# มาตรการของอาเซียนในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ: กรณีแก๊งคอลเซ็นเตอร์

# ASEAN MEASURES TO PREVENT AND SUPPRESS TRANSNATIONALCRIMES: A CASE OF CRIMES COMMITTED BY CALL CENTER GANGS

สุพิชญา ศิรินภาดล

นิติศาสตรมหาบัณฑิต

สำนักวิชานิติศาสตร์
มหาวิทยาลัยแม่ฟ้าหลวง
2567

# มาตรการของอาเซียนในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ: กรณีแก๊งคอลเซ็นเตอร์

# ASEAN MEASURES TO PREVENT AND SUPPRESS TRANSNATIONAL CRIMES: A CASE OF CRIMES COMMITTED BY CALL CENTER GANGS

**สุพิชญา ศิรินภาดล**

**วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษา**
**ตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต**

**สำนักวิชานิติศาสตร์**
**มหาวิทยาลัยแม่ฟ้าหลวง**
**2567**

**หน้าอนุมัติวิทยานิพนธ์**

**มหาวิทยาลัยแม่ฟ้าหลวง**

**ปริญญานิติศาสตรมหาบัณฑิต**

**วิทยานิพนธ์เรื่อง** มาตรการของอาเซียนในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ: กรณีแก๊งคอลเซ็นเตอร์

ASEAN Measures to Prevent and Suppress Transnational Crimes: A Case of Crimes Committed by Call Center Gangs

**ผู้ประพันธ์** สุพิชญา ศิรินภาดล

**คณะกรรมการสอบ**

| | |
|---|---|
| ศาสตราจารย์ ดร.ประสิทธิ์ ปิวาวัฒนพานิช | ประธานกรรมการ |
| รองศาสตราจารย์ ดร.ชูเกียรติ น้อยฉิม | กรรมการ |
| ผู้ช่วยศาสตราจารย์ ดร.ยศพนธ์ นิติรุจิโรจน์ | กรรมการ |
| รองศาสตราจารย์ ดร.ทศพล ทรรศนพรรณ | กรรมการ |
| ผู้ช่วยศาสตราจารย์ ดร.ณัฐกร วิทิตานนท์ | กรรมการ |

**อาจารย์ที่ปรึกษา**

..... อาจารย์ที่ปรึกษาหลัก

(รองศาสตราจารย์ ดร.ชูเกียรติ น้อยฉิม)

**คณบดี**

.....

(ผู้ช่วยศาสตราจารย์ สุชิน กฤตลักษณ์วงศ์)

# กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ประสบความสำเร็จลุล่วงด้วยดีได้ด้วยความเมตตากรุณาและความช่วยเหลือเอาใจใส่จากผู้มีพระคุณหลายท่าน ผู้เขียนขอกราบขอบพระคุณ รองศาตราจารย์ ดร.ชูเกียรติ น้อยฉิม กรรมการและที่ปรึกษาวิทยานิพนธ์ฉบับนี้ ซึ่งเป็นผู้ประสิทธิประสาทความรู้ เป็นผู้จุดประกายความคิด คำแนะนำ และขอขอบพระคุณที่ได้กรุณาสละเวลาให้คำปรึกษาชี้แนะ ให้ข้อมูลและข้อเสนอแนะข้อคิดเห็นอันเป็นประโยชน์ ตลอดจนช่วยตรวจสอบแก้ไขข้อบกพร่องต่างๆ

ผู้เขียนขอกราบขอบพระคุณ ศาสตราจารย์ ดร.ประสิทธิ์ ปิวาวัฒนพานิช ที่กรุณารับเป็นประธานกรรมการวิทยานิพนธ์ โดยท่านได้กรุณาให้คำแนะนำและชี้แนะแนวทางอันเป็นประโยชน์ในการจัดทำวิทยานิพนธ์ นอกจากนี้ผู้เขียนขอกราบขอบพระคุณผู้ช่วยศาสตราจารย์ ดร.ยศพนธ์ นิติรุจิโรจน์ ผู้ช่วยศาสตราจารย์ ดร.ณัฐกร วิทิตานนท์ และรองศาสตราจารย์ ดร.ทศพล ทรรศนพรรณ ที่ได้กรุณาเป็นกรรมการวิทยานิพนธ์ ซึ่งได้ให้ข้อคำแนะนำในประเด็นที่มีความสำคัญต่อการศึกษาและการจัดทำวิทยานิพนธ์ ขอกราบขอบพระคุณมหาวิทยาลัยแม่ฟ้าหลวงเป็นอย่างสูงที่ได้มอบทุนสนับสนุนเพื่อการทำวิทยานิพนธ์ฉบับนี้ ซึ่งเป็นทุนที่มีความสำคัญอย่างยิ่งในการส่งเสริมและสนับสนุนให้ผู้เขียนได้มีโอกาสศึกษาค้นคว้าและวิจัยในหัวข้อที่สนใจ ทุนดังกล่าวเป็นแรงสนับสนุนที่ทำให้ข้าพเจ้าสามารถทุ่มเทเวลาและความพยายามในการทำวิจัยได้อย่างเต็มที่ และเป็นแรงผลักดันสำคัญในการพัฒนาศักยภาพทางวิชาการให้ก้าวหน้าอย่างต่อเนื่อง

สุดท้ายผู้เขียนขอกราบขอบพระคุณบุคคลที่มีความสำคัญยิ่งในชีวิต คุณยายจริยา อุดมทรัพย์ในการสนับสนุนการศึกษาระดับปริญญาโทของข้าพเจ้า อีกทั้งคุณแม่วาริธร วโรตมพงษ์ ที่ได้อุปการะเลี้ยงดู ให้ความรัก ความห่วงใย และเป็นกำลังใจที่สำคัญโดยเฉพาะอย่างยิ่งในยามที่ผู้เขียนท้อแท้จน ผู้เขียนประสบความสำเร็จในการจัดทำวิทยานิพนธ์ฉบับนี้ และขอขอบคุณสมาชิกครอบครัว อันเป็นที่รักยิ่งทุกคน รวมทั้งกัลยาณมิตร เพื่อนนักศึกษา ทุกคนรวมทั้งรุ่นพี่ โดยเฉพาะอย่างยิ่ง คุณกะรัต พลอย อูปแก้ว เพื่อนร่วมรุ่นที่ร่วมทุกข์ร่วมสุขกันมาตลอดจนประสบความสำเร็จในการจัดทำวิทยานิพนธ์ฉบับนี้ และคอยให้กำลังใจอยู่เคียงข้างผู้เขียนเสมอมา

หากวิทยานิพนธ์ฉบับนี้สร้างคุณประโยชน์ต่อการศึกษาและให้ความรู้ ความเข้าใจ ต่อทุกท่านที่มีความสนใจ ผู้เขียนขอมอบความดีทั้งหมดให้แก่บิดา มารดา ผู้บาอาจารย์ผู้ประสิทธิ์ประสาทวิชาความรู้ให้แก่ศิษย์ แต่หากวิทยานิพนธ์ฉบับนี้มีความผิดพลาดหรือบกพร่องในประการใดผู้เขียน ขอน้อมรับไว้แต่เพียงผู้เดียว

สุพิชญา ศิรินภาดล

| | |
|---|---|
| **ชื่อเรื่องวิทยานิพนธ์** | มาตรการของอาเซียนในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ: กรณีแก๊งคอลเซ็นเตอร์ |
| **ผู้ประพันธ์** | สุพิชญา ศิรินภาดล |
| **หลักสูตร** | นิติศาสตรมหาบัณฑิต |
| **อาจารย์ที่ปรึกษา** | รองศาสตราจารย์ ดร.ชูเกียรติ น้อยฉิม |

## บทคัดย่อ

วิทยานิพนธ์ฉบับนี้มุ่งศึกษาปัญหาอาชญากรรมข้ามชาติรูปแบบใหม่ในกรณีแก๊งคอลเซ็นเตอร์ ซึ่งแพร่ระบาดอย่างกว้างขวางในภูมิภาคเอเชียตะวันออกเฉียงใต้ อันเป็นผลจากการเปลี่ยนแปลงทางเทคโนโลยีและการสื่อสารในยุคดิจิทัล แก๊งคอลเซ็นเตอร์ใช้ช่องทางออนไลน์ในการหลอกลวงประชาชนข้ามพรมแดน ก่อให้เกิดความเสียหายต่อทรัพย์สินและความมั่นคงของประชาชนในหลายประเทศ โดยเฉพาะกลุ่มเปราะบางอย่างผู้สูงอายุหรือผู้ขาดทักษะด้านดิจิทัล ปัญหานี้มีลักษณะซับซ้อนและเกี่ยวพันกับการค้ามนุษย์ การใช้แรงงานโดยมิชอบ และการลักลอบข้ามพรมแดน ซึ่งส่งผลให้การบังคับใช้กฎหมายในหลายประเทศยังไม่สามารถจัดการกับปัญหาได้อย่างมีประสิทธิภาพ จากการศึกษาพบว่า แม้กลุ่มประเทศอาเซียนจะมีความพยายามร่วมมือกัน เช่น การออกแผนยุทธศาสตร์ความมั่นคงทางไซเบอร์ และการลงนามในปฏิญญาต่าง ๆ แต่ยังขาดอนุสัญญาพหุภาคีเฉพาะด้านที่สามารถกำหนดมาตรการทางกฎหมายร่วมกันในการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์อย่างชัดเจน นอกจากนี้ ความเหลื่อมล้ำทางเศรษฐกิจและกฎหมายระหว่างประเทศสมาชิกยังเป็นอุปสรรคสำคัญต่อการบังคับใช้มาตรการร่วมในระดับภูมิภาค ดังนั้น วิทยานิพนธ์จึงเสนอให้สมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้จัดทำอนุสัญญาพหุภาคีว่าด้วยการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ โดยมีเนื้อหาครอบคลุมมาตรการทางกฎหมายที่เป็นมาตรฐานร่วมกัน เช่น การสืบสวนข้ามพรมแดน การคุ้มครองเหยื่อ การติดตามและยึดทรัพย์ที่เกี่ยวข้องกับอาชญากรรม รวมทั้งการให้สัตยาบันและการอนุวัติกฎหมายดังกล่าวเข้าสู่ระบบกฎหมายภายในของแต่ละประเทศอย่างมีประสิทธิภาพ พร้อมทั้งเสนอให้จัดตั้งองค์กรกลางในระดับภูมิภาคเพื่อทำหน้าที่เป็นกลไกประสานงาน สะสมข้อมูลข่าวกรอง และติดตามการดำเนินคดีข้ามชาติ โดยมีสถานะเป็นกลางและเป็นที่ยอมรับของประเทศสมาชิกทั้ง 10 ประเทศ ซึ่งจะช่วยเสริมสร้างความเข้มแข็งให้แก่มาตรการของอาเซียนในการรับมือกับอาชญากรรมคอลเซ็นเตอร์อย่างยั่งยืนและเป็นรูปธรรมในระยะยาว

**คำสำคัญ :** อาชญากรรมข้ามชาติ, แก๊งคอลเซ็นเตอร์, อาเซียน, มาตรการทางกฎหมาย

| | |
|---|---|
| **Thesis Title** | ASean Measures to Prevent and Suppress Transnational Crimes: A Case of Crimes Committed Call Center Gangs |
| **Author** | Supichaya Sirinapadon |
| **Degree** | Master of Laws |
| **Advisor** | Associate Professor Chukeat Noichim, Ph. D. |


## ABSTRACT

This thesis aims to examine the emerging form of transnational crime represented by call center gangs, which have rapidly spread across Southeast Asia. This phenomenon is a consequence of technological and communication advancements in the digital age. Call center gangs exploit online platforms to deceive victims across borders, resulting in financial losses and threats to the security of individuals in multiple countries—particularly among vulnerable groups such as the elderly and those lacking digital literacy. The complexity of this issue is compounded by its connections to human trafficking, forced labor, and illegal border crossings, making it difficult for law enforcement agencies in many countries to address the problem effectively. The study finds that although ASEAN member states have taken steps toward cooperation—such as implementing the ASEAN Cybersecurity Cooperation Strategy and signing various declarations—there remains a lack of a specific multilateral convention that clearly outlines joint legal measures to prevent and suppress call center scams. Furthermore, disparities in economic development and legal systems among member countries pose significant challenges to the implementation of regional measures. Accordingly, this thesis proposes that the Association of Southeast Asian Nations (ASEAN) develop a multilateral convention focused on the prevention and suppression of transnational crimes committed by call center gangs. This convention should establish shared legal standards, including provisions for cross-border investigations, victim protection, the tracing and confiscation of crime-related assets, and effective incorporation of these measures into each member state's domestic legal system. In addition, the thesis recommends the establishment of a

neutral and widely accepted regional central agency to act as a coordination mechanism, intelligence repository, and body for monitoring transnational prosecutions. Such an initiative would significantly strengthen ASEAN's capacity to address call center scams in a sustainable and concrete manner over the long term.

**Keywords:** Transnational Crime, Call Center Gangs, ASEAN, Legal Measures

# สารบัญ

# สารบัญ

# สารบัญตาราง

# สารบัญภาพ

# บทที่ 1

# บทนำ

## 1.1 ความเป็นมาและความสำคัญของปัญหา

นับตั้งแต่สิ้นสุดภาวะสงครามเย็นจะเห็นได้ว่าบทบาทของรัฐค่อย ๆ ลดลงอย่างต่อเนื่อง ในขณะเดียวกันบทบาทของกลุ่มองค์กรนอกภาครัฐได้เพิ่มมากขึ้นและขยายวงกว้างออกไปเรื่อย ๆ หนึ่งในองค์กรนอกภาครัฐที่มีอิทธิพลอย่างมากในยุคปัจจุบัน คือ องค์กรอาชญากรรมข้ามชาติ[1] โดยส่วนใหญ่แล้วองค์กรอาชญากรรมข้ามชาติจะมุ่งเน้นไปที่ผลประโยชน์ทางเศรษฐกิจเป็นหลัก องค์กรอาชญากรรมข้ามชาติจะทำธุรกิจที่ผิดกฎหมายในประเทศอื่น ๆ และปัญหาภัยจากอาชญากรรมข้ามชาติถือว่าเป็นหนึ่งในภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของสังคมมนุษย์และประเทศชาติโดยตรง[2] ซึ่งในปัจจุบันสังคมโลกอยู่ในยุคของโลกาภิวัตน์ (Globalization)[3] ซึ่งเป็นผลมาจากการพัฒนาของเทคโนโลยีและคมนาคมของสังคมโลกที่ทำให้การเคลื่อนย้ายของมนุษย์ง่ายขึ้น อีกทั้งเป็นยุคที่มีการติดต่อสื่อสารกันอย่างไร้พรมแดนและมีความเจริญก้าวหน้าทางเทคโนโลยีเป็นอย่างมาก[4] ดังนั้น นอกจากอาชญากรรมข้ามชาติที่บั่นทอนความมั่นคงของภูมิภาคแล้ว ยังมีอาชญากรรมใน

---

[1] องค์กรอาชญากรรมข้ามชาติ หมายถึง การกระทำความผิดต่อเนื่องจากประเทศหนึ่ง ไปยังอีกประเทศหนึ่ง หรือมีผลกระทบเกี่ยวเนื่อง ตั้งแต่สองประเทศขึ้นไป ของกลุ่มบุคคลเพื่อให้ได้มา ซึ่งผลประโยชน์และอำนาจที่ขัดต่อหลักกฎหมาย และศีลธรรม ก่อให้เกิดผลกระทบต่อความมั่นคง ของบุคคล องค์กร เศรษฐกิจ สังคม การเมือง :โปรดดู, สำนักงานตำรวจแห่งชาติ, 'คู่มือป้องกันภัยจากอาชญากรรมข้ามชาติ' (สำนักงานตำรวจแห่งชาติ, 20 ธันวาคม 2565) <https://talatphlu.metro.police.go.th/wp-content/uploads/2022/12/คู่มือป้องกันภัยจากอาชญากรรมข้ามชาติ.pdf> สืบค้นเมื่อ 14 พฤศจิกายน 2566.

[2] นวภัทร สมกำเนิด และธรรมวิทย์ เทอดอุดมธรรม."อาชญากรรมข้ามชาติ: การใช้บัตรเครดิตปลอมของอาชญากรข้ามรัสเซียและกลุ่มประเทศยุโรปตะวันออก." *วารสารวิชาอาชญาวิทยาและนิติวิทยาศาสตร์โรงเรียนนายร้อยตำรวจ*, *17*(2), 137–152.

[3] โลกาภิวัตน์ (Globalization) เป็นผลจากการพัฒนาการติดต่อสื่อสาร การคมนาคมขนส่ง และเทคโนโลยีสารสนเทศ อันแสดงให้เห็นถึงการเจริญเติบโตของความสัมพันธ์ทางเศรษฐกิจ การเมือง เทคโนโลยี และวัฒนธรรมที่เชื่อมโยงระหว่างปัจเจกบุคคล ชุมชน หน่วยธุรกิจ และรัฐบาล ทั่วทั้งโลก :โปรดดู, วิกิพีเดีย, 'โลกาภิวัตน์' (วิกิพีเดีย, 22 พฤศจิกายน 2567) <https://th.wikipedia.org/wiki/โลกาภิวัตน์> สืบค้นเมื่อ 18 พฤษภาคม 2568.

[4] Law for ASEAN, 'อาเซียนกับการจัดการปัญหาอาชญากรรมไซเบอร์' (Law for ASEAN, 2 ธันวาคม 2565) <https://lawforasean.krisdika.go.th/File/files/cybersecurity_dec2.pdf> สืบค้นเมื่อ 14 พฤศจิกายน 2566.

ลักษณะที่เรียกได้ว่าเป็นภัยคุกคามจากความมั่นคงรูปแบบใหม่ (Non Traditional Security: NTS) นั้นก็คือ ภัยจาก “แก๊งคอลเซ็นเตอร์” (Call Center Gang) โดยแก๊งคอลเซ็นเตอร์ถือเป็นหนึ่งในอาชญากรรมไซเบอร์[5] ที่มาพร้อมกับความทันสมัยของเทคโนโลยีและโทรคมนาคม ด้วยบทบาทที่โดดเด่นของโซเชียลมีเดียและแพลตฟอร์มดิจิทัลต่างๆ ทำให้การติดต่อสื่อสารง่ายมากขึ้นซึ่งในขณะเดียวกันนั้นก็ถือเป็นคุณลักษณะของการดำเนินการหลอกลวงทางออนไลน์โดยถือเป็นภัยคุกคามต่อสันติภาพและความสงบสุขของประชาคมโลก

กว่า 57 ปีที่ผ่านมาภูมิภาคเอเชียตะวันออกเฉียงใต้ (Southeast Asian Region) ซึ่งเป็นภูมิภาคที่มีความแตกต่างมากมาย ทั้งทางด้านเชื้อชาติ วัฒนธรรม ศาสนา และภาษา โดยประเทศเพื่อนบ้านในภูมิภาคนี้ได้มีการรวมกลุ่มตั้งเป็นสมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ (Association of Southeast Asian Nations) ประชาคมอาเซียน หรือ ASEAN Community ที่จะเน้นการรวมตัวที่สำคัญใน 3 ด้านหลัก ๆ ด้วยกัน คือ ด้านประชาคมความมั่นคง หรือ ASEAN Security Community (ASC) ด้านประชาคมเศรษฐกิจ หรือ ASEAN Economic Community

---

[5] อาชญากรรมทางไซเบอร์ (Cyber Crime) หมายถึง (1) เป็นการทุจริตหลอกลวงที่เกิดขึ้นบนโลกออนไลน์ทุกประเภท ทั้งเว็บไซต์ แพลตฟอร์มโซเชียลมีเดีย แอปพลิเคชันบนโทรศัพท์มือถือ:โปรดดู, , จิราภพ ทวีสูงส่ง, เรื่องใกล้ตัวกว่าที่คิด! “อาชญากรรมทางไซเบอร์” รู้จักไว้..ป้องกันภัยไม่ตกเป็นเหยื่อ, Thai PBS 23 กุมภาพันธ์ 2566, https://www.thaipbs.or.th/now/content/68 (8 กรกฎาคม 2567) และ/หรือ (2) เป็นการกระทำความผิดทางกฎหมายโดยใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือในการก่อให้เกิดความเสียหายและ/หรือแสวงหาผลประโยชน์ส่วนตัวโดยมิชอบด้วยกฎหมาย อาชญากรรมไซเบอร์สามารถเกิดขึ้นในหลายรูปแบบ เช่น การโจมตีระบบคอมพิวเตอร์ ฯลฯ :โปรดดู, ธิติรัตน์ สมบูรณ์, ‘รู้ เข้าใจและตระหนัก “อาชญากรรมทางไซเบอร์” (Cybercrime) ป้องกันภัยคุกคามใกล้ตัว’ (Chulalongkorn University, 25 ตุลาคม 2566) <https://www.chula.ac.th/news/138291/> สืบค้นเมื่อ 8 กรกฎาคม 2567.

ทั้งนี้ ประเภทของอาชญากรรมทางไซเบอร์ มีทั้งหมด 10 ประเภท ประกอบด้วย: 1. Abusive Content (เนื้อหาที่เป็นภัยคุกคาม) 2. Availability (การโจมตีสภาพความพร้อมใช้งานของระบบ) 3. Fraud (การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์) 4. Information Gathering (ความพยายามรวบรวมข้อมูลของระบบ) 5. Information Security (การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต) 6. Intrusion Attempts (ความพยายามจะบุกรุกเข้าระบบ) 7. Intrusions (การบุกรุกหรือเจาะระบบได้สำเร็จ) 8. Malicious Code (โปรแกรมไม่พึงประสงค์) 9. Vulnerability (ช่องโหว่หรือข้อบกพร่องที่เกิดขึ้นโดยไม่ตั้งใจ) และ 10. Other (ภัยคุกคามอื่น ๆ นอกเหนือจากที่กำหนดไว้ข้างต้น): โปรดดู, จิราภพ ทวีสูงส่ง, ‘เรื่องใกล้ตัวกว่าที่คิด! “อาชญากรรมทางไซเบอร์” รู้จักไว้ป้องกันภัยไม่ตกเป็นเหยื่อ’ (Thai PBS, 23 กุมภาพันธ์ 2566) <https://www.thaipbs.or.th/now/content/68> สืบค้นเมื่อ 8 กรกฎาคม 2567.

(AEC) และด้านประชาสังคมและวัฒนธรรม หรือ ASEAN Socio-Cultural Community (ASCC)[6] ทั้งนี้ในช่วงไม่กี่ปีที่ผ่านมาอาเซียนหรือสมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ (The Association of Southeast Asian Nations)[7] ได้มีการเติบโตแบบก้าวกระโดดทั้งในเทคโนโลยีดิจิทัล (Digital technology) ธุรกิจ[8] (Business) และอีคอมเมิร์ซ[9] (E-commerce) ซึ่งนานาประเทศในภูมิภาคอาเซียนได้มีการเชื่อมโยงกันทางด้านดิจิทัลประกอบกับการพึ่งพาระบบดิจิทัลในการสร้างความมั่นคง ความรุ่งเรืองทางเศรษฐกิจ และการเชื่อมโยงทางสังคม อีกทั้งทางด้านเศรษฐกิจจะมีการเปิดเสรีการค้าสินค้า การค้าบริการ การลงทุน การเคลื่อนย้ายเงินทุนในอาเซียนทำได้เสรียิ่งขึ้น นักวิชาชีพ ผู้มีความสามารถพิเศษ แรงงานฝีมือสามารถเคลื่อนย้ายไปทำงานในประเทศอาเซียนอื่นได้สะดวกขึ้น จึงทำให้ภูมิภาคนี้มีความสุ่มเสี่ยงต่อการถูกคุกคามทางด้านความมั่นคงปลอดภัยจากอาชญากรและผู้ไม่หวังดีในการแสวงหาผลประโยชน์จากช่องโหว่ระหว่างข้อบังคับกฎหมายกับความก้าวหน้าของวิทยาการ และเนื่องด้วยช่วงที่ผ่านมามีการแพร่ระบาดใหญ่ของโรคโควิด-19 ได้มี

---

[6] พัลลภ หริ่งรอด, *มาตรการตามกฎหมายในการปราบปรามองค์กรอาชญากรรมข้ามชาติ ศึกษาเฉพาะกลุ่มคอลเซ็นเตอร์* (วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต สาขากฎหมายอาญาและอาชญาวิทยา คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา, 2562).

[7] องค์กรที่ก่อตั้งขึ้นตามปฏิญญากรุงเทพ เมื่อวันที่ 8 สิงหาคม พ.ศ.2510 มีประเทศสมาชิกรวม 10 ประเทศ ได้แก่ ประเทศไทย ประเทศบรูไน ดารุสซาลาม ประเทศกัมพูชา ประทศอินโดนีเซีย ประเทศเวียดนาม ประเทศลาว ประเทศเมียนมา ประเทศฟิลิปปินส์ ประเทศสิงคโปร์ และประเทศมาเลเซีย โดยอาเซียนก่อตั้งขึ้นโดยมีวัตถุประสงค์เริ่มแรกเพื่อสร้างสันติภาพในภูมิภาคเอเชียตะวันออกเฉียงใต้อันนำมาซึ่งเสถียรภาพทางการเมืองและความเจริญก้าวหน้าทางเศรษฐกิจ สังคม และวัฒนธรรม ต่อมาเมื่อมีการค้าขายระหว่างประเทศในโลกมีแนวโน้มกีดกันการค้ารุนแรงขึ้นทำให้อาเซียนหันมามุ่งกระชับและขยายความร่วมมือทางเศรษฐกิจมากขึ้นเพื่อประโยชน์ในการพัฒนาศักยภาพในการร่วมมือกับปัญหาและความท้าทายตลอดจนเพื่อสร้างความแข็งแกร่งและอำนาจต่อรองให้กับประเทศสมาชิก

[8] ธุรกิจ หมายถึง องค์การหรือกิจการที่ก่อให้เกิดสินค้า และบริการ ธุรกิจเป็นกระบวนการทั้งหมดของการนำเอาทรัพยากรธรรมชาติ มาเปลี่ยนสภาพตามกรรมวิธีการผลิตด้วยแรงคน และเครื่องจักรให้เป็นสินค้า เพื่อประโยชน์แก่ผู้ที่ต้องการ กิจกรรมของธุรกิจจึงรวมทั้งการผลิต การซื้อ ขาย การจำแนกแจกจ่ายสินค้า การขนส่ง การธนาคาร การประกันภัย และอื่น ๆ

[9] อีคอมเมิร์ซ (E-commerce) หมายถึง การทำธุรกรรมผ่านสื่ออิเล็กทรอนิกส์ในทุกช่องทางที่เป็นอิเล็กทรอนิกส์ ได้แก่ อินเทอร์เน็ตและระบบเครือข่ายคอมพิวเตอร์ การพาณิชย์อิเล็กทรอนิกส์สามารถกระทำผ่านโทรศัพท์เคลื่อนที่ การโอนเงินอิเล็กทรอนิกส์ การจัดการห่วงโซ่อุปทาน การโฆษณาในอินเทอร์เน็ต แม้กระทั่งซื้อขายออนไลน์ โดยมีวัตถุประสงค์เพื่อลดค่าใช้จ่ายและเพิ่มประสิทธิภาพขององค์กร โดยการลดบทบาทของความสำคัญขององค์ประกอบทางธุรกิจลง เช่น ทำเลที่ตั้ง อาคารประกอบการ โกดังเก็บสินค้า ห้องแสดงสินค้า รวมถึงพนักงานขาย พนักงานแนะนำสินค้า พนักงานต้อนรับลูกค้าเป็นต้น ดังนั้นจึงลดข้อจำกัดของระยะทางและเวลาในการทำธุรกรรมลงได้

มาตรการปิดเมือง ผู้คนหลายล้านคนต้องเก็บตัวอยู่กับบ้านและใช้เวลาทางออนไลน์มากขึ้นทำให้ประชาชนเหล่านี้ตกเป็นเป้าหมายของผู้บงการที่วางแผนฉ้อโกงทางออนไลน์ ซึ่งสถานการณ์ปัญหาอาชญากรรมข้ามชาติที่เกิดจากแก๊งคอลเซ็นเตอร์ในภูมิภาคอาเซียนนั้นในรายงานขององค์กรสหประชาชาติ (United Nations) ระบุว่ามีผู้คนนับแสนคนถูกบังคับหรือถูกหลอกลวงให้ไปทำงานกับเครือข่ายอาชญากรรมทางออนไลน์ส่วนมากเป็นเหยื่อค้ามนุษย์[10] ที่ถูกล่อลวงให้ไปทำงาน ซึ่งกลุ่มผู้คนที่ถูกล่อลวงนั้นจะถูกเชิญชวนจากโฆษณาที่มักจะอ้างว่าไปทำงานง่าย ๆ แต่รายได้หรือผลตอบแทนสูง เมื่อเหยื่อเดินทางไปถึงก็จะถูกคุมขังและบังคับให้ทำงานในสำนักงานหรือฐานที่ตั้งของแก๊งคอลเซ็นเตอร์ ผู้ที่ตกเป็นเหยื่อจะถูกหลอกโดยบังคับให้ทำงานในแก๊งคอลเซ็นเตอร์ แก๊งSMS หลอกลวง และเว็บไซต์พนันผิดกฎหมาย ผู้ที่ตกเป็นเหยื่อต้องเผชิญกับการละเมิดอย่างร้ายแรง ตกอยู่ภายใต้การทรมานและปฏิบัติลงโทษที่โหดร้ายไร้มนุษยธรรม เช่น การโดนกักขังตามอำเภอใจ การบังคับใช้แรงงาน รวมไปถึงการถูกคุกคามและความรุนแรงทางเพศ

มาตรการที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมข้ามชาติแก๊งคอลเซ็นเตอร์ในภูมิภาคอาเซียนนี้ มีแต่เพียงปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ ค.ศ.2017[11] (ASEAN Declaration to Prevent and Combat Cybercrime)[12] ซึ่งในการประชุมสุดยอดผู้นำอาเซียน ครั้งที่ 31 ระหว่างวันที่ 13 - 14 พฤศจิกายน 2560 ณ กรุงมะนิลา สาธารณรัฐ

---

[10]การค้ามนุษย์ เป็นการค้าแรงงานทาสยุคใหม่รูปแบบหนึ่ง ของอาชญากรรมที่บุคคลหนึ่งแสวงหาประโยชน์ส่วนตนทางการเงินจากบุคคลอื่น ผู้ค้ามนุษย์หาโอกาสจากสถานการณ์ที่เปราะบางของเหยื่อเพื่อบังคับขู่เข็ญเหยื่อ โดยมักจะใช้ความรุนแรงทางร่างกายหรือจิตใจเพื่อจำกัดอิสรภาพของเหยื่อ และยังอาจรวมถึงกีดกันเหยื่อในกรณีที่มีการพึ่งพาทางการเงิน (เพื่อที่อยู่อาศัย อาหาร เอกสาร) และ/หรือเพียงแค่ข่มเหงเหยื่อที่อ่อนแอ ผู้ค้ามนุษย์อาจดำเนินการกันเป็นขบวนการ แต่ก็อาจดำเนินการเพียงลำพังได้เช่นกัน

[11] Law for ASEAN, ‘ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ และบทวิเคราะห์กฎหมายไทยที่เกี่ยวข้อง’ (2566) *Law for ASEAN Journal*, <https://lawforasean.krisdika.go.th/Content/View?Id=349&Type=1> สืบค้นเมื่อ 14 พฤศจิกายน 2566.

[12]ASEAN Declaration to Prevent and Combat Cybercrime คือ ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ให้ความสำคัญกับการปรับปรุงกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์และหลักฐานทางอิเล็กทรอนิกส์ รวมทั้งสนับสนุนการร่างกรอบการทำงานระดับภูมิภาคเพื่อสร้างความร่วมมือระหว่างประเทศสมาชิกและการกำหนดแผนปฏิบัติการระดับชาติในการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์ รวมถึงการให้ความช่วยเหลือด้านผู้เชี่ยวชาญทางเทคนิคในการป้องกันและต่อต้านอาชญากรรมไซเบอร์ อันเป็นการยกระดับความร่วมมือระหว่างประเทศสมาชิกอาเซียนและประเทศคู่เจรจา รวมทั้งหน่วยงานและองค์กรต่าง ๆ ที่เกี่ยวข้องทั้งใน ระดับภูมิภาคและนานาชาติ นอกจากนี้ ปฏิญญาฯ ยังมีวัตถุประสงค์ในการเสริมสร้างความมั่นคงทางเทคโนโลยี การป้องกัน และความสามารถในการแก้ไขปัญหาเกี่ยวกับอาชญากรรมทางไซเบอร์ และเพื่อพัฒนาขีดความสามารถของอาเซียนในการสร้างและพัฒนาศักยภาพในการต่อสู้กับอาชญากรรมทางไซเบอร์

ฟิลิปปินส์ ผู้นำอาเซียนได้ตระหนักถึงความจำเป็นในการเสริมสร้างความร่วมมือในการต่อต้านอาชญากรรมทางไซเบอร์ โดยมุ่งเน้นไปที่การป้องกันสังคมของภูมิภาคอาเซียน รวมถึงการริเริ่มวิธีการในระดับภูมิภาคที่มั่นคงและมีประสิทธิภาพ โดยผู้นำอาเซียนทั้ง 10 ประเทศได้รับรองไว้ ซึ่งปฏิญญาดังกล่าวนี้มีวัตถุประสงค์ในการเสริมสร้างความมั่นคงทางเทคโนโลยี การป้องกัน และความสามารถในการแก้ไขปัญหาเกี่ยวกับอาชญากรรมทางไซเบอร์ เพื่อพัฒนาขีดความสามารถของอาเซียนในการสร้างและพัฒนาศักยภาพในการต่อสู้กับอาชญากรรมทางไซเบอร์ แต่อย่างไรก็ตามเป็นเพียงการแสดงเจตนารมณ์ร่วมกันระหว่างประเทศสมาชิกในการสร้างความร่วมมือระหว่างกันในการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์ของภูมิภาคอาเซียนเท่านั้น โดยในทางกฎหมายระหว่างประเทศการจัดทำปฏิญญาในลักษณะนี้ไม่ก่อให้เกิดพันธกรณีระหว่างประเทศที่ร่วมรับรองปฏิญญาแสดงให้เห็นว่าอาเซียนยังไม่มีมาตรการในการป้องกันและปราบปรามอาชญากรรมข้ามชาติที่เกิดจากแก๊งคอลเซ็นเตอร์ไว้อย่างชัดเจน

ดังนั้น อาชญากรรมข้ามชาติในรูปแบบของแก๊งคอลเซ็นเตอร์ได้กลายเป็นปัญหาสำคัญที่แพร่ระบาดอย่างต่อเนื่องในภูมิภาคเอเชียตะวันออกเฉียงใต้ ด้วยเหตุที่อาชญากรรมข้ามชาติที่เกิดจากแก๊งคอลเซ็นเตอร์เป็นการกระทำผิดข้ามแดนหรือเกี่ยวพันกับพื้นที่ตั้งแต่สองประเทศขึ้นไป ทำให้เกิดปัญหาในการกระบวนการยุติธรรมเนื่องจากภาครัฐในหลายประเทศไม่สามารถจัดการกับอาชญากรรมข้ามชาตินี้ได้อย่างมีประสิทธิภาพ แม้เจ้าหน้าที่ตำรวจและหน่วยงานที่เกี่ยวข้องจะได้ป้องกันและปราบปรามอย่างเต็มที่แต่ผู้กระทำความผิดที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์อาจไม่ถูกดำเนินการทั้งหมด อีกทั้งยังขาดความร่วมจากภาครัฐในประเทศที่เป็นฐานที่ตั้งปฏิบัติการของแก๊งคอลเซ็นเตอร์และมีปัญหาเกี่ยวกับเขตอำนาจรัฐที่หน่วยงานรักษากฎหมายในประเทศยังถูกจำกัดโดยรัฐของแต่ละประเทศทำให้การปราบปรามนั้นเป็นไปได้ยากจะต้องอาศัยความร่วมมือระหว่างรัฐเพื่อให้สามารถสกัดกั้นและจับกุมตัวผู้กระทำผิดมาลงโทษตามกฎหมายของรัฐที่ความผิดเกิดขึ้นให้ได้และจะต้องได้รับความร่วมมือระหว่างประเทศทางอาญาให้ชัดเจน เนื่องจากเป็นปัญหาข้ามชาติที่ไร้พรมแดน อาชญากร เครือข่าย และเหยื่อ อาจจะอยู่กันคนละประเทศโดยเชื่อมต่อกันด้วยระบบออนไลน์อาชญากรรมข้ามชาติที่เกิดจากแก๊งคอลเซนเตอร์นี้จึงไม่ใช่เรื่องที่รัฐใดรัฐหนึ่งจะจัดการได้อย่างเด็ดขาด[13] โดยสภาพปัญหาทางกฎหมายที่สำคัญในปัจจุบัน คือ การ ไม่มีมาตรการทางกฎหมายที่เฉพาะเจาะจงของอาเซียนในการรับมือกับอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์สถานการณ์ดังกล่าวส่งผลให้ภูมิภาคอาเซียนกลายเป็นแหล่งศูนย์กลางของกลุ่มอาชญากรคอลเซ็นเตอร์ที่มี

[13] สักกรินทร์ นิยมศิลป์, วิจารณ์เรื่อง อาชญากรรมข้ามชาติ ภัยคุกคามไทยและอาเซียน, ใน เอกสารการประชุมวิชาการสถาบันวิจัยประชากรและสังคม มหาวิทยาลัยมหิดล (2565), <https://ipsr.mahidol.ac.th/wp-content/uploads/2022/03/447-IPSR-Conference-A15-fulltext.pdf >สืบค้นเมื่อ 16 พฤศจิกายน 2566.

