคงไซเบอร์ของประเทศไทย เพราะไม่เพียงแต่เสนอแนวทางทางกฎหมาย แต่ยังเปิดมุมมองใหม่ต่อ “การบังคับใช้กฎหมายในฐานะกระบวนการทางสังคม” ที่ต้องอาศัยการมีส่วนร่วมจากทุกภาคส่วน ทั้งภาครัฐ เอกชน และประชาชน เพื่อสร้างสังคมดิจิทัลที่โปร่งใส ปลอดภัย และยั่งยืน.

สรุป

การวิจัยเรื่อง “มาตรการทางกฎหมายเกี่ยวกับการควบคุมการฉ้อโกงผ่านระบบออนไลน์จากอาชญากรรมข้ามชาติ” ได้สะท้อนให้เห็นภาพรวมของปัญหาเชิงโครงสร้างในระบบกฎหมายไทยที่ยังไม่สามารถรับมือกับอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพ ผลการศึกษาพบว่า การควบคุมอาชญากรรมไซเบอร์ไม่สามารถพึ่งพากฎหมายเพียงอย่างเดียว แต่จำเป็นต้องใช้แนวทางแบบบูรณาการที่เชื่อมโยงกฎหมาย เทคโนโลยี บุคลากร สถาบัน และความร่วมมือระหว่างประเทศ เพื่อสร้างกลไกทางนิติรัฐที่ตอบสนองต่อความซับซ้อนของอาชญากรรมสมัยใหม่

ในภาพรวม การศึกษาครั้งนี้สรุปได้ว่า “จุดอ่อนของระบบกฎหมายไทย” อยู่ที่การบังคับใช้มากกว่าตัวบทกฎหมาย กล่าวคือ แม้จะมีกฎหมายที่เกี่ยวข้องหลายฉบับ แต่ยังขาดกลไกเชิงสถาบันที่ชัดเจนและการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง นอกจากนี้ บุคลากรทางกฎหมายยังมีข้อจำกัดด้านความรู้ความเข้าใจเกี่ยวกับเทคโนโลยี ส่งผลให้ไม่สามารถจัดการกับคดีอาชญากรรมทางไซเบอร์ได้อย่างเท่าทันการเปลี่ยนแปลงของเทคโนโลยีโลก

จากการเปรียบเทียบกับประเทศที่ประสบความสำเร็จในการจัดการอาชญากรรมไซเบอร์ เช่น สหรัฐอเมริกา สหราชอาณาจักร และสิงคโปร์ พบว่า ประเทศเหล่านี้มีการพัฒนากฎหมายเฉพาะทาง (Specialized Cybercrime Law) ร่วมกับการจัดตั้งหน่วยงานกลางที่ทำหน้าที่กำกับและบูรณาการข้อมูล เช่น FBI Cyber Division, National Crime Agency (UK) และ Cybersecurity Agency (Singapore) ตลอดจนมีระบบคุ้มครองผู้เสียหายและกลไกเยียวยาที่มีประสิทธิภาพ ซึ่งสามารถนำมาประยุกต์ใช้เป็นแนวทางปรับปรุงกฎหมายไทยได้อย่างเหมาะสม

ในเชิงแนวทางการพัฒนา ผู้วิจัยเสนอให้มีการดำเนินการใน 4 ด้านหลัก ได้แก่

1. การพัฒนาโครงสร้างสถาบันกลาง เพื่อทำหน้าที่เป็นศูนย์ประสานงานด้านอาชญากรรมทางเทคโนโลยีในระดับประเทศ และเชื่อมโยงกับหน่วยงานต่างประเทศเพื่อแลกเปลี่ยนข้อมูล
2. การเสริมสร้างศักยภาพบุคลากรภาครัฐ ให้มีทักษะด้านนิติวิทยาศาสตร์ดิจิทัล (Digital Forensics) และการใช้เทคโนโลยีเพื่อสืบสวนสอบสวน
3. การปรับปรุงบทบัญญัติกฎหมายและบทลงโทษ ให้สอดคล้องกับสภาพปัญหาและมูลค่าความเสียหายที่เกิดขึ้นจริง
4. การคุ้มครองและเยียวยาผู้เสียหาย ผ่านกองทุนเฉพาะกิจที่สนับสนุนการช่วยเหลือทางการเงินและให้คำปรึกษาทางกฎหมายแก่ผู้ที่ได้รับผลกระทบจากอาชญากรรมไซเบอร์

ในมิติขององค์ความรู้ทางวิชาการ การวิจัยนี้ได้สร้าง “Legal Enforcement Integration Model (LEIM)” ซึ่งเป็นกรอบแนวคิดใหม่ที่เสนอให้บูรณาการกฎหมาย เทคโนโลยี สถาบัน และการคุ้มครองผู้เสียหายให้ทำงานร่วมกันอย่างเป็นระบบ โดยมีเป้าหมายเพื่อพัฒนา “ระบบนิติรัฐดิจิทัล” ที่มีความโปร่งใส มีประสิทธิภาพ และสอดคล้องกับมาตรฐานสากล โมเดลนี้สามารถใช้เป็นแนวทางเชิงนโยบายและเชิงปฏิบัติสำหรับหน่วยงานรัฐและนักกฎหมายไทยในการปรับปรุงระบบการบังคับใช้กฎหมายให้เข้มแข็งยิ่งขึ้น

การวิจัยครั้งนี้ชี้ให้เห็นว่า การรับมือกับอาชญากรรมทางเทคโนโลยีไม่ใช่เพียงภารกิจของรัฐเท่านั้น แต่ต้องอาศัยความร่วมมือจากทุกภาคส่วน ทั้งภาครัฐ ภาคเอกชน ภาคประชาชน และความร่วมมือระดับนานาชาติ เพื่อสร้างระบบนิเวศทางกฎหมายที่พร้อมรับมือกับการเปลี่ยนแปลงของโลกดิจิทัลในอนาคต และนำพาประเทศไทยไปสู่การเป็นสังคมดิจิทัลที่ปลอดภัยและยั่งยืนอย่างแท้จริง.

ข้อเสนอแนะ

จากผลการวิจัย ผู้วิจัยมีข้อเสนอแนะ ดังนี้

1. ข้อเสนอแนะในการนำผลการวิจัยไปใช้ประโยชน์

ผลจากการวิจัยวัตถุประสงค์ที่ 1 พบว่า การควบคุมอาชญากรรมทางเทคโนโลยีในประเทศไทยยังขาดกลไกการบูรณาการเชิงระบบและไม่มีศูนย์กลางในการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง ทำให้การบังคับใช้กฎหมายไม่ต่อเนื่องและไม่ทันต่อสถานการณ์อาชญากรรมที่เปลี่ยนแปลง

อย่างรวดเร็ว ผู้วิจัยจึงเสนอว่า หน่วยงานภาครัฐควรจัดตั้ง ศูนย์ประสานงานอาชญากรรมทางเทคโนโลยีระดับชาติ (National Cybercrime Coordination Center) เพื่อรวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภาครัฐและเอกชน อันจะช่วยให้การดำเนินงานเป็นไปในทิศทางเดียวกัน มีเอกภาพ และสามารถตอบสนองต่อเหตุการณ์ได้อย่างทันท่วงที นอกจากนี้ ควรมีการปรับปรุงบทบัญญัติกฎหมายให้สอดคล้องกับอนุสัญญาระหว่างประเทศ โดยเฉพาะ Budapest Convention on Cybercrime เพื่อให้กระบวนการดำเนินคดีข้ามชาติมีความราบรื่นและมีประสิทธิภาพมากยิ่งขึ้น

ผลจากการวิจัยวัตถุประสงค์ที่ 2 พบว่า บุคลากรผู้บังคับใช้กฎหมายยังขาดทักษะทางเทคโนโลยีและขีดความสามารถในการสืบสวนคดีไซเบอร์ ส่งผลให้การตรวจสอบหลักฐานดิจิทัลล่าช้า และขาดความแม่นยำ ซึ่งเป็นอุปสรรคต่อการบังคับใช้กฎหมายในยุคดิจิทัล ผู้วิจัยจึงเสนอให้มีการจัดตั้ง สถาบันฝึกอบรมด้านนิติวิทยาศาสตร์ดิจิทัล (Digital Forensics Training Institute) เพื่อพัฒนาทักษะการสืบสวนและการวิเคราะห์ข้อมูลทางเทคโนโลยีของเจ้าหน้าที่ตำรวจ อัยการ และผู้พิพากษา โดยเฉพาะในด้านการตรวจสอบข้อมูลทางเทคนิค การติดตามธุรกรรมดิจิทัล และการเก็บรักษาหลักฐานอิเล็กทรอนิกส์อย่างถูกต้องตามหลักสากล นอกจากนี้ ควรส่งเสริมให้มีการแลกเปลี่ยนองค์ความรู้กับหน่วยงานต่างประเทศ เช่น Interpol และ Europol เพื่อยกระดับขีดความสามารถของบุคลากรในกระบวนการยุติธรรมไทยให้ทัดเทียมมาตรฐานสากล