พัฒนาการต่อเนื่องและขยายตัวเพิ่มขึ้น หากไม่มีมาตรการที่เป็นรูปธรรมและประสานงานอย่างเป็นระบบระหว่างประเทศก็อาจนำไปสู่การสูญเสียที่มากขึ้น ทั้งในแง่จำนวนเหยื่อ การระบาดของการชักชวนแรงงานเข้าเครือข่ายอย่างผิดกฎหมาย และความเสื่อมถอยของความเชื่อมั่นในระบบยุติธรรมและความมั่นคงของรัฐด้วยเหตุนี้ เพื่อบรรเทาความเดือดร้อนและความเสียหายที่เกิดขึ้นภายในภูมิภาคอาเซียนอย่างยั่งยืน จึงมีความจำเป็นเร่งด่วนที่จะต้องทำการศึกษาวิจัยถึงรูปแบบและลักษณะการกระทำความผิดของแก๊งคอลเซ็นเตอร์ในภูมิภาคอาเซียน ควบคู่กับการศึกษา แนวทางทางกฎหมายและกลไกระหว่างประเทศที่มีประสิทธิภาพ ซึ่งอาจนำมาปรับใช้ในบริบทของอาเซียน ทั้งนี้เพื่อจัดทำข้อเสนอเชิงนโยบายและแนวทางทางกฎหมายที่สามารถป้องกันและปราบปรามอาชญากรรมข้ามชาติประเภทนี้ได้อย่างมีประสิทธิภาพและเป็นรูปธรรมในอนาคต

## 1.2 วัตถุประสงค์ของการศึกษา

1.2.1 เพื่อศึกษาวิวัฒนาการ แนวความคิด และทฤษฎี ที่เกี่ยวกับอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ที่เป็นภัยต่อความมั่นคงของโลกและภูมิภาคอาเซียน

1.2.2 เพื่อศึกษาถึงนโยบายและมาตรการทางกฎหมายระดับระหว่างประเทศและระดับภูมิภาค รวมทั้งระดับประเทศในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

1.2.3 เพื่อศึกษาสภาพปัญหาในปัจจุบันที่เกี่ยวกับอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ที่เป็นภัยต่อความมั่นคงในภูมิภาคอาเซียน

1.2.4 เพื่อวิเคราะห์หาแนวทางและมาตรการของอาเซียนในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

## 1.3 สมมติฐานของการศึกษา

ปัจจุบันอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ยังคงเป็นปัญหาสำคัญที่ยังคงเกิดขึ้นอย่างต่อเนื่องและในภูมิภาคอาเซียนยังไม่มีมาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมข้ามชาติที่เกิดจากแก๊งคอลเซ็นเตอร์ไว้อย่างชัดเจน ทำให้อาชญากรรมข้ามชาติที่เกิดจากแก๊งคอลเซ็นเตอร์นี้ไม่มีท่าทีว่าจะสามารถจำกัดได้โดยเร็ว จึงส่งผลกระทบต่อประชาชนจำนวนมากที่จะต้องถูกล่อลวงให้เข้าไปทำงานกับแก๊งคอลเซ็นเตอร์หรือสูญเสียเงินจากการถูกหลอกลวงให้แก่แก๊งคอลเซ็นเตอร์ ดังนั้น เห็นควรทำการศึกษาวิจัยเพื่อหาแนวทางและมาตรการ

ในการป้องกันและปราบปรามอาชญากรรมข้ามชาติที่เกิดจากแก๊งคอลเซ็นเตอร์ที่มีประสิทธิภาพและประสิทธิผลต่อการป้องกันและปราบปรามอาชญากรรมข้ามชาติประเภทดังกล่าวในอนาคต

## 1.4 ขอบเขตของการศึกษาวิจัย

งานวิจัยฉบับนี้จะทำการศึกษาถึงแนวคิดและทฤษฎีที่เกี่ยวข้องกับอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ซึ่งเป็นภัยคุกคามต่อความมั่นคงของโลกและภูมิภาคอาเซียน โดยจะวิเคราะห์พัฒนาการ รูปแบบ และกลไกการดำเนินการของแก๊งคอลเซ็นเตอร์ในบริบทของภูมิภาคดังกล่าว ตลอดจนทำการศึกษากฎหมายที่เกี่ยวข้องทั้งในระดับสากล ระดับภูมิภาค และระดับประเทศไม่ว่าจะเป็นกฎหมายภายในประเทศ กฎหมายระหว่างประเทศ และกฎหมายอาเซียนว่าด้วยความร่วมมือในการป้องกันและปราบปรามอาชญากรรมข้ามชาติเพื่อประเมินความเหมาะสมและความครอบคลุมของแนวทางต่าง ๆ ที่สามารถนำมาใช้เป็นมาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีของแก๊งคอลเซ็นเตอร์

## 1.5 วิธีการดำเนินการวิจัย

การดำเนินการวิจัยเชิงคุณภาพ (Qualitative Research) โดยใช้วิธีการค้นคว้าและรวบรวมข้อมูลจากเอกสาร (Document research) โดยศึกษา แนวคิด ทฤษฎี หลักกฎหมาย บทบัญญัติของกฎหมาย วิทยานิพนธ์ งานวิจัย วารสาร บทความ เอกสารทางวิชาการ ข้อมูลอินเตอร์เน็ต เพื่อนำข้อมูลที่ได้มาวิเคราะห์ปัญหาและเสนอแนะแนวทางการแก้ไข

## 1.6 ประโยชน์ที่คาดว่าจะได้รับจากการศึกษา

1.6.1 ทราบถึงวิวัฒนาการ แนวคิด และทฤษฎีที่เกี่ยวกับอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ที่เป็นภัยต่อความมั่นคงของโลกและภูมิภาคอาเซียน

1.6.2 ทราบถึงมาตรการทางกฎหมายระดับระหว่างประเทศและระดับภูมิภาค รวมทั้งระดับประเทศในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีกรณีแก๊งคอลเซ็นเตอร์

1.6.3 ทราบถึงสภาพปัญหาในปัจจุบันที่เกี่ยวกับอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ที่เป็นภัยต่อความมั่นคงในภูมิภาคอาเซียน

1.6.4 ได้แนวทางและมาตรการของอาเซียนในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

# บทที่ 2

# วิวัฒนาการ แนวความคิดและทฤษฎีที่เกี่ยวกับอาชญากรรมข้ามชาติ กรณีแก๊งคอลเซ็นเตอร์

ปัจจุบันอาชญากรรมข้ามชาติยิ่งทวีความรุนแรงมาก และมีวิธีการ รูปแบบที่หลากหลายยิ่งขึ้นกว่าที่เคยเป็นมาในอดีต เนื่องจากการขยายตัวของอาชญากรรมข้ามชาติในภูมิภาคอาเซียนนั้นส่วนหนึ่งเกิดจากความเหลื่อมล้ำทางด้านกฎหมายและการบังคับใช้กฎหมายภายในรัฐของประเทศสมาชิกดังนั้นการแก้ไขปัญหาการก่ออาชญากรรมข้ามชาติจึงจำเป็นที่จะต้องมีความครอบคลุม ทันต่อสถานการณ์การเปลี่ยนแปลงของสภาพปัญหาและมีความจำเป็นอย่างมากที่จะต้องอาศัยความร่วมมือจากทุกภาคส่วนในการร่วมมือกันแก้ไขปัญหา การป้องกันและปราบปรามอาชญากรรมข้ามชาติเพื่อบูรณาการข้อมูล ข่าวสารระหว่างองค์กรหน่วยงานที่มีหน้าที่เกี่ยวข้องตลอดจนประสานความร่วมมือกับประเทศในกลุ่มอาเซียนและประเทศอื่น ๆ ซึ่งพบว่ามีแนวความคิดและทฤษฎีที่เกี่ยวข้องกับการศึกษาวิจัย ดังนี้

## 2.1 นิยามความหมายขององค์กรอาชญากรรมข้ามชาติ อาชญากรรมข้ามชาติ และแก๊งคอลเซ็นเตอร์

### 2.1.1 นิยามความหมายขององค์กรอาชญากรรมข้ามชาติ

ในยุคโลกาภิวัตน์มีความเปลี่ยนแปลงอย่างรวดเร็วทั้งทางด้านสังคม เศรษฐกิจ และเทคโนโลยี ความเปลี่ยนแปลงดังกลาวนี้ก่อให้เกิดผลกระทบในหลายด้าน โดยเฉพาะอย่างยิ่งลักษณะของอาชญากรรมที่เปลี่ยนรูปแบบจากอาชญากรรมที่ใช้ความรุนแรงธรรมดาไปสู่องค์กรอาชญากรรมและพัฒนาตอเนื่องไปสู่รูปแบบของอาชญากรรมข้ามชาติในที่สุด[31] ซึ่งกรณีของการกระทำผิดของแก๊งคอลเซ็นเตอร์มีลักษณะขององค์กรอาชญากรรมข้ามชาติที่มีความสอดคล้องกับการกระทำผิดในลักษณะขององค์กรอาชญากรรมข้ามชาติตามอนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร ค.ศ.2000 (United Nations Convention against Transnational

[31] วัชรพล ประสารราชกจ, ปัญหาอาชญากรรมข้ามชาติและนโยบายความมั่นคงมุมมองไทยยุโรปและนานาชาติ (กรุงเทพฯ: จุฬาลงกรณ์มหาวิทยาลัย 2544), 59.

Organized Crime-UNTOC) ที่ได้กำหนดคำนิยามและความหมายของคำว่า “องค์กรอาชญากรรม” ไว้ว่า

1. กลุ่มอาชญากรที่จัดตั้งในลักษณะองค์กร[32] (Organized Criminal Group) หมายถึง กลุ่มที่มีการจัดโครงสร้างประกอบด้วยบุคคลตั้งแต่ 3 คนขึ้นไปที่ดำรงอยู่เป็นระยะเวลาหนึ่งและที่มี

---

[32] The United Nations Office on Drugs and Crime (UNODC), Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime and the Protocol Thereto, New York, 2004

Article 2 Use of terms for the purposes of this Convention:

(a) “Organized criminal group” shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit ;

(b) “Serious crime” shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty ;

(c) “Structured group” shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure ;

(d) “Property” shall mean assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets ;

(e) “Proceeds of crime” shall mean any property derived from or obtained, directly or indirectly, through the commission of an offence;

(f) “Freezing” or “seizure” shall mean temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority; Annex I United Nations Convention against Transnational Organized Crime 6

(g) “Confiscation”, which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority;

(h) “Predicate offence” shall mean any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in article 6 of this Convention ;

(i) “Controlled delivery” shall mean the technique of allowing illicit or suspect consignments to pass out of, through or into the territory of one or more States, with the knowledge

การประสานการดำเนินงานระหว่างกันโดยมีเป้าหมายในการก่ออาชญากรรมร้ายแรงตั้งแต่หนึ่งฐานความผิดขึ้นไปตามที่ได้กำหนดไว้ในอนุสัญญานี้เพื่อให้ได้มาซึ่งผลประโยชน์ทางการเงินหรือผลประโยชน์ทางวัตถุอย่างอื่นไม่ว่าโดยทางตรงหรือทางอ้อม

2. อาชญากรรมร้ายแรง (Serious Crime) หมายถึง การกระทำที่เป็นความผิดซึ่งสามารถลงโทษ โดยการทำให้สูญเสียเสรีภาพขั้นสูงสุดเป็นเวลาอย่างน้อย 4 ปีหรือโดยโทษที่รุนแรงกว่า

3. ทรัพย์สินที่ได้จากอาชญากรรม (Proceeds of Crime) หมายถึง ทรัพย์สินใดที่เกิดจากหรือได้รับมาไม่ว่าโดยทางตรงหรือทางอ้อมจากการกระทำความผิด

นอกจากนี้ลักษณะขององค์กรอาชญากรรมโดยสรุปจากทัศนะและข้อเสนอของนักวิชาการหลายท่าน เห็นว่า กลุ่มองค์กรอาชญากรรมมีลักษณะ คือ ไม่มีอุดมการณ์ทาง การเมือง มีการจัดลำดับชั้นองค์กร มีสมาชิกจำนวนจำกัดหรือเฉพาะกลุ่มใดกลุ่มหนึ่ง มีการดำเนินงานอย่างต่อเนื่อง ใช้วิธีการที่ผิดกฎหมายหรือใช้ความรุนแรงหรือข่มขู่และการติดสินบน มีการกำหนดหน้าที่และการแบ่งงานกันทำอย่างชัดเจน มีลักษณะเป็นการผูกขาด มีกฎข้อบังคับ ระหว่างสมาชิกที่ชัดเจนรวมถึงข้อกำหนดในการปฏิบัติงานที่เป็นความลับ

จากนิยามความหมายขององค์กรอาชญากรรมข้างต้นจะเห็นได้ว่า องค์กรอาชญากรรมมีนัยสะท้อนให้เห็นถึงการก่ออาชญากรรมที่ไม่ได้มีอาชญากรหรือผู้กระทำความผิดเพียงคนเดียว หากแต่มีลักษณะของการจัดระเบียบองค์กร[33] (Organization) โดยผู้กระทำความผิดหรือร่วมคบคิดกระทำความผิดมีหลายคนและแต่ละคนมีหน้าที่ความรับผิดชอบเฉพาะ มีระบบการติดต่อสื่อสารที่ปกปิดและมีการตัดตอน การรับรู้ในข้อมูลเท่าที่จำเป็น มีระบบควบคุมอย่างเคร่งครัด มีผู้บงการใหญ่อยู่เบื้องหลังผู้ลงมือทำความผิดส่วนใหญ่เป็นลูกน้องระดับล่าง และองค์กรอาชญากรรมส่วนใหญ่มีพฤติกรรมการกระทำความผิดเป็นกระบวนการหรือมีรูปแบบการกระทำความผิดที่สลับซับซ้อน จัดตั้งเป็นองค์กร

---

and under the supervision of their competent authorities, with a view to the investigation of an offence and the identification of persons involved in the commission of the offence.

(j) “Regional economic integration organization” shall mean an organization constituted by sovereign States of a given region, to which its member States have transferred competence in respect of matters governed by this Convention and which has been duly authorized, in accordance with its internal procedures, to sign, ratify, accept, approve or accede to it; references to “States Parties” under this Convention shall apply to such organizations within the limits of their competence.

[33] แคทราย จันทรากา, *มาตรการทางกฎหมายของอาเซียนในการป้องกันและปราบปรามการค้ามนุษย์* (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยแม่ฟ้าหลวง, 2558), 20.

เพื่อกระทำผิดกฎหมายในองค์กรมีการจัดระบบป้องกนการสืบสวนลงโทษจากฝ่ายเจ้าหน้าที่อย่างดี การสั่งการหรือการสื่อสารจะใช้ช่องทางลับหรือใช้รหัสมีการควบคุมและรักษาความลับอย่างเคร่งครัด ผู้ใดผิดพลาดจะได้รับการลงโทษจากองค์กรอย่างรุนแรง เมื่อถูกจับกุมหากรับสารภาพจะปกปิดข้อมูล ไม่ซัดทอดมีระบบตัดสัมพันธ์พยานหลักฐานที่อาจพาดพิงถึงตัวกลางใหญ่ไว้อย่างรัดกุม โดยการจัดลำดับชั้นของผู้ร่วมกระทำความผิดด้วยการมอบหมายงานกันเป็นทอด ๆ[34]

**2.1.2 นิยามความหมายของอาชญากรรมข้ามชาติ**

สำนักงานตำรวจแห่งชาติ ได้กำหนดความหมายของ “อาชญากรรมข้ามชาติ” ไว้ตามหนังสือที่ 0003.24/7505 ลงวันที่ 18 สิงหาคม 2542 ไว้ว่า อาชญากรรมข้ามชาติ คือ การกระทำที่มีประเทศที่เกี่ยวข้องอย่างน้อย 2 ประเทศ ถือว่าเป็นความผิดตามกฎหมายอาญาและกำหนดโทษไว้ กระทำร่วมกันโดยกลุ่มบุคคลตั้งแต่ 2 คนขึ้นไปในรูปแบบขององค์กร มีจุดมุ่งหมายเพื่อแสวงหาประโยชน์ ร่วมกนโดยมีการตระเตรียมการพยายามและลงมือกระทำความผิดต่อเนื่องกันจากประเทศหนึ่งไปยังอีกประเทศหนึ่งหรือหลายประเทศ[35]

สหประชาชาติได้นิยามคำว่าอาชญากรรมข้ามชาติไว้ในอนุสัญญาว่าด้วยการต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร ค.ศ.2000 (UNITED NATIONS CONVENTION AGAINST TRANSNATIONAL ORGANIZED CRIME 2000; UNTOC) ว่าหมายถึง การกระทำความผิดทางอาญาที่ได้กระทำลงมากกว่า ในหนึ่งประเทศ หรือมีส่วนหนึ่งส่วนใดของการกระทำผิดหรือผลกระทบเกี่ยวข้อง ตั้งแต่ 2 ประเทศขึ้นไป ซึ่งอยู่ในข้อ 3 ของอนุสัญญาฯ ว่าด้วย “ขอบเขตการใช้บังคับ” ระบุไว้ชัดเจนว่า ลักษณะความผิดต่อไปนี้ให้ถือว่าเป็นอาชญากรรมข้ามชาติหาก[36]

1. เป็นการกระทำที่เกิดขึ้นในรัฐมากกว่า 1 รัฐขึ้นไป

---

[34] วันชัย รุจนวงศ์, ผ่านองค์กรอาชญากรรม มะเร็งร้ายของสังคม, 24-26.

[35] วัชรพล ประสารราชกจ, ปัญหาอาชญากรรมข้ามชาติและนโยบายความมั่นคงมุมมองไทยยุโรปและนานาชาติ, 60.

[36] Article 3 - Scope of Application for the purposes of this Article, an offence is transnational in nature if:

(a) It is committed in more than one State;

(b) It is committed in one State but a substantial part of its preparation, planning, direction, or control takes place in another State;

(c) It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or

(d) It is committed in one State but has substantial effects in another State.

2. เป็นการกระทำความผิดอาญาที่เกิดขึ้นในรัฐหนึ่งแต่การเตรียมการณ์เพื่อกระทำความผิดที่สำคัญ หมายถึง การกระทำความผิดเกิดในรัฐเดียวแต่มีการควบคุมในอีกรัฐหนึ่ง

3. เป็นการกระทำความผิดอาญาในรัฐหนึ่งและมีกลุ่มอาชญากรที่มีการจัดตั้งในลักษณะองค์กรซึ่งเกี่ยวข้องกับกิจการผิดกฎหมายที่มีการดำเนินการในรัฐมากกว่าหนึ่งรัฐ

4. เป็นการกระทำความผิดอาญาในรัฐหนึ่งแต่มีผลกระทบอย่างสำคัญอีกรัฐหนึ่ง

**2.1.3 นิยามความหมายของแก๊งคอลเซ็นเตอร์**

ในปัจจุบันยังไม่มีนักวิชาการที่ได้ให้คำนิยามของคำว่า “แก๊งคอลเซ็นเตอร์” ไว้อย่างชัดเจนในเชิงวิชาการหรือตามบทบัญญัติกฎหมายโดยตรง แต่จากการศึกษาผู้วิจัยสามารถสรุปจากเอกสารทางวิชาการที่ได้สืบค้นเพิ่มเติมว่า “แก๊งคอลเซ็นเตอร์” หมายถึง กลุ่มองค์กรอาชญากรรมข้ามชาติที่มีการจัดโครงสร้างเป็นขบวนการ โดยอาศัยเทคโนโลยีการสื่อสารและแพลตฟอร์มดิจิทัลเป็นเครื่องมือในการกระทำความผิด ลักษณะสำคัญคือการแอบอ้างเป็นเจ้าหน้าที่รัฐหรือสถาบันทางการเงิน เพื่อหลอกลวงหรือข่มขู่ให้เหยื่อโอนเงินหรือเปิดเผยข้อมูลสำคัญ อันก่อให้เกิดความเสียหายต่อทรัพย์สินและสิทธิเสรีภาพของประชาชน มักดำเนินการข้ามพรมแดน โดยใช้แรงงานผิดกฎหมายหรือบังคับแรงงาน ซึ่งมีลักษณะคล้ายคลึงกับการค้ามนุษย์ในรูปแบบใหม่ และเป็นภัยคุกคามต่อความมั่นคงของภูมิภาคในยุคดิจิทัล

รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง รองศาสตราจารย์ ดร.ปิยะพร ตันณีกุล และดร.นัทธี จิตสว่าง[37] ได้อธิบายไว้ว่า “กลุ่มบุคคลตั้งแต่ 3 คนขึ้นไปที่กระทำความผิดโดยเกี่ยวข้องกับการใช้โทรศัพท์หรืออินเทอร์เน็ตในการหลอกลวงเหยื่อให้โอนเงินให้แก่แก๊งคอลเซ็นเตอร์ โดยมักใช้วิธีโทรศัพท์ หรือโทรศัพท์ผ่านระบบคอมพิวเตอร์ หรือ VoIP (Voice over IP) เพื่อทำการแปลงสัญญาณปลอมเป็นหมายเลขโทรศัพท์ของหน่วยงานภาครัฐหรือสถาบันการเงิน อันเป็นการสร้างความน่าเชื่อถือและทำให้เหยื่อหลงเชื่อจนถูกหลอกลวง

การกระทำความผิดของแก๊งคอลเซ็นเตอร์ประกอบด้วยองค์ประกอบสำคัญ 4 กลุ่ม ได้แก่

กลุ่มคอลเซ็นเตอร์ หมายถึง กลุ่มผู้ที่ปฏิบัติงานประจำศูนย์คอลเซ็นเตอร์ ซึ่งทำหน้าที่โทรศัพท์หรือใช้อินเทอร์เน็ตในการหลอกลวงเหยื่อ

กลุ่มม้าถอนเงิน หมายถึง กลุ่มผู้ที่ใช้บัตรอิเล็กทรอนิกส์ (บัตรเอทีเอ็ม) ในการถอนเงินจากตู้เอทีเอ็ม หรือถอนเงินโดยไม่ใช้บัตรจากตู้ถอนเงินสดอัตโนมัติ

กลุ่มจัดหาบัญชีธนาคารหรือบัตรอิเล็กทรอนิกส์ หมายถึง กลุ่มผู้ที่ทำหน้าที่รวบรวมบัญชีธนาคารและบัตรเอทีเอ็มเพื่อส่งมอบให้แก่กลุ่มม้าถอนเงิน

---

[37] สุมนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และ นัทธี จิตสว่าง, *อาชญากรรมข้ามชาติ: ภัยคุกคามประเทศไทยเกี่ยวกับแก๊งคอลเซ็นเตอร์* (รายงานวิจัย, 2563), 9-10.

กลุ่มจัดการทางการเงิน หมายถึง กลุ่มผู้ที่ทำหน้าที่รวบรวมเงินสดจากกลุ่มม้าถอนเงินเพื่อนำส่งให้หัวหน้าแก๊งหรือผู้บังคับบัญชาในระดับถัดไป ”

ดังนั้น จากคำนิยามแก๊งคอลเซ็นเตอร์ดังที่กล่าวมาข้างต้น ผู้วิจัยสามารถสรุปคำนิยามของคำว่า “แก๊งคอลเซ็นเตอร์ หมายถึง กลุ่มองค์กรอาชญากรรมข้ามชาติที่มีโครงสร้างเป็นขบวนการและดำเนินการอย่างเป็นระบบโดยอาศัยเทคโนโลยีสารสนเทศและการสื่อสารเป็นเครื่องมือหลักในการกระทำความผิด ซึ่งไม่จำกัดเฉพาะการใช้โทรศัพท์เพื่อหลอกลวงเท่านั้น แต่ยังรวมถึงช่องทางอื่น ๆ เช่น การใช้โซเชียลมีเดีย แพลตฟอร์มออนไลน์ และสื่อดิจิทัลต่าง ๆ เพื่อเข้าถึงและหลอกลวงเหยื่อ โดยมีวัตถุประสงค์เพื่อให้เหยื่อเปิดเผยข้อมูลส่วนบุคคลสำคัญหรือโอนทรัพย์สินทางการเงินไปยังผู้กระทำความผิด การกระทำของแก๊งคอลเซ็นเตอร์เหล่านี้ส่งผลกระทบโดยตรงต่อความมั่นคงของทรัพย์สินและสิทธิเสรีภาพของประชาชน อีกทั้งยังสร้างความเสียหายทางเศรษฐกิจและสังคมในระดับกว้างขวาง”

## 2.2 วิวัฒนาการของอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

ปรากฏการณ์ของ “แก๊งคอลเซ็นเตอร์” ถือเป็นรูปแบบของอาชญากรรมข้ามชาติที่สะท้อนถึงพัฒนาการของอาชญากรรมในยุคดิจิทัล โดยมีลักษณะเฉพาะคือการใช้เทคโนโลยีโทรคมนาคมและเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือในการกระทำผิด พร้อมกับการจัดองค์กรอย่างเป็นระบบ มีการแบ่งหน้าที่ภายในกลุ่มอย่างชัดเจน และมุ่งเป้าหมายไปที่ผลประโยชน์ทางเศรษฐกิจผ่านการหลอกลวงประชาชนในหลายประเทศพร้อมกัน อาชญากรรมลักษณะนี้ไม่สามารถจำกัดกรอบไว้เฉพาะในประเทศใดประเทศหนึ่งอีกต่อไป หากแต่เคลื่อนไหวข้ามพรมแดนอย่างซับซ้อนและยากต่อการติดตามตรวจสอบโดยกลไกของรัฐชาติแบบดั้งเดิม ต้นกำเนิดของแก๊งคอลเซ็นเตอร์สามารถสืบย้อนกลับไปยังประเทศไต้หวันในช่วงปลายคริสต์ทศวรรษ 1990 ซึ่งเป็นช่วงที่เทคโนโลยีโทรคมนาคมเริ่มแพร่หลายสู่สาธารณะ โดยแก๊งอาชญากรในไต้หวันเริ่มต้นจากการหลอกลวงผู้เสียหายให้ไปที่เครื่องเอทีเอ็มและโอนเงินให้แก่คนร้าย โดยใช้เทคนิคการแอบอ้างเป็นเจ้าหน้าที่รัฐ เช่น ตำรวจ หรือเจ้าหน้าที่ธนาคาร เพื่อสร้างแรงกดดันให้เหยื่อเกิดความกลัว เทคนิคนี้ต่อมาได้ถูกเรียกว่า “ATM Game” หรือ “เกมส์ตู้เอทีเอ็ม” ซึ่งถือเป็นต้นแบบของแก๊งคอลเซ็นเตอร์ในยุคปัจจุบัน[38]การกระทำผิดในช่วงแรกเริ่มจำกัดอยู่ในไต้หวัน แต่ภายหลังกลับขยายตัวอย่างรวดเร็วไปยังประเทศเพื่อนบ้าน เช่น จีน เกาหลีใต้ ญี่ปุ่น

[38] กรมสอบสวนคดีพิเศษ, ‘รายงานสถานการณ์อาชญากรรมข้ามชาติ ประเภทแก๊งคอลเซ็นเตอร์’ (2565) <https://www.dsi.go.th> สืบค้นเมื่อ 18 พฤษภาคม 2568.

และประเทศในอาเซียน เช่น ไทย เวียดนาม มาเลเซีย และกัมพูชา โดยเฉพาะในช่วงปีค.ศ. 2010 เป็นต้นมา แก๊งคอลเซ็นเตอร์เริ่มใช้ประเทศในเอเชียตะวันออกเฉียงใต้เป็นฐานปฏิบัติการหลัก เนื่องจากมีช่องว่างด้านการบังคับใช้กฎหมาย ความเหลื่อมล้ำทางเศรษฐกิจ และการเข้าถึงเทคโนโลยีที่ไม่เท่าเทียมกัน ซึ่งเอื้ออำนวยให้เครือข่ายอาชญากรรมสามารถใช้ภูมิภาคนี้เป็นที่ตั้งศูนย์โทรศัพท์และหลอกลวงเหยื่อในต่างประเทศได้โดยยากต่อการติดตาม

ดังนั้น ต้นกำเนิดของขบวนการแก๊งคอลเซ็นเตอร์ที่มีพฤติการณ์ในการหลอกลวงประชาชน มีรากฐานมาจากการกระทำความผิดของเครือข่ายอาชญากรรมข้ามชาติ ซึ่งมีลักษณะการประสานงานอย่างเป็นระบบระหว่างผู้บงการรายสำคัญที่มีสัญชาติไต้หวันกับกลุ่มอาชญากรท้องถิ่นในประเทศต่าง ๆ ภายในภูมิภาคเอเชีย เช่น สาธารณรัฐประชาชนจีน ราชอาณาจักรกัมพูชา มาเลเซีย สหรัฐอาหรับเอมิเรตส์ และราชอาณาจักรไทย โดยผู้บงการชาวไต้หวันดังกล่าวจะมอบหมายให้ตัวแทนเดินทางไปเจรจาและจัดตั้งความร่วมมือกับกลุ่มอาชญากรในแต่ละประเทศซึ่งกลุ่มอาชญากรเหล่านี้มักมีความรู้และความเชี่ยวชาญเฉพาะด้านเกี่ยวกับระบบการเงิน กฎหมาย และบริบททางสังคมของประเทศตนเอง ซึ่งความเชี่ยวชาญดังกล่าวถูกนำมาใช้เป็นกลไกสำคัญในการลวงเหยื่อเพื่อหลีกเลี่ยงการถูกติดตาม ตรวจสอบ หรือจับกุมจากเจ้าหน้าที่ของรัฐในประเทศต้นทางของผู้เสียหาย โดยมีการจัดระบบการควบคุมและกำกับดูแลเป็นลำดับชั้นผ่านตัวแทนที่ได้รับการแต่งตั้งจากกลุ่มผู้บงการชาวไต้หวัน ซึ่งมีความเชื่อมโยงโดยตรงกับหัวหน้าเครือข่ายที่พำนักอยู่ในไต้หวัน ตัวอย่างเช่น แก๊งอาซื่อ ซึ่งมีฐานปฏิบัติการอยู่ในย่านศรีเปอร์ตาลิง กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย และแก๊งฉีเคอซึ่งมีศูนย์บัญชาการอยู่ที่นครดูไบ ประเทศสหรัฐอาหรับเอมิเรตส์[39] กล่าวโดยสรุปคือ ต้นตอของแก๊งคอลเซ็นเตอร์มีรากฐานจากการร่วมมือกันของเครือข่ายอาชญากรรมข้ามชาติ โดยเฉพาะกลุ่มอิทธิพลจากไต้หวันซึ่งประสานงานกับแก๊งท้องถิ่นในหลายประเทศเอเชีย เพื่อดำเนินการหลอกลวงข้ามพรมแดนผ่านระบบที่ซับซ้อนและยากต่อการตรวจสอบของเจ้าหน้าที่รัฐ

## 2.3 รูปแบบของอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

### 2.3.1 รูปแบบการกระทำความผิดของอาชญากรรมข้ามชาติ

องค์กรอาชญากรรมข้ามชาติเป็นอาชญากรรมที่ดำเนินการข้ามพรมแดนของประเทศต่าง ๆ ที่มีความเกี่ยวข้องเชื่อมโยงกับกลุ่มองค์กรหรือเครือข่ายบุคคลในประเทศต่าง ๆ ด้วยแผนการที่จะก่อ

[39] สุมนทิพย์ จิตสว่าง ปิยะพร ตันณีกุล และ นัทธี จิตสว่าง, ‘อาชญากรรมข้ามชาติ: ภัยคุกคามประเทศไทยเกี่ยวกับแก๊งคอลเซ็นเตอร์’ (รายงานวิจัย, 2563) 2.

อาชญากรรม องค์กรอาชญากรรมมีบทบาทมากขึ้นในภูมิภาคอาเซียนพร้อม ๆ กับความเจริญก้าวหน้าทางเศรษฐกิจ เนื่องจากผู้กระทำผิดแสวงหาหนทางในการสร้างผลประโยชน์แก่ตนเองผ่านข้ามพรมแดน การกระทำผิดในลักษณะนี้เป็นภัยอย่างยิ่งต่อความมั่นคงและการพัฒนาอย่างยั่งยืนในภูมิภาคเอเชีย[40] ซึ่งในปัจจุบันปัญหาอาชญากรรมข้ามชาตินั้นนับวันจะยิ่งทวีความรุนแรงและสลับซับซ้อนเพิ่มมากขึ้น ซึ่งประเทศในภูมิภาคอาเซียนมีส่วนเกี่ยวข้องทุกระดับทั้งเป็นต้นทางของปัญหา เป็นจุดพักหรือทางผ่าน รวมทั้งเป็นเป้าหมายของอาชญากรรมซึ่งมีทั้งอาชญากรรมข้ามชาติ (Transnational crime) และอาชญากรรมข้ามพรมแดน (Cross-border crime) โดยองค์การสหประชาชาติได้แบ่งประเภทขององค์กรอาชญากรรมข้ามชาติออกเป็น 10 ลักษณะ[41] คือ

1. การลักลอบค้ายาเสพติด (Illicit trafficking in Drugs)
2. การลักลอบคนเข้าเมือง (Smuggling of Illegal Migrants)
3. การค้าอาวุธ (Arms Trafficking)
4. การลักลอบค้าอาวุธ อุปกรณ์นิวเคลียร์ (Trafficking in Nuclear Material)
5. กลุ่มองค์กรอาชญากรรมข้ามชาติและการก่อการร้าย (Transnational Criminal Organization and Terrorism)
6. การค้าหญิงและเด็ก (Trafficking in Women and Children)
7. การลักลอบค้าชิ้นส่วนมนุษย์ (Trafficking in Body Part)
8. การโจรกรรมและลักลอบค้ายานพาหนะ (Theft and Smuggling of Vehicles)
9. การฟอกเงิน (Money Laundering)
10. การกระทำความผิดอื่นๆ (Other activities) ได้แก่
    1) การโจรกรรมศิลปวัตถุและวัตถุโบราณ
    2) การให้สินบนเจ้าหน้าที่ตำรวจและข้าราชการอื่น ๆ
    3) อาชญากรรมทางคอมพิวเตอร์
    4) อาชญากรรมด้านสิ่งแวดล้อม
    5) อาชญากรรมเกี่ยวกับทรัพย์สินทางปัญญา
    6) การฉ้อโกงประกันภัยทางทะเล
    7) การแทรกซึมเข้าสู่ธุรกิจที่ถูกกฎหมายโดยองค์กรอาชญากรรม

---

[40] Thailand Institute of Justice, 'องค์กรอาชญากรรมข้ามชาติ' (TIJ, 29 มกราคม 2566) <https://www.tijthailand.org/area_of_work/detail/2> สืบค้นเมื่อ 2 กุมภาพันธ์ 2566.

[41] วีระพงษ์ บุญโญภาส, 'ยุโรปกับนโยบายความมั่นคง : อาชญากรรมข้ามชาติทางเศรษฐกิจ' (2543) 8(1) *วารสารยุโรปศึกษา ศูนย์ยุโรปศึกษา จุฬาลงกรณ์มหาวิทยาลัย* 57–58.

ลักษณะทั่วไปองค์กรอาชญากรรมข้ามชาติมักรวมตัวกันจากสายสัมพันธ์บางอย่าง อาทิ เป็นกลุ่มเครือญาติ กลุ่มชาติพันธุ์เดียวกัน และกลุ่มที่พูดภาษาเดียวกัน เป็นต้น 2 โดยกลุ่มมาเฟียต่าง ๆ เหล่านี้จะมีลักษณะร่วมบางอย่างที่คล้ายคลึงกัน ได้แก่

1. มีการสมรู้ร่วมคิดเพื่อประกอบธุรกิจผิดกฎหมายหรืออาจเป็นธุรกิจถูกกฎหมายแต่ด้วยวิธีการที่ฉ้อฉล

2. มีกฎเหล็กที่สมาชิกต้องปฏิบัติ การละเมิดกฎข้อห้ามต่าง ๆ จะถูกลงโทษอย่างเด็ดขาดรุนแรง ซึ่งอาจรวมถึงการสังหารผู้ทรยศ

3. มีโครงสร้างที่เป็นลำดับชั้นโดยสายบังคับบัญชาจะเป็นตัวกำหนดตำแหน่ง สถานภาพและส่วนแบ่งจากผลกำไร

4. มีเป้าหมายชัดเจนในการแสวงหาผลประโยชน์ทางเศรษฐกิจเป็นหลัก โดยมุ่งผูกขาดธุรกิจผิดกฎหมายที่ตนเองมีความเชี่ยวชาญ ส่วนการแสวงหาอำนาจและสถานภาพในสังคมเป็นเรื่องรองที่อาจตามมาในภายหลัง[42]

5. ใช้ยุทธวิธีต่าง ๆ เพื่อขยายผลจากความโลภหรือความหวาดกลัวของผู้คนโดยข่มขู่ ลักพาตัว ให้สินบน วางเพลิงหรือใช้ความรุนแรงต่าง ๆ เพื่อให้บรรลุเป้าหมาย

6. ทำธุรกิจทั้งผิดกฎหมายและถูกกฎหมายควบคู่กัน เพื่อช่วยสนับสนุนธุรกิจที่ผิดกฎหมายของตน เช่น นำเงินจากการค้ายาเสพติดมาลงทุนในตลาดหลักทรัพย์เพื่อฟอกเงิน เป็นต้น

7. มีการปรับตัวอยู่ตลอดเวลาในเรื่องเทคโนโลยีโลจิสติกส์และอุปกรณ์ที่ใช้ อาทิ การใช้โลกออนไลน์เป็นเครื่องมือในการประกอบอาชญากรรมรูปแบบต่าง ๆ (Shaw, 2008)

**2.3.2 รูปแบบของอาชญากรรมข้ามชาติกับการกระทำในลักษณะของแก๊งคอลเซ็นเตอร์**

แก๊งคอลเซ็นเตอร์สามารถถือได้ว่าเป็นรูปแบบหนึ่งขององค์กรอาชญากรรมที่มีลักษณะเชื่อมโยงกันข้ามพรมแดน โดยปรากฏในลักษณะเป็นเครือข่ายที่มีการจัดตั้งอย่างเป็นระบบ มีการแบ่งหน้าที่กันทำอย่างชัดเจนโดยมีโครงสร้างคล้ายองค์กรธุรกิจเถื่อนที่มีระบบเงินเดือนและส่วนแบ่งผลกำไรจากการหลอกลวงประชาชน ผู้กระทำความผิดจำนวนมากมักปลอมแปลงตัวตนโดยแอบอ้างเป็นเจ้าหน้าที่รัฐหรือองค์กรทางกฎหมายเพื่อให้เหยื่อหลงเชื่อ รูปแบบการกระทำความผิดยังมีการเปลี่ยนแปลงอยู่ตลอดเวลาเพื่อลดความเสี่ยงจากการถูกจับกุมและติดตามตัว โดยความเสียหายที่เกิดขึ้นไม่เพียงแต่ส่งผลกระทบต่อเหยื่อในเชิงเศรษฐกิจโดยตรงเท่านั้น หากแต่ยังส่งผลต่อภาพลักษณ์

---

[42] สักกรินทร์ นิยมศิลป์, ‘อาชญากรรมข้ามชาติ ภัยคุกคามไทยและอาเซียน’ (2565) *วารสารนิติศาสตร์* 238 <https://ipsr.mahidol.ac.th/wp-content/uploads/2022/03/447-IPSR-Conference-A15-fulltext.pdf> สืบค้นเมื่อวันที่ 27 มกราคม 2567.