ผลจากการวิจัยวัตถุประสงค์ที่ 3 พบว่า เมื่อเปรียบเทียบกับกฎหมายต่างประเทศแล้ว กฎหมายไทยยังขาดระบบการคุ้มครองผู้เสียหายที่เป็นรูปธรรมและยังไม่มีมาตรการทางแพ่งที่ครอบคลุมเพียงพอ ผู้วิจัยจึงเสนอให้จัดตั้ง กองทุนเยียวยาผู้เสียหายจากอาชญากรรมทางเทคโนโลยี (Cybercrime Victim Compensation Fund) เพื่อให้ความช่วยเหลือเบื้องต้นแก่ผู้เสียหายโดยไม่ต้องรอผลการตัดสินคดี ซึ่งจะช่วยลดความเสียหายทางเศรษฐกิจและจิตใจของผู้ที่ได้รับผลกระทบจากอาชญากรรมออนไลน์ นอกจากนี้ ควรมีการพัฒนาแนวทางการร่วมมือระหว่างหน่วยงานรัฐ ภาคเอกชน และองค์กรภาคประชาชน เพื่อสร้างเครือข่ายการป้องกันและเยียวยาผู้เสียหายอย่างยั่งยืน สอดคล้องกับแนวคิดการคุ้มครองสิทธิมนุษยชนในมิติของความเป็นธรรมทางสังคม

ผลจากการวิจัยวัตถุประสงค์ที่ 4 พบว่า การปรับปรุงระบบกฎหมายไทยควรมุ่งเน้นการบูรณาการเชิงสถาบันและเทคโนโลยี พร้อมส่งเสริมความร่วมมือระหว่างประเทศในระดับโครงสร้าง เพื่อเพิ่มประสิทธิภาพของการสืบสวนและการบังคับใช้กฎหมายข้ามพรมแดน ผู้วิจัยจึงเสนอให้พัฒนากลไกการแลกเปลี่ยนข้อมูลกับหน่วยงานต่างประเทศ เพื่อให้สามารถติดตามและจับกุมผู้กระทำผิดได้อย่างมีประสิทธิภาพมากขึ้น รวมถึงควรส่งเสริมให้มีการออกกฎหมายเฉพาะทาง (Specialized Cybercrime Law) ที่รองรับอาชญากรรมดิจิทัลและความผิดรูปแบบใหม่ เช่น การฉ้อโกงผ่านสกุลเงินดิจิทัล หรือการโจมตีทางไซเบอร์ที่ส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญของประเทศ เพื่อให้กฎหมายไทยมีความทันสมัยและตอบสนองต่อภัยคุกคามยุคดิจิทัลได้อย่างแท้จริง

โดยสรุป ข้อเสนอแนะเหล่านี้สะท้อนให้เห็นถึงแนวทางการปรับปรุงเชิงโครงสร้างและเชิงนโยบายที่จำเป็นต่อการยกระดับระบบกฎหมายไทยให้มีความเข้มแข็ง และสามารถรับมือกับอาชญากรรมทางเทคโนโลยีในระดับนานาชาติได้อย่างยั่งยืน ทั้งนี้ การนำข้อเสนอแนะไปใช้จริงจำเป็นต้องอาศัยความร่วมมือจากทุกภาคส่วน ทั้งหน่วยงานภาครัฐ เอกชน และภาคประชาชน เพื่อสร้างระบบนิเวศทางกฎหมายที่มีประสิทธิภาพและเป็นธรรมสำหรับทุกคนในสังคมไทย

2. ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

งานวิจัยนี้ได้ข้อค้นพบที่สำคัญคือ “โมเดลการบังคับใช้กฎหมายแบบบูรณาการ (Legal Enforcement Integration Model: LEIM)” ซึ่งสามารถนำไปประยุกต์ใช้กับการพัฒนาระบบกฎหมายไทยในยุคดิจิทัล โดยควรให้ความสำคัญกับการวิจัยในประเด็นเชิงปฏิบัติ เช่น การออกแบบระบบฐานข้อมูลกลางของหน่วยงานบังคับใช้กฎหมาย หรือการสร้างกลไกเชื่อมโยงข้อมูลผู้เสียหายระหว่างประเทศ