และความน่าเชื่อถือของประเทศในเวทีระหว่างประเทศอย่างร้ายแรง โดยองค์กรลักษณะนี้สามารถอธิบายได้ ดังนี้

2.3.2.1 การตั้งองค์กร

แก๊งคอลเซ็นเตอร์มีรูปแบบการทำงานกันเป็นกระบวนการซึ่งมีการแบ่งหน้าที่กันอย่างชัดเจนซึ่งมีการจัดรูปแบบในการทำงาน[43] ดังนี้

1. กลุ่มคอลเซ็นเตอร์ การตั้งศูนย์โทรศัพท์หรือ Call Center มักจะตั้งอยู่ในต่างประเทศเพื่อความสะดวกในการควบคุมพนักงานโทรศัพท์ไม่ให้หลบหนีหรือเปิดเผยความลับ นอกจากนี้ หลักทางจิตวิทยาสำหรับการพูดโทรศัพท์ยังช่วยให้พนักงานสามารถพูดคุยและแสดงบทบาทของตนเองได้อย่างเต็มที่โดยไม่ต้องเกรงกลัวว่าจะถูกเจ้าหน้าที่ตำรวจเข้าจับกุม เนื่องจากอยู่ในต่างประเทศ ซึ่งศูนย์โทรศัพท์จะติดตั้งอินเตอร์เน็ตความเร็วสูงเพื่อใช้ระบบโทรศัพท์ผ่านทางอินเตอร์เน็ตหรือ VOIP (Voice Over Internet Protocol)[44] ทำให้ประหยัดค่าใช้จ่าย, การติดตามค่อนข้างยาก, สัญญาณเสียงชัดเจน โดยจะมีชาวไต้หวันหรือชาวจีนเป็นผู้มีความชำนาญในการควบคุมระบบและการโทรศัพท์หาผู้เสียหายจะใช้โปรแกรมในการสุ่มไปเรื่อย ๆ ส่วนหมายเลขที่ปรากฏปลายทาง(มือถือของผู้เสียหาย)จะใช้โปรแกรมในการตั้งหมายเลขให้ปรากฏเป็นหน่วยงานราชการตามที่อ้างถึงหรือเรียกว่า Fake Numberเช่น ปปง., DSI, หน่วยงานของตำรวจที่เกี่ยวข้องต่าง ๆ เพื่อสร้างความน่าเชื่อถือว่าเป็นโทรศัพท์จากหน่วยงานนั้น ๆ[45]

2. กลุ่มบัญชีม้าจะมีหน้าที่ประสานงานระหว่างศูนย์โทรศัพท์ (Call Center) ว่ามีเงินสดที่ทำการหลอกลวงได้โอนเข้าบัญชีธนาคารหมายเลขใด (บัตรเอทีเอ็มใด) และรีบแจ้งให้ม้าถอนเงินรีบไปทำการถอนเงินสดจากตู้ถอนเงินสดอัตโนมัติทันที เพื่อป้องกันการอายัดบัญชีธนาคารจากผู้เสียหาย

3. กลุ่มจัดหาบัญชีธนาคารหรือบัตรอิเล็กทรอนิกส์ กลุ่มจัดหาบัญชีธนาคารหรือบัตรอิเล็กทรอนิกส์ (บัตรเอทีเอ็ม) จะมีหน้าที่ในการไปรวบรวมบัญชีและบัตรเอทีเอ็มเพื่อส่งให้กับกลุ่มม้าถอนเงินและแจ้งรายละเอียดเจ้าของบัญชี, หมายเลขบัญชี, หมายเลขบัตรเอทีเอ็มให้กับผู้ควบคุมม้า

---

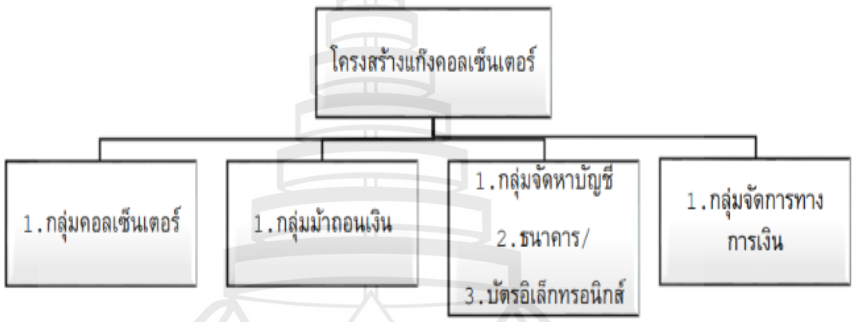
[43] พัลลภ หริ่งรอด, มาตรการตามกฎหมายในการปราบปรามองค์กรอาชญากรรมข้ามชาติ ศึกษาเฉพาะกลุ่มคอลเซ็นเตอร์ (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขากฎหมายอาญาและอาชญาวิทยา มหาวิทยาลัยบูรพา 2562).

[44] Voice Over Internet Protoc เป็นการสื่อสารผ่านเสียงซึ่งมีความล้ำกว่าการโทรศัพท์แบบแต่ก่อน เพราะเทคโนโลยีของโทรศัพท์คือการสื่อสารด้วยเสียงผ่านเสาสื่อสารจากผู้ส่งสารไปยังผู้รับสาร ส่วน VoIP นั้น เป็นการสื่อสารผ่านสาย LAN หรือเชื่อมข้อมูลระหว่าผู้ส่งและผู้รับที่อยู่บนเครือข่าย

[45] สำนักงานกฎหมายทรีลอเยอร์, ‘โพสต์ | Facebook’< https://www.facebook.com/1613823358894164/posts/1647293065547193/> สืบค้นเมื่อ 27 มกราคม 2567.

ถอนเงินและศูนย์โทรศัพท์ (Call Center) โดยการจ้างประชาชนทั่วไปให้เปิดบัญชีธนาคารประเภทสะสมทรัพย์พร้อมขอใช้บัตรอิเล็กทรอนิกส์หรือบัตรเอทีเอ็ม[46]

4. กลุ่มจัดการทางการเงิน ผู้ทำหน้าที่ดังกล่าวจะมีหน้าที่ในการรวบรวมเงินสดจากม้าถอนเงินที่ทำการถอนเงินสดจากตู้ถอนเงินสดอัตโนมัติที่ทำการหลอกลวงมาได้ส่งเงินให้กับเจ้าของหรือระดับหัวหน้าต่อไป ซึ่งหากพบหลักฐานเชื่อมโยงไปถึงก็จะต้องถูกดำเนินคดีในความผิดฐานร่วมกันฉ้อโกงประชาชนเช่นเดียวกัน




**ภาพที่ 2.1** โครงสร้างแก๊งคอลเซ็นเตอร์[47]

2.3.2.2 รูปแบบการหลอกลวง

ลักษณะการหลอกลวงของแก๊งคอลเซ็นเตอร์นั้นจะกระทำต่อผู้เสียหายหรือเหยื่อใน 2 ลักษณะ[48] ที่สำคัญ คือ การอาศัยความโลภของเหยื่อซึ่งโดยทั่วไปแล้วอาชญากรจะหลอกลวงผู้เสียหายเพื่อให้ผู้เสียกายนั้นเกิดความโลภ เช่น เหยื่อได้รับคืนภาษีหรือถูกรางวัลชิงโชคต่าง ๆ เป็นต้น แต่เพื่อการดำเนินการเหยื่อจะต้องจ่ายค่าบริการเบื้องต้น เป็นค่าบริการและค่าธรรมเนียมต่าง ๆ เมื่อผู้เสียหายหลงเชื่อเพราะความโลภอยากได้เงินหรือทรัพย์สินจะโอนเงินเข้าบัญชีธนาคารของคนร้ายที่ได้เตรียมเปิดรองรับไว้และการอาศัยความกลัวของเหยื่อเป็นการหลอกลวงซึ่งเป็นรูปแบบที่จะหลอกลวงผู้เสียหายว่าเป็นหนี้ค่าบริการสาธารณะต่าง ๆ เช่น ค่าโทรศัพท์ เป็นหนี้บัตร

---

[46] ธนาคารแห่งประเทศไทย, ‘กลโกงบัตรต่าง ๆ’ <https://www.bot.or.th/th/satang-story/fraud/card-fraud.html> สืบค้นเมื่อ 27 มกราคม 2567.

[47] จักรพงษ์ กังวานโสภณ, ‘ความผิดฐานฉ้อโกง: ศึกษากรณีการหลอกลวงทางโทรศัพท์ (แก๊งคอลเซ็นเตอร์)’ (2565) 14(2) วารสารวิจัยและพัฒนา มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา <https://so06.tci-thaijo.org/index.php/rdibsru/article/view/255877> สืบค้นเมื่อ 18 พฤษภาคม 2568.

[48] Research Cafe, ‘อาชญากรรมแก๊งคอลเซ็นเตอร์’ <https://researchcafe.tsri.or.th/call-center-crime/> สืบค้นเมื่อ 1 กุมภาพันธ์ 2567.

เครดิต หรือมีบัญชีธนาคารพัวพันกับการค้ายาเสพติด ซึ่งบัญชีธนาคารของเหยื่อจะต้องถูกอายัดและถูกตรวจสอบโดยสำนักงาน ปปง. เมื่อผู้เสียหายหลงเชื่อจะทำธุรกรรมทางการเงินตามที่กลุ่มคนร้ายแนะนำ เช่น นำบัตรถอนเงินอัตโนมัติหรือบัตรเอทีเอ็มไปทำรายการที่ตู้ถอนเงินอัตโนมัติ เมื่อถอนเงินสดจากบัญชีธนาคารแล้วก็จะนำไปฝากเข้าบัญชีธนาคารที่หน้าเคาน์เตอร์หรือฝากผ่านตู้รับฝากเงินอัตโนมัติ (CDM) เพื่อเข้าบัญชีธนาคารที่กลุ่มคนร้ายเปิดรองรับไว้

เนื่องจากรูปแบบการหลอกลวงในลักษณะของแก๊งคอลเซ็นเตอร์ที่อาศัยความก้าวหน้าทางเทคโนโลยี แก๊งคอลเซ็นเตอร์จึงมีรูปแบบการหลอกลวงที่ปรับเปลี่ยนอยู่ตลอดเวลาตามแต่สถานการณ์โดยในปัจจุบันแก๊งคอลเซ็นเตอร์ได้มีการใช้การฟิชชิ่ง (Phishing )[49]เข้ามาเป็นเครื่องมือในการหลอกล่อเหยื่อ ซึ่งการหลอกลวงแบบฟิชชิ่งของแก๊งคอลเซ็นเตอร์นี้ยังมีรูปแบบที่แตกต่างกันออกไป ซึ่งจากการศึกษาพบว่า ในปัจจุบันมีรูปแบบการกระทำความผิดของอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์มีทั้งหมด 8 รูปแบบ ได้แก่

1. Phishing emails เป็นการส่งอีเมลหลอกลวงต่าง ๆ โดยอาจจะใช้ความสัมพันธ์ของบุคคล สถาบันการเงินหรือตำแหน่ง มักจะใช้เพื่อขโมยข้อมูลผู้ใช้รวมถึงข้อมูลการเข้าสู่ระบบและหมายเลขบัตรเครดิตจะเกิดขึ้นเมื่อผู้โจมตีปลอมตัวเป็นหน่วยงานที่เชื่อถือได้จากนั้นผู้รับจะถูกหลอกให้คลิกลิงก์ที่เป็นอันตรายซึ่งอาจนำไปสู่การติดตั้งมัลแวร์ การค้างของระบบซึ่งเป็นส่วนหนึ่งของการโจมตีแรนซัมแวร์หรือการเปิดเผยข้อมูลที่ละเอียดอ่อน[50]

2. Spear Phishing การพยายามล้วงข้อมูลสำคัญหรือเข้าถึงระบบคอมพิวเตอร์ โดยส่งข้อความปลอมที่ดูเหมือนจริง โจมตีแบบสเปียร์ฟิชชิ่งต่างจากฟิชชิ่งทั่วไป ตรงที่มันมุ่งเป้าไปที่บุคคลหรือกลุ่มบุคคลที่เฉพาะเจาะจง มักจะมีข้อมูลที่เกี่ยวข้องกับเป้าหมายนั้นผสมอยู่ ไม่ว่าจะเป็นข่าวสารปัจจุบัน เอกสารการเงิน หรือข้อมูลส่วนตัว

3. Whaling Phishing เป็นการโจมตีที่มีกลุ่มเป้าหมายเฉพาะเจาะจงที่เป็นบุคคลสำคัญ โดยมีลักษณะคล้ายกับ Spear Phishing แต่มีรูปแบบที่ซับซ้อนมากกว่าเป้าหมายของ Whaling จะเล็งไปที่บุคคลเพียงคนเดียวและมักจะเป็นบุคคลที่มีตำแหน่งงานอยู่ในระดับสูง เช่น

---

[49] phishing คือรูปแบบของการหลอกลวงผ่านช่องทางการใช้งานอินเทอร์เน็ตของผู้ใช้ทั่วไป ซึ่งไม่ใช่การล่อลวงธรรมดาแบบทั่วไป แต่จะเป็นกลยุทธ์การหลอกที่ใช้วิธีทางจิตวิทยาเข้าร่วมด้วย ส่วนใหญ่แล้วจะมาในรูปแบบของอีเมล์ เว็บไซต์ และสื่อสังคมออนไลน์ในรูปแบบต่าง ๆ ที่จะทำการหลอกให้ผู้ใช้กรอกข้อมูลส่วนบุคคลที่เป็นความลับ ไม่ว่าจะเป็นรหัสผ่าน หมายเลขบัตรประชาชน เลขที่ Passport รวมไปถึงข้อมูลลับทางการเงิน ทั้งเลขที่บัญชีและรหัสผ่าน หรือจะเป็นการหลอกให้กดยอมรับและติดตั้งไวรัสตัวร้ายเข้าสู่คอมพิวเตอร์

[50] What is phishing | Attack techniques & scam examples | Imperva' (Imperva) <https://www.imperva.com/learn/application-security/phishing-attack-scam/> accessed 17 February 2024.

ผู้จัดการ หรือซีอีโอ เป็นต้น โดยการโจมตีทางไซเบอร์เหล่านี้สามารถหลอกเหยื่อได้ เนื่องจากผู้โจมตีเต็มใจที่จะใช้เวลาและความพยายามมากขึ้นในการสร้างพวกมันเนื่องจากอาจได้รับผลตอบแทนสูงผู้โจมตีมักจะใช้โซเชียลมีเดีย เช่น Facebook, Twitter และ LinkedIn เพื่อรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเหยื่อ

4. Vishing Phishing เป็นการหลอกลวงข้อมูลผ่านเสียง โดยแฮกเกอร์จะใช้วิธีการปลอมตัวแล้วโทรศัพท์เข้ามาเพื่อขอข้อมูลส่วนบุคคลไป เช่น อาจจะโทรมาแล้วแอบอ้างว่าเป็นเจ้าหน้าที่ธนาคารแล้วขอเลขบัตรเครดิตหรือเลขบัตรประชาชน[51]

5. Smishing Phishing เป็นการหลอกลวงผ่านทางข้อความสั้น SMS โดยผู้ส่งจะพยายามโน้มน้าวให้ผู้อ่านคลิกเปิดลิงก์ที่แนบมากับข้อความ SMS เพื่อเข้าสู่หน้าเว็บไซต์ปลอมที่ถูกสร้างเตรียมไว้ ซึ่งในเว็บดังกล่าวก็จะมีช่องให้กรอกข้อมูลส่วนตัวที่สำคัญ เป้าหมายของการหลอกลวงคือการหลอกล่อบุคคลที่ไม่สงสัยให้เปิดเผยข้อมูลส่วนบุคคลหรือทำสิ่งที่ทำให้ความปลอดภัยตกอยู่ในความเสี่ยง โดยมีวิธีการคือแฮกเกอร์จะส่งข้อความที่ดูเหมือนว่ามาจากแหล่งที่เชื่อถือได้

6. Angler Phishing เป็นการหลอกลวงโดยการสังเกตพฤติกรรมทางโซเชียล โดยแฮกเกอร์จะเฝ้าจับตาดูพฤติกรรมการใช้งานบน Social media ของเหยื่อ แล้วสวมรอยเป็นเจ้าหน้าที่มาหลอกลวงเหยื่อให้หลงเชื่อ

7. CEO Fraud Phishing เป็นการหลอกลวงโดยใช้บุคคลสำคัญเป็นตัวล่อซึ่งเทคนิคการหลอกลวงในรูปแบบนี้มีความคล้ายคลึงกับเทคนิค Whaling Phishing โดยเป้าหมายของแฮกเกอร์ คือ ซีอีโอ หรือคนที่อยู่ในระดับผู้บริหารที่เป็นบุคคลสำคัญขององค์กรแต่วิธีการโจมตีนั้นจะรุนแรงกว่ามาก หลักการสำคัญคือจะใช้บุคคลสำคัญเป็นตัวล่อให้ผู้อื่นหลงเชื่อเพื่อกระทำการอย่างใดอย่างหนึ่ง

8. Search Engine Phishing เป็นการหลอกลวงที่สร้างความน่าเชื่อถือจากเครื่องมือค้นหาโดยที่จะวางเหยื่อล่อเป้าหมายผ่านผลลัพธ์การค้นหาของเครื่องมือค้นหา ( Search Engine) หรือบริการค้นหาเว็บไซต์ ได้แก่ google เป็นต้น การโจมตีรูปแบบนี้แฮกเกอร์จะสร้างเว็บไซต์ที่ยื่นข้อเสนอส่วนลด, บริการ, แจกของฟรี หรือแม้แต่ประกาศรับสมัครงาน จากนั้นก็อาศัยเทคนิคการปรับแต่งเครื่องมือค้นหา หรือที่เรียกว่า "SEO (Search Engine Optimization)" ในการทำให้เว็บปลอมที่สร้างขึ้นมาติดอยู่ในผลลัพธ์การค้นหาที่สูงเพื่อทำให้เหยื่อหลงเชื่อก่อนจะเข้าไปกรอกข้อมูลสำคัญ[52]

---

[51] ยุวมิตร, ‘Phishing คืออะไร ป้องกันอย่างไร’ (ThaiCERT, 15 สิงหาคม 2566) <https://www.thaicert.or.th/phishing-awareness.html> สืบค้นเมื่อ 8 กรกฎาคม 2567.

[52] เพิ่งอ้าง.

**2.3.3 รูปแบบการกระทำความผิดของแก๊งคอลเซ็นเตอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้**

การกระทำความผิดของแก๊งคอลเซ็นเตอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้มีลักษณะเป็นอาชญากรรมข้ามชาติที่มีการจัดโครงสร้างองค์กรเป็นระบบมีการแบ่งหน้าที่อย่างชัดเจน และใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือหลักในการก่ออาชญากรรม โดยทั่วไปแล้วรูปแบบการกระทำความผิดดังกล่าวสามารถจำแนกได้เป็นลำดับขั้นตอน โดยแก๊งคอลเซ็นเตอร์มักเลือกตั้งศูนย์ปฏิบัติการในประเทศที่มีการบังคับใช้กฎหมายที่อ่อนแอหรือมีช่องว่างทางกฎหมาย รวมถึงพื้นที่ชายแดนหรือพื้นที่ที่มีการควบคุมของรัฐน้อย เช่น พื้นที่บางส่วนในเมียนมา ลาว หรือกัมพูชา โดยมีวัตถุประสงค์เพื่อหลีกเลี่ยงการตรวจสอบจากหน่วยงานบังคับใช้กฎหมายของประเทศต้นทางของเหยื่อ โครงสร้างแก๊งคอลเซ็นเตอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้จะมีการแบ่งสายงานและควบคุมโดยผู้มีอิทธิพลจากต่างประเทศอย่าง ไต้หวันหรือจีน ซึ่งเป็นตัวการในการวางแผนส่งเทคโนโลยี และกำกับการดำเนินงานในประเทศต่าง ๆ[53]

แก๊งคอลเซ็นเตอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้มีการปรับเปลี่ยนและพัฒนารูปแบบการหลอกลวงอย่างต่อเนื่อง โดยอาศัยทั้งเทคโนโลยีและกลยุทธ์ทางจิตวิทยา เพื่อเจาะกลุ่มเป้าหมายที่มีความเปราะบางในหลายประเทศซึ่งสามารถจำแนกได้ ดังนี้

1. การแอบอ้างเป็นเจ้าหน้าที่รัฐ เป็นรูปแบบที่พบมากที่สุด โดยกลุ่มผู้กระทำผิดจะโทรศัพท์หาเหยื่อ โดยอ้างตนเป็นเจ้าหน้าที่ตำรวจ อัยการ เจ้าหน้าที่ธนาคาร หรือเจ้าหน้าที่จากหน่วยงานของรัฐ เช่น กรมสรรพากร สำนักงานตรวจคนเข้าเมือง หรือศาล เพื่อข่มขู่ว่าเหยื่อมีส่วนเกี่ยวข้องกับอาชญากรรม เช่น ค้ายาเสพติด ฟอกเงิน หรือหลีกเลี่ยงภาษี จากนั้นจะเสนอทางเลือกให้เหยื่อนำเงินมาชำระหรือโอนเงินเพื่อตรวจสอบความบริสุทธิ์ เหยื่อส่วนใหญ่มักตื่นตระหนกและหลงเชื่อในความเป็นทางการของผู้หลอกลวง จึงยอมโอนเงินจำนวนมากไปยังบัญชีปลอมของแก๊งอาชญากรรม[54]

2. การหลอกลวงเพื่อชักชวนลงทุน แก๊งคอลเซ็นเตอร์จำนวนมากใช้เทคนิคชวนเชื่อในการเสนอโอกาสในการลงทุน โดยใช้เว็บไซต์หรือแอปพลิเคชันปลอมที่เลียนแบบหน้าตาของแพลตฟอร์มการลงทุนจริง เช่น ซื้อขายคริปโทเคอร์เรนซี, หุ้น, ฟอเร็กซ์ หรือโครงการเงินดิจิทัลต่าง ๆ

---

[53] UNODC, Transnational Organized Crime in Southeast Asia: Evolution, Growth and Impact (2019), available at: <https://www.unodc.org/> accessed 5 July 2024.

[54] Justice Channel, “Call Center Gang: เปิดโปงขบวนการหลอกเงินคนไทย สูญหลายพันล้าน,” *Justice Channel*, <https://justicechannel.org/listen/cybercrime/callcentergang> เข้าถึงล่าสุด 18 มกราคม 2567.

เหยื่อจะได้รับผลตอบแทนในช่วงแรกเพื่อสร้างความเชื่อมั่น ก่อนที่เงินจำนวนมากจะถูกถอนออกไปโดยไม่สามารถติดตามได้ รูปแบบนี้แพร่หลายในหมู่เยาวชนและกลุ่มคนรุ่นใหม่ที่สนใจการเงินออนไลน์[55]

3. การหลอกลวงผ่านความสัมพันธ์ อาชญากรจะใช้โซเชียลมีเดียหรือแอปพลิเคชั่นหาคู่เพื่อสร้างความสัมพันธ์กับเหยื่อ โดยปลอมตัวเป็นชาวต่างชาติที่มีสถานะทางสังคมสูง เช่น ทหาร นักธุรกิจ หรือวิศวกรในต่างประเทศ เมื่อเหยื่อตกหลุมรักพวกเขาจะถูกหลอกให้โอนเงินโดยอ้างว่าเพื่อค่าขนส่ง การรักษาพยาบาลหรือเอกสารราชการ เหยื่อจำนวนมากมักไม่ยอมแจ้งความเนื่องจากความรู้สึกอับอายและสูญเสียทางจิตใจ[56]

4. การหลอกลวงเกี่ยวกับการจัดส่งพัสดุ เป็นรูปแบบที่พัฒนาขึ้นจากการขยายตัวของธุรกิจ อีคอมเมิร์ซ โดยอาชญากรจะโทรศัพท์หรือส่งข้อความอ้างว่าเหยื่อมีพัสดุที่ถูกยึดหรือมีสิ่งผิดกฎหมายปะปนอยู่ โดยจะให้เหยื่อยืนยันตัวตนหรือจ่ายค่าธรรมเนียมปลอมผ่านบัญชีที่จัดเตรียมไว้ รูปแบบนี้แพร่หลายเป็นพิเศษในช่วงที่ประชาชนใช้บริการส่งพัสดุจำนวนมาก[57]

5. การหลอกลวงผ่านแอปปลอม อาชญากรมักสร้างแอปพลิเคชันที่ปลอมตัวเป็นบริการเงินกู้, แพลตฟอร์มการเงิน หรือหน่วยงานภาครัฐ เมื่อเหยื่อดาวน์โหลดและให้ข้อมูลส่วนตัว เช่น เลขบัตรประชาชน ข้อมูลบัญชีธนาคาร หรือรหัส OTP แอปเหล่านี้จะนำข้อมูลไปใช้ในการขโมยเงินหรือนำไปขายต่อในตลาดมืด

6. การหลอกลวงเพื่อจัดหางาน แก๊งคอลเซ็นเตอร์ในประเทศชายแดนอย่างเมียนมาร์ ลาว และกัมพูชา ใช้ช่องทางสื่อสังคมออนไลน์ในการล่อลวงเหยื่อจากประเทศเพื่อนบ้าน โดยเฉพาะจากไทย มาเลเซีย และเวียดนาม ให้เดินทางไปทำงานต่างประเทศ พร้อมสัญญาว่าจะมีรายได้ดี แต่เมื่อไปถึงกลับถูกยึดหนังสือเดินทางและบังคับให้ทำงานหลอกลวงผู้อื่นแทน นี่เป็นรูปแบบที่มีการค้ามนุษย์และบังคับใช้แรงงานควบคู่กับการฉ้อโกงออนไลน์[58]

รูปแบบการหลอกลวงของแก๊งคอลเซ็นเตอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้ จึงไม่ได้เป็นเพียงการโทรศัพท์เพื่อหลอกลวงอย่างที่เคยเป็นในอดีต หากแต่ได้พัฒนาเป็นอุตสาหกรรมอาชญากรรมที่มีระบบซับซ้อน และเชื่อมโยงกับเครือข่ายอาชญากรรมข้ามชาติ เทคโนโลยีสารสนเทศ

---

[55] AIS Aunjai Cyber, “รวม 22 กลโกงมิจฉาชีพ ที่ใช้หลอกลวงเหยื่อบนโลกออนไลน์ พร้อมวิธีรับมือ,” *AIS Sustainability*, <https://sustainability.ais.co.th/th/update/aunjai-cyber/795> สืบค้นเมื่อ 18 มกราคม 2567.

[56] เพิ่งอ้าง.

[57] เพิ่งอ้าง.

[63] UNODC, *Transnational Organized Crime in Southeast Asia: Evolution, Growth and Impact* (2019) 27–29.

จึงกลายเป็นเครื่องมือหลักที่ช่วยให้ขยายผลกระทบของอาชญากรรมสู่สังคมในวงกว้างได้อย่างรวดเร็วและรุนแรง

## 2.4 แนวความคิดเกี่ยวกับอาชญากรรมข้ามชาติที่เป็นภัยต่อความมั่นคงกรณีแก๊งคอลเซ็นเตอร์

### 2.4.1 แนวความคิดที่เกี่ยวกับสาเหตุในการกระทำความผิดของแก๊งคอลเซ็นเตอร์

แนวความคิดในการศึกษาและทำความเข้าใจสาเหตุในการกระทำความผิดของแก๊งคอลเซ็นเตอร์สามารถมองได้จากหลายมุมมอง ในปัจจุบันมี 2 แนวความคิดสำคัญที่ได้อธิบายถึงสาเหตุของอาชญากรรมข้ามชาติ ดังนี้

2.4.1.1 แนวความคิดทางเศรษฐศาสตร์ของอาชญากรรม

แนวความคิดทางเศรษฐศาสตร์ของอาชญากรรมได้พัฒนาขึ้นโดยนักเศรษฐศาสตร์ชาวอเมริกัน Gary S. Becker ซึ่งได้รับรางวัลโนเบลสาขาเศรษฐศาสตร์ โดยเขาเสนอว่าการตัดสินใจกระทำความผิดของบุคคลมิใช่เพียงผลของแรงผลักดันภายในหรือสภาพแวดล้อมทางสังคมเท่านั้น หากแต่เป็นผลของการตัดสินใจที่มีเหตุมีผลซึ่งอิงกับการคำนวณต้นทุนและผลประโยชน์ทางเศรษฐกิจที่อาจได้รับจากการกระทำความผิดนั้น ๆ ทั้งนี้ Becker ระบุว่า[59] บุคคลจะเลือกกระทำความผิดเมื่อประโยชน์ที่เขาคาดว่าจะได้รับมีค่ามากกว่าความเสียหายที่อาจเกิดขึ้นจากการถูกลงโทษในทางกฎหมาย อาชญากรไม่ใช่ผู้กระทำความผิดที่ไร้เหตุผล แต่เป็นผู้ที่ประเมินว่าความเสี่ยงของการถูกจับกุม (ต้นทุนของการถูกลงโทษ) นั้นมีค่าน้อยกว่าผลตอบแทนที่ได้รับจากการกระทำความผิด

แนวคิดนี้ถูกนำมาใช้วิเคราะห์พฤติการณ์ของ แก๊งคอลเซ็นเตอร์ กล่าวคือ กลุ่มอาชญากรเหล่านี้มักดำเนินกิจกรรมในลักษณะเครือข่ายข้ามชาติ โดยมีเป้าหมายในการแสวงหาผลประโยชน์ทางเศรษฐกิจผ่านการหลอกลวงเหยื่อด้วยวิธีการทางเทคโนโลยีโดยไม่มีการปะทะทางกายภาพ และมีโอกาสถูกจับกุมค่อนข้างต่ำเนื่องจากอุปสรรคด้านเขตอำนาจศาลและขาดความร่วมมือระหว่างประเทศ ภายใต้แนวคิดของ Becker พฤติกรรมของแก๊งคอลเซ็นเตอร์จึงสามารถมองว่าเป็นผลลัพธ์ของการ “ลงทุน” ที่มีความคุ้มค่าทางเศรษฐศาสตร์ กล่าวคือ ต้นทุนของการกระทำความผิด ได้แก่ ค่าอุปกรณ์เทคโนโลยี ค่าจ้างผู้ร่วมขบวนการ และความเสี่ยงจากการถูกจับกุม ถือว่าต่ำเมื่อเทียบกับผลตอบแทนจำนวนมากที่อาจได้จากเหยื่อหลายราย และยิ่งในประเทศที่มีกฎหมายอ่อนแอหรือการ

---

[59] Gary S. Becker, *‘Crime and Punishment: An Economic Approach’* (1968) *Journal of Political Economy* 76(2): 169–217.

บังคับใช้ไม่เข้มงวด ยิ่งส่งเสริมให้การลงทุนในอาชญากรรมประเภทนี้ให้ผลตอบแทนสูงและเป็นแรงจูงใจให้มีการขยายตัวขององค์กรอาชญากรรมประเภทนี้ในภูมิภาคเอเชียตะวันออกเฉียงใต้ ดังที่องค์การสหประชาชาติว่าด้วยยาเสพติดและอาชญากรรม[60] (UNODC) ระบุไว้ว่า เครือข่ายอาชญากรรมข้ามชาติในเอเชียตะวันออกเฉียงใต้มีแนวโน้มพัฒนาอย่างซับซ้อนมากขึ้น และหันมาใช้รูปแบบอาชญากรรมผ่านระบบเทคโนโลยีเป็นช่องทางหลักในการแสวงหากำไรเพราะมีต้นทุนต่ำ ความเสี่ยงน้อย และเข้าถึงเหยื่อจำนวนมากได้ในเวลาอันสั้น[2] ซึ่งสอดคล้องกับแนวคิดทางเศรษฐศาสตร์ของอาชญากรรมโดยตรงcจากมุมมองทางเศรษฐศาสตร์ การกระทำของแก๊งคอลเซ็นเตอร์เป็นผลลัพธ์จากการประเมินผลตอบแทนที่สูงและความเสี่ยงที่ต่ำ โดยการใช้เทคโนโลยีและการหลีกเลี่ยงการบังคับใช้กฎหมายทำให้การดำเนินการเหล่านี้มีประสิทธิภาพสูงขึ้น การลดอัตราการกระทำความผิดดังกล่าวจึงจำเป็นต้องมีการปรับปรุงระบบการบังคับใช้กฎหมายและการพัฒนาเครื่องมือทางเศรษฐกิจเพื่อเพิ่มต้นทุนของการกระทำความผิด

2.4.1.2 แนวความคิดอาชญวิทยาสิ่งแวดล้อม

แนวความคิดทางอาชญวิทยาสิ่งแวดล้อมเป็นแนวคิดที่มุ่งเน้นการศึกษาความสัมพันธ์ระหว่างสถานที่ เวลา และโอกาสในการเกิดอาชญากรรม โดยเน้นว่าสภาพแวดล้อมทางกายภาพมีบทบาทสำคัญในการกำหนดพฤติกรรมของผู้กระทำผิด แนวคิดนี้ถือเป็นการเปลี่ยนมุมมองจากการศึกษาลักษณะส่วนบุคคลของอาชญากรไปสู่การวิเคราะห์ปัจจัยภายนอกที่เอื้อต่อการกระทำผิด โดยเฉพาะอย่างยิ่งในแง่ของโอกาสและ สถานที่ โดยนักอาชญาวิทยาที่มีบทบาทสำคัญในการพัฒนาแนวคิดนี้คือ Paul J. Brantingham และ Patricia L. Brantingham ซึ่งได้เสนอทฤษฎีแบบแผนอาชญากรรม (Crime Pattern Theory) โดยมีสาระสำคัญว่า อาชญากรไม่ได้เลือกเหยื่อหรือสถานที่ในการกระทำผิดอย่างสุ่มเสมอไปแต่การตัดสินใจดังกล่าวเกิดขึ้นภายใต้บริบทของกิจวัตรประจำวันของพวกเขา และจากความคุ้นเคยกับโครงสร้างของพื้นที่ ที่พวกเขาใช้ชีวิตประจำวัน เช่น ที่พักอาศัย ที่ทำงาน โรงเรียน หรือเส้นทางเดินทางระหว่างสถานที่ต่างๆ ซึ่งเรียกว่า “nodes” (จุด), “paths” (เส้นทาง), และ “edges” (ขอบเขตของพื้นที่เปราะบางต่ออาชญากรรม)[61] จากแนวคิดนี้ การกระทำความผิดจึงเป็นผลจากการปฏิสัมพันธ์ระหว่างผู้กระทำผิด โอกาสในการก่อเหตุและสิ่งแวดล้อมทาง

---

[60] United Nations Office on Drugs and Crime (UNODC), *Transnational Organized Crime in Southeast Asia: Evolution, Growth and Impact* (2019), available at: https://www.unodc.org/ accessed 25 December 2024.

[61] Patricia L. Brantingham and Paul J. Brantingham, “Nodes, Paths and Edges: Considerations on the Complexity of Crime and the Physical Environment,” *Journal of Environmental Psychology* 13, no. 1 (1993).

กายภาพ กล่าวคือ อาชญากรมีแนวโน้มจะก่อเหตุในสถานที่ที่รู้จักและสามารถประเมินความเสี่ยงได้ เช่น บริเวณที่ไม่มีการเฝ้าระวัง กล้องวงจรปิด หรือการบังคับใช้กฎหมายอย่างเข้มงวด แนวคิดนี้ช่วยให้เข้าใจว่าอาชญากรรมไม่ใช่เพียงพฤติกรรมที่เกิดจากแรงจูงใจภายในของบุคคล แต่เป็นพฤติกรรมที่ตอบสนองต่อสิ่งแวดล้อมที่เอื้อต่อการกระทำความผิดและหลีกเลี่ยงความเสี่ยงต่อการถูกจับกุมหรือลงโทษ[62]

เมื่อนำแนวคิดนี้มาประยุกต์ใช้กับกรณีของแก๊งคอลเซ็นเตอร์ในภูมิภาคอาเซียน จะพบว่าแก๊งคอลเซ็นเตอร์มักเลือก “สถานที่ตั้ง” ของศูนย์ปฏิบัติการในประเทศที่ไม่ใช่ถิ่นพำนักของเหยื่อ เพื่อหลีกเลี่ยงการถูกตรวจสอบและจับกุมโดยตรงจากเจ้าหน้าที่รัฐของประเทศที่เหยื่ออาศัยอยู่ ลักษณะเช่นนี้สะท้อนให้เห็นถึงการใช้ประโยชน์จากพื้นที่เปราะบาง ตามแนวคิดของ Brantingham กล่าวคือ เป็นพื้นที่ที่มีโครงสร้างทางกฎหมายไม่เข้มงวด ขาดการเฝ้าระวัง และไม่มีความร่วมมือระหว่างประเทศในกระบวนการส่งผู้ร้ายข้ามแดน ทำให้กลุ่มอาชญากรรมสามารถปฏิบัติการได้โดยมีความเสี่ยงต่ำ นอกจากนี้เครือข่ายแก๊งคอลเซ็นเตอร์ยังอาศัยความคุ้นเคยกับระบบสังคม กฎหมาย และโครงสร้างพื้นฐานของประเทศที่ตนตั้งฐานเพื่อออกแบบรูปแบบการหลอกลวงที่มีประสิทธิภาพสูงสุด ตัวอย่างเช่น การปลอมเสียงเป็นเจ้าหน้าที่รัฐ การหลอกว่าเหยื่อมีหมายจับ หรือการใช้ระบบโอนเงินผ่านช่องทางที่ตรวจสอบได้ยาก สิ่งเหล่านี้สะท้อนถึงการเลือกพื้นที่กระทำความผิดอย่างเป็นระบบและมีแบบแผน

**2.4.2 แนวความคิดที่เกี่ยวกับการปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์**

กฎบัตรสหประชาชาติได้กำหนดภารกิจสำคัญของรัฐภาคีสมาชิกในด้านการส่งเสริมความสัมพันธ์ระหว่างประเทศไว้ในมาตรา 1 (1) และ (3) โดยเน้นถึงความร่วมมือของรัฐสมาชิกในการรักษาสันติภาพ ความมั่นคงระหว่างประเทศ การส่งเสริมความร่วมมือทางเศรษฐกิจ สังคม และมนุษยธรรม[63] ดังนั้น ซึ่งสะท้อนให้เห็นว่าการดำเนินความสัมพันธ์ระหว่างประเทศบนพื้นฐานของการ

---

[62] Paul J. Brantingham and Patricia L. Brantingham, *Environmental Criminology*, (Beverly Hills: Sage Publications, 1981).

[63] United Nations, “UNITED NATION CHARTER”, Article 1 The Purposes of the United Nations are: 1. To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace;

ร่วมมือกันเพื่อประโยชน์ส่วนรวมของประชาคมโลกนั้น เป็นหลักการสำคัญที่รัฐสมาชิกต้องยึดถือในฐานะภาคีของประชาคมระหว่างประเทศ ภายใต้บริบทของกฎหมายระหว่างประเทศ ย่อมไม่มีรัฐใดสามารถดำรงอยู่โดยลำพังโดยปราศจากการติดต่อสัมพันธ์หรือการร่วมมือกับรัฐอื่น ๆ ได้อย่างมีเสถียรภาพและยั่งยืน โดยเฉพาะอย่างยิ่งในยุคที่ภัยคุกคามมีลักษณะข้ามพรมแดนและมีความซับซ้อนมากขึ้น โดยในปัจจุบันมีแนวความคิดในด้านความร่วมมือระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ที่สำคัญ มีดังนี้

2.4.2.1 แนวคิดว่าด้วยความร่วมมือระหว่างประเทศ (International Co – Operation)

แนวคิดเรื่องความร่วมมือระหว่างประเทศมีรากฐานอยู่บนหลักการสำคัญของความสัมพันธ์ระหว่างรัฐในเวทีระหว่างประเทศที่ตระหนักว่าไม่มีรัฐใดสามารถดำรงตนอยู่อย่างโดดเดี่ยวและมีอำนาจอธิปไตยโดยสมบูรณ์ได้โดยไม่อาศัยความร่วมมือกับรัฐอื่น การดำรงอยู่ร่วมกันอย่างสันติและมั่นคงของประชาคมโลกจำเป็นต้องอาศัยการเอื้อเฟื้อ ช่วยเหลือ และแบ่งปันผลประโยชน์ร่วมกันระหว่างรัฐ ซึ่งเป็นสาระสำคัญที่สะท้อนผ่านแนวคิดของสำนักเสรีนิยมสมัยใหม่ (Neo-Liberalism) ที่เชื่อว่าความร่วมมือสามารถเกิดขึ้นได้ผ่านกระบวนการสร้างบรรทัดฐานร่วมและการประสานนโยบายระหว่างรัฐ ซึ่งเรียกว่า “วิถีปฏิบัติระหว่างประเทศ” (international practice) อันเป็นกระบวนการที่รัฐต่าง ๆ ปรับพฤติกรรมของตนให้สอดคล้องกับรัฐอื่น เพื่อให้เกิดผลลัพธ์ที่เป็นประโยชน์ร่วมกัน ในบริบทของภัยคุกคามร่วมสมัยแนวคิดความร่วมมือระหว่างประเทศได้แสดงให้เห็นถึงความสำคัญอย่างชัดเจน โดยเฉพาะเมื่อรัฐต่าง ๆ เผชิญกับภัยคุกคามที่มีลักษณะคล้ายคลึงกัน ซึ่งยากเกินกว่าที่รัฐใดรัฐหนึ่งจะจัดการได้โดยลำพัง รัฐจึงจำเป็นต้องหันหน้าเข้าหากัน ทั้งในระดับนโยบายและในระดับปฏิบัติการ เพื่อจัดตั้งกลไกความร่วมมือในการป้องกันและขจัดภัยคุกคามดังกล่าวให้เกิดประสิทธิภาพสูงสุด ความร่วมมือดังกล่าวสามารถปรากฏในหลายรูปแบบ ทั้งความตก

---

2.To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace.

3.To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and

4. To be a centre for harmonizing the actions of nations in the attainment of these common ends.

ลงแบบทวิภาคี การจัดตั้งองค์กรระหว่างประเทศและความร่วมมือเชิงปฏิบัติการของหน่วยงานบังคับใช้กฎหมายในระดับภูมิภาคและระดับโลก ทั้งในลักษณะที่เป็นทางการและไม่เป็นทางการ[64]

2.4.2.2 แนวความคิดในการช่วยเหลือระหว่างประเทศในทางอาญา (International Mutual Assistance in Criminal Matters)

อาชญากรรมข้ามชาติที่เกิดจากแก๊งคอลเซ็นเตอร์นั้นเป็นปัญหาที่ไม่สามารถจัดการได้เพียงรัฐเดียว จะต้องได้รับความร่วมมือในการดำเนินการช่วยเหลือในด้านต่างๆ ในการดำเนินคดีอาญาตั้งแต่การสืบสวน สอบสวน การสืบพยานบุคคลและการสอบปากคำบุคคล การจัดหาเอกสารบันทึก และพยานหลักฐาน การปฏิบัติตามคำร้องในการค้น การยึด การสืบหาตัวบุคคล การให้ความช่วยเหลือเกี่ยวกับการดำเนินการริบทรัพย์สิน ตลอดจนถึงการบังคับโทษตามคำพิพากษา หรือมีความหมายครอบคลุมกว้างขวางเกี่ยวกับการดำเนินคดีอาญา ไม่ว่าจะเป็นการส่งผู้ร้ายข้ามแดน (Extradition) การโอนตัวนักโทษ (Transfer of Sentenced Persons) และการให้ความช่วยเหลือซึ่งกันและกันในทางเรื่องอาญามีรูปแบบของการให้ความช่วยเหลือระหว่างประเทศในทางอาญาที่สามารถแบ่งออกได้เป็น 3 ระดับ ได้แก่

1. ความช่วยเหลือซึ่งกันและกันทางอาญาในรูปแบบไม่เป็นทางการ เป็นการให้ความร่วมมือกันในระดับเจ้าหน้าที่รัฐกันเองโดยอาศัยความสัมพันธ์ระหว่างบุคคล ซึ่งการให้ความช่วยเหลือแบบไม่เป็นทางการนี้มักจะเป็นเรื่องเล็กน้อยไม่จำเป็นต้องอาศัยหลักเกณฑ์ในการพิจารณารายละเอียดมากนัก

2. ความช่วยเหลือซึ่งกันและกันทางอาญาในรูปแบบกึ่งทางการจะเป็นการให้ความช่วยเหลือซึ่งกันและกันซึ่งเป็นไปตามความตกลงหรือความตกลงหรือความร่วมมือของหน่วยงานระหว่างประเทศที่มีหน้าที่รับผิดชอบเกี่ยวกับกระบวนการทางอาญาต่าง ๆ

3. ความช่วยเหลือซึ่งกันและกันทางอาญาในรูปแบบอย่างเป็นทางการ สามารถแบ่งออกได้เป็น 2 รูปแบบ ได้แก่

1) ความช่วยเหลือซึ่งกันและกันทางอาญาโดยไม่มีข้อตกลงต่อกันสำหรับหลักต่างตอบแทนหรือหลักถ้อยทีถ้อยปฏิบัติ (Reciprocity) การที่รัฐหนึ่งยอมรับในการบังคับให้ตามคำร้องขอของรัฐอื่นภายใต้เงื่อนไขว่าหากรัฐตนได้ร้องขอให้รัฐอื่นนั้นดำเนินการเช่นเดียวกันแล้ว รัฐนั้นจะยอมปฏิบัติตามเช่นเดียวกัน ซึ่งเป็นข้อผูกมัดตามกฎหมาย (Legal obligation) หลักต่างตอบแทนหรือหลักถ้อยทีถ้อยปฏิบัตินี้ท้าให้รัฐทังสองต่างมีความผูกพันตามกฎหมายระหว่างประเทศมากกว่าหลักไมตรีจิต (Comity) ซึ่งรัฐจะไม่มีข้อผูกมัดทางกฎหมายมาเป็นตัวบังคับ

---

[64] ชิตพล กาญจนกิจ, ‘สหวิทยาการในการจัดการปัญหาอาชญากรรมข้ามชาติ (Interdisciplinary Approach to Fighting Transnational Crime)’ (ฝ่ายสนธิสัญญาและกฎหมาย กองการต่างประเทศ, 2556) 10.

2) ความช่วยเหลือซึ่งกันและกันทางอาญาโดยมีข้อตกลงต่อกัน เช่น อนุสัญญาสหประชาชาติว่าด้วยการต่อต้านองค์กรอาชญากรรมข้ามชาติที่จัดตังในลักษณะองค์กร ค.ศ. 2000 พิธีสารเพื่อป้องกันปราบปรามและลงโทษการค้ามนุษย์โดยเฉพาะผู้หญิงและเด็ก[65]

2.4.2.3 แนวคิดเครือข่ายเชิงนโยบายด้านกระบวนการยุติธรรมทางอาญา (Criminal Justice Policy Network)

แนวคิดนี้ชี้ให้เห็นว่าการป้องกันและปราบปรามอาชญากรรมข้ามชาติไม่อาจประสบความสำเร็จได้โดยการดำเนินการของรัฐใดรัฐหนึ่งหรือองค์กรใดองค์กรหนึ่งเพียงลำพัง เนื่องจากลักษณะของอาชญากรรมประเภทนี้มีความซับซ้อน ข้ามเขตอำนาจศาล และอาศัยความร่วมมือระหว่างกลุ่มอาชญากรในหลายประเทศ จึงทำให้การจัดการกับปัญหาดังกล่าวจำเป็นต้องอาศัยการพึ่งพาและความร่วมมือกันระหว่างรัฐผ่านกลไกที่เป็นระบบ โดยเฉพาะในรูปของเครือข่ายข้อมูลข่าวสารที่สามารถแบ่งปันข้อมูล แลกเปลี่ยนหลักฐาน และสนับสนุนซึ่งกันและกันได้อย่างมีประสิทธิภาพ การจัดตั้งเครือข่ายความร่วมมือเชิงนโยบายระหว่างหน่วยงานในกระบวนการยุติธรรม เช่น ตำรวจ อัยการ ศาล และหน่วยงานที่เกี่ยวข้อง จึงเป็นกลไกสำคัญในการเสริมสร้างขีดความสามารถของรัฐในการป้องกันและตอบโต้ภัยคุกคามจากอาชญากรรมข้ามชาติ โดยเฉพาะในยุคที่ข้อมูลและเทคโนโลยีมีบทบาทอย่างมากต่อการกระทำความผิด ข้อเสนอในการบูรณาการแนวคิดดังกล่าว จึงเป็นการสร้างกรอบความร่วมมือในลักษณะสถาบันที่มีหน้าที่ในการรวบรวม วิเคราะห์และประสานการบังคับใช้กฎหมายในระดับภูมิภาคและระหว่างประเทศ ทั้งนี้ McDonald ได้กล่าวไว้ว่า “การขยายขอบเขตอำนาจของหน่วยงานบังคับใช้กฎหมายของรัฐ และการจัดตั้งสถาบันบังคับใช้กฎหมายระดับภูมิภาคและระหว่างประเทศ เป็นสิ่งจำเป็นในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ” ซึ่งสะท้อนให้เห็นถึงความสำคัญของกลไกเชิงสถาบันที่สามารถทำงานได้อย่างรวดเร็ว มีประสิทธิภาพ และข้ามพรมแดน[66]

ดังนั้นเพื่อให้สามารถจัดการกับปัญหาอาชญากรรมข้ามชาติที่เกิดจากแก๊งคอลเซ็นเตอร์ได้อย่างมีประสิทธิภาพในระดับนานาชาติ รัฐจำเป็นต้องลดข้อจำกัดทางกฎหมายบางประการลงและ

---

[65] วรรณวิภา เมืองถ้ำ, ‘แนวคิด หลักทฤษฎี นิยามกฎหมายอาชญากรรมข้ามชาติ ชุดวิชา 41719 กฎหมายกระบวนการยุติธรรมเกี่ยวกับการควบคุมและปราบปรามอาชญากรรมในประเทศและข้ามชาติที่สำคัญ’ (มหาวิทยาลัยสุโขทัยธรรมาธิราช) <https://www.stou.ac.th/schoolsweb/law/UploadedFile/หน่วยที่1.pdf> สืบค้นเมื่อ 20 กุมภาพันธ์ 2567.

[66] ชิตพล กาญจนกิจ, ‘สหวิทยาการในการจัดการปัญหาอาชญากรรมข้ามชาติ (Interdisciplinary Approach to Fighting Transnational Crime)’ (การประชุมวิชาการระดับชาติคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2566) 48.

ให้ความสำคัญกับความมั่นคงของสังคมโลกในรูปของการจัดทำกฎหมายป้องกันปราบปรามอาชญากรรมข้ามชาติ โดยการนำกรอบความร่วมมือด้านอาชญากรรมข้ามชาติในระดับต่าง ๆ มาปฏิบัติให้เกิดผลอย่างจริงจังและการพัฒนาโครงสร้างการทำงานในระดับปฏิบัติการเพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพ[67]

## 2.5 ทฤษฎีเกี่ยวกับอาชญากรรมข้ามชาติที่เป็นภัยต่อความมั่นคงกรณีแก๊งคอลเซ็นเตอร์

### 2.5.1 ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory)

ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) ได้อธิบายถึงสาเหตุหรือองค์ประกอบของ การเกิดอาชญากรรมประกอบด้วยด้านต่าง ๆ ของสามเหลี่ยม 3 ด้าน[68]

1. ผู้กระทำผิด/คนร้าย (Offender) หมายถึง ผู้ที่มีความต้องการ (Desire) จะก่อเหตุหรือลงมือกระทำความผิดต้องพยายามลดหรือควบคุมจำนวนผู้กระทำความผิดหรือคนร้ายในพื้นที่ที่รับผิดชอบ โดยมุ่งเน้นใช้ทฤษฎีบังคับใช้กฎหมาย (Law Enforcement Theory)

2. เหยื่อ (Victim)/เป้าหมาย (Target) หมายถึง บุคคล สถานที่หรือวัตถุสิ่งของที่ผู้กระทำผิดหรือคนร้ายมุ่งหมายกระทำต่อ หรือเป็นเป้าหมายที่ต้องการ

3. โอกาส (Opportunity) หมายถึง ช่วงเวลา (Time) และสถานที่ (Place) ที่เหมาะสมที่ผู้กระทำผิดหรือคนร้ายมีความสามารถจะลงมือกระทำความผิดหรือก่ออาชญากรรม

เมื่อเหตุการณ์หรือสถานการณ์ครบองค์ประกอบทั้ง 3 ด้าน ดังกล่าวข้างต้นจะทำให้เกิดอาชญากรรมขึ้น ทฤษฎีดังกล่าวได้เสนอแนวคิดในการแก้ไขปัญหาอาชญากรรมหรือการป้องกันไม่ให้เกิดอาชญากรรม โดยต้องพยายามทำอย่างไรก็ตามที่จะให้องค์ประกอบของสามเหลี่ยมอาชญากรรมด้านใดด้านหนึ่งหายไปก็จะทำให้อาชญากรรมไม่เกิดขึ้น โดยมีวิธีการดังนี้

ด้านผู้กระทำผิดหรือคนร้าย (Offender) ต้องพยายามลดหรือควบคุมจำนวนผู้กระทำความผิดหรือคนร้ายในพื้นที่ที่รับผิดชอบ โดยมุ่งเน้นใช้ทฤษฎีบังคับใช้กฎหมาย (Law Enforcement Theory)

---

[67] เขตต์เทพหัสดิน ณ อยุธยา, การจัดตั้งองค์การตำรวจอาเซียน: ศึกษาเปรียบเทียบองค์การตำรวจสากล และสำนักงานตำรวจยุโรป (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยแม่ฟ้าหลวง, 2561) 11–12.

[68] สภ.โพธิ์กลาง อ.เมือง จว. นครราชสีมา, ‘การป้องกันอาชญากรรมเชิงรุก โดย ทฤษฎีสามเหลี่ยมอาชญากรรม’ (Phoklang Police Blogspot, 10 ตุลาคม 2016) <https://phoklangpolice.blogspot.com/2016/10/blog-post.html> สืบค้นเมื่อ 10 กุมภาพันธ์ 2024.

ด้านเหยื่อ (Victim)/เป้าหมาย (Target) ประชาชนจะต้องรู้จักการป้องกันตนเอง โดยที่มีการประชาสัมพันธ์ให้ความรู้ ข้อมูลข่าวสาร ที่เป็นประโยชน์ต่อประชาชนในการป้องกันอาชญากรรม หรือไม่ให้ตกเป็นเหยื่ออาชญากรรม

ด้านโอกาส (Opportunity) โอกาสที่ผู้กระทำผิดหรือคนร้ายจะกระทำผิดในรูปแบบของแก๊งคอลเซ็นเตอร์ในการหลอกลวงเหยื่อจะต้องอาศัยเวลาและการสร้างสถานการณ์เพื่อหลอกเหยื่อจึงจำเป็นต้องตัดโอกาสด้านเวลาด้วยการประชาสัมพันธ์ให้เหยื่อไม่หลงเชื่อต่อการหลอกลวงของแก๊งคอลเซ็นเตอร์[69]

การป้องกันอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์จะต้องทำให้องค์ประกอบของการเกิดอาชญากรรมด้านใดด้านหนึ่งของสามเหลี่ยมหายไปตามหลักการของทฤษฎีสามเหลี่ยมอาชญากรรมที่กล่าวมาแล้วข้างต้น ดังนั้นจึงเห็นควรที่จะนำแนวคิดการป้องกันอาชญากรรมเชิงรุกโดยการนำทฤษฎีสามเหลี่ยมอาชญากรรมมาปรับใช้เพื่อให้การปฏิบัติหน้าที่แก้ไขปัญหาอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์นี้ได้อย่างบรรลุเป้าหมายและเกิดประโยชน์สูงสุด

**2.5.2 ทฤษฎีกิจวัตประจำวัน (Routine Activity Theory)**

ทฤษฎีนี้วางอยู่บนพื้นฐานแนวคิดที่สอดคล้องกับทฤษฎีการเลือกอย่างมีเหตุผลโดยมีความเชื่อว่าการเพิ่มคนดูแล (Guardian) จะสามารถลดเป้าประสงค์หรือเป้าหมายในการก่ออาชญากรรมได้ในขณะเดียวกันจะลดสถิติของผู้กระทำความผิดลงด้วยและในทางกลับกัน ถ้าลดจำนวนคนดูแล สถิติอาชญากรรมก็จะสูงขึ้น เนื่องจากทฤษฎีกิจวัตรประจำวันนั้นมองว่า อาชญากรสามารถเลือกวางแผนในการประกอบอาชญากรรมได้โดยผ่านการสังเกตจากกิจกรรมประจำวันของผู้ที่เป็นเป้าหมายในการกระทำความผิดและเมื่อได้ทำการชั่งน้ำหนักโดยการเลือกอย่างมีเหตุผลแล้วว่ามีความเสี่ยงที่จะเกิดความเสียหายแก่ตนเองได้น้อยจึงตัดสินใจกระทำความผิดต่อไป ถูกเสนอครั้งแรกโดย Marcus Felson และ Lawrence E. Cohen (1979) ได้อธิบายการเปลี่ยนแปลงของอัตราการเกิดอาชญากรรมในสหรัฐอเมริการะหว่างปี 1947 และ 1974 ซึ่งทฤษฎีนี้ถูกนำไปใช้อย่างกว้างขวาง ทฤษฎีนี้ได้ศึกษาถึงความสัมพันธ์อย่างใกล้ชิดระหว่างอาชญากรรมกับสิ่งแวดล้อมและเน้นกระบวนการทางนิเวศวิทยา สถิติอาชญากรรมเป็นผลผลิตของโอกาสอาชญากรรม จึงเสนอแนวคิดว่าถ้ามีการดูแลมากขึ้นจะสามารถลดเป้าหมายของการเกิดอาชญากรรมได้และในขณะเดียวกันสถิติของผู้กระทำความผิดก็จะลดลงด้วย[70]

---

[69] สุมนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และ นัทธี จิตสว่าง, อาชญากรรมข้ามชาติ: ภัยคุกคามประเทศไทยเกี่ยวกับแก๊งคอลเซ็นเตอร์ (รายงานวิจัย, 2563), 31.

[70] อัณณพ ชูบำรุง, ทฤษฎีอาชญาวิทยา (กรุงเทพฯ: สำนักพิมพ์โอเดียนสโตร์, 2527).

ทฤษฎีนี้จะเน้นการอธิบายสาเหตุของการก่ออาชญากรรมผ่านมุมมองของกิจวัตประจำวันของคนทั่วไป โดยเสนอว่าอาชญากรรมเกิดขึ้นเมื่อมี 3 ปัจจัยหลักมาพบกัน คือ ผู้กระทำผิดที่ได้รับแรงจูงใจ (Motivated Offender) เป้าหมายที่เหมาะสม (Suitable Target) และการขาดผู้ป้องกันที่มีประสิทธิภาพ (Lack of Capable Guardianship) ซึ่งถ้ามานำวิเคราะห์ในกรณีของแก๊งคอลเซ็นเตอร์อาจกล่าวได้ว่า

1. ผู้กระทำผิดที่ได้รับแรงจูงใจ แก๊งคอลเซ็นเตอร์มักประกอบด้วยบุคคลที่มีแรงจูงใจในการกระทำผิดในระดับสูง ไม่ว่าจะเป็นแรงกดดันทางเศรษฐกิจ ความโลภ หรือแม้แต่แรงกดดันจากเครือข่ายอาชญากรรมข้ามชาติที่มีการจัดองค์กรอย่างเป็นระบบ พวกเขามองเห็นการหลอกลวงทางโทรศัพท์และอินเทอร์เน็ตเป็นช่องทางในการแสวงหาผลประโยชน์ที่รวดเร็วและมีความเสี่ยงต่อการถูกจับกุมน้อยกว่าการกระทำความผิดในรูปแบบอื่น

2. เป้าหมายที่เหมาะสม เป้าหมายของแก๊งคอลเซ็นเตอร์มักเป็นบุคคลที่มีลักษณะเปราะบางหรือมีแนวโน้มที่จะตกเป็นเหยื่อสูง เช่น ผู้สูงอายุ ผู้ที่มีพื้นฐานความรู้ด้านเทคโนโลยีต่ำ หรือบุคคลที่อยู่ในภาวะความเครียดทางการเงิน โดยเหยื่อส่วนใหญ่มักถูกจูงใจผ่านกลไกทางอารมณ์ เช่น ความโลภจากการอ้างว่าถูกรางวัลหรือความกลัวจากการอ้างว่าเป็นเจ้าหน้าที่รัฐหรือมีความผิดทางกฎหมาย ทั้งนี้ กลุ่มเหยื่อมักดำรงชีวิตในรูปแบบที่ขาดการป้องกันตนเองหรือไม่มีเครื่องมือทางเทคโนโลยีที่สามารถช่วยตรวจจับภัยคุกคามดังกล่าวได้

3. การขาดผู้ป้องกันที่มีประสิทธิภาพ การขาดกลไกป้องกันที่มีประสิทธิภาพทั้งในเชิงสถาบันและในระดับสาธารณะ ยิ่งทำให้แก๊งคอลเซ็นเตอร์สามารถดำเนินการได้โดยไม่มีการต่อต้านอย่างเพียงพอ ซึ่งรวมถึงการขาดแคลนเจ้าหน้าที่บังคับใช้กฎหมายที่มีความเชี่ยวชาญด้านอาชญากรรม ไซเบอร์ การไม่มีระบบแจ้งเตือนภัยในระดับชุมชน รวมถึงการที่ประชาชนยังขาดความรู้ในการแยกแยะภัยคุกคามจากการหลอกลวงออนไลน์ นอกจากนี้ ประเทศในภูมิภาคอาเซียนหลายแห่งยังมีความเหลื่อมล้ำด้านเทคโนโลยีและขีดความสามารถในการบังคับใช้กฎหมาย ซึ่งยิ่งเปิดช่องให้แก๊งคอลเซ็นเตอร์สามารถดำเนินการได้ข้ามพรมแดนอย่างไร้ข้อจำกัด

โดยสรุปแล้วผู้ที่ต้องตกเป็นเหยื่อของแก๊งคอลเซ็นเตอร์ข้ามชาติอาจเกิดจากกิจวัตรประจำวันในการดำรงชีวิตของเหยื่ออาชญากรรมที่เป็นตัวกระตุ้นให้เกิดอาชญากรรม โดยมีพฤติกรรมที่อาจขาดความสามารถในการดูแลทรัพย์สิน เนื่องจากถูกแก๊งคอลเซ็นเตอร์หลอกลวงทำให้หลงเชื่อและต้องตกเป็นเหยื่ออาชญากรรม รวมทั้งผู้ที่ต้องตกเป็นเหยื่อของแก๊งคอลเซ็นเตอร์อาจเนื่องจากมีความโลภหรือความกลัว เนื่องจากแก๊งคอลเซ็นเตอร์ได้หลอกลวงเหยื่อและแก๊งคอลเซ็นเตอร์ที่มีการกระทำผิด

เนื่องจากเห็นว่าค่าตอบแทนจำนวนมากจากการกระทำผิดมีเป้าหมายที่เหยื่อซึ่งมีกิจวัตรประจำวันที่อาจขาดการดูแลปกป้องทรัพย์ที่เหมาะสม[71]

**2.5.3 ทฤษฎีคิดก่อนกระทำ (Rational Choice Theory)**

ทฤษฎีนี้เชื่อว่าบุคคลมีอิสระในการเลือกกระทำผิดกฎหมาย โดยการเลือกพฤติกรรมผิดกฎหมายขึ้นอยู่กับความพึงพอใจหรือผลประโยชน์ที่ต้องการ ซึ่งไม่จำกัดเฉพาะในรูปของทรัพย์สินเท่านั้น แต่ยังรวมถึงผลประโยชน์หรือความพึงพอใจด้านจิตใจด้วย ประเด็นสำคัญคือบุคคลได้คิดคำนึงถึงผลที่จะตามมาหลังจากการกระทำอาชญากรรม ไม่ว่าจะเป็นผลประโยชน์ที่ได้รับความเป็นไปได้ที่จะถูกจับกุม อัตราโทษที่ได้รับหากถูกจับกุม ตลอดจนหนทางเลือกอื่นที่ถูกกฎหมาย นอกจากนี้ทฤษฎีนี้ยังมองว่าอาชญากรรมมีคุณสมบัติ 2 ประการ[72]คือ

คุณสมบัติของการประกอบอาชญากรรม ซึ่งอาชญากรจะมีพฤติกรรมแตกต่างกันไปตามรูปแบบของอาชญากรรม เช่น ความชำนาญในการประกอบอาชญากรรม ทรัพย์สินหรือผลประโยชน์ที่ได้รับจากการกระทำผิดและการมีอยู่อย่างแพร่หลายของเหยื่ออาชญากรรม

คุณสมบัติของอาชญากร ซึ่งมีความแตกต่างของตัวอาชญากรในการตัดสินใจที่จะประกอบอาชญากรรม โดยต้องคำนึงถึงสภาพแวดล้อมทั่วไป เช่น โอกาสในการกระทำผิด ผลเสีย ผลประโยชน์ตลอดจนความเสี่ยง รวมทั้งแรงกระตุ้นหรือมูลเหตุจูงใจในการกระทำผิดของอาชญากรผู้นั้น

ดังนั้นทฤษฎีคิดก่อนกระทำผิดมีสมมติฐาน 2 ประการคือ (1) ทฤษฎีกลุ่มนี้เชื่อว่าบุคคลเป็นผู้มีอิสระ ในการเลือกที่จะกระทำผิดกฎหมายและ (2) คือ แนวทางในการเลือกพฤติกรรมอาชญากรรมผิด กฎหมายขึ้นอยู่กับการที่บุคคลจะได้รับความพึงพอใจหรือผลประโยชน์สูงสุดนั่นเอง ซึ่งความพึงพอใจหรือ ผลประโยชน์ไม่ได้เฉพาะในรูปแบบเงินเท่านั้นแต่ยังคงรวมถึงด้านจิตใจด้วย

จากทฤษฎีดังกล่าวจึงสรุปได้ว่าเป็นทฤษฎีที่อธิบายพฤติกรรมอาชญากรรมผ่านการตัดสินใจที่มีสติและมีเหตุผลของผู้กระทำผิด โดยเชื่อว่าผู้กระทำผิดจะชั่งน้ำหนักระหว่างผลประโยชน์และผลเสียก่อนตัดสินใจกระทำความผิด การที่อาชญากรจะตัดสินใจในการประกอบอาชญากรรมอย่างใดอย่างหนึ่ง อาชญากรต้องคำนึงการตัดสินใจสภาพแวดล้อมในการประกอบอาชญากรรม โอกาสในการกระทำผิดผลที่จะได้รับประโยชน์ ความเสี่ยงเพื่อชั่งน้ำหนักที่จะกระทำความผิดและต้องมีแรงจูงใจที่จะประกอบอาชญากรรม เช่น ผลตอบแทนมีมูลค่าสูง เป็นต้น นอกจากนี้แล้ว หากอาชญากรคำนวนระหว่างโทษและผลประโยชน์ที่จะได้รับอีกด้วย หากโทษน้อยกว่าและได้ผลประโยชน์อาชญากรก็

---

[71] สุมนทิพย์ จิตสว่าง, ปิยะพร ตันณีกุล และ นัทธี จิตสว่าง, *อาชญากรรมข้ามชาติ: ภัยคุกคามประเทศไทยเกี่ยวกับแก๊งคอลเซ็นเตอร์* (รายงานวิจัย, 2563), 26–27.

[72] เพิ่งอ้าง, 23.

ตัดสินใจที่จะประกอบอาชญากรรมอยู่ดี[73] เช่นกรณีของแก๊งคอลเซ็นเตอร์ที่มักจะคำนวณผลประโยชน์ที่พวกเขาจะได้รับจากการหลอกลวง เช่น เงินที่สามารถหาได้จากเหยื่อ เทียบกับความเสี่ยงที่จะถูกจับกุมและลงโทษ เป็นการตัดสินใจจะกระทำความผิดที่มาจากการเห็นว่าผลประโยชน์มีมากกว่าผลเสีย อีกทั้งผู้กระทำผิดจะพิจารณาถึงโอกาสที่จะถูกจับกุมและโทษที่อาจได้รับ พวกเขาอาจมองว่าความเสี่ยงต่ำเนื่องจากการบังคับใช้กฎหมายที่ไม่เข้มงวดหรือขาดการตรวจสอบที่มีประสิทธิภาพ

**2.5.4 ทฤษฎีปัจจัยทางสภาวะแวดล้อม**

เป็นทฤษฎีที่มองว่าสาเหตุของการกระทำผิดกฎหมายหรือพฤติกรรมอาชญากรรมของบุคคลได้รับอิทธิพลจากปัจจัยทางสภาวะแวดล้อมมากกว่าจากปัจจัยทางพันธุกรรมหรือบุคลิกภาพส่วนตัว ทฤษฎีนี้เชื่อว่าพฤติกรรมของบุคคลเป็นผลมาจากการตอบสนองต่อสภาพแวดล้อมที่พวกเขาอาศัยอยู่ ซึ่งรวมถึงปัจจัยต่าง ๆ เช่น ปัจจัยทางเศรษฐกิจ โดยทฤษฎีนี้มองว่าสภาพเศรษฐกิจมีผลต่อการประกอบอาชญากรรมของคน กล่าวคือ หากประเทศประสบปัญหาด้านเศรษฐกิจ คนในประเทศมีอัตราการว่างงานสูง จะส่งผลให้คนมีการประกอบอาชญากรรมเกี่ยวกับทรัพย์มากขึ้น เพื่อการดำรงชีพอยู่ในสังคม เนื่องจาก เศรษฐกิจเป็นปัจจัยที่สำคัญขั้นพื้นฐานในการดำรงชีวิตของมนุษย์ และปัจจัยทางด้านสังคม ซึ่งเกี่ยวข้องกับการประกอบอาชญากรรมโดยตรงเนื่องจากมนุษย์เป็นสัตว์สังคม มีความสัมพันธ์กันโดยตรงในสังคมโดยมนุษย์มีการกำหนดบรรทัดฐาน ตลอดจนการมีค่านิยมเดียวกันร่วมกันในสังคม เพื่อแสดงออกถึงความเป็นกลุ่มทางสังคมเดียวกัน[74]

ทฤษฎีปัจจัยทางสภาวะแวดล้อม (Environmental Criminology Theory) เน้นการศึกษาและทำความเข้าใจพฤติกรรมอาชญากรรมผ่านมุมมองของสภาพแวดล้อมและบริบทที่อาชญากรรมเกิดขึ้น ทฤษฎีนี้เสนอว่าอาชญากรรมไม่ได้เกิดขึ้นโดยบังเอิญ แต่มีปัจจัยด้านสภาพแวดล้อมและสถานการณ์ที่เอื้อต่อการกระทำความผิด ซึ่งมีความสอดคล้องกับสาเหตุของการกระทำผิดของแก๊งคอลเซ็นเตอร์ ดังนี้

1. สภาพแวดล้อมทางสังคมและเศรษฐกิจ สภาพแวดล้อมทางสังคมและเศรษฐกิจที่ไม่มั่นคงหรือมีความยากลำบาก เช่น การว่างงานและการขาดโอกาสทางการเงิน เช่นนี้จะสามารถเพิ่มแรงจูงใจให้บุคคลหันมาสู่อาชญากรรม เช่น การเข้าร่วมกับองค์กรอาชญากรรมข้ามชาติแก๊งคอลเซ็นเตอร์เพื่อเป็นการหาทางรอด

---

[73] เพิ่งอ้าง, 24

[74] บุญวัฒน์ สว่างวงศ์, ‘ทฤษฎีที่เกี่ยวข้องกับการก่ออาชญากรรมและการวัดสถิติอาชญากรรม’ (ระบบการเรียนรู้อิเล็กทรอนิกส์ E-Learning มหาวิทยาลัยราชภัฏสวนสุนันทา), <https://elcpg.ssru.ac.th/boonwat_sa/pluginfile.php/44/block_html/content/อาชญาวิทยา%20บทที่%204.pdf> , สืบค้นเมื่อ 23 กุมภาพันธ์ 2567.