สำหรับการวิจัยในอนาคต ควรศึกษาประเด็นเกี่ยวกับ “การประยุกต์ใช้ปัญญาประดิษฐ์ (AI) และบิ๊กดาต้า (Big Data) ในกระบวนการบังคับใช้กฎหมาย” เพื่อวิเคราะห์ศักยภาพและความเสี่ยงของเทคโนโลยีใหม่ในการเสริมสร้างประสิทธิภาพของกระบวนการยุติธรรม รวมถึงควรขยายขอบเขตการศึกษาลุ่มมิติของการคุ้มครองสิทธิส่วนบุคคลและความมั่นคงทางไซเบอร์ เพื่อให้เกิดความสมดุลระหว่าง “ความปลอดภัย” และ “สิทธิมนุษยชน” ในระบบกฎหมายยุคดิจิทัล

เอกสารอ้างอิง

- ราชกิจจานุเบกษา. (2568). พระราชกำหนดการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2568. เล่ม 142 ตอนที่ 27 ก หน้า 5-13 (12 เมษายน 2568).
- ราชกิจจานุเบกษา. (2562). พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. เล่ม 136 ตอนที่ 69 ก หน้า 20-51 (27 พฤษภาคม 2562).
- ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.). (2567). รายงานสถานการณ์อาชญากรรมทางเทคโนโลยีในประเทศไทย. กรุงเทพฯ: สำนักงานตำรวจแห่งชาติ.
- องค์กรพันธมิตรต่อต้านการฉ้อโกงโลก (Global Anti-Scam Alliance: GASA) และสแกมแอดไวเซอร์ (ScamAdviser). (2566). รายงานสถานการณ์การฉ้อโกงโลก ประจำปี 2023. กรุงเทพฯ, ประเทศเนเธอร์แลนด์: องค์กรพันธมิตรต่อต้านการฉ้อโกงโลก.
- Akers, R. L. (1998). ทฤษฎีการเรียนรู้ทางสังคมและโครงสร้างทางสังคม: ทฤษฎีทั่วไปว่าด้วยอาชญากรรมและความเบี่ยงเบน. บอสตัน, แมสซาชูเซตส์: มหาวิทยาลัยนอร์ทอีสเทิร์น.
- Bandura, A. (1977). *Social learning theory*. Englewood Cliffs, New Jersey: Prentice-Hall.
- Council of Europe. (2021). *Guidance notes on cybercrime and international cooperation*. Strasbourg: COE Publications.

- Clarke, R. V. (1997). *Situational crime prevention: Successful case studies*. (2nd ed.). Guilderland, New York: Harrow and Heston.
- Cornish, D. B., & Clarke, R. V. (2003). *Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention theory for practice in situational crime prevention*. Monsey, New York: Criminal Justice Press
- Eck, J. E. (2003). *Police problems: The complexity of problem theory, research, and evaluation*. Monsey, New York: Criminal Justice Press.
- Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and digital forensics: An introduction*. London: Routledge.
- Johnson, R., & Miller, T. (2018). *Transnational online fraud: Challenges and responses*. London, UK: Palgrave Macmillan.
- Office for Victims of Crime. (2020). *VOCA crime victim compensation program guidelines*. U.S. Department of Justice.
- Reiss, A. J. (1983). *Crime control as a social process*. Chicago: University of Chicago Press.
- Singapore Ministry of Law. (2021). *Criminal injuries compensation scheme*. Government of Singapore.
- Smith, A. (2020). *Cybercrime in the digital age: Global perspectives and legal frameworks*. New York: Routledge.
- United Nations. (1985). *Declaration of basic principles of justice for victims of crime and abuse of power*. New York: Audiovisual library of International Law.
- United Nations Office on Drugs and Crime. (2022). *Global report on cybercrime and transnational crime*. Office on Drugs and Crime.
- Wemmers, J.-A. (2017). *Victims' rights and the international movement*. Routledge.
- Wilson, J. Q., & Kelling, G. L. (1982). Broken windows: The police and neighborhood safety. *Atlantic Monthly*, 249(3), 29–38. Retrieved from <https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/185996>
- Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society*. (3rd ed.). SAGE.