2. สภาพแวดล้อมทางเทคโนโลยี การพัฒนาเทคโนโลยีและการใช้เทคโนโลยีในการกระทำความผิด เช่น โทรศัพท์มือถือ อินเทอร์เน็ต และแอพพลิเคชันต่าง ๆ ทำให้การหลอกลวงสามารถทำได้ง่ายและมีประสิทธิภาพมากขึ้น แก๊งคอลเซ็นเตอร์สามารถใช้เทคโนโลยีเหล่านี้ในการติดต่อและหลอกลวงเหยื่อได้อย่างรวดเร็วและมีประสิทธิภาพ

3. สภาพแวดล้อมทางกฎหมายและการบังคับใช้ การขาดการบังคับใช้กฎหมายที่เข้มงวดและมีประสิทธิภาพ สามารถทำให้แก๊งคอลเซ็นเตอร์มีความกล้าที่จะกระทำความผิดมากขึ้น การขาดทรัพยากรและความสามารถในการติดตามและจับกุมผู้กระทำความผิดสามารถทำให้การกระทำความผิดมีโอกาสสำเร็จสูง

โดยสรุปแล้วทฤษฎีปัจจัยทางสภาวะแวดล้อมให้มุมมองที่สำคัญในการทำความเข้าใจสาเหตุของการกระทำความผิดของแก๊งคอลเซ็นเตอร์ โดยมุ่งเน้นการจัดการกับปัจจัยทางสภาพแวดล้อมที่เอื้อต่อการเกิดอาชญากรรม

**2.5.5 ทฤษฎีอาชญากรรมทางเศรษฐกิจ (Economic Crime Theory)**

อาชญากรรมทางเศรษฐกิจ (Economic Crime) เป็นการกระทำที่มุ่งแสวงหาผลประโยชน์ทางการเงินหรือทรัพย์สิน โดยไม่คำนึงถึงความชอบด้วยกฎหมาย และมักเกิดขึ้นในลักษณะที่ไม่มีความรุนแรงโดยตรง แต่สร้างความเสียหายต่อระบบเศรษฐกิจและสังคมอย่างกว้างขวาง ทั้งนี้ แนวคิดเกี่ยวกับอาชญากรรมประเภทนี้มีรากฐานจากแนวคิดของ เอ็ดวิน เอช. ซัทเธอร์แลนด์ (Edwin H. Sutherland) ซึ่งได้เสนอคำว่า *"White-Collar Crime"* หรือ "อาชญากรรมปกขาว" ไว้ตั้งแต่ ค.ศ. 1939 โดยอธิบายว่าเป็น "อาชญากรรมของบุคคลที่มีสถานะทางสังคมสูงและมีเกียรติในกระบวนการประกอบอาชีพของตน"[75]

แนวคิดของซัทเธอร์แลนด์ชี้ให้เห็นว่า บุคคลที่มีตำแหน่งหน้าที่ในสังคมหรือองค์กรมีแนวโน้มที่จะกระทำความผิดเพื่อประโยชน์ส่วนตนหรือกลุ่ม โดยใช้อำนาจหรือความรู้ในทางที่ผิด อาชญากรรมประเภทนี้จึงมีลักษณะเฉพาะ คือ วางแผนอย่างเป็นระบบ ซับซ้อน และใช้กลไกทางกฎหมายหรือการเงินเป็นเครื่องมือในการอำพรางเจตนา ต่อมา แนวคิดนี้ได้รับการพัฒนาโดยเชื่อมโยงกับ ทฤษฎีทางเลือกอย่างมีเหตุผล (Rational Choice Theory) ซึ่งอธิบายว่า ผู้กระทำผิดจะประเมินต้นทุนและผลประโยชน์ก่อนการตัดสินใจกระทำความผิด กล่าวคือ หากเห็นว่าความเสี่ยงที่จะถูกจับน้อย แต่ได้ผลตอบแทนสูง ก็มีแนวโน้มจะกระทำผิด[76]

---

[75] Edwin H. Sutherland, *White Collar Crime* (New York: Dryden Press, 1949), 9.

[76] Gilbert Geis, "White-Collar and Corporate Crime," in *The Oxford Handbook of Criminology*, 3rd ed., ed. by Mike Maguire et al. (Oxford: Oxford University Press, 2002) 981–1010.

ในกรณีของแก๊งคอลเซ็นเตอร์สามารถจำแนกได้ว่าเป็นอาชญากรรมทางเศรษฐกิจประเภทหนึ่งที่มีลักษณะสอดคล้องกับแนวคิดของ Edwin H. Sutherland ซึ่งมองว่าอาชญากรรมที่ก่อขึ้นโดยบุคคลหรือกลุ่มที่มีสถานะทางสังคมหรือมีความรู้เฉพาะทาง มักแฝงมาในรูปแบบที่ไม่ใช้ความรุนแรงโดยตรง แต่สามารถก่อให้เกิดความเสียหายทางเศรษฐกิจอย่างร้ายแรง แก๊งคอลเซ็นเตอร์จำนวนไม่น้อยมีโครงสร้างเป็นองค์กรข้ามชาติที่มีการแบ่งหน้าที่กันทำงานอย่างเป็นระบบ ใช้เทคโนโลยีสารสนเทศขั้นสูง เช่น ระบบ VoIP การปลอม Caller ID หรือการส่งลิงก์หลอกลวงผ่านแอปพลิเคชัน เพื่อให้เหยื่อเปิดเผยข้อมูลส่วนตัวหรือโอนเงิน ซึ่งทั้งหมดล้วนเกิดจากการวางแผนอย่างเป็นขั้นตอน โดยมีจุดมุ่งหมายเพื่อแสวงหาผลประโยชน์ทางการเงินโดยผิดกฎหมาย การวิเคราะห์ภายใต้ทฤษฎีอาชญากรรมทางเศรษฐกิจช่วยให้เข้าใจว่า แก๊งคอลเซ็นเตอร์ไม่ใช่อาชญากรรมรายย่อยเฉพาะบุคคล แต่เป็นผลลัพธ์ของระบบที่เอื้อให้เกิดอาชญากรรมจากแรงจูงใจทางเศรษฐกิจ การบังคับใช้กฎหมายที่ไม่ทันสมัย ช่องว่างระหว่างประเทศ และความไม่สมดุลของเทคโนโลยีและการกำกับดูแล ดังนั้น การแก้ไขปัญหานี้จึงต้องอาศัยแนวทางแบบองค์รวมที่บูรณาการระหว่างการพัฒนากฎหมาย การควบคุมเทคโนโลยี และความร่วมมือระดับภูมิภาค

# บทที่ 3

## นโยบายและมาตรการในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

ในปัจจุบันแก๊งคอลเซ็นเตอร์ได้กลายเป็นปัจจัยสำคัญที่ส่งผลกระทบต่อเศรษฐกิจของภูมิภาคอาเซียนอย่างมีนัยสำคัญ เนื่องจากการกระทำความผิดในลักษณะการหลอกลวงผ่านโทรศัพท์ส่งผลให้เกิดความสูญเสียทางการเงินเป็นวงกว้าง ทั้งนี้ อาชญากรรมข้ามชาติที่เกิดขึ้นในรูปแบบแก๊งคอลเซ็นเตอร์ เป็นการกระทำผิดที่ข้ามพรมแดนหรือเกี่ยวข้องกับพื้นที่ของมากกว่าหนึ่งประเทศ ดังนั้น การป้องกันและปราบปรามจึงจำเป็นต้องอาศัยความร่วมมือระหว่างรัฐต่าง ๆ อย่างเข้มแข็งและเป็นระบบ เพื่อให้สามารถติดตาม สกัดกั้น และจับกุมผู้กระทำความผิด พร้อมทั้งนำตัวมาลงโทษตามกฎหมายของรัฐที่เกิดเหตุการณ์ผิดกฎหมายขึ้นได้อย่างมีประสิทธิภาพ ในแง่ของการบังคับใช้กฎหมายระหว่างประเทศ ความร่วมมือระหว่างประเทศจึงถือเป็นกลไกสำคัญที่สุดในการตอบโต้ปัญหาอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ เนื่องจากการดำเนินคดีในลักษณะนี้เกี่ยวข้องกับกระบวนการถ่ายโอนข้อมูลผ่านระบบอินเทอร์เน็ตที่มีการเชื่อมโยงข้ามประเทศอย่างซับซ้อน การโจมตีหรือการกระทำผิดในระบบดังกล่าวจึงส่งผลกระทบไปยังหลายประเทศพร้อมกัน นอกจากนี้ในกรณีที่ผู้กระทำผิดและผู้เสียหายไม่ได้อยู่ในเขตอำนาจศาลเดียวกัน การสืบสวนและสอบสวนจำเป็นต้องอาศัยความร่วมมือของหน่วยงานบังคับใช้กฎหมายในแต่ละประเทศที่ได้รับผลกระทบ เพื่อให้สามารถดำเนินการทางกฎหมายได้อย่างครบถ้วนและถูกต้องตามหลักนิติธรรม อย่างไรก็ดี การดำเนินการสืบสวนสอบสวนข้ามพรมแดนนี้ยังต้องอยู่ภายใต้กรอบของหลักอำนาจอธิปไตยของรัฐ ซึ่งกำหนดไว้ว่าประเทศใดประเทศหนึ่งไม่สามารถดำเนินการสืบสวนในเขตอำนาจของอีกประเทศหนึ่งโดยไม่ได้รับอนุญาต[60]

ซึ่งในบทนี้จะทำการศึกษาถึงนโยบายและมาตรการในระดับสากล ระดับภูมิภาค รวมถึงระดับภายในประเทศที่สำคัญอันเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์เพื่อนำไปใช้ในการวิเคราะห์เพื่อหาแนวทางและมาตรการทางกฎหมายของอาเซียนในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีของแก๊งคอลเซ็นเตอร์ในบทที่ 5 ต่อไป

---

[60] นันทวดี คาดคะเน, ปัญหาในการปราบปรามอาชญากรรมไซเบอร์ภายใต้กฎหมายระหว่างประเทศ (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์, 2561) 41–42.

## 3.1 นโยบายในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

### 3.1.1 ระดับสากล

3.1.1.1 องค์การสหประชาชาติ[61]

สำหรับนโยบายการป้องกันและปราบปรามอาชญากรรมข้ามชาติเกี่ยวกับแก๊งคอลเซ็นเตอร์ของสหประชาชาติ (United Nations) จากการศึกษา พบว่า องค์การสหประชาชาติ ไม่มีนโยบายเฉพาะที่จัดการกับ “แก๊งคอลเซ็นเตอร์” โดยตรง แต่ได้กำหนดนโยบายและกรอบความร่วมมือในการป้องกันและปราบปรามอาชญากรรมข้ามชาติที่มีลักษณะเกี่ยวข้องโดยตรงกับแก๊งคอลเซ็นเตอร์ผ่านอนุสัญญาและเอกสารสำคัญหลายฉบับ เช่น อนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร ค.ศ.2000[62] ประเทศที่เข้าร่วมลงนามได้ต่างเล็งเห็นถึงภัยจากองค์กรอาชญากรรมที่คุกคามในแต่ละประเทศและเห็นด้วยว่าการกำหนดมาตรฐานสากลในเรื่องการให้ความร่วมมือและช่วยเหลือระหว่างประเทศจะช่วยลดช่องว่างของกฎหมายภายในของประเทศสมาชิกได้

ซึ่งองค์การสหประชาชาติได้มีการเรียกร้องให้รัฐบาลของประเทศสมาชิกได้ตระหนักถึงความสำคัญตัวแสดงอื่นที่เป็นรัฐและที่มิใช่รัฐที่เกี่ยวข้องกับปัญหาอาชญากรรมข้ามชาติเพื่อมาร่วมมือกันในการต่อสู้กับอาชญากรรมข้ามชาติ ทั้งยังได้สนับสนุนเงินทุน บุคลากร และเทคโนโลยีในโครงการพัฒนาหลายรูปแบบ เช่น การฝึกอบรมเจ้าหน้าที่บังคับใช้กฎหมาย การสร้างความตระหนักรู้ให้แก่

---

[61] สหประชาชาติ (United Nations: UN) เป็นองค์การระหว่างประเทศที่จัดตั้งขึ้นภายหลังการสิ้นสุดของสงครามโลกครั้งที่สองในปี พ.ศ. 2488 โดยมีวัตถุประสงค์หลักเพื่อส่งเสริมความร่วมมือระหว่างประเทศในด้านกฎหมายระหว่างประเทศ การธำรงไว้ซึ่งสันติภาพและความมั่นคงระหว่างประเทศ การพัฒนาเศรษฐกิจและสังคม การเคารพสิทธิมนุษยชน รวมถึงการส่งเสริมการแก้ไขปัญหาข้อพิพาทระหว่างรัฐด้วยสันติวิธี โดยมีบทบาทเป็นเวทีกลางในการเจรจาและประสานความร่วมมือระหว่างประเทศสมาชิกทั่วโลก องค์การนี้ถือกำเนิดขึ้นเพื่อทดแทนสันนิบาตชาติ (League of Nations) ซึ่งไม่สามารถยับยั้งความขัดแย้งที่นำไปสู่สงครามโลกได้อย่างมีประสิทธิภาพ สหประชาชาติประกอบด้วยองค์การย่อยจำนวนมากที่มีบทบาทในการดำเนินพันธกิจเฉพาะด้านตามขอบเขตอำนาจหน้าที่ที่ได้รับมอบหมาย เดิมทีมีชื่อเต็มในภาษาอังกฤษว่า *United Nations Organization (UNO)* แต่ตั้งแต่ปี ค.ศ. 1950 เป็นต้นมา นิยมเรียกโดยย่อว่า *United Nations (UN)* ซึ่งเป็นที่รู้จักอย่างแพร่หลายทั้งในระดับภูมิภาคและระดับนานาชาติ

[62] ชิตพล กาญจนกิจ, ‘ความท้าทายของรัฐอาเซียนในการต่อต้านอาชญากรรมข้ามชาติ’, วารสารสังคมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ปีที่ 46 ฉบับที่ 1 (2560) 51–78 <https://doi.org/10.61462/cujss.v46i1.1155> สืบค้นเมื่อ 25 มีนาคม 2567.

ประชาชนถึงภัยของอาชญากรรมข้ามชาติ การจัดหาเครื่องมือพิเศษใน การสืบสวนและป้องกันปราบปรามอาชญากรรม องค์กรรูปแบบต่าง ๆ ภายใต้แนวคิดบูรณาการความเป็นหุ้นส่วนเพื่อการสร้างรัฐซึ่งมุ่งเน้นการทำงานร่วมกันแบบบูรณาการ หลักนิติธรรม และการพัฒนา กฎหมายและนโยบายให้ตอบสนองต่อวิกฤตการณ์ และสภาพแวดล้อมที่เอื้ออำนวยต่อการขยายตัวของอาชญากรรมข้ามชาติให้ได้[63]

3.1.1.2 องค์การตำรวจสากล

องค์การตำรวจสากล (INTERPOL) ถือกำเนิดจากแนวคิดริเริ่มในปี ค.ศ. 1914 ในการประชุมตำรวจระหว่างประเทศทางอาญา (International Criminal Police Congress) ซึ่งมีผู้แทนจาก 24 ประเทศเข้าร่วม เพื่อหารือแนวทางรับมือกับอาชญากรรมที่มีลักษณะข้ามพรมแดน และการจัดตั้งฐานข้อมูลอาชญากรรมที่ใช้ร่วมกัน[64] โดยต่อมาในปี ค.ศ. 1923 ได้มีการจัดตั้งเป็นทางการในชื่อ “คณะกรรมการข้าราชการตำรวจทางอาญาระหว่างประเทศ” (The International Criminal Police Commission) และในปี ค.ศ. 1956 ได้เปลี่ยนชื่อเป็น “องค์การตำรวจอาชญากรรมระหว่างประเทศ” หรือที่รู้จักกันในนาม INTERPOL โดยมีสถานะเป็นองค์การระหว่างประเทศในระดับรัฐบาล ปัจจุบันองค์การตำรวจสากลมีประเทศสมาชิกจำนวน 195 ประเทศนับเป็นองค์กรที่มีจำนวนสมาชิกมากที่สุดในโลกในด้านความร่วมมือด้านกฎหมาย โดยให้เป็นหน่วยประสานงานกลางในการแลกเปลี่ยนข้อมูลการสืบสวนสอบสวนคดีอาชญากรรมระหว่างประเทศและให้ความช่วยเหลือกันระหว่างกลุ่มประเทศสมาชิก[65] ในการติดตามจับกุมผู้กระทำความผิดมาลงโทษโดยการแลกเปลี่ยนข้อมูลระหว่างสำนักงานกลางแห่งชาติ (National Central Bureau: NCB) ซึ่งเป็นหน่วยงานภายในของประเทศสมาชิกที่ถูกกำหนดให้เป็นศูนย์กลางในการติดต่อประสานงานกับสำนักงานเลขาธิการองค์การตำรวจสากล ผ่านระบบข้อมูลกลางที่เรียกว่า ไอ-24/7 (I-24/7) ทุกวันตลอด 24 ชั่วโมง โดยองค์การตำรวจสากลจะไม่เข้าไปยุ่งเกี่ยวกับกิจการภายในและเรื่องทางการเมืองหรือศาสนาของประเทศ

---

[63] ที่ประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา สมัยที่ 13 (UN Congress) ได้ให้ความสำคัญต่อความเชื่อมโยงระหว่างหลักนิติธรรม ความมั่นคง และการพัฒนาโดยให้รัฐสมาชิกคำนึงถึง คำประกาศของการประชุมระดับสูงของสมัชชาสหประชาชาติว่าด้วยหลักนิติธรรมในระดับชาติและระดับระหว่างประเทศ และเป้าหมายการพัฒนาแห่งสหัสวรรษ (MDGs) ที่ต้องคำนึงถึง 4 มิติที่เป็นอิสระต่อกัน ได้แก่ การพัฒนาทางเศรษฐกิจแบบองค์รวม การพัฒนาทางสังคมแบบองค์รวม ความยั่งยืนของ สิ่งแวดล้อม และสันติภาพและความมั่นคง

[64] ‘History’ (INTERPOL) http://www.interpol.int/en/About-INTERPOL/History accessed 7 March 2024.

[65]‘องค์การตำรวจสากล’ (LIRT คลังสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร) <https://dl.parliament.go.th/handle/20.500.13072/617970> สืบค้นเมื่อ 7 มีนาคม 2567.

สมาชิก[66] โดยภารกิจและหน้าที่ขององค์การตำรวจสากลเป็นการดำเนินการด้านการติดต่อกับประเทศสมาชิก เพื่อขอทราบรายงานและสถิติอาชญากรรมของประเทศเหล่านั้นโดยประเทศสมาชิกจะจัดส่งรายงานและสถิติอาชญากรรมไปยังสำนักงานกลางทุก ๆ ปี โดยสำนักงานกลางจะจัดทำรายงานส่งให้ประเทศสมาชิก เพื่อให้ทราบถึงความเคลื่อนไหวของผู้กระทำความผิดในประเทศภาคี แจ้งข่าวสารการเคลื่อนไหวของผู้กระทำความผิดเพื่อเป็นการแลกเปลี่ยนข้อมูลข่าวกรองและประสานงานในการที่จะจับกุมต่อไป ตลอดจนรวบรวมประวัติอาชญากรสำคัญของโลก เพื่อสะดวกในการสืบสวนสอบสวนและจับกุมของประเทศสมาชิกและประสานความร่วมมือกับสมาชิกตำรวจสากลประเทศอื่นในการจับกุมปราบปรามและดำเนินการสอบสวนคดีอาชญากรรมหรือความผิด ตามกฎหมายระหว่างประเทศสำหรับอาชญากรรมที่องค์การตำรวจสากลทำการป้องกันปราบปรามอย่างเป็นรูปธรรม[67]

จากที่ได้กล่าวมาข้างต้นเห็นได้ว่า องค์การตำรวจสากล (Interpol) เป็นองค์กรสำคัญที่มีบทบาทในการประสานงานและสนับสนุนประเทศสมาชิกในการป้องกันและปราบปรามอาชญากรรมข้ามชาติที่มีการหลอกลวงผู้คนทั่วโลก ซึ่งเป็นกลไกความร่วมมือระหว่างประเทศในทางอาญารูปแบบหนึ่งที่ช่วยให้การปราบปรามอาชญากรรมระหว่างประเทศเป็นไปอย่างมีประสิทธิภาพมากขึ้น โดยมีการดำเนินการปฏิบัติการร่วมกับประเทศสมาชิกในการจับกุมและปิดกั้นการทำงานของเหล่าองค์กรอาชญากรรมข้ามชาติ ปฏิบัติการเหล่านี้มักเกี่ยวข้องกับการรวบรวมข้อมูลและการทำงานร่วมกันระหว่างหน่วยงานบังคับใช้กฎหมายในหลายประเทศ ปัจจุบันในกรณีของแก๊งคอลเซ็นเตอร์ ตำรวจสากล Interpol มีนโยบายในการประสานงานระหว่างประเทศ มีทำหน้าที่เป็นศูนย์กลางในการประสานงานการบังคับใช้กฎหมายระหว่างประเทศสมาชิก โดยมีการแลกเปลี่ยนข้อมูลและข่าวกรองเกี่ยวกับแก๊งคอลเซ็นเตอร์อย่างต่อเนื่อง ซึ่งการแลกเปลี่ยนข้อมูลเหล่านี้ช่วยให้ประเทศสมาชิกสามารถระบุและติดตามกลุ่มอาชญากรรมข้ามชาติที่เกี่ยวข้องกับการหลอกลวงทางโทรศัพท์

---

[66] เพิ่งอ้าง.

[67] มาตรา 2 “ จุดมุ่งหมายขององค์การตำรวจสากล

(1) เพื่อให้แน่ใจและส่งเสริมความช่วยเหลือซึ่งกันและกันระหว่างตารวจภายใน ขอบเขตของกฎหมายที่อยู่ในแต่ละประเทศโดย “ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน”

(2) เพื่อสร้างและพัฒนาทุกสถาบันที่มีแนวโน้มที่จะมีส่วนร่วมได้อย่างมีประสิทธิภาพ ในการป้องกันและการปราบปรามการก่ออาชญากรรมตามกฎหมายทั่วไปอันเกี่ยวข้องกับข่าวกรอง ระหว่างประเทศสมาชิก”: โปรดดู, เขตต์เทพหัสดิน ณ อยุธยา, “การจัดตั้งองค์การตำรวจอาเซียน: ศึกษาเปรียบเทียบองค์การตำรวจสากล และสำนักงานตำรวจยุโรป”. วิทยานิพนธ์ปริญญามหาบัณฑิต, คณะนิติศาสตร์ มหาวิทยาลัยแม่ฟ้าหลวง, 2561.

**3.1.2 ระดับภูมิภาค**

3.1.2.1 สหภาพยุโรป

สหภาพยุโรป[68] พบว่าเป็นสังคมเปิดที่มีการรวมตัวกันในหลายด้านซึ่งทำให้บุคคลสามารถข้ามพรมแดนได้อย่างเสรีระหว่างประเทศสมาชิกด้วยกันเอง ดังนั้นประเทศสมาชิกทั้งหมดจึงมีความจำเป็นที่จะต้องร่วมมือและประสานงานกันในนโยบายต่อต้านอาชญากรรมข้ามชาติกันอย่างใกล้ชิดเพื่อก่อให้เกิดความมั่นคงร่วมกัน โดยความรับผิดชอบหลักของงานต่อต้านอาชญากรรมข้ามชาติของประเทศในสหภาพยุโรปยังคงเป็นของหน่วยงานด้านความมั่นคงของประเทศสมาชิก (เช่น งานข่าวกรอง งานปราบปราม งานป้องกันและรักษาความปลอดภัย ฯลฯ) โดยสหภาพยุโรปได้มีหน่วยงานหลักในการประสานงานในทางอาญาระหว่างประเทศสมาชิก คือ

Europol (European Union Agency for Law Enforcement Cooperation) เป็นหน่วยงานหลักในการประสานงานและสนับสนุนการบังคับใช้กฎหมายระหว่างประเทศสมาชิก EU โดยมีบทบาทสำคัญในการแบ่งปันข้อมูล การวิเคราะห์ข่าวกรอง และการร่วมมือในการปฏิบัติการต่าง ๆ เช่น การต่อต้านการก่อการร้าย การค้ามนุษย์ และอาชญากรรมทางไซเบอร์ ซึ่งมีบทบาทในการสืบสวนอาชญากรรมข้ามชาติที่ซับซ้อน โดยร่วมมือกับหน่วยงานที่บังคับใช้กฎหมายของประเทศสมาชิก EU ในการรวบรวมและวิเคราะห์ข้อมูลทางการสืบสวนที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์ อีกทั้งยังมีการประสานงานการดำเนินการกับอาชญากรรมไซเบอร์ คือ European Cybercrime Centre[69] (EC3) ซึ่งเน้นการสืบสวนและปราบปรามอาชญากรรมทางอินเทอร์เน็ตและการฟอกเงินที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์[70] และสหภาพยุโรปได้มีการแลกเปลี่ยนข้อมูลกับหน่วยงานบังคับใช้กฎหมายในประเทศสมาชิก EU และองค์กรระหว่างประเทศอื่นๆ เช่น Interpol และ Eurojust เพื่อเพิ่มประสิทธิภาพในการสืบสวนและปราบปรามอาชญากรรมข้ามชาติ ซึ่งสหภาพยุโรป (European Union – EU) ถือเป็นหนึ่งในแบบอย่างของกลไกความร่วมมือระดับภูมิภาคที่มีความก้าวหน้าในการจัดการกับภัยคุกคามจากอาชญากรรมข้ามชาติอย่างเป็นระบบด้วยการวางรากฐานทางนโยบายและ

---

[68] สหภาพยุโรปเป็นการรวมกลุ่มของประเทศในภูมิภาคยุโรปทั้งด้านการเมือง เศรษฐกิจ และสังคมในลักษณะสถาบันแบบเหนือรัฐ (Supranational Institution) ที่ใหญ่ที่สุดและก้าวหน้าที่สุดในโลก โดยมีวัตถุประสงค์เพื่อเสริมสร้างสันติภาพเป็นการถาวรระหว่างประเทศในภูมิภาคยุโรปภายหลังสงครามโลกครั้งที่ 2 รวมไปถึงการเสริมสร้างความเข้มแข็งทางเศรษฐกิจแก่ประเทศสมาชิกและการมีบทบาทนำของ EU ในประชาคมโลก

[69] European Cybercrime Center (EC3) ได้รับการจัดตั้งขึ้นโดย Europol เพื่อเสริมสร้างการตอบสนองของหน่วยงานบังคับใช้กฎหมายต่ออาชญากรรมทางไซเบอร์ในสหภาพยุโรป และเพื่อช่วยปกป้องพลเมือง ธุรกิจ และรัฐบาลในยุโรปจากอาชญากรรมออนไลน์

[70] Europol, 'European Cybercrime Centre - EC3'<https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> accessed 27 June 2024.

สถาบันในลักษณะของการบูรณาการด้านความมั่นคงภายใน (Internal Security) ร่วมกัน เพื่อให้สามารถรับมือกับอาชญากรรมที่ข้ามพรมแดน ซึ่งรวมถึงการก่อการร้าย อาชญากรรมทางไซเบอร์ การค้ามนุษย์ และอาชญากรรมที่เกิดจากเครือข่ายข้ามชาติในการรับมือกับภัยคุกคามจากอาชญากรรมข้ามชาติที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว สหภาพยุโรป (European Union: EU) ได้ให้ความสำคัญต่อการกำหนดกรอบนโยบายและยุทธศาสตร์ในระดับภูมิภาคที่มีเป้าหมายชัดเจนและมีผลบังคับใช้ในทางปฏิบัติ โดยเฉพาะอย่างยิ่งในกรณีของอาชญากรรมที่มีการจัดตั้งเป็นเครือข่ายซึ่งต่างอาศัยประโยชน์จากช่องว่างของพรมแดน การใช้เทคโนโลยี และความไม่สอดคล้องของกฎหมายระหว่างประเทศเพื่อตอบสนองต่อปัญหาเหล่านี้ สหภาพยุโรปจึงได้จัดทำแผนยุทธศาสตร์ระดับภูมิภาค ได้แก่

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021–2025 (COM (2021) 170 final) ซึ่งเป็นแนวทางสำคัญในการบูรณาการความร่วมมือของประเทศสมาชิกและเสริมสร้างขีดความสามารถของหน่วยงานที่เกี่ยวข้องในการป้องกันและปราบปรามอาชญากรรมที่มีลักษณะข้ามชาติและมีการจัดตั้งเป็นเครือข่าย โดยยุทธศาสตร์ดังกล่าวสะท้อนให้เห็นถึงความมุ่งมั่นของสหภาพยุโรปในการสร้างระบบความมั่นคงแบบองค์รวม ทั้งในด้านการบังคับใช้กฎหมาย การพัฒนากลไกสืบสวนทางดิจิทัล การป้องกันความเสียหายต่อสาธารณะ และการเสริมสร้างความร่วมมือระหว่างประเทศอย่างเป็นรูปธรรม โดยหัวใจสำคัญของยุทธศาสตร์นี้คือการมุ่งรื้อถอนโครงสร้างขององค์กรอาชญากรรม ไม่ว่าจะเป็นการสืบสวนเส้นทางทางการเงิน การติดตามและยึดทรัพย์สินที่ได้จากการกระทำความผิด ตลอดจนการทำลายกลไกทางเศรษฐกิจที่สนับสนุนอาชญากรรมเหล่านี้ ยุทธศาสตร์ยังให้ความสำคัญกับการยกระดับการสืบสวนดิจิทัลและการใช้เทคโนโลยีในการต่อสู้กับอาชญากรรมที่เน้นการพัฒนาเครื่องมือดิจิทัลและการเข้าถึงข้อมูลอย่างถูกกฎหมายเพื่อเพิ่มขีดความสามารถในการสืบสวนและติดตามอาชญากรรม อีกทั้งยังเน้นการเสริมสร้างกลไกในการปกป้องประชาชนและระบบเศรษฐกิจจากภัยคุกคามที่เกิดจากอาชญากรรมข้ามชาติผ่านมาตรการที่หลากหลาย เช่น การเสริมศักยภาพของเจ้าหน้าที่ การให้ข้อมูลและสร้างความตระหนักแก่สาธารณชน รวมถึงการคุ้มครองโครงสร้างพื้นฐานที่สำคัญของรัฐจากการแทรกแซงของกลุ่มอาชญากร ขณะเดียวกัน ยุทธศาสตร์ดังกล่าวยังตระหนักถึงความสำคัญของการสร้างความร่วมมือระหว่างประเทศอย่างเป็นระบบ ทั้งในระดับประเทศสมาชิกสหภาพยุโรปผ่านองค์กรกลางอย่าง Europol, Eurojust และ Frontex และใน

ระดับโลกผ่านความร่วมมือกับประเทศภายนอก โดยมีเป้าหมายเพื่อบูรณาการความพยายามในการป้องกันและปราบปรามอาชญากรรมข้ามชาติให้ครอบคลุมและมีประสิทธิภาพมากยิ่งขึ้น[71]

ทั้งนี้ ในกรณีแก๊งคอลเซ็นเตอร์ที่เป็นหนึ่งในอาชญากรรมไซเบอร์ทางสหภาพยุโรปได้มีการรักษาความปลอดภัยเครือข่ายและระบบข้อมูลในโลกไซเบอร์ของสหภาพยุโรปซึ่งเป็นสิ่งสำคัญเพื่อให้ธุรกิจออนไลน์ดำเนินไปอย่างราบรื่นทำให้เกิดความมั่งคั่งทางเศรษฐกิจ โดยการเพิ่มขีดความสามารถของประเทศสมาชิกในการให้ความร่วมมือระหว่างประเทศในด้าน ความปลอดภัยในโลกไซเบอร์และอาชญากรรมในโลกไซเบอร์ หน่วยงานกลางที่มีบทบาทประสานงานนโยบายและส่งเสริมขีดความสามารถของรัฐสมาชิกได้กลายเป็นกุญแจสำคัญในการรับมือกับอาชญากรรมไซเบอร์ที่มีลักษณะซับซ้อนและข้ามพรมแดน ในบริบทของสหภาพยุโรป หน่วยงานที่มีบทบาทหลักในการดำเนินภารกิจดังกล่าว คือ European Union Agency for Cybersecurity (ENISA) ก่อตั้งขึ้นเมื่อปี ค.ศ. 2004 ภายใต้กฎระเบียบของสหภาพยุโรปเพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่ทวีความซับซ้อนและขยายตัวอย่างรวดเร็ว[1] หน่วยงานนี้มีบทบาทเป็น “ศูนย์กลางทางเทคนิคและยุทธศาสตร์” ของสหภาพยุโรปในการวางแผน ส่งเสริม และประสานความร่วมมือด้านความมั่นคงทางไซเบอร์ระหว่างประเทศสมาชิกและภาคส่วนต่าง ๆ ทั้งภาครัฐ เอกชน และภาคประชาสังคม โดยภารกิจหลักของ ENISA ประกอบด้วย 3 ด้านสำคัญ ได้แก่ (1) การสนับสนุนประเทศสมาชิกในการกำหนดและดำเนินยุทธศาสตร์ความมั่นคงไซเบอร์แห่งชาติ (2) การพัฒนาขีดความสามารถในการรับมือกับภัยคุกคามไซเบอร์ เช่น การฝึกอบรม การจัดทำแนวทางปฏิบัติที่ดีและการประเมินความเสี่ยง และ (3) การส่งเสริมความร่วมมือระดับภูมิภาคและระหว่างประเทศ โดยเฉพาะในประเด็นที่ต้องการการตอบสนอง[72] หนึ่งในความสำเร็จสำคัญของ ENISA คือการสนับสนุนให้สหภาพยุโรปพัฒนากฎหมายและมาตรฐานด้านไซเบอร์อย่างมีระบบ ENISA ยังทำหน้าที่เป็นศูนย์กลางในการจัดการฝึกซ้อมด้านความมั่นคงไซเบอร์ในระดับยุโรป (Cyber Europe) และการวิเคราะห์ภัยคุกคามในระดับทวีปเพื่อให้ประเทศสมาชิกมีข้อมูลที่จำเป็นต่อการตัดสินใจด้านนโยบาย ด้วยภารกิจของ ENISA ในการส่งเสริมความมั่นคงปลอดภัยทางไซเบอร์ของสหภาพยุโรป

---

[71] European Commission, ‘EU Strategy to Tackle Organised Crime 2021–2025’ (Brussels: European Commission, 2021), available at: <https://ec.europa.eu/home-affairs/eu-strategy-tackle-organised-crime-2021-2025_en> accessed 16 May 2025.

[72] ENISA, ‘ENISA Mandate and Mission’ (2020), <https://www.enisa.europa.eu/about-enisa> accessed 16 May 2025.

หน่วยงาน European Union Agency for Cybersecurity (ENISA) ทำหน้าที่สนับสนุนด้านเทคนิคและยุทธศาสตร์ในระดับภูมิภาค และมีบทบาทสำคัญในการพัฒนากรอบแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ให้กับประเทศสมาชิก ภายใต้บริบทนี้ สหภาพยุโรปได้จัดทำ

ยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ของสหภาพยุโรป (EU Cybersecurity Strategy) ซึ่งได้รับการจัดตั้งขึ้นเพื่อทำหน้าที่เสริมสร้างความสามารถของประเทศสมาชิกในการป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์ ตลอดจนส่งเสริมความร่วมมือเชิงยุทธศาสตร์ทั้งภายในภูมิภาคและกับพันธมิตรระหว่างประเทศ ยุทธศาสตร์นี้มีการปรับปรุงต่อเนื่อง โดยฉบับล่าสุดคือ The EU's Cybersecurity Strategy for the Digital Decade ที่ประกาศใช้เมื่อเดือนธันวาคม ค.ศ. 2020 ซึ่งเป็นส่วนหนึ่งของยุทธศาสตร์ความมั่นคงของสหภาพยุโรป (EU Security Union Strategy 2020–2025) โดยมีกรอบวัตถุประสงค์หลัก[73] คือ

1. การเสริมสร้างขีดความสามารถในการป้องกันและตอบสนองต่อภัยคุกคามไซเบอร์ ยุทธศาสตร์ไซเบอร์ของสหภาพยุโรปมุ่งเน้นการพัฒนาขีดความสามารถของทั้งประเทศสมาชิกและสถาบันส่วนกลางในการตรวจจับ ป้องกัน และตอบสนองต่อการโจมตีทางไซเบอร์อย่างมีประสิทธิภาพ โดยเสนอการจัดตั้ง Joint Cyber Unit เพื่อเป็นศูนย์ประสานงานระดับยุโรปในการรวบรวมข่าวกรอง การวิเคราะห์ภัยคุกคาม และการบริหารจัดการเหตุการณ์อย่างรวดเร็ว อีกทั้งยังมีกลไก "Cyber Diplomacy Toolbox" ซึ่งเป็นเครื่องมือทางการทูตที่ใช้ตอบโต้ภัยไซเบอร์จากรัฐหรือกลุ่มที่ไม่ใช่รัฐ (non-state actors) ในเวทีระหว่างประเทศ[74]

2. ทำให้สหภาพยุโรปมีบทบาทสำคัญด้านความปลอดภัยในโลกไซเบอร์ สหภาพยุโรปต้องการรักษาความได้เปรียบทางการแข่งขันทางการค้า จึงแสวงหามาตรการด้านความมั่นคงปลอดภัยไซเบอร์เพื่อสร้างความมั่นใจว่าพลเมืองของสหภาพ ยุโรป รัฐวิสาหกิจ (วิสาหกิจขนาดกลางและขนาดย่อม) และหน่วยงานของรัฐสามารถเข้าถึงเทคโนโลยี ด้านความปลอดภัยเพื่อให้สามารถทำงานร่วมกันได้และยังให้ความสำคัญกับการเคารพในสิทธิขั้นพื้นฐาน รวมถึงสิทธิในความเป็นส่วนตัวด้วย นอกจากนี้ยังต้องการใช้ประโยชน์จากตลาดในโลกไซเบอร์ที่กำลังเฟื่องฟูอยู่ เพื่อให้สหภาพยุโรปมีส่วนแบ่งทางการตลาดในโลกไซเบอร์และส่งเสริม อุตสาหกรรมเกี่ยวกับความปลอดภัยในโลกไซเบอร์ของสหภาพยุโรป

---

[73] นันทวดี คาดคะเน (2561). *ปัญหาในการปราบปรามอาชญากรรมไซเบอร์ภายใต้กฎหมายระหว่างประเทศ*. มหาวิทยาลัยธรรมศาสตร์. หน้า 93.

[74] European Commission, 'The EU's Cybersecurity Strategy for the Digital Decade' (JOIN(2020) 18 final, 16 December 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN> accessed 27 June 2024.

3. การบูรณาการความปลอดภัยในโลกไซเบอร์ตามนโยบายของสหภาพยุโรป เป้าหมายของสหภาพยุโรปในเรื่องความมั่นคงปลอดภัย คือ การริเริ่มนโยบายใหม่ ๆ โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีใหม่และภาคอุตสาหกรรมที่เกิดขึ้นใหม่ เช่น Connected Car (รถยนต์อัจฉริยะที่มีการติดตั้งระบบเครือข่ายอินเทอร์เน็ตแบบไร้สาย) Smart grid (โครงข่ายไฟฟ้าอัจฉริยะ) และสิ่งต่างๆ ที่ถูกเชื่อมโยงเข้าด้วยกันในโลกของอินเทอร์เน็ต

สหภาพยุโรปมุ่งมั่นที่จะปกป้องสภาพแวดล้อมในโลกออนไลน์ให้มีเสรีภาพและความมั่นคงสูงสุดเท่าที่จะเป็นไปได้เพื่อประโยชน์ของทุกคน ยุทธศาสตร์นี้ได้รับการรับรองร่วมกัน โดยคณะกรรมาธิการและผู้แทนระดับสูง โดยมีเป้าหมายเพื่อให้แน่ใจว่าสหภาพยุโรปมีการคุ้มครอง ที่เข้มแข็ง มีประสิทธิภาพ และมีการส่งเสริมสิทธิของประชาชน เพื่อทำให้สภาพแวดล้อมในโลกออนไลน์ของสหภาพยุโรปปลอดภัยที่สุดในโลก ซึ่งการดำเนินการเหล่านี้รวมถึงการบรรลุขีดความสามารถด้านไซเบอร์ โดยการเพิ่มขีดความสามารถ การเตรียมความพร้อม ความร่วมมือ การแลกเปลี่ยนข้อมูลและการรักษาความปลอดภัยของข้อมูล สำหรับภาครัฐและเอกชนทั้งในระดับประเทศและในสหภาพยุโรป การลดอาชญากรรมร้ายแรงในโลกไซเบอร์ด้วยการเสริมสร้างความชำนาญของผู้ที่มีหน้าที่รับผิดชอบในการสืบสวน สอบสวน และฟ้องร้องดำเนินคดีโดยใช้แนวทางการประสานงานระหว่างหน่วยงานบังคับใช้กฎหมายทั่วสหภาพยุโรปและเสริมสร้างความร่วมมือกับหน่วยงานอื่น ๆ การพัฒนานโยบายและความสามารถในการป้องกันทางไซเบอร์ของสหภาพยุโรปภายใต้กรอบนโยบายด้านความมั่นคงและการป้องกันประเทศ อีกทั้งยังเพื่อเสริมสร้างนโยบายด้านไซเบอร์สเปซของสหภาพยุโรป เพื่อกำหนดบรรทัดฐานสำหรับความรับผิด เพื่อสนับสนุนการใช้กฎหมายระหว่างประเทศในโลกไซเบอร์ และเพื่อช่วยเหลือประเทศต่าง ๆ นอกสหภาพยุโรปในการพัฒนาความสามารถรักษาความปลอดภัยในโลกไซเบอร์[75]

3.1.2.2 อาเซียน

กลุ่มประเทศอาเซียน[76]นั้นมีความตื่นตัวในการต่อต้านอาชญากรรมข้ามชาติมาเป็นเวลากว่าทศวรรษแล้ว เนื่องจากอาชญากรรมข้ามชาตินั้นเป็นเรื่องที่ไม่ได้เกิดภายในขอบเขตของประเทศ

---

[75] European Commission, 'Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace' <https://bit.ly/2YrH1kl> accessed 24 April 2024.

[76] องค์กรที่ก่อตั้งขึ้นตามปฏิญญากรุงเทพ เมื่อวันที่ 8 สิงหาคม พ.ศ.2510 มีประเทศสมาชิกรวม 10 ประเทศ ได้แก่ ประเทศไทย ประเทศบรูไน ดารุสซาลาม ประเทศกัมพูชา ประทศอินโดนีเซีย ประเทศเวียดนาม ประเทศลาว ประเทศเมียนมา ประเทศฟิลิปปินส์ ประเทศสิงคโปร์ และประเทศมาเลเซีย โดยอาเซียนก่อตั้งขึ้นโดยมีวัตถุประสงค์เริ่มแรกเพื่อสร้างสันติภาพในภูมิภาคเอเชียตะวันออกเฉียงใต้อันนำมาซึ่งเสถียรภาพทางการเมืองและความเจริญก้าวหน้าทางเศรษฐกิจ สังคม และวัฒนธรรม ต่อมาเมื่อมีการค้าขายระหว่างประเทศในโลกมีแนวโน้มกีดกัน

ใดประเทศหนึ่ง อาเซียนได้มีการร่วมมือกันแก้ไขรวมถึงการพัฒนากลไกความร่วมมือต่าง ๆ เพื่อรับมือกับอาชญากรรมข้ามชาติที่พัฒนาตัวเองตามการเปลี่ยนแปลงของโลก ในปัจจุบันผู้เชี่ยวชาญด้านอาเซียนรวมถึงผู้ที่เกี่ยวข้องด้านความมั่นคงในอาเซียนได้แสวงหาปัจจัยที่จะชักจูงประเทศสมาชิกให้เข้ามาร่วมมือกัน หลายท่านได้ชี้ไปที่การหาภัยคุกคามต่อความมั่นคงร่วมกัน (Common Threat) โดยเฉพาะภัยด้านความมั่นคงนอกรูปแบบ (Non-Traditional Security) หวังว่าประเทศสมาชิกจะสามารถแสวงหาจุดร่วมได้จนเป็นจุดเริ่มต้นให้เกิดประชาคมการเมืองและความมั่นคงอาเซียนอย่างเป็นรูปธรรม โดยอาเซียนมีแผนการจัดตั้งประชาคมการเมืองและความมั่นคงอาเซียนเป็นการผสมผสานระหว่าง ASEAN Security Community Plan of Action และ Vientiane Action Programmer (VAP) รวมถึงงานในส่วนอื่น ๆ ที่เกี่ยวข้อง สำหรับเป้าหมายหลักของประชาคมการเมืองและความมั่นคงอาเซียน[77] ได้แก่

1. ประชาคมที่มีกติกาและมีการพัฒนาค่านิยมและบรรทัดฐานร่วมกัน ซึ่งเป็น 2 หลักการที่ถ่วงดุลซึ่งกันและกัน กล่าวคือ การไม่แทรกแซงกิจการภายในและการส่งเสริมค่านิยมของประชาคม

2. ประชาคมที่ทำให้ภูมิภาคมีความเป็นเอกภาพ มีความสงบสุข มีความแข็งแกร่ง พร้อมทั้งมีความรับผิดชอบ ร่วมกันเพื่อแก้ไขปัญหาความมั่นคงที่ครอบคลุมในทุกมิติ ซึ่งเป็นความพยายามที่จะส่งเสริมให้อาเซียนพึ่งพาอาศัยกลไกของตนมากขึ้นในการแก้ไขปัญหาและความท้าทายต่าง ๆ ในภูมิภาค

3. ประชาคมที่ทำให้เป็นภูมิภาคที่มีพลวัตและมองไปยังโลกภายนอกที่มีการรวมตัวและลักษณะพึ่งพาซึ่งกันและกันมากยิ่งขึ้น ซึ่งสะท้อนถึงการที่อาเซียนยอมรับว่าไม่ควรมุ่งเพียงเรื่องภายในแต่เน้นการสร้างหุ้นส่วนกับโลกภายนอกให้บรรลุเป้าหมายร่วมกัน[78]

ดังนั้น ภัยคุกคามต่อความมั่นคงนอกรูปแบบซึ่งรวมถึงอาชญากรรมข้ามชาติจึงเป็นส่วนหนึ่งของกุญแจสำคัญของ ประชาคมการเมืองและความมั่นคงอาเซียนใน ข้อ “การส่งเสริมให้เกิดภูมิภาคที่มีเสถียรภาพ ความสงบสุขและความเป็นอันหนึ่งอันเดียวกันโดยมีความรับผิดชอบทางด้าน

---

การค้ารุนแรงขึ้นทำให้อาเซียนหันมามุ่งกระชับและขยายความร่วมมือทางเศรษฐกิจมากขึ้นเพื่อประโยชน์ในการพัฒนาศักยภาพในการร่วมมือกับปัญหาและความท้าทายตลอดจนเพื่อสร้างความแข็งแกร่งและอำนาจต่อรองให้กับประเทศสมาชิก

[77] พรพล น้อยธรรมราช, ‘ประชาคมการเมืองและความมั่นคงอาเซียน 2015 กับทฤษฎีการรวมตัวเชิงภูมิภาค : กรณีศึกษา เรื่องอาชญากรรมข้ามชาติในอาเซียน’ <http://dtad.dti.or.th/index.php?option=com_content&view=article&id=244:asean2015&catid=6:analysis&Itemid=11> สืบค้นเมื่อ 28 มีนาคม 2567.

[78] เพิ่งอ้าง, 10.

ความมั่นคงในวงกว้างร่วมกัน” ซึ่งมีกิจกรรมหลักคือ เพิ่มความร่วมมือในการรับมือกับภัยความมั่นคงนอกรูปแบบต่าง ๆ โดยเฉพาะอย่างยิ่งการต่อสู้กับอาชญากรรมข้ามชาติและปัญหาข้ามพรมแดนอื่น ๆ ปัจจุบันนี้มีความซับซ้อนมากขึ้นกว่าเมื่อก่อนมาก เนื่องจากมีการพัฒนาด้านเทคโนโลยีและด้านการสื่อสารคมนาคม ทำให้อาชญากรรมข้ามชาติในปัจจุบันนั้นยกระดับเป็นปัญหาระดับโลก ยิ่งพฤติกรรมทาง เศรษฐกิจในปัจจุบันนั้นยกระดับจากเศรษฐกิจภายในประเทศเป็นเศรษฐกิจระดับภูมิภาคและระดับโลก ส่งผลให้เกิดการแก้กฎหมายหรือข้อบังคับต่าง ๆ ให้ผ่อนปรนมากขึ้นเพื่อเอื้อกับการค้าและแรงงานระหว่างประเทศ แต่ผลที่ตามมา คือ กลุ่ม อาชญากรรมข้ามชาตินั้นก็ได้ใช้ช่องว่างเหล่านี้แสวงหาผลประโยชน์และประกอบอาชญากรรม อาเซียนจึงได้มีความร่วมมือกันในทางอาญาระหว่างประเทศในระดับนโยบาย ดังนี้

1. การประชุมรัฐมนตรีอาเซียนด้านอาชญากรรมข้ามชาติ (ASEAN Ministerial Meeting on Transnational Crime - AMMTC) เป็นเวทีการหารือระดับรัฐมนตรีของประเทศสมาชิกอาเซียน ซึ่งมีหน้าที่กำกับดูแลนโยบายด้านความมั่นคงที่เกี่ยวข้องกับปัญหาอาชญากรรมข้ามชาติในภูมิภาค โดยการประชุมนี้จัดขึ้นตามมติของที่ประชุมสุดยอดอาเซียน (ASEAN Summit) อย่างเป็นทางการครั้งที่ 5 ซึ่งจัดขึ้นที่กรุงเทพมหานคร ประเทศไทย เมื่อปี พ.ศ. 2538 (ค.ศ. 1995) เพื่อจัดตั้งกลไกระดับภูมิภาคในการกำหนดทิศทางและเสริมสร้างความร่วมมือในการต่อต้านอาชญากรรมข้ามชาติ ซึ่งมีแนวโน้มทวีความรุนแรงและขยายตัวอย่างต่อเนื่อง การประชุม AMMTC จัดขึ้นเป็นประจำทุกสองปี โดยมีเป้าหมายเพื่อพิจารณาและประสานความร่วมมือเชิงนโยบายระหว่างประเทศสมาชิกอาเซียนในการป้องกันและปราบปรามอาชญากรรมข้ามชาติในมิติต่างๆ อาทิ การต่อต้านการก่อการร้าย การค้ามนุษย์ การลักลอบขนยาเสพติด การฟอกเงิน และอาชญากรรมทางเทคโนโลยีสารสนเทศ นอกจากนี้ ยังมีการประชุมร่วมกับประเทศคู่เจรจาของอาเซียนเพื่อแลกเปลี่ยนข้อมูลและแนวทางปฏิบัติที่ดีในการจัดการกับอาชญากรรมข้ามชาติอย่างมีประสิทธิภาพ

2. การประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ (ประเด็นเกี่ยวกับการจัดการปัญหาอาชญากรรมทางไซเบอร์ได้ถูกหยิบยกขึ้นหารือในเวทีการประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ (ASEAN Telecommunications and Information Technology Ministers Meeting: TELMIN) ซึ่งเป็นเวทีความร่วมมือระดับรัฐมนตรีของประเทศสมาชิกอาเซียนที่มีบทบาทสำคัญในการกำหนดทิศทางด้านนโยบายและความร่วมมือในด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ของภูมิภาค โดยเฉพาะในการประชุม TELMIN ครั้งที่ 14 ซึ่งจัดขึ้นเมื่อเดือนมกราคม พ.ศ. 2558 (ค.ศ. 1995) ที่ประชุมได้ให้ความเห็นชอบให้บรรจุประเด็นความมั่นคงทางไซเบอร์ (Cybersecurity) เป็นส่วนหนึ่งใน แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของอาเซียน ฉบับที่ 2 (ASEAN ICT Masterplan 2020) ซึ่งถือเป็นการยกระดับความสำคัญ

ของปัญหาอาชญากรรมไซเบอร์ในระดับนโยบายของภูมิภาค[79] แผนแม่บทดังกล่าวได้กำหนด “ยุทธศาสตร์ด้านความปลอดภัยและหลักประกันด้านข้อมูลข่าวสาร” (Strategic Thrusts on Information Security and Assurance) เป็นหนึ่งในหัวใจสำคัญของแผน โดยมีเป้าหมาย ดังนี้

1) พัฒนาแนวทางร่วมระดับภูมิภาคว่าด้วยหลักการด้านความปลอดภัยของข้อมูล (Regional Data Security Principles)

2) ส่งเสริมความเข้มแข็งของโครงสร้างพื้นฐานความมั่นคงไซเบอร์ในประเทศสมาชิก

3) เพิ่มประสิทธิภาพของความร่วมมือในการรับมือเหตุการณ์ฉุกเฉินด้านไซเบอร์ (Cyber Emergency Response Collaboration) ให้สามารถตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที

4) สร้างความเชื่อมั่นให้กับเศรษฐกิจดิจิทัลของอาเซียน เพื่อรองรับการเติบโตของภาคธุรกิจและการบริการที่ใช้เทคโนโลยีเป็นพื้นฐาน

การบรรจุความมั่นคงไซเบอร์ไว้ในแผนแม่บท ICT ฉบับใหม่นี้สะท้อนให้เห็นถึงความตระหนักของประเทศสมาชิกอาเซียนต่อความท้าทายที่มาพร้อมกับการพัฒนาดิจิทัล โดยเฉพาะการเพิ่มขึ้นของอาชญากรรมไซเบอร์ อาทิ การโจมตีข้อมูล การหลอกลวงผ่านระบบออนไลน์ และการละเมิดความเป็นส่วนตัว ซึ่งต้องอาศัยความร่วมมือในระดับภูมิภาคเพื่อรับมืออย่างมีประสิทธิภาพ

อีกทั้ง การป้องกันและปราบปรามอาชญากรรมข้ามชาติจำเป็นต้องอาศัยกลไกความร่วมมือที่มีประสิทธิภาพและต่อเนื่องระหว่างหน่วยงานด้านการบังคับใช้กฎหมายของประเทศต่าง ๆ ทั้งในระดับภูมิภาคและระดับนานาชาติ ความร่วมมือดังกล่าวไม่เพียงแต่ช่วยให้สามารถแลกเปลี่ยนข้อมูลข่าวสารและแนวทางการปฏิบัติงานได้อย่างทันท่วงทีเท่านั้น แต่ยังเป็นการเสริมสร้างขีดความสามารถในการรับมือกับภัยคุกคามที่มีลักษณะไร้พรมแดนซึ่งใช้เทคโนโลยีในการหลบเลี่ยงการบังคับใช้กฎหมายของรัฐแต่ละประเทศ กลไกในระดับปฏิบัติจึงกลายเป็นแนวหน้าสำคัญในการผลักดันการต่อต้านอาชญากรรมข้ามชาติให้เกิดผลอย่างเป็นรูปธรรม อาเซียนจึงได้มีความร่วมมือกันในทางอาญาระหว่างประเทศในระดับปฏิบัติ ดังนี้

1. การประชุมหัวหน้าตำรวจอาเซียน (ASEN Chiefs of Police Conference ASEANAPOL) เป็นกลไกความร่วมมือระหว่างองค์การตำรวจอาเซียนในระดับปฏิบัติ โดยเป็นผลมาจากความตระหนักถึงผลร้ายของอาชญากรรมข้ามชาติต่อการเติบโตและการพัฒนาในภูมิภาคและต่อ

---

[79] กองอาเซียน กรมอาเซียน, ‘การประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมือง และความมั่นคงในภูมิภาคเอเชีย - แปซิฟิก (ASEAN Regional Forum – ARF)’ <http://www.led.go.th/asean/pdf/4/4-3.pdf> สืบค้นเมื่อ 12 เมษายน 2567.

สังคมอาเซียนโดยรวม มีวัตถุประสงค์เพื่อสนับสนุนระเบียบและกฎหมายที่ใช้กลุ่มประเทศอาเซียน ส่งเสริมการพัฒนาและการดำเนินงานที่เป็นระบบในการบังคับใช้กฎหมายและการรักษาความสงบเรียบร้อย เสริมสร้างความร่วมมือร่วมใจ และความสามัคคีของตำรวจอาเซียนในการต่อต้านอาชญากรรมข้ามชาติ รวมถึงพัฒนาขีดความสามารถทั้งในระดับองค์กรและบุคลากร และเพื่อเสริมสร้างความสัมพันธ์ระหว่างองค์กรตำรวจในภูมิภาคอาเซียนให้แน่นมากยิ่งขึ้น ผลลัพธ์ที่ได้จากการประชุมอยู่ในรูปแบบแถลงการณ์ร่วมที่เป็นข้อเสนอแนะที่เกิดขึ้นจะเป็นเพียงกรอบนโยบายกว้าง ๆ และไม่มีพันธะผูกพันทางกฎหมาย แต่ในทางปฏิบัติแล้ว แถลงการณ์ดังกล่าวถือเป็นเจตจำนงร่วมของผู้นำองค์กรบังคับใช้กฎหมายหลักของแต่ละประเทศที่จะต้องใช้ความพยายามอย่างสุดความสามารถในอันที่จะปฏิบัติตามให้ได้[80]

2. การประสานความร่วมมือทางอาญาผ่านองค์การตำรวจอาชญากรรมระหว่างประเทศ (International Criminal Police Organization - INTERPOL) หรือเรียกทั่วไปว่า องค์การตำรวจสากล ซึ่งเป็นองค์การระหว่างประเทศที่เป็นหน่วยประสานงานกลางในการแลกเปลี่ยนข้อมูลการสืบสวนสอบสวนคดีอาชญากรรมระหว่างประเทศ และช่วยเหลือกันในการติดตามจับกุมผู้กระทำผิดมาลงโทษ[81] ผ่านช่องทางตำรวจสากล คือ ระบบข้อมูลข่าวสารตลอด 24 ชั่วโมง (1-24/7) ซึ่งเป็นการส่งและรับข้อมูลผ่านแหล่งข้อมูลกลาง (server) ของตำรวจสากลที่มีสำนักงานใหญ่อยู่ที่ประเทศฝรั่งเศสสำหรับแลกเปลี่ยนข้อมูลทางอาชญากรรมระหว่างกันเพื่อประโยชน์ในการสืบสวน สอบสวนคดีอาชญากรรมข้ามชาติหรือคดีที่อาชญากรหลบหนีไปต่างประเทศในลักษณะต่าง ๆ ในรูปแบบของ

---

[80] ชิตพล กาญจนกิจ, ‘ความร่วมมือระหว่างประเทศว่าด้วยกระบวนการยุติธรรมทางอาญาอาเซียน: ข้อเสนอเชิงยุทธศาสตร์เพื่อการเตรียมความพร้อมเข้าสู่ประชาคมอาเซียน,’ NIDA Development Journal ปีที่ 56, ฉบับที่ 3 (2559) 1–32.

[81] องค์การตำรวจสากล ก่อตั้งขึ้นเป็นครั้งแรกที่ประเทศโมนาโค ในปี 1914 ปัจจุบันมีประเทศสมาชิกรวม 190 ประเทศ สำนักงานเลขาธิการองค์การตำรวจสากล ตั้งอยู่ที่เมือง Lyon ประเทศฝรั่งเศส มีวัตถุประสงค์เพื่อทำหน้าที่ประสาน งานและติดต่อแลกเปลี่ยนข้อสนเทศหรือข้อมูลเกี่ยวกับอาชญากรรมต่อองค์การตำรวจสากล หรือต่อสำนักงานกลาง แห่งชาติ (National Central Bureau; NCB) ซึ่งเป็นกลไกของประเทศสมาชิกที่สำคัญในการดำเนินงานประสาน การติดต่อระหว่างประเทศสมาชิกด้วยกัน โดยองค์การตำรวจสากลจะมีบทบาทในการเป็นช่องทางการติดต่อ ประสานความร่วมมือกับระหว่างประเทศสมาชิกผ่านระบบเทคโนโลยีสมัยใหม่ในการต่อสู้กับอาชญากรรมและ อาชญากรรมข้ามชาติในศตวรรษที่ 21 โดยคดีสำคัญหลัก ๆ ที่เป็นเป้าหมายของตำรวจสากล ได้แก่ การก่อ การร้าย การค้ามนุษย์ ยาเสพติดให้โทษ การลักลอบขนคนผิดกฎหมาย อาชญากรรมทางการเงิน อาชญากรรม คอมพิวเตอร์ การลักลอบขนสินค้าผิดกฎหมาย โจรสลัด การลักขโมยวัตถุโบราณ การลักลอบขนยาผิดกฎหมาย อาชญากรรมองค์กร นักโทษหลบหนี และอาชญากรสงคราม เป็นต้น: โปรดดู, INTERPOL, ‘About INTERPOL: Overview,’ http://www.interpol.int/About-INTERPOL/Overview accessed 18 May 2024.

หมายตำรวจสากล (INTERPOL Notices) 8 ประเภท[82] ตามลักษณะของประเภทคดีและคำร้องขอความร่วมมือที่กำหนดไว้ตามระเบียบการใช้หมายตำรวจสากล เช่น หมายสีแดงใช้สำหรับการติดตามบุคคลที่เป็นที่ต้องการตัวเพื่อส่งกลับไปดำเนินคดีหรือรับโทษทางอาญาในประเทศผู้ร้องขอหรือหมายสีดำใช้สำหรับติดตามบุคคลสูญหาย เป็นต้น เพื่อให้ประเทศสมาชิกตำรวจสากลช่วยเหลือในการสืบสวนสอบสวนและติดตามอาชญากรข้ามชาติที่หลบหนีจากประเทศหนึ่งเข้าไปในอีกประเทศหนึ่ง[83] คดีอาชญากรรมสำคัญที่น่าสนใจ ได้แก่ การก่อการร้าย การค้ามนุษย์ การค้ายาเสพติดการลักลอบขนคนผิดกฎหมาย อาชญากรรมทางการเงิน อาชญากรรมคอมพิวเตอร์ การลักลอบ ขนสินค้าผิดกฎหมาย การลักขโมยวัตถุโบราณ การลักลอบขนยาผิดกฎหมาย อาชญากรรมองค์กร ตลอดจนการติดตามบุคคลหลบหนีการดำเนินคดีอาญาและคำพิพากษาและอาชญากรสงคราม เป็นต้น

อีกทั้งอาเซียนในฐานะองค์กรความร่วมมือระดับภูมิภาคได้ตระหนักถึงความท้าทายจากอาชญากรรมข้ามชาติที่ส่งผลกระทบต่อเสถียรภาพ ความมั่นคง และเศรษฐกิจของภูมิภาค ภายใต้บริบทดังกล่าวอาเซียนได้จัดทำกรอบความร่วมมือเพื่อรับมืออาชญากรรมข้ามชาติ ได้แก่

แผนปฏิบัติการอาเซียนว่าด้วยการต่อต้านอาชญากรรมข้ามชาติ พ.ศ. 2559–2570 (ASEAN Plan of Action to Combat Transnational Crime: POA 2016–2025) ซึ่งถือเป็นกลไกที่เสริมสร้างและพัฒนาจาก *ASEAN Plan of Action to Combat Transnational Crime (2002)* โดยมีจุดมุ่งหมายหลักในการสร้างความร่วมมืออย่างเป็นระบบระหว่างประเทศสมาชิกในการป้องกันและปราบปรามอาชญากรรมข้ามชาติในทุกรูปแบบ และมีเป้าหมายในการสร้างเครือข่ายข้อมูล การ

---

[82] หมายตำรวจสากล (INTERPOL, Notices) เป็นคำร้องขอความร่วมมือ หรือการแจ้งเตือนระหว่างประเทศซึ่งอนุญาตให้ตำรวจของประเทศสมาชิกแบ่งปันข้อมูลข่าวสารสำคัญระหว่างกัน ได้ถูกจัดทำและเผยแพร่โดยสำนักงานเลขาธิการตำรวจสากลตามคำร้องขอของสำนักงานกลางแห่งชาติหรือหน่วยงานที่ได้รับมอบหมายของประเทศสมาชิก ซึ่งจะเผยแพร่ด้วยภาษาทางการ 4 ภาษา ได้แก่ อารบิค, อังกฤษ, ฝรั่งเศส, และสเปน โดยแบ่งหมายออกเป็น 8 ลักษณะ ประกอบด้วย หมายสีแดง หมายสีค่า หมายสีส้ม หมายสีฟ้า หมายสีเหลือง หมายสีเขียว หมายสีม่วง และหมายสีขาว: โปรดดู, INTERPOL, 'INTERPOL Notices', <http://www.interpol.int/INTERPOL-expertise/Notices> accessed 18 May 2024.

[83] ตัวอย่างความร่วมมือที่น่าสนใจ เช่น การประสานงานของตำรวจสากลในการจับกุมนายไบรอัน สมิธ บุคคล ที่เป็นที่ต้องการตัวตามหมายแดงตำรวจสากล และเป็นผู้ต้องหาตามหมายจับของสำนักงานสืบสวนกลาง สหรัฐอเมริกา (เอฟไอ) ในข้อหาล่วงละเมิดทางเพศเด็กและข่มขืนผู้หญิงในปี พ.ศ. 2532 ในลาสเวกัส และได้หลบหนีมาซ่อนตัวอยู่ในพื้นที่ จ.น่าน เป็นครูสอนพิเศษวิชาภาษาอังกฤษให้กับเด็กนักเรียนในโรงเรียน บ้านปรางค์ ต.บ้านปรางค์ อ.ปัว จ.น่าน โดยหลังจากแจ้งข้อหาตำรวจสากลได้ควบคุมตัวไปดำเนินการเพื่อส่งไป ดำเนินคดีที่ประเทศสหรัฐอเมริกาตามข้อตกลงเรื่องส่งผู้ร้ายข้ามแดนต่อไป เป็นต้น (ข้อมูลจากฝ่ายตำรวจสากลและ ประสานงานภูมิภาค 3 กองการต่างประเทศ สำนักงานตำรวจแห่งชาติ)

บังคับใช้กฎหมาย การฝึกอบรม และการวางมาตรการทางกฎหมายร่วมกันในระยะยาว สาระสำคัญของแผนปฏิบัติการนี้แบ่งออกเป็น 8 สาขาอาชญากรรม ได้แก่ (1) การก่อการร้าย (2) การค้ายาเสพติด (3) การค้ามนุษย์ (4) การลักลอบขนคนข้ามแดน (5) การค้าสัตว์ป่า (6) การค้ายาเสพติดผิดกฎหมาย (7) การฟอกเงิน และ (8) อาชญากรรมทางไซเบอร์ ถือเป็นหนึ่งในสาขาที่อาเซียนเน้นย้ำว่าจะต้องมีการพัฒนากลไกความร่วมมืออย่างเร่งด่วน ในแผนปฏิบัติการดังกล่าว อาเซียนได้กำหนดเป้าหมายเชิงกลยุทธ์ (Strategic Goals) ซึ่งเกี่ยวข้องกับอาชญากรรมไซเบอร์ไว้โดยเฉพาะ เช่น การพัฒนาโครงสร้างพื้นฐานดิจิทัลเพื่อสนับสนุนการแลกเปลี่ยนข้อมูลระหว่างกัน การสร้างศูนย์ความเชี่ยวชาญในภูมิภาค และการส่งเสริมให้ประเทศสมาชิกมีกฎหมายที่ทันสมัยและสอดคล้องกับมาตรฐานสากล[3] นอกจากนี้ แผนปฏิบัติการยังเรียกร้องให้รัฐสมาชิกพัฒนา “National Action Plan” ของตนเองที่สอดคล้องกับกรอบภูมิภาค ซึ่งจะช่วยเสริมความสามารถในการป้องกัน ตรวจจับและตอบโต้การกระทำผิดที่ข้ามพรมแดน[84]

นอกจากนี้ในกรณีแก๊งคอลเซ็นเตอร์ที่เป็นอาชญากรรมข้ามชาติโดยมีการอาศัยเทคโนโลยีสารสนเทศเป็นเครื่องมือก่ออาชญากรรม โดยเฉพาะในรูปแบบของแก๊งคอลเซ็นเตอร์กำลังกลายเป็นภัยคุกคามสำคัญที่ท้าทายความมั่นคงในภูมิภาคเอเชียตะวันออกเฉียงใต้ การหลอกลวงประชาชนผ่านระบบโทรศัพท์และอินเทอร์เน็ตโดยกลุ่มอาชญากรข้ามชาติได้สร้างความเสียหายทางเศรษฐกิจและบั่นทอนความเชื่อมั่นในระบบดิจิทัลของภูมิภาค ด้วยเหตุนี้ สมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ (ASEAN) จึงได้กำหนด

ยุทธศาสตร์และแผนความร่วมมือด้านความมั่นคงทางไซเบอร์ (ASEAN Cybersecurity Cooperation Strategy: ACCS) เป็นกรอบนโยบายระดับภูมิภาคที่มีวัตถุประสงค์เพื่อเสริมสร้างความมั่นคงทางไซเบอร์ในอาเซียน โดยมีเป้าหมายหลักในการสนับสนุนการจัดตั้งระเบียบสากลที่มีพื้นฐานบนกฎหมายสำหรับไซเบอร์สเปซที่เปิดกว้าง ปลอดภัย มีเสถียรภาพ เข้าถึงได้ และสันติภาพ ผ่านการนำแนวปฏิบัติของรัฐที่มีความรับผิดชอบ การสร้างความเชื่อมั่น และการพัฒนาศักยภาพร่วมกันในระดับภูมิภาคและพันธมิตรของอาเซียน ซึ่งมีเป้าหมายหลัก 5 ประการ ที่เป็นกลไกขับเคลื่อนหลักของความร่วมมือระหว่างประเทศสมาชิก ได้แก่

1) การเสริมสร้างความพร้อมด้านไซเบอร์ในยุทธศาสตร์นี้ อาเซียนให้ความสำคัญกับการสร้างความสามารถในการเตรียมความพร้อมและตอบสนองต่อภัยคุกคามทางไซเบอร์ในระดับภูมิภาค โดยเน้นการพัฒนาและเสริมความเข้มแข็งของหน่วยงานรับมือภัยไซเบอร์ (Computer Emergency Response Teams: CERTs) ของแต่ละประเทศสมาชิก พร้อมทั้งส่งเสริม

---

[84] ASEAN Secretariat, ASEAN Plan of Action to Combat Transnational Crime (2016–2025) (Jakarta: ASEAN Secretariat, 2016) 2.

การทำงานร่วมกันในรูปแบบเครือข่าย เช่น การแลกเปลี่ยนข้อมูลภัยคุกคาม การซักซ้อมแผนรับมือภัยคุกคามข้ามพรมแดน และการพัฒนาชุดเครื่องมือมาตรฐานสำหรับการตอบโต้ภัยคุกคามไซเบอร์ นอกจากนี้ ยังมีเป้าหมายระยะยาว คือ การจัดตั้ง CERT ระดับภูมิภาค (ASEAN Regional CERT) เพื่อเป็นกลไกกลางในการประสานและบริหารจัดการเหตุการณ์ทางไซเบอร์ที่ส่งผลกระทบข้ามพรมแดน ซึ่งจะช่วยลดเวลาการตอบสนองและเพิ่มประสิทธิภาพการฟื้นฟูระบบที่ถูกโจมตีได้อย่างทันท่วงที

2) การประสานนโยบายไซเบอร์ระดับภูมิภาค เพื่อหลีกเลี่ยงความแตกต่างของกฎหมาย มาตรฐาน และแนวทางปฏิบัติของแต่ละประเทศ อาเซียนได้เสนอให้มีการประสานนโยบายด้านไซเบอร์ในระดับภูมิภาค โดยมีการจัดตั้ง คณะกรรมการประสานงานด้านความมั่นคงทางไซเบอร์ของอาเซียน (Cybersecurity Coordination Committee: Cyber-CC) ซึ่งทำหน้าที่กำหนดนโยบายร่วม วางทิศทางการดำเนินการ และติดตามความคืบหน้าในการดำเนินยุทธศาสตร์นี้อย่างใกล้ชิด การมี Cyber-CC ยังช่วยเสริมบทบาทของอาเซียนในการกำหนดจุดยืนร่วมในเวทีความร่วมมือระหว่างประเทศ เช่น สหประชาชาติ โดยเฉพาะในประเด็นที่เกี่ยวกับการกำกับดูแลไซเบอร์สเปซ กฎหมายไซเบอร์ และจริยธรรมดิจิทัล

3) การเสริมสร้างความเชื่อมั่นในโลกไซเบอร์ หนึ่งในความท้าทายของภูมิภาคอาเซียน คือความไม่ไว้วางใจระหว่างประเทศสมาชิกในกรณีที่เกิดภัยคุกคามหรือปฏิบัติการทางไซเบอร์ที่ส่งผลกระทบข้ามพรมแดน ยุทธศาสตร์ ACCS จึงเสนอให้พัฒนากลไก มาตรการสร้างความเชื่อมั่น (Confidence-Building Measures: CBMs) ซึ่งรวมถึงการแจ้งเตือนภัยล่วงหน้า การแลกเปลี่ยนข้อมูลภัยคุกคามแบบไม่เปิดเผยตัวตน การซักซ้อมเหตุการณ์ร่วม และการส่งเสริมความโปร่งใสผ่านรายงานประจำปีของอาเซียนเกี่ยวกับภัยไซเบอร์ อาเซียนยังสนับสนุนให้มีการบูรณาการแนวทางของคณะทำงานสหประชาชาติว่าด้วยพฤติกรรมของรัฐในไซเบอร์สเปซ (UN GGE and OEWG norms) มาใช้เป็นพื้นฐานสำหรับการสร้างบรรทัดฐานในระดับภูมิภาค

4) การพัฒนาศักยภาพระดับภูมิภาค อาเซียนมุ่งเน้นการยกระดับขีดความสามารถของประเทศสมาชิก โดยเฉพาะในประเทศที่ยังขาดโครงสร้างพื้นฐานด้านความมั่นคงทางไซเบอร์ผ่านโครงการฝึกอบรม กิจกรรมแลกเปลี่ยนบุคลากร การฝึกซ้อมจำลองเหตุการณ์ไซเบอร์ (Cyber Drills) และการส่งเสริมการวิจัยและพัฒนาด้านความมั่นคงทางดิจิทัล มีการจัดตั้งศูนย์ความเป็นเลิศอาเซียนด้านไซเบอร์ (ASEAN-Singapore Cybersecurity Centre of Excellence: ASCCE) ในประเทศสิงคโปร์เป็นศูนย์กลางในการฝึกอบรมผู้ปฏิบัติงาน เจ้าหน้าที่ด้านนโยบายและหน่วยบังคับใช้กฎหมายให้สามารถรับมือกับภัยคุกคามยุคใหม่

5) ความร่วมมือระหว่างประเทศ เน้นการสร้างความร่วมมือกับภาคีระหว่างประเทศทั้งในระดับทวิภาคีและพหุภาคี โดยอาเซียนมีเป้าหมายที่จะเป็น “ผู้เล่นเชิงรุก” ในเวทีความมั่นคงไซเบอร์ระดับโลก เช่น การมีส่วนร่วมกับองค์กรอย่าง UN, ITU, INTERPOL และ OSCE รวมถึงการพัฒนาแนวปฏิบัติร่วมกับพันธมิตรอย่าง สหภาพยุโรป สหรัฐอเมริกา ญี่ปุ่น ออสเตรเลีย และเกาหลีใต้ ความร่วมมือเหล่านี้เน้นไปที่การถ่ายทอดความรู้ การใช้เครื่องมือและเทคโนโลยีร่วมกัน การสนับสนุนด้านการเงินและเทคนิค เพื่อขับเคลื่อนนโยบายไซเบอร์ของอาเซียนให้มีมาตรฐานสากล

**3.1.3 ระดับประเทศ**

3.1.3.1 ประเทศไทย

แก๊งคอลเซ็นเตอร์ได้เข้ามามีบทบาทและสร้างผลกระทบอย่างมีนัยสำคัญต่อเศรษฐกิจของประเทศไทย โดยเฉพาะในด้านความสูญเสียทางการเงินจากการหลอกลวงประชาชนผ่านช่องทางโทรคมนาคม อันเป็นรูปแบบของอาชญากรรมทางเทคโนโลยีที่ขยายตัวอย่างรวดเร็ว ส่งผลให้เกิดความเดือดร้อนและความไม่มั่นคงในสังคมอย่างกว้างขวาง การระบาดของอาชญากรรมประเภทนี้ไม่เพียงแต่สร้างความรำคาญให้แก่ประชาชนเท่านั้น หากแต่ยังก่อให้เกิดความเสียหายต่อระบบเศรษฐกิจโดยรวมในรูปแบบของการสูญเสียทรัพย์สินและความเชื่อมั่นของประชาชนต่อระบบดิจิทัลของรัฐ ด้วยเหตุนี้ สำนักงานตำรวจแห่งชาติในฐานะหน่วยงานหลักด้านการบังคับใช้กฎหมายจึงได้ดำเนินการเชิญหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้องเข้าร่วมประชุมเพื่อพิจารณาแนวทางในการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์ โดยมีหน่วยงานหลักในภาครัฐคือ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ร่วมกับหน่วยงานรัฐอื่น ๆ ที่มีหน้าที่กำกับดูแลด้านความมั่นคงทางไซเบอร์และการคุ้มครองผู้บริโภค รวมถึงภาคเอกชนที่เป็นผู้ให้บริการโทรคมนาคม เพื่อหาแนวทางการป้องกันและรับมือกับปัญหาอาชญากรรมข้ามชาติรูปแบบใหม่นี้อย่างเป็นระบบ[85]

หน่วยงานภาครัฐที่เข้ามามีบทบาทและเกี่ยวข้องกับเรื่องแก๊งคอลเซ็นเตอร์มีด้วยกันหลายหน่วยงาน ซึ่งแต่ละหน่วยงานจะมีหน้าที่ที่เป็นอิสระต่อกันโดยมีหน่วยงานที่สำคัญ ดังนี้

1. สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช) ซึ่งเป็นองค์กรอิสระภายใต้รัฐธรรมนูญมีหน้าที่ในการกำกับดูแลกิจการโทรคมนาคมของประเทศให้เป็นไปตามหลักเกณฑ์แห่งความมั่นคง ความเป็นธรรม และการคุ้มครองผู้บริโภค โดยเฉพาะในด้านการควบคุมหมายเลขโทรศัพท์และโครงข่ายสื่อสารที่มักถูกนำมาใช้เป็น

---

[85] ขวัญชนก ศรีภมร, ‘แนวทางการป้องกันอาชญากรรมที่เกิดจากแก๊งคอลเซ็นเตอร์ออนไลน์โดยมาตรการกำกับดูแลของอุตสาหกรรมโทรคมนาคม’ (วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต, คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย 2565) 31–34.

เครื่องมือในการกระทำความผิดโดยแก๊งคอลเซ็นเตอร์ โดยบทบาทของ กสทช. ในการจัดการกับปัญหาแก๊งคอลเซ็นเตอร์มีความเชื่อมโยงโดยตรงกับอาชญากรรมข้ามชาติในรูปแบบที่ใช้เทคโนโลยีเป็นเครื่องมือ เช่น การใช้ หมายเลขโทรศัพท์ปลอม การเช่าหมายเลขแบบชั่วคราว หรือการใช้ระบบ VoIP เพื่อโทรหลอกลวงจากต่างประเทศมาประเทศไทยโดยไม่สามารถระบุตัวตนได้ กสทช. จึงมีอำนาจในการ กำกับดูแลการจัดสรรเลขหมายโทรศัพท์ การออกใบอนุญาตประกอบกิจการโทรคมนาคม และการควบคุมโครงข่ายสื่อสารทั้งในระดับประเทศและระหว่างประเทศ อันเป็นกลไกสำคัญในการจำกัดช่องทางที่แก๊งคอลเซ็นเตอร์ใช้ในการเข้าถึงเหยื่อ

2. สำนักงานตำรวจแห่งชาติ เป็นหน่วยงานหลักที่มีอำนาจหน้าที่ในการรับแจ้งความร้องทุกข์และดำเนินการสืบสวนสอบสวนเกี่ยวกับอาชญากรรมต่าง ๆ รวมถึงอาชญากรรมจากแก๊งคอลเซ็นเตอร์ โดยมีบทบาทในการรวบรวมพยานหลักฐาน ตรวจสอบข้อมูล และดำเนินคดีตามกฎหมายที่เกี่ยวข้อง ทั้งนี้ เพื่อให้การให้บริการประชาชนเป็นไปอย่างทั่วถึงและสะดวกรวดเร็ว สำนักงานตำรวจแห่งชาติได้พัฒนาระบบการแจ้งความผ่านช่องทางออนไลน์ผ่านเว็บไซต์ ซึ่งเปิดให้บริการตลอด 24 ชั่วโมง ระบบดังกล่าวเป็นช่องทางให้ประชาชนสามารถแจ้งเบาะแสหรือร้องเรียนกรณีที่ตกเป็นเหยื่อของอาชญากรรมคอลเซ็นเตอร์ได้โดยไม่จำเป็นต้องเดินทางไปยังสถานีตำรวจ นอกจากนี้ ยังมีการจัดทำคู่มือการใช้งาน และเบอร์สายด่วน “1441” เพื่อให้คำปรึกษาและรับเรื่องร้องเรียนเกี่ยวกับการหลอกลวงผ่านโทรศัพท์หรือระบบอิเล็กทรอนิกส์ โดยเจ้าหน้าที่จะให้บริการข้อมูลอย่างต่อเนื่องตลอดทั้งวัน[86]

3. กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บช.สอท) เป็นหน่วยงานเฉพาะทางภายใต้สำนักงานตำรวจแห่งชาติ มีหน้าที่รับผิดชอบหลักในการสืบสวนและปราบปรามอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ มีบทบาทสำคัญในการเผยแพร่ข้อมูลข่าวสาร ความรู้ และคำเตือนภัยเกี่ยวกับภัยคุกคามทางไซเบอร์ต่อประชาชน เพื่อส่งเสริมการรับรู้และการป้องกันตัวจากอาชญากรรมดิจิทัลในวงกว้าง ถือเป็นการวางรากฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศ[87]

4. กองการต่างประเทศสำนักงานตำรวจแห่งชาติ เป็นหน่วยงานภายใต้สำนักงานตำรวจแห่งชาติที่มีบทบาทสำคัญในการดำเนินความร่วมมือระหว่างประเทศในด้านการบังคับใช้

---

[86] ผู้จัดการออนไลน์, ‘เปิดขั้นตอนแจ้งความออนไลน์ thaipoliceonline.com รับเฉพาะคดีอาชญากรรมทางเทคโนโลยี’< https://mgronline.com/onlinesection/detail/9650000021035> สืบค้นเมื่อ 24 เมษายน 2567.

[87] สุภาพิชญ์ ถิระวัฒน์, ‘กองบัญชาการตำรวจไซเบอร์’ <https://library.parliament.go.th/th/radioscript-rr2564-nov1> สืบค้นเมื่อ 24 เมษายน 2567.

กฎหมาย โดยเฉพาะอย่างยิ่งในบริบทของอาชญากรรมข้ามชาติ ซึ่งมีลักษณะการกระทำผิดที่เชื่อมโยงกับหลายประเทศ กองการต่างประเทศทำหน้าที่เป็นจุดประสานงานกลางกับองค์กรตำรวจระหว่างประเทศ เช่น INTERPOL, ASEANAPOL และหน่วยงานผู้บังคับใช้กฎหมายในประเทศอื่น ๆ[88]

5. ธนาคารแห่งประเทศไทย (ธปท.) ในฐานะหน่วยงานกำกับดูแลระบบสถาบันการเงินของประเทศ มีบทบาทสำคัญในการวางแนวทางและกำหนดมาตรการในการป้องกันและปราบปรามการใช้บัญชีธนาคารในทางมิชอบหรือที่เรียกว่าบัญชีม้าซึ่งเป็นบัญชีธนาคารที่บุคคลทั่วไปยินยอมหรือถูกหลอกให้นำไปใช้รับโอนเงินที่ได้มาจากการกระทำความผิด[89] ในเชิงนโยบาย ธปท. ได้ร่วมมือกับหน่วยงานด้านความมั่นคงและสมาคมธนาคารไทยในการพัฒนาแนวทางกลางในการระงับบัญชีต้องสงสัย การแลกเปลี่ยนข้อมูลข้ามธนาคาร รวมถึงการรณรงค์ประชาสัมพันธ์ให้ประชาชนตระหนักถึงความเสี่ยงจากการขายหรือให้ใช้บัญชีธนาคาร โดยมีบทลงโทษทางอาญากับเจ้าของบัญชีที่เกี่ยวข้องกับการกระทำผิด

6. สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ภายใต้การกำกับดูแลของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) มีอำนาจหน้าที่ในการส่งเสริม ควบคุม และกำกับให้มีการดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของหน่วยงานทั้งภาครัฐและภาคเอกชนให้เป็นไปตามที่กฎหมายกำหนดในบริบทของการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์ สำนักงานฯ มีบทบาทในการคุ้มครองข้อมูลของประชาชนจากการถูกนำไปใช้ในทางที่ผิด โดยเฉพาะการนำข้อมูลส่วนบุคคล เช่น หมายเลขโทรศัพท์ เลขประจำตัวประชาชน เลขบัญชีธนาคาร หรือข้อมูลทางดิจิทัลอื่น ๆ ไปใช้ในการหลอกลวงหรือปลอมแปลงตัวตน สำนักงานฯ ยังมีอำนาจในการออกระเบียบหรือแนวทางปฏิบัติเพื่อให้หน่วยงานและผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามหลักความปลอดภัยของข้อมูล (data security) และการแจ้งเหตุละเมิดข้อมูลแก่เจ้าของข้อมูลภายในระยะเวลาที่กฎหมายกำหนด เพื่อให้เกิดการแจ้งเตือนล่วงหน้าและการตอบสนองต่อภัยคุกคามจากอาชญากรรมไซเบอร์อย่างมีประสิทธิภาพ[90]

---

[88] กองการต่างประเทศ สำนักงานตำรวจแห่งชาติ, ‘ภารกิจหน้าที่’ [ออนไลน์], <https://foreign.police.go.th/about-us/>, สืบค้นเมื่อ 18 เมษายน 2567.

[89] พิมพ์ธัญญา ฆ้องเสนาะ, ‘บัญชีม้า’ <https://library.parliament.go.th/th/radioscript/rr2565-may6> สืบค้นเมื่อ 24 เมษายน 2567.

[90] ไทยรัฐออนไลน์, ‘หวัง PDPA ลดแก๊งคอลเซ็นเตอร์’ <https://www.thairath.co.th/business/economics/2429726> สืบค้นเมื่อ 24 เมษายน 2567.

7. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หน้าที่หลัก คือ เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

8. กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี[91] (บก.ปอท.) เป็นหน่วยงานภายใต้สังกัด กองบัญชาการตำรวจสอบสวนกลาง (บช.ก.) มีอำนาจหน้าที่ในการสืบสวน สอบสวน และดำเนินคดีกับผู้กระทำความผิดที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศหรือโครงข่ายอินเทอร์เน็ตเป็นเครื่องมือในการกระทำความผิดทางอาญา โดยเฉพาะอย่างยิ่งความผิดที่เกี่ยวข้องกับ เนื้อหาบนโลกออนไลน์ เช่น ความผิดเกี่ยวกับการหมิ่นประมาทผ่านระบบคอมพิวเตอร์ การเผยแพร่ข้อมูลลามกอนาจาร การหลอกลวงประชาชนผ่านแพลตฟอร์มออนไลน์ ตลอดจนความผิดที่กระทบต่อความมั่นคงภายในราชอาณาจักรที่มีลักษณะของการกระทำผ่านระบบเทคโนโลยี หน้าที่หลักของ บก.ปอท. ประกอบด้วย (1) รับแจ้งความร้องทุกข์จากประชาชนที่ตกเป็นเหยื่อของอาชญากรรมทางเทคโนโลยี (2) ตรวจสอบและเก็บพยานหลักฐานทางดิจิทัล (digital evidence) เพื่อนำมาใช้ในการดำเนินคดี (3) ประสานงานกับหน่วยงานที่เกี่ยวข้อง ทั้งในและต่างประเทศ เพื่อการปราบปรามอาชญากรรมไซเบอร์ และ (4) รณรงค์เผยแพร่ความรู้เพื่อป้องกันมิให้ประชาชนตกเป็นเหยื่อของการกระทำความผิดผ่านระบบเทคโนโลยี[92]

9. กองบัญชาการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) เป็นหน่วยงานระดับกองบัญชาการภายใต้สำนักงานตำรวจแห่งชาติ ซึ่งจัดตั้งขึ้นโดยคำสั่งสำนักงานตำรวจแห่งชาติ ที่ 46/2564 ลงวันที่ 9 กุมภาพันธ์ 2564 เพื่อเป็นกลไกหลักในการรับมือกับอาชญากรรมทางเทคโนโลยีที่มีแนวโน้มเพิ่มสูงขึ้นและมีลักษณะซับซ้อนมากยิ่งขึ้น โดยเฉพาะในระดับข้ามพรมแดน บทบาทของ บช.สอท. มีลักษณะ เชิงยุทธศาสตร์ และ เชิงปฏิบัติการระดับสูง โดยเฉพาะอย่างยิ่งในคดีที่เกี่ยวข้องกับอาชญากรรมข้ามชาติ เช่น แก๊งคอลเซ็นเตอร์, การหลอกลวงทางการเงินออนไลน์, การฟอกเงินผ่านช่องทางดิจิทัล, และ การละเมิดข้อมูลส่วนบุคคล บช.สอท. ทำหน้าที่เป็นตัวกลางในการประสานงานกับหน่วยงานบังคับใช้กฎหมายในต่างประเทศ ทั้งผ่านกลไกความร่วมมือทวิภาคีและพหุภาคี[93]

---

[91] กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี, ‘หน้าที่และภารกิจ,’ <https://www.tcybercrime.police.go.th> สืบค้นเมื่อ 28 มิถุนายน 2568.

[92] กองบัญชาการสอบสวนกลาง, ‘กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี,’ <https://www.cib.go.th/organization/technologycrime> สืบค้นเมื่อ 28 มิถุนายน 2568.

[93] สำนักงานตำรวจแห่งชาติ, ‘คำสั่งสำนักงานตำรวจแห่งชาติ ที่ 46/2564 เรื่อง “การจัดตั้งกองบัญชาการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี”’ (2564) <https://www.royalthaipolice.go.th> สืบค้นเมื่อ 22 มิถุนายน 2568.

10. ศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (AOC) โดยมติของคณะรัฐมนตรีเมื่อเดือนพฤศจิกายน พ.ศ. 2565 เพื่อทำหน้าที่เป็น “ศูนย์บัญชาการร่วม” ที่มีบทบาทในการประสานงานระหว่างหน่วยงานที่เกี่ยวข้องทั้งหมด ได้แก่ สำนักงานตำรวจแห่งชาติ ธนาคารแห่งประเทศไทย คณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กสทช.) สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) และภาคเอกชน เช่น ธนาคารพาณิชย์ และผู้ให้บริการโทรคมนาคม โดยมีเป้าหมายในการเร่งรัดกระบวนการระงับความเสียหายเชิงรุก เช่น การอายัดบัญชีหรือปิดซิมที่ต้องสงสัยในระยะเวลาไม่เกิน 24 ชั่วโมง

นโยบายในการป้องกันและปราปรามแก๊งคอลเซ็นเตอร์ของประเทศไทย

จากสถานการณ์แก๊งคอลเซ็นเตอร์ระบาดในประเทศไทยได้สร้างความตื่นตัวให้กับภาครัฐรวมไปถึงภาคเอกชนอย่างมาก เนื่องจากได้สร้างความเสียหายให้กับประชาชนเป็นจำนวนมาก ซึ่งในปัจจุบันประเทศไทยยังไม่มีการกำหนดแนวทางที่แน่ชัดและเป็นรูปธรรมในการวางแผนปฏิบัติการการป้องกันแก๊งคอลเซ็นเตอร์ดังกล่าวเหมือนของต่างประเทศ โดยประเทศไทยส่วนใหญ่จะเน้นที่การจับกุมหลังจากที่เกิดผู้เสียหายแล้วมากกว่าการวางแผนป้องกัน ซึ่งในประเทศไทยในปัจจุบันจะมีแอปพลิเคชันฮูส์คอลล์ (Who call) ที่ใช้ในการตรวจสอบหมายเลขโทรศัพท์ว่าสายที่โทรเข้ามานั้นเป็นสายของมิจฉาชีพ หรือไม่ แต่ก็ทำได้แค่เช็คเบื้องต้นเท่านั้น โดยแอปพลิเคชันดังกล่าวได้รับการพัฒนาจากบริษัท Gogo look ซึ่งเป็นบริษัทพัฒนาแอปพลิเคชันสัญชาติไต้หวันที่โดดเด่นทางด้านเทคโนโลยีในการป้องกันการทุจริต (Anti-Fraud Technology) และมีฐานข้อมูลที่ใหญ่ที่สุดในภูมิภาคเอเชียตะวันออกและเอเชียตะวันออกเฉียงใต้ โดยมีข้อมูลเบอร์โทรศัพท์มากกว่า 1.6 พันล้านหมายเลข[94] ในปัจจุบันคณะทำงานพหุภาคี 11 หน่วยงานที่เกี่ยวข้องกับการแก้ไขปัญหาคอลเซ็นเตอร์ใน ประเทศไทยได้ทำการเสนอต่อบอร์ด กสทช ว่าให้ที่ประชุม กสทช. พิจารณากำหนดในเงื่อนไขท้ายใบอนุญาตให้ผู้ประกอบการโทรศัพท์เคลื่อนที่ทุกรายสร้างระบบหรือแอปพลิเคชันที่ให้ประชาชนสามารถเลือกสมัครบริการปฏิเสธไม่รับสายที่โทรมาจากต่างประเทศได้รวมถึงมีมาตรการในการแก้ไขปัญหาและประสานงานกับบริษัทเครือข่ายมือถือเพื่อหาวิธีเตือนให้ผู้ใช้โทรศัพท์ให้ตระหนักถึงการโทรเข้าของมิจฉาชีพโดยหากเป็นเลขหมายที่โทรมาจากต่างประเทศหรือโทรผ่านระบบอินเทอร์เน็ตทาง

[94] Mobile Octa Admin, ‘Gogolook ปั้น Whoscall แพลตฟอร์มต่อต้านการฉ้อโกงแห่งแรกในประเทศไทย ปกป้องคนไทยไม่ให้ตกเป็นเหยื่อการใช้โทรศัพท์และข้อความหลอกลวง’ (2565) <https://www.mobileocta.com/gogolook-creates-whoscall-the-first-anti-fraud-platform-in-thailand/> สืบค้นเมื่อ 5 กรกฎาคม 2568.

ค่ายมือถือจะโชว์เป็นเครื่องหมายบวกบนหมายเลขโทรศัพท์[95] เพื่อแจ้งเตือนผู้รับสาย ดังนั้น ในส่วนของประชาชนต้องมีความสร้างความตระหนักรู้ต่อปัญหาร่วมกันมีสติและคอยติดตามข่าวสารด้านอาชญากรรมในยุคดิจิทัลเพื่อป้องกันตัวเองในการตกเป็นเหยื่อ โดย 11 หน่วยงานดังกล่าวประกอบไปด้วย[96] กสทช. ผู้แทนกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ก.ดีอีเอส) ผู้แทนกองคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ผู้แทนธนาคารแห่งประเทศไทย (ธปท.) ผู้แทนกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บช.สอท) ผู้แทนประกอบการโทรศัพท์เคลื่อนที่รายใหญ่ทั้ง 4 ราย (AIS TRUE DTAC NT) ผู้แทนสมาคมโทรคมนาคมแห่งประเทศไทยในพระบรมราชูปถัมภ์ และผู้แทนสภาองค์กรของผู้บริโภค

อย่างไรก็ตาม ในช่วงปี พ.ศ. 2568 เป็นต้นมา รัฐบาลไทยภายใต้การนำของนายกรัฐมนตรี ได้เริ่มผลักดันนโยบายเชิงรุกเพื่อตอบสนองต่อปัญหาแก๊งคอลเซ็นเตอร์ โดยมีการประกาศใช้ “มาตรการ 3 ตัด” ซึ่งประกอบด้วยการตัดกระแสไฟฟ้า ตัดสัญญาณอินเทอร์เน็ต และตัดน้ำมันหรือเชื้อเพลิงในพื้นที่เป้าหมายที่มีความเชื่อมโยงกับกิจกรรมของเครือข่ายอาชญากรรมข้ามชาติ โดยเฉพาะในเขตชายแดนไทย-กัมพูชา เพื่อขัดขวางการปฏิบัติการของแก๊งคอลเซ็นเตอร์ตั้งแต่ต้นทาง เป็นการดำเนินมาตรการเชิงพื้นที่เพื่อตัดวงจรปัจจัยสนับสนุนการกระทำผิดของแก๊งคอลเซ็นเตอร์ โดยเฉพาะในพื้นที่แนวชายแดนที่มักเป็นฐานปฏิบัติการของแก๊งเหล่านี้ มาตรการนี้ประกอบด้วย[97]

1. ตัดกระแสไฟฟ้า เพื่อป้องกันไม่ให้แก๊งคอลเซ็นเตอร์สามารถใช้พลังงานไฟฟ้าในการดำเนินงาน เช่น การเปิดอุปกรณ์โทรคมนาคม คอมพิวเตอร์ หรือระบบเครือข่ายภายในศูนย์หลอกลวง ซึ่งเป็นปัจจัยสำคัญที่ช่วยให้กลุ่มอาชญากรรมสามารถทำงานได้อย่างต่อเนื่องและแพร่หลาย

2. ตัดสัญญาณอินเทอร์เน็ต การตัดการเชื่อมต่ออินเทอร์เน็ตจะทำให้แก๊งคอลเซ็นเตอร์ไม่สามารถติดต่อสื่อสารกับเหยื่อหรือเครือข่ายข้ามชาติได้ ทั้งยังเป็นการจำกัดการใช้โครงข่าย

---

[95] ปฐมพงศ์ ศรีแสงจันทร์, ‘คณะทำงานพหุภาคีแก้ไขปัญหาคอลเซ็นเตอร์เสนอบอร์ด กสทช. ขีดเส้นตายให้โอเปอร์เรเตอร์ทุกรายสร้างระบบให้ประชาชนเลือกสมัครบริการปฏิเสธไม่รับสายที่โทรมาจากต่างประเทศ เพื่อลดความเดือดร้อนจากปัญหาดังกล่าวโดยเร็วที่สุด’ <https://www.nbtc.go.th/News/Press-Center/55326.aspx?lang=th-th> สืบค้นเมื่อ 3 พฤษภาคม 2567.

[96] ข่าวเศรษฐกิจ, กสทช., ‘ค่ายมือถือ’ วันละล้านไร้น้ำยาปราบคอลเซ็นเตอร์’ <https://www.bangkokbiznews.com/business/1014117> สืบค้นเมื่อ 3 พฤษภาคม 2567.

[97] สำนักงานประชาสัมพันธ์จังหวัดสระแก้ว, ‘มาตรการ 3 ตัด: รัฐบาลเดินหน้ายุทธศาสตร์สกัดแก๊งคอลเซ็นเตอร์แนวชายแดน’ (เว็บไซต์กรมประชาสัมพันธ์) <https://www.prd.go.th/th/content/category/detail/id/39/iid/366469> สืบค้นเมื่อ 22 มิถุนายน 2568.

โทรคมนาคมที่ผิดกฎหมาย เช่น การใช้หมายเลขโทรศัพท์ปลอมหรือการใช้ระบบ VoIP อย่างผิดกฎหมาย

3. ตัดน้ำมันและเชื้อเพลิง การตัดน้ำมันและเชื้อเพลิงเป็นการปิดกั้นการใช้ทรัพยากรที่จำเป็นในการดำเนินกิจกรรม เช่น การขนส่ง การหลบหนี หรือการรักษาความเคลื่อนไหวของกลุ่มแก๊งในพื้นที่ ทั้งนี้มาตรการนี้ช่วยเพิ่มแรงกดดันต่อแก๊งคอลเซ็นเตอร์ให้ยุติการกระทำผิด

ดังนั้น จะเห็นได้ว่าการดำเนินมาตรการของประเทศไทยในการรับมือกับอาชญากรรมทางเทคโนโลยียังคงขาดแผนปฏิบัติการเชิงยุทธศาสตร์ที่เป็นระบบและต่อเนื่องในระดับชาติ แม้ว่าจะมีความพยายามในการกำหนดนโยบายเชิงรุกนการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์ ซึ่งมีลักษณะตอบสนองภัยคุกคามในระยะสั้นแต่ในทางโครงสร้างแล้ว กลไกการป้องกันเชิงรุกตั้งแต่ต้นทาง เช่น การคัดกรองข้อมูล ความรู้เท่าทันทางดิจิทัล หรือการจัดการความเสี่ยงเชิงระบบ ยังไม่ปรากฏในรูปของนโยบายถาวรที่มีผลบังคับใช้และมีหน่วยงานเจ้าภาพหลักที่รับผิดชอบโดยเฉพาะ นอกจากนี้หน่วยงานของรัฐที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีในประเทศไทยยังมีลักษณะการดำเนินงานที่กระจายอยู่ในหลายหน่วยงาน เช่น สำนักงานตำรวจแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ธนาคารแห่งประเทศไทย สำนักงานป้องกันและปราบปรามการฟอกเงิน และหน่วยงานในสังกัดกระทรวงยุติธรรม โดยไม่มีโครงสร้างกลางที่ทำหน้าที่บูรณาการนโยบาย กำหนดมาตรฐาน หรือประเมินผลร่วมกันในระดับชาติ ส่งผลให้การดำเนินงานในทางปฏิบัติมักมีลักษณะเป็นมาตรการเฉพาะหน้าหรือการตอบสนองเป็นรายกรณี มากกว่าการดำเนินการในลักษณะเชิงป้องกันอย่างยั่งยืน ด้วยเหตุนี้ การจัดการปัญหาอาชญากรรมไซเบอร์ในประเทศไทยจึงยังมีลักษณะที่ขาดเอกภาพ ขาดทิศทางร่วม อันเป็นอุปสรรคสำคัญต่อการรับมือกับภัยคุกคามไซเบอร์ที่มีลักษณะซับซ้อน รวดเร็ว และข้ามพรมแดนในยุคปัจจุบัน

3.1.3.2 ประเทศออสเตรเลีย

ประเทศออสเตรเลียต้องเผชิญกับปัญหาแก๊งคอลเซ็นเตอร์ออนไลน์ในหลายรูปแบบ โดยเฉพาะการหลอกลวงทางโทรศัพท์ ซึ่งยังคงเป็นวิธีการที่มิจฉาชีพนิยมใช้มากที่สุดในการเข้าถึงเหยื่อ ทั้งนี้ยังถือเป็นรูปแบบการฉ้อโกงที่สร้างความเสียหายทางการเงินมากที่สุดเมื่อเปรียบเทียบกับวิธีการอื่น จากการศึกษาพบว่า ออสเตรเลียได้จัดทำแผนปฏิบัติการ (Action Plan) ที่มีรูปธรรมชัดเจน ภายใต้ความร่วมมือระหว่างหน่วยงานภาครัฐหลายภาคส่วน ซึ่งแนวทางดังกล่าวมีส่วนช่วยในการลดความสูญเสียทางเศรษฐกิจจากการหลอกลวงได้อย่างมีนัยสำคัญ โดยประเทศออสเตรเลียมีหน่วยงานภาครัฐที่มีส่วนเกี่ยวข้องและมีหน้าที่ความรับผิดชอบโดยตรงเกี่ยวกับปัญหาแก๊งคอลเซ็นเตอร์ออนไลน์ โดยมีหน่วยงานที่มีความรับผิดชอบหลัก ดังต่อไปนี้

1. ACMA (Australian Communication and Media AuthorityAustralian Communications and Media Authority (ACMA) เป็นหน่วยงานของรัฐบาลกลางออสเตรเลีย ซึ่งมีบทบาทสำคัญในการกำกับดูแลกิจการแพร่ภาพกระจายเสียง อินเทอร์เน็ต วิทยุสื่อสาร และโทรคมนาคมทั่วประเทศ โดยทำหน้าที่ควบคุมการให้บริการด้านการสื่อสารและสื่อสารมวลชน รวมถึงมีอำนาจในการพิจารณาและกำหนดเงื่อนไขของใบอนุญาต (license conditions) สำหรับผู้ประกอบการในอุตสาหกรรมที่เกี่ยวข้อง บทบาทสำคัญของ ACMA คือ การจัดวางมาตรฐานอุตสาหกรรม ซึ่งจะต้องดำเนินการตามคำสั่งของรัฐมนตรีผู้มีอำนาจ โดยมาตรฐานเหล่านี้มีผลบังคับใช้กับผู้ให้บริการโทรคมนาคม และมีวัตถุประสงค์เพื่อควบคุมกิจกรรมที่เกี่ยวข้องกับระบบการสื่อสารเพื่อให้เป็นไปตามกรอบกฎหมายและรักษาความมั่นคงของโครงสร้างพื้นฐานด้านการสื่อสารของประเทศ[98]

2. Australian Competition and Consumer Commission (ACCC) หรือคณะกรรมการการแข่งขันและผู้บริโภคแห่งออสเตรเลีย เป็นหน่วยงานของรัฐบาลกลางที่มีบทบาทสำคัญในการคุ้มครองสิทธิและผลประโยชน์ของผู้บริโภค ตลอดจนดูแลให้เกิดการแข่งขันที่เป็นธรรมในระบบเศรษฐกิจ หน้าที่หลักของ ACCC คือ การรับเรื่องร้องเรียนจากผู้บริโภคเกี่ยวกับพฤติกรรมที่อาจเข้าข่ายการละเมิดสิทธิผู้บริโภค หรือการประกอบธุรกิจที่ไม่เป็นธรรม รวมถึงดำเนินการสืบสวนสอบสวนกรณีดังกล่าวโดยมุ่งเน้นไปที่การคุ้มครองผลประโยชน์ของผู้บริโภคโดยรวม หน่วยงานนี้ยังมีบทบาทเชิงรุกในการเผยแพร่ข้อมูลให้ประชาชนตระหนักถึงกลโกงทางธุรกิจต่าง ๆ โดยเฉพาะในบริบทของอาชญากรรมไซเบอร์และการหลอกลวงผ่านระบบโทรคมนาคมซึ่งส่งผลกระทบต่อประชาชนในวงกว้าง[99]

3. Australian Cyber Security Centre (ACSC) หรือศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติของออสเตรเลีย เป็นหน่วยงานภายใต้รัฐบาลกลางที่มีภารกิจหลักในการดูแลและส่งเสริมความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ หน้าที่สำคัญของ ACSC ได้แก่ การป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่อาจกระทบต่อประชาชน หน่วยงานภาครัฐ ภาคเอกชน รวมถึง

---

[98] The Telecommunication Act 1997, subsection 125AA (1).

[99] รังสรรค์ โรจน์ชีวิน, มนตรี จิตร์วิวัฒน์, ดิลก เสริมวิริยะกุล, สมชาติ เลิศลิขิตวรกุล, ชัชวาล วิบุลสันติ และหฤทัย ประพุทธนิติสาร,"กฎหมายคุ้มครองผู้บริโภค และการดำเนินคดีคุ้มครองผู้บริโภค ประเทศออสเตรเลีย ศึกษาเกี่ยวกับกรณี การกระทำในทางการค้าทำให้ผู้บริโภคเกิดความเข้าใจผิด หรือหลอกลวงผู้บริโภคทางการค้า การเอาเปรียบผู้บริโภคที่มีความด้อยหรือความเสียเปรียบในทางการค้า หลักประกันผู้บริโภค การเยียวยาและอำนาจการบังคับใช้ของ ACCC การพิจารณาคดีผู้บริโภคโดยช่องทางพิเศษ การนำอิเล็กทรอนิกส์และเทคโนโลยีมาใช้ในการดำเนินกระบวนพิจารณาคดีของศาล " , การฝึกอบรมหลักสูตร "กฎหมายเกี่ยวกับวิธีพิจารณาความแพ่งชั้นสูง" ณ มหาวิทยาลัยนิวเซาท์เวลส์ ประเทศออสเตรเลีย, สำนักการต่างประเทศ.

โครงสร้างพื้นฐานสำคัญของประเทศ ทั้งนี้ ACSC ยังทำหน้าที่ในการจัดทำระเบียบ แนวปฏิบัติ และทรัพยากรด้านความปลอดภัยทางไซเบอร์ระดับชาติ พร้อมทั้งทำการศึกษา วิเคราะห์ และตรวจสอบภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง เพื่อให้สามารถดำเนินการตอบสนองได้อย่างมีประสิทธิภาพและเป็นผู้นำในการประสานความร่วมมือด้านความมั่นคงไซเบอร์ทั้งในระดับประเทศและระหว่างประเทศ[100]

4. Scam watch เป็นหน่วยงานเฉพาะทางที่จัดตั้งขึ้นภายใต้การกำกับดูแลของคณะกรรมการการแข่งขันและผู้บริโภคแห่งออสเตรเลีย (Australian Competition and Consumer Commission – ACCC) โดยมีบทบาทสำคัญในการให้ข้อมูลข่าวสารแก่ประชาชนเกี่ยวกับกลโกงและการหลอกลวงในรูปแบบต่าง ๆ รวมถึงการให้คำแนะนำในการหลีกเลี่ยงและป้องกันตนเองจากการตกเป็นเหยื่อ ภารกิจหลักของ Scam watch ได้แก่ การจัดทำและเผยแพร่ข้อมูล ข่าวสาร เอกสารข้อเท็จจริง และรายงานประจำปีที่เกี่ยวข้องกับแนวโน้มและรูปแบบของการฉ้อโกง เพื่อให้ประชาชนสามารถรับรู้และระมัดระวังภัยได้อย่างทันท่วงที นอกจากนี้ ยังเปิดช่องทางให้ประชาชนสามารถแจ้งหรือรายงานเหตุการณ์การหลอกลวงได้โดยตรงผ่านทางเว็บไซต์

นโยบายในการป้องกันและปราปรามแก๊งคอลเซ็นเตอร์ของประเทศออสเตรเลีย

หนึ่งในมาตรการสำคัญของออสเตรเลียในการป้องกันและแก้ไขปัญหาการหลอกลวงทางโทรศัพท์ คือ การจัดทำ *Scam Technology Project* คือ โครงการเชิงนโยบายและเทคโนโลยีที่จัดทำโดยหน่วยงาน Australian Communications and Media Authority (ACMA) ซึ่งมีวัตถุประสงค์ในการสำรวจและรับมือกับปัญหาการโทรศัพท์หลอกลวงที่ส่งผลกระทบต่อประชาชนผ่านเครือข่ายโทรคมนาคมของประเทศ โครงการดังกล่าวสะท้อนแนวทางการบูรณาการความร่วมมือระหว่างหน่วยงานรัฐและภาคเอกชนอย่างเป็นระบบ โดยเฉพาะกับหน่วยงานสำคัญอย่างคณะกรรมการการแข่งขันและผู้บริโภคแห่งออสเตรเลีย (ACCC) และศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (ACSC) รวมถึงการประสานงานกับหน่วยงานกำกับดูแลในต่างประเทศและผู้ให้บริการโทรคมนาคมภายในประเทศ ซึ่งมีบทบาทในการวิเคราะห์รูปแบบการหลอกลวงและพัฒนาแนวทางรับมือที่มีประสิทธิภาพยิ่งขึ้นในเชิงเทคนิคและกฎหมาย

ภายหลังจากการดำเนินโครงการดังกล่าว ACMA ได้ประกาศใช้ *Combating Scams Action Plan* ซึ่งถือเป็นแผนปฏิบัติการเชิงกลยุทธ์ที่มีเป้าหมายหลักในการลดปริมาณและผลกระทบจากการหลอกลวงในทุกรูปแบบ โดยเฉพาะอย่างยิ่งรูปแบบที่เรียกว่า “Wangiri scam” ซึ่ง

---

[100] ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักข่าวกรองแห่งชาติ, ‘ออสเตรเลียเริ่มปิดกั้นข้อความหลอกลวงที่อ้างว่ามาจากหน่วยงานของรัฐบาล’ <https://www.nia.go.th/cyber/cyberpage/588/> สืบค้นเมื่อ 10 มีนาคม 2568.

เป็นการหลอกลวงผ่านหมายเลขต่างประเทศที่โทรเข้าสู่หมายเลขปลายทางในออสเตรเลียเพียงครั้งเดียวแล้ววางสาย หากผู้รับสายโทรกลับ ระบบจะคิดค่าบริการพิเศษ และมิจฉาชีพจะพยายามดึงให้เหยื่ออยู่ในสายให้นานที่สุด เช่น การเปิดเสียงเพลงค้างไว้หรือใช้ข้อความอัตโนมัติเพื่อถ่วงเวลา[2] การวางมาตรการป้องกันต่อกลโกงลักษณะนี้ไม่เพียงเป็นการปกป้องสิทธิของผู้บริโภค แต่ยังช่วยลดภาระของระบบโทรคมนาคมและสร้างความเชื่อมั่นต่อโครงสร้างพื้นฐานดิจิทัลของประเทศ[101]

3.1.3.3 ประเทศสหราชอาณาจักร

สหราชอาณาจักรเผชิญกับปัญหาการหลอกลวงจากแก๊งคอลเซ็นเตอร์มาเป็นระยะเวลานาน โดยเฉพาะในรูปแบบของการโทรศัพท์เสนอขายสินค้าและบริการที่เป็นการตลาดฉ้อฉล ซึ่งไม่เพียงแต่สร้างความรำคาญแก่ประชาชน แต่ยังส่งผลให้เกิดความสูญเสียทั้งในเชิงเศรษฐกิจและความเชื่อมั่นในระบบการสื่อสารโดยรวม อันเป็นภัยคุกคามต่อความปลอดภัยของผู้บริโภคโดยตรง จากสถานการณ์ดังกล่าว หน่วยงานภาครัฐของสหราชอาณาจักรจึงได้ริเริ่มจัดทำแผนปฏิบัติการอย่างเป็นรูปธรรมตั้งแต่ปี ค.ศ. 2013 เพื่อวางแนวทางการป้องกันและจัดการกับภัยคุกคามที่เกิดจากการโทรศัพท์และข้อความหลอกลวงดังกล่าว โดยมีเป้าหมายในการยกระดับการคุ้มครองผู้บริโภค พร้อมทั้งพัฒนากลไกการกำกับดูแลและความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องทั้งในประเทศและระดับนานาชาติให้มีประสิทธิภาพมากยิ่งขึ้น[102]ประเทศสหราชอาณาจักรมีหน่วยงานภาครัฐที่มีส่วนเกี่ยวข้องและมีหน้าที่ความรับผิดชอบโดยตรง เกี่ยวกับปัญหาแก๊งคอลเซ็นเตอร์ออนไลน์ โดยหน่วยงานที่มีความรับผิดชอบหลัก ดังต่อไปนี้

1. Ofcom Office of Communications (Ofcom) เป็นหน่วยงานอิสระของสหราชอาณาจักรที่ปฏิบัติหน้าที่ภายใต้การกำกับดูแลของรัฐบาล โดยมีอำนาจตามพระราชบัญญัติการสื่อสาร ค.ศ. 2003 (The Communication Act 2003) ทำหน้าที่เป็นองค์กรกำกับดูแลกิจการด้านการสื่อสารของประเทศ ครอบคลุมทั้งกิจการโทรทัศน์ วิทยุกระจายเสียง โทรคมนาคมทั้งแบบมีสายและไร้สาย ตลอดจนกิจการไปรษณีย์ ทั้งนี้ บทบาทของ Ofcom มีลักษณะคล้ายคลึงกับสำนักงาน กสทช. ของประเทศไทย และ ACMA ของออสเตรเลีย ในปี ค.ศ. 2017 และ 2018 Ofcom ได้กำหนดยุทธศาสตร์ด้านการคุ้มครองผู้บริโภคไว้อย่างชัดเจน โดยมีเป้าหมายเพื่อรับมือกับภัยคุกคามที่อาจเกิดขึ้นจากการใช้บริการด้านการสื่อสารในรูปแบบต่าง ๆ ซึ่งหนึ่งในประเด็นสำคัญ คือ การแก้ไข

---

[101] Scamwatch, ‘Wangiri Scam – Missed Call Scams,’ <https://www.scamwatch.gov.au> accessed May 19 2025.

[102] Ofcom, ‘Tackling Nuisance Calls and Messages,’ <https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/tackling-nuisance-calls-messages> accessed July 6 2025.

ปัญหาการรบกวนทางโทรศัพท์ (nuisance calls) ที่มักถูกใช้เป็นช่องทางในการหลอกลวงผู้บริโภค โดย Ofcom ได้ดำเนินความร่วมมือกับผู้ให้บริการเครือข่ายโทรคมนาคมและหน่วยงานที่เกี่ยวข้องในการติดตาม ตรวจสอบ และดำเนินมาตรการป้องกันอย่างเป็นระบบ เพื่อเสริมสร้างความปลอดภัยและความเชื่อมั่นของประชาชนในการใช้บริการด้านการสื่อสารอย่างมีประสิทธิภาพและปลอดภัย[103]

2. The Information Commissioner's Office (ICO) หรือที่แปลเป็นภาษาไทยว่า *สำนักงานกรรมาธิการด้านข้อมูลข่าวสารแห่งสหราชอาณาจักร* เป็นหน่วยงานอิสระซึ่งมีหน้าที่หลักในการคุ้มครองข้อมูลส่วนบุคคลและกำกับดูแลการใช้ข้อมูลของประชาชนอย่างเหมาะสม โดยเฉพาะในด้านการสื่อสารทางโทรคมนาคม หน่วยงานนี้มีบทบาทสำคัญในการจัดการกับปัญหาการโทรขายทางโทรศัพท์ที่ก่อความรำคาญให้กับประชาชน รวมถึงการโทรอัตโนมัติด้วยข้อความทางการตลาดและข้อความหลอกลวงในรูปแบบต่าง ๆ ที่ละเมิดสิทธิของเจ้าของข้อมูล นอกจากนี้ ICO ยังมีภารกิจในการบริหารจัดการรายชื่อหมายเลขโทรศัพท์ของบุคคลและธุรกิจที่ไม่ประสงค์จะรับสายการตลาดแบบสดหรือแฟกซ์โฆษณาที่ไม่พึงประสงค์ผ่านระบบที่เรียกว่า *Telephone Preference Service (TPS)* และ *Fax Preference Service (FPS)* ซึ่งถือเป็นเครื่องมือสำคัญในการให้ประชาชนสามารถปกป้องตนเองจากการถูกรบกวนและมีสิทธิควบคุมการเข้าถึงข้อมูลส่วนบุคคลของตนอย่างเป็นรูปธรรม

3. Action Fraud เป็นศูนย์กลางของสหราชอาณาจักรที่จัดตั้งขึ้นเพื่อรับแจ้งเหตุเกี่ยวกับการฉ้อโกงและอาชญากรรมทางไซเบอร์โดยเฉพาะ โดยเริ่มดำเนินงานตั้งแต่ปี ค.ศ. 2005 ด้วยบทบาทในการติดตามสถานการณ์ภัยคุกคามที่ส่งผลกระทบต่อผู้บริโภคอย่างใกล้ชิด ทั้งนี้ การฉ้อโกงและอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยีทุกรูปแบบที่เกิดขึ้นภายในดินแดนของสหราชอาณาจักรสามารถถูกรายงานไปยัง Action Fraud เพื่อเข้าสู่กระบวนการวิเคราะห์ข้อมูลโดย National Fraud Intelligence Bureau (NFIB) ซึ่งเป็นหน่วยงานภายใต้สำนักงานตำรวจแห่งชาติ[104] เว็บไซต์ทางการของหน่วยงานให้บริการข้อมูลอย่างครอบคลุมแก่ประชาชนเกี่ยวกับรูปแบบการหลอกลวงที่พบได้บ่อย พร้อมทั้งเผยแพร่แนวทางป้องกันตนเองจากการตกเป็นเหยื่อของกลโกงสมัยใหม่ โดยเน้นการสร้างความตระหนักรู้ ความเข้าใจ และการมีส่วนร่วมของประชาชนในการต่อสู้กับอาชญากรรมไซเบอร์และการฉ้อโกงในทุกรูปแบบ

---

[103] จิตสุภา ฤทธิผลิน, “ทิศทางและนโยบายการกำกับดูแลกิจการกระจายเสียง และกิจการโทรทัศน์ในยุคของการหลอมรวมสื่อ: กรณีศึกษาเปรียบเทียบยุทธศาสตร์ของ FCC และ OFCOM” (วิทยานิพนธ์, สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ, 2560) 253.

[104] โชคสุข กรกิตติชัย, ‘สหราชอาณาจักรบริเตนใหญ่และไอร์แลนด์เหนือ กับการป้องกันและปราบปรามการทุจริต’ เอกสารวิชาการ อิเล็กทรอนิกส์ สำนักวิชาการ สำนักงานเลขาธิการสภาผู้แทนราษฎร (สิงหาคม 2565) 13.

นโยบายในการป้องกันและปราปรามแก๊งคอลเซ็นเตอร์ของประเทศสหราชอาณาจักร

แนวทางการป้องกันอาชญากรรมจากแก๊งคอลเซ็นเตอร์ในภาคอุตสาหกรรมโทรคมนาคมของประเทศสหราชอาณาจักรได้ถูกจัดวางไว้อย่างเป็นระบบและมีการดำเนินงานอย่างต่อเนื่องผ่านแผนปฏิบัติการร่วมระหว่างหน่วยงานที่เกี่ยวข้อง โดยสหราชอาณาจักรได้จัดทำแผนปฏิบัติการในระดับชาติภายใต้ชื่อ “Nuisance Calls and Messages: Update to ICO/Ofcom Joint Action Plan” ซึ่งริเริ่มครั้งแรกในปี ค.ศ. 2013 โดยมีการทบทวนและปรับปรุงแผนดังกล่าวเป็นประจำทุกปี เพื่อให้สามารถรองรับและตอบสนองต่อความเปลี่ยนแปลงของพฤติกรรมอาชญากรที่ใช้เทคโนโลยีสื่อสารในรูปแบบต่าง ๆ ในการแสวงหาผลประโยชน์จากประชาชน โดยแผนปฏิบัติการนี้เป็นความร่วมมือระหว่าง สำนักงานกรรมาธิการสารสนเทศ (Information Commissioner’s Office – ICO) และ สำนักงานกำกับดูแลการสื่อสารแห่งสหราชอาณาจักร (Office of Communications – Ofcom) โดยมีการแบ่งหน้าที่ความรับผิดชอบอย่างชัดเจน กล่าวคือ ICO มีบทบาทหลักในการบังคับใช้กฎหมายต่อองค์กรที่ละเมิดกฎเกี่ยวกับการใช้ข้อมูลส่วนบุคคลในการโทรศัพท์หรือส่งข้อความเพื่อการตลาด เช่น การโทรด้วยระบบอัตโนมัติ (automated calls) การโฆษณาทางการตลาดโดยใช้พนักงาน รวมถึงการส่งข้อความหรืออีเมลที่ก่อให้เกิดความรำคาญแก่ผู้บริโภค

ในขณะที่ Ofcom รับผิดชอบในการดูแลและกำกับการใช้หมายเลขโทรศัพท์ โดยเฉพาะการติดตามหมายเลขที่ถูกจดทะเบียนแต่ไม่มีการใช้งานหรือถูกนำมาใช้ในทางที่ผิด ซึ่งมักถูกใช้โดยอาชญากรไซเบอร์ในการหลอกลวงผ่านทางโทรศัพท์ ทั้งสองหน่วยงานยังร่วมมือกับผู้ให้บริการโทรคมนาคมและองค์กรด้านเทคนิคอื่น ๆ ในการสนับสนุนด้านการวิจัย พัฒนาเทคโนโลยีที่สามารถตรวจจับและป้องกันการหลอกลวง ตลอดจนให้คำแนะนำแก่ผู้บริโภคในการปกป้องตนเองจากการตกเป็นเหยื่อ ซึ่งแผนปฏิบัติการล่าสุดที่ได้รับการเผยแพร่ คือ Nuisance Calls and Messages: Update to ICO/Ofcom Joint Action Plan 2021 ซึ่งได้สะท้อนถึงความคืบหน้าและผลลัพธ์ของมาตรการที่ได้ดำเนินการในช่วงปีที่ผ่านมา พร้อมทั้งวางแนวทางในการยกระดับความร่วมมือและประสิทธิภาพของมาตรการในอนาคต เพื่อสร้างระบบการสื่อสารที่ปลอดภัยและเชื่อถือได้สำหรับประชาชนในสหราชอาณาจักร

แผนปฏิบัติการร่วมระหว่าง Ofcom และ ICO ในการรับมือกับการโทรและข้อความที่ก่อให้เกิดความรำคาญในสหราชอาณาจักรนั้น ได้ให้ความสำคัญกับการรวบรวมข้อมูลเชิงประจักษ์เพื่อใช้ในการวิเคราะห์ความคืบหน้าและประสิทธิภาพของมาตรการที่นำมาใช้ โดยหนึ่งในกลไกสำคัญของแผนปฏิบัติการคือ การวิจัยเพื่อติดตามการโทรรบกวน (Nuisance Calls Tracking Research) ซึ่งดำเนินการโดย Ofcom อย่างต่อเนื่องในแต่ละปี งานวิจัยดังกล่าวจัดขึ้นโดยปกติปีละสามครั้ง โดยมีวัตถุประสงค์เพื่อติดตามประสบการณ์ของประชาชนที่ได้รับการติดต่อทางโทรศัพท์บ้านหรือ

โทรศัพท์มือถือที่ก่อให้เกิดความรำคาญ ทั้งนี้การเก็บข้อมูลจะกระทำผ่านการสัมภาษณ์ประชาชนแบบตัวต่อตัว โดยคัดเลือกจากกลุ่มตัวอย่างที่เป็นตัวแทนในระดับประเทศ เพื่อให้ได้มาซึ่งข้อมูลที่สะท้อนสถานการณ์จริงอย่างครอบคลุมและแม่นยำ ซึ่งข้อมูลที่ได้จะช่วยให้หน่วยงานกำกับดูแลสามารถประเมินสถานการณ์และปรับปรุงนโยบายได้อย่างมีประสิทธิภาพ นอกจากนี้ แผนปฏิบัติการยังส่งเสริม การทำงานร่วมกันระหว่าง Ofcom กับบริษัทผู้ให้บริการโทรคมนาคมและหน่วยงานกำกับดูแลอื่น ๆ ผ่านการจัดตั้ง กลุ่มคณะทำงานเชิงกลยุทธ์ ที่มีวัตถุประสงค์เพื่อแลกเปลี่ยนข้อมูล แนวโน้มของภัยคุกคาม และร่วมกันพัฒนากลไกในการป้องกันการหลอกลวง เช่น การระบุและปิดกั้นหมายเลขโทรศัพท์ที่ไม่ถูกต้องหรือใช้ในทางที่ผิด ในระดับการดำเนินงาน กลุ่มคณะทำงานดังกล่าวประกอบด้วยบริษัทผู้ให้บริการโทรคมนาคม 11 ราย ซึ่งมีพันธกิจในการส่งข้อมูลรายเดือนเกี่ยวกับหมายเลขโทรศัพท์ที่ได้รับการร้องเรียนจากผู้บริโภคมายัง Ofcom โดย Ofcom จะทำหน้าที่รวบรวม วิเคราะห์ และเผยแพร่ข้อมูลดังกล่าวในหมู่สมาชิกของกลุ่ม เพื่อเป็นฐานข้อมูลกลางที่สามารถใช้ในการเฝ้าระวังและยับยั้งพฤติกรรมหลอกลวงทางโทรศัพท์ได้อย่างทันท่วงที[105]

3.1.3.4 ประเทศฟิลิปปินส์

ฟิลิปปินส์ได้ดำเนินมาตรการเชิงรุกเพื่อต่อสู้กับการฉ้อโกงทางโทรศัพท์และแก๊งคอลเซ็นเตอร์ที่มีส่วนเกี่ยวข้องกับกิจกรรมทางอาญา การดำเนินการเหล่านี้เป็นส่วนหนึ่งของความพยายามที่กว้างขวางในการปกป้องพลเมืองและชาวต่างชาติจากการตกเป็นเหยื่อของการหลอกลวงทางโทรศัพท์ที่ซับซ้อนและเพิ่มขึ้นเรื่อย ๆ ประเทศฟิลิปปินส์มีหน่วยงานภาครัฐที่มีส่วนเกี่ยวข้องและมีหน้าที่ความรับผิดชอบโดยตรง เกี่ยวกับปัญหาแก๊งคอลเซ็นเตอร์ออนไลน์ โดยหน่วยงานที่มีความรับผิดชอบหลักดังต่อไปนี้

1. Philippine National Police (PNP) Anti-Cybercrime Group (ACG)

เป็นหน่วยงานภายใต้สำนักงานตำรวจแห่งชาติของฟิลิปปินส์ที่มีหน้าที่ในการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ หน่วยงานนี้มีบทบาทสำคัญในการรักษาความปลอดภัยทางข้อมูลและเทคโนโลยีสารสนเทศภายในประเทศ หน้าที่หลักของ ACG คือ การสืบสวนอาชญากรรมทางไซเบอร์ ACG มีความรับผิดชอบในการตรวจสอบและสืบสวนคดีอาชญากรรมทางไซเบอร์และการจับกุมและดำเนินคดีกับผู้กระทำผิด เช่น การแฮ็ก การฟิชชิ่ง การโจมตีทางไซเบอร์ การขโมยข้อมูลส่วนบุคคล การหลอกลวงออนไลน์ และการป้องกันอาชญากรรม ซึ่งหน่วยงานนี้ดำเนินการป้องกันการก่ออาชญากรรมทางไซเบอร์ผ่านการเฝ้าระวังและติดตามกิจกรรมที่น่าสงสัย รวมถึงการให้ความรู้และคำแนะนำแก่ประชาชนและองค์กรต่าง ๆ เกี่ยวกับการป้องกันตนเองจากอาชญากรรมทางไซ

[105] The Information Commissioner's Office (ICO) and Ofcom Nuisance calls and messages, Update to ICO-Ofcom joint action plan 2021.

เบอร์ อีกทั้งยังมีความร่วมมือระหว่างประเทศที่ ACG ทำงานร่วมกับหน่วยงานด้านความมั่นคงทางไซเบอร์และตำรวจสากลจากประเทศอื่น ๆ เพื่อแลกเปลี่ยนข้อมูลและเทคนิคในการปราบปรามอาชญากรรมทางไซเบอร์ที่มีลักษณะข้ามชาติ[106]

2. National Bureau of Investigation (NBI) Cybercrime Division

เป็นหน่วยงานภายใต้สำนักงานสืบสวนแห่งชาติของฟิลิปปินส์ที่มีหน้าที่หลักในการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ หน่วยงานนี้ทำงานเพื่อสืบสวนและดำเนินการตามกฎหมายต่ออาชญากรรมที่เกิดขึ้นในโลกดิจิทัล ซึ่งหน้าที่ของ NBI Cybercrime Division คือ การรวบรวมและวิเคราะห์หลักฐานดิจิทัล โดยเทคโนโลยีและเครื่องมือทางนิติวิทยาศาสตร์ดิจิทัลในการรวบรวมและวิเคราะห์หลักฐานที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์ เพื่อให้สามารถระบุตัวผู้กระทำผิดและนำเสนอหลักฐานในศาลได้อย่างมีประสิทธิภาพ

ซึ่งภารกิจของกลุ่ม PNP Anti-Cybercrime คือ การดำเนินการและบังคับใช้กฎหมายที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์และอาชญากรรมทางไซเบอร์อื่น ๆ ที่เกี่ยวข้องและดำเนินการรณรงค์ต่อต้านอาชญากรรมทางไซเบอร์ที่มีประสิทธิผล ซึ่งกลุ่มต่อต้านอาชญากรรมทางไซเบอร์สืบสวนอาชญากรรมทางไซเบอร์และอาชญากรรมอื่น ๆ ทั้งหมดที่มีการใช้เทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ถูกนำมาใช้ในการก่ออาชญากรรมหรือเป็นเป้าหมายของการโจมตี

เพื่อเสริมสร้างการป้องกันและรับมือกับปัญหาการฉ้อโกงทางโทรศัพท์ รัฐบาลฟิลิปปินส์ได้จัดตั้ง (I-ARC) ขึ้น ศูนย์นี้เป็นศูนย์บริการ 24 ชั่วโมง ที่มีหมายเลขสายด่วน 1326 สำหรับเหยื่อของอาชญากรรมทางไซเบอร์ รวมถึงการหลอกลวงต่าง ๆ ที่สามารถรายงานเหตุการณ์ได้[107] โดยเป็นบริการสายด่วนศูนย์กลางที่จัดตั้งขึ้นเพื่อต่อสู้กับอาชญากรรมทางไซเบอร์หลายรูปแบบ โดยเฉพาะการหลอกลวงทางออนไลน์ศูนย์ I-ARC ประกอบด้วยหน่วยงานหลายหน่วยงาน เช่น ศูนย์ประสานงานและสืบสวนอาชญากรรมทางไซเบอร์ (Cybercrime Investigation and Coordinating Center), คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (National Privacy Commission), และคณะกรรมการโทรคมนาคมแห่งชาติ (National Telecommunications Commission) นอกจากนี้ยังมีหน่วยงานบังคับใช้กฎหมาย เช่น ตำรวจแห่งชาติฟิลิปปินส์ (Philippine National Police) และ

---

[106] 'Philippine National Police Anti-Cybercrime Group' (PNP-ACG) <https://www.cybersecurityintelligence.com/philippine-national-police-anti-cybercrime-group-pnp-acg-4731.html> accessed May 27 2024.

[107] AFP, "Hundreds Rescued from Philippines Scam Center—Police," <https://manilastandard.net/news/314426243/hundreds-rescued-from-philippines-scam-center-police.html> accessed March 15 2024.

สำนักงานสอบสวนแห่งชาติ (National Bureau of Investigation) ที่ทำงานร่วมกันเพื่อให้ความช่วยเหลือเหยื่อในการกู้คืนความสูญเสียและดำเนินคดีกับผู้กระทำผิด[108]

แนวทางในการป้องกันแก๊งคอลเซ็นเตอร์ในประเทศฟิลิปปินส์ พบว่าฟิลิปปินส์มีการจัดทำแผนปฏิบัติอย่างเป็นรูปธรรมในการวางแผนการป้องกันเพื่อจัดการกับอันตรายทางอาชญากรรมไซเบอร์โดยแผนที่จัดทำคือ Operation against Cybercrime ซึ่งเป็นปฏิบัติการที่ดำเนินการโดยหน่วยงานบังคับใช้กฎหมาย เช่น Philippine National Police (PNP) Anti-Cybercrime Group (ACG) เพื่อป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ ปฏิบัติการเหล่านี้มีจุดประสงค์ในการตรวจสอบ สืบสวน และจับกุมผู้กระทำความผิดที่ใช้เทคโนโลยีและอินเทอร์เน็ตในการก่ออาชญากรรม เป็นปฏิบัติการที่ดำเนินการ โดย PNP-ACG ร่วมกับหน่วยงานบังคับใช้กฎหมายจากหลายประเทศเพื่อปราบปรามแก๊งคอลเซ็นเตอร์ที่ดำเนินการหลอกลวงผ่านโทรศัพท์และอินเทอร์เน็ต ปฏิบัติการนี้ประสบความสำเร็จในการจับกุมผู้ต้องสงสัยหลายคนและปิดกั้นกิจกรรมที่ผิดกฎหมาย โดย Operation "One Ring เป็นปฏิบัติการที่มุ่งเน้นในการปิดกั้นและจับกุมแก๊งคอลเซ็นเตอร์ที่ดำเนินการหลอกลวงผ่านการโทรข้ามประเทศ หน่วยงานบังคับใช้กฎหมายในฟิลิปปินส์ได้ทำงานร่วมกับหน่วยงานในประเทศอื่น ๆ เพื่อปิดกั้นเครือข่ายอาชญากรรมเหล่านี้

## 3.2 มาตรการที่ใช้ในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

การกระทำความผิดของแก๊งคอลเซ็นเตอร์ในภูมิภาคอาเซียนยังคงเป็นปัญหาสำคัญที่ยังคงเกิดขึ้นอย่างต่อเนื่องด้วยเหตุที่อาชญากรรมข้ามชาติที่เกิดจากแก๊งคอลเซ็นเตอร์เป็นการกระทำผิดข้ามแดนหรือเกี่ยวพันกับพื้นที่ตั้งแต่สองประเทศขึ้นไป ซึ่งในหัวข้อนี้จะทำการศึกษาถึงมาตรการระหว่างประเทศสำคัญอันเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ทั้งในระดับสากล ระดับภูมิภาค และระดับประเทศ ดังนี้

### 3.2.1 ระดับสากล

มาตรการในระดับสากลที่ใช้ในการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์และอาชญากรรมข้ามชาติที่มีลักษณะข้ามพรมแดน โดยองค์กรระหว่างประเทศและประเทศต่าง ๆ ร่วมกันดำเนินการในด้านต่าง ๆ เพื่อเสริมสร้างความร่วมมือและเพิ่มประสิทธิภาพในการปราบปราม

---

[108] ‘Netizens Urged to Save Gov’t Anti-Scam Response Hotline 1326’ <https://www.pna.gov.ph/articles/1207775> accessed June 7 2024.

อาชญากรรมเหล่านี้ ซึ่งองค์การสหประชาชาติได้มีมาตรการในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ ได้แก่

1. อนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร (United Nations Convention Against Transnational Organized Crime)

อนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร ค.ศ. 2000 เป็นกฎหมายระหว่างประเทศฉบับสำคัญที่เปิดโอกาสให้ประเทศที่เป็นภาคีมาร่วมมือกันในการต่อสู้กับองค์กรอาชญากรรมข้ามชาติโดยไม่คำนึงถึงความแตกต่างทั้งทางด้านการเมือง การปกครอง วัฒนธรรม และเชื้อชาติของประเทศ โดยอนุสัญญาฯ ได้วางหลักเกณฑ์พื้นฐานอย่างกว้างให้ประเทศสมาชิกต้องนำเข้าไปบัญญัติไว้เป็นกฎหมายภายใน โดยมีข้อบทที่น่าสนใจ ได้แก่ ความผิดทางอาญาของการเข้าร่วมในองค์กรอาชญากรรม การฟอกเงิน การทุจริตคอร์รัปชั่น และมาตรการตอบโต้ความรับผิดชอบของนิติบุคคล การฟ้องร้องและการพิพากษา การยึดทรัพย์ ความร่วมมือระหว่างประเทศเพื่อวัตถุประสงค์ในการยึดทรัพย์ เขตอำนาจศาล การส่งผู้ร้ายข้ามแดน การส่งมอบตัวผู้ต้องคำพิพากษา ความช่วยเหลือซึ่งกันและกันทางอาญา การสืบสวนร่วมกัน เทคนิคการสืบสวนพิเศษการจัดทำฐานข้อมูลความผิดทางอาญา การป้องกันพยาน มาตรการความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายและการรวบรวม การแลกเปลี่ยนและการวิเคราะห์ข้อมูลที่เกี่ยวข้องกับลักษณะทั่วไปขององค์กรอาชญากรรม เป็นต้น

ซึ่งวัตถุประสงค์หลักของอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมที่จัดตั้งในลักษณะองค์กร คือ เพื่อส่งเสริมความร่วมมือระหว่างประเทศในการป้องกันและต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กรให้มีประสิทธิภาพ[109]และเพื่อขจัดความเหลื่อมล้ำของมาตรฐานทางกฎหมายอันเนื่องมาจากระบบกฎหมายที่แตกต่างกัน ส่งเสริมความร่วมมือและการให้ความช่วยเหลือซึ่งกันและกันในทางกฎหมายของประเทศต่าง ๆ อย่างมีประสิทธิภาพ ทั้งยังเป็นการกำหนดมาตรฐานขั้นต่ำในการยกร่างกฎหมาย เพื่อดำเนินการต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งองค์กรให้เป็นไปอย่างมีประสิทธิภาพ โดยอนุสัญญาฉบับนี้กำหนดให้ประเทศภาคีสมาชิกมีส่วนร่วมในการป้องกันและปราบปรามอาชญากรรมที่จัดตั้งในลักษณะองค์กร การฟอกเงิน การทุจริตคอร์รัปชันและการขัดขวางความยุติธรรม

มาตรการสำคัญภายใต้อนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร (United Nations Convention against Transnational Organized Crime –

---

[109] United Nations Convention Against Transnational Organized Crime. Article 1 Statement of purpose: The purpose of this Convention is to promote cooperation to prevent and combat transnational organized crime more effectively.

UNTOC) เป็นกลไกที่มีเป้าหมายเพื่อเสริมสร้างความร่วมมือระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ โดยมีมาตรการสำคัญที่กำหนดไว้อย่างเป็นระบบเพื่อให้รัฐภาคีดำเนินการตามแนวทางเดียวกัน ดังนี้

1. การบัญญัติกฎหมายภายในประเทศ รัฐภาคีต้องจัดให้มีกฎหมายภายในประเทศที่กำหนดความผิดฐานเกี่ยวข้องกับองค์กรอาชญากรรม เช่น ความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรม ความผิดฐานฟอกเงิน ความผิดฐานขัดขวางกระบวนการยุติธรรมและความผิดฐานติดสินบนเจ้าหน้าที่ของรัฐหรือเจ้าหน้าที่ต่างประเทศโดยกำหนดบทลงโทษที่เหมาะสมเพื่อให้สามารถใช้บังคับได้จริง[110]

2. การยึดและอายัดทรัพย์สินที่เกี่ยวข้องกับอาชญากรรม อนุสัญญากำหนดให้รัฐภาคีสามารถดำเนินการอายัดหรือยึดทรัพย์สินที่ได้มาจากการกระทำผิด หรือที่ใช้ในการกระทำผิด เช่น เงินสด บัญชีธนาคาร อสังหาริมทรัพย์ ยานพาหนะ เป็นต้น รวมทั้งให้สามารถโอนหรือแบ่งปันทรัพย์สินที่ยึดได้ให้แก่รัฐอื่นที่เกี่ยวข้อง[111]

3. การคุ้มครองพยานและผู้แจ้งเบาะแส กำหนดให้มีมาตรการคุ้มครองพยานผู้เสียหาย และผู้แจ้งเบาะแสที่ให้ข้อมูลเกี่ยวกับการกระทำความผิดขององค์กรอาชญากรรมข้ามชาติ เช่น การเปลี่ยนชื่อ การย้ายถิ่นฐาน หรือใช้กระบวนการปิดบังตัวตน เพื่อความปลอดภัยจากการคุกคามหรือการตอบโต้[112]

4. การส่งผู้ร้ายข้ามแดน อนุสัญญากำหนดให้การกระทำความผิดที่ครอบคลุมในอนุสัญญา เป็นความผิดที่สามารถใช้เป็นเหตุในการส่งผู้ร้ายข้ามแดนได้ และหากไม่มีสนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างรัฐภาคี ก็สามารถใช้อนุสัญญาฉบับนี้เป็นพื้นฐานทางกฎหมายได้[113]

5. ความร่วมมือทางกฎหมายระหว่างประเทศ รัฐภาคีต้องให้ความร่วมมือในการสอบสวน รวบรวมพยานหลักฐาน การส่งเอกสาร การสอบปากคำ การค้นและยึดของกลาง หรือการให้ความช่วยเหลือในรูปแบบอื่น ๆ ตามคำร้องขอจากรัฐคู่ภาคี เพื่อให้การบังคับใช้กฎหมายในคดีอาชญากรรมข้ามชาติเป็นไปอย่างมีประสิทธิภาพ[114]

---

[110] United Nations Office on Drugs and Crime (UNODC), United Nations Convention against Transnational Organized Crime and the Protocols Thereto, Articles 5–8 (2004), <https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html> accessed July 6 2025.

[111] United Nations Convention Against Transnational Organized Crime. Article 12-14.

[112] United Nations Convention Against Transnational Organized Crime. Article 24-25.

[113] United Nations Convention Against Transnational Organized Crime. Article 16.

[114] United Nations Convention Against Transnational Organized Crime. Article 18.

6. การดำเนินคดีในเขตอำนาจของรัฐ รัฐภาคีต้องกำหนดเขตอำนาจในการดำเนินคดีเมื่อความผิดเกิดขึ้นภายในอาณาเขตของตน หรือเมื่อผู้กระทำผิดเป็นพลเมืองของรัฐ หรือเมื่อผลของความผิดมีผลกระทบต่อรัฐ แม้การกระทำนั้นจะเกิดขึ้นนอกราชอาณาจักรก็ตาม[115]

7. การส่งเสริมความร่วมมือด้านเทคนิคและการฝึกอบรม อนุสัญญาสนับสนุนให้รัฐภาคีร่วมมือกันในการถ่ายทอดเทคโนโลยี การฝึกอบรมเจ้าหน้าที่ การจัดทำแนวปฏิบัติที่ดี และการแลกเปลี่ยนความรู้เพื่อเพิ่มศักยภาพในการปราบปรามอาชญากรรมข้ามชาติอย่างมีประสิทธิภาพและทันต่อสถานการณ์ที่เปลี่ยนแปลง[116]

มาตรการดังกล่าวนับว่าเป็นแนวทางที่มีความสำคัญอย่างยิ่งในการสนับสนุนการบังคับใช้กฎหมายและการสร้างความร่วมมือในระดับสากล เพื่อให้สามารถรับมือกับองค์กรอาชญากรรมข้ามชาติที่มีลักษณะซับซ้อนและดำเนินการอย่างเป็นระบบ ซึ่งก่อให้เกิดผลกระทบทั้งต่อบุคคลและระบบเศรษฐกิจของรัฐโดยรวม

2. อนุสัญญาปูดาเปสต์ (Budapest Convention on Cybercrime) ซึ่งจัดทำขึ้นโดยคณะมนตรีแห่งยุโรป (Council of Europe) และเปิดให้ลงนามเมื่อวันที่ 23 พฤศจิกายน ค.ศ. 2001 นับเป็นสนธิสัญญาฉบับแรกของโลกที่มีวัตถุประสงค์เฉพาะในการแก้ไขปัญหาอาชญากรรมทางไซเบอร์และการกระทำผิดที่เกี่ยวข้องกับระบบคอมพิวเตอร์[1] อนุสัญญาฉบับนี้กำหนดมาตรฐานขั้นต่ำของกฎหมายภายในประเทศในการรับมือกับภัยคุกคามทางไซเบอร์ และวางหลักการความร่วมมือระหว่างประเทศในการสอบสวนและดำเนินคดีที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ซึ่งมักมีลักษณะข้ามพรมแดน สาระสำคัญของอนุสัญญาฉบับนี้ครอบคลุม 4 ประเด็นหลัก ได้แก่ (1) การกำหนดประเภทความผิดทางอาญาที่เกี่ยวข้องกับระบบคอมพิวเตอร์ เช่น การเข้าถึงโดยมิชอบ การขัดขวางข้อมูล หรือการดักฟังข้อมูล (2) มาตรการด้านกระบวนการยุติธรรม เช่น การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ การค้นและยึดข้อมูลอิเล็กทรอนิกส์ (3) กลไกความร่วมมือระหว่างประเทศ คือ การส่งข้อมูลระหว่างรัฐ การช่วยเหลือทางกฎหมาย และการส่งผู้ร้ายข้ามแดน และ (4) มาตรการสร้างขีดความสามารถของประเทศภาคีในการปรับปรุงกฎหมายภายในให้ทันต่อพฤติกรรมอาชญากรรมรูปแบบใหม่ แม้อนุสัญญาฉบับนี้จะเริ่มต้นโดยประเทศในยุโรป แต่ปัจจุบันมีประเทศภาคีมากกว่า 65 ประเทศทั่วโลก รวมถึงสหรัฐอเมริกา แคนาดา ญี่ปุ่น ออสเตรเลีย และฟิลิปปินส์ โดย ฟิลิปปินส์ได้ให้สัตยาบันเข้าร่วมเป็นภาคีเมื่อปี ค.ศ. 2018 ถือเป็นประเทศแรกในอาเซียนที่เข้าร่วมอนุสัญญานี้[3] การเข้าร่วมของฟิลิปปินส์แสดงให้เห็นถึงความมุ่งมั่นในการปฏิรูปกฎหมายและขยายความร่วมมือกับ

[115] United Nations Convention Against Transnational Organized Crime. Article 15.

[116] United Nations Convention Against Transnational Organized Crime. Article 29-30.

นานาชาติเพื่อต่อสู้กับอาชญากรรมไซเบอร์ โดยเฉพาะในกรณีที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์และการหลอกลวงออนไลน์ข้ามพรมแดน

3. อนุสัญญาต่อต้านอาชญากรรมไซเบอร์ (United Nations Convention against Cybercrime) ในบริบทของความร่วมมือระหว่างประเทศเพื่อรับมือกับภัยคุกคามจากอาชญากรรมไซเบอร์ที่ทวีความซับซ้อนและขยายตัวอย่างรวดเร็ว องค์การสหประชาชาติได้มีมติในการประชุมสมัชชาใหญ่แห่งสหประชาชาติ สมัยที่ 78 เมื่อวันที่ 24 ธันวาคม พ.ศ. 2566 เห็นชอบให้มีการจัดทำ “อนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมทางไซเบอร์” (United Nations Convention against Cybercrime) ซึ่งนับเป็นความริเริ่มในระดับโลกฉบับแรกที่มีวัตถุประสงค์ในการกำหนดมาตรฐานร่วมด้านการป้องกัน ปราบปราม และอำนวยความยุติธรรมในคดีอาชญากรรมไซเบอร์ โดยจะเปิดให้มีการลงนามรับรองอนุสัญญาดังกล่าวอย่างเป็นทางการในปี พ.ศ. 2568 ณ กรุงฮานอย สาธารณรัฐสังคมนิยมเวียดนาม ซึ่งเป็นประเทศสมาชิกอาเซียนแห่งแรกที่ได้รับเกียรติเป็นเจ้าภาพในการประกาศใช้อนุสัญญาฉบับประวัติศาสตร์นี้

เนื้อหาหลักของอนุสัญญาดังกล่าวประกอบด้วย 67 มาตรา แบ่งออกเป็น 10 หมวด ซึ่งมีสาระสำคัญครอบคลุมทั้งในด้าน (1) การกำหนดความผิดอาญาใหม่เกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ การแทรกแซงข้อมูล การฉ้อโกงทางออนไลน์ และการใช้เทคโนโลยีเพื่อการกระทำความผิดอื่นๆ; (2) การวางมาตรการในการป้องกันอาชญากรรมไซเบอร์ภายในประเทศสมาชิกทั้งในมิติของกฎหมาย การบังคับใช้ และการพัฒนาศักยภาพของหน่วยงานที่เกี่ยวข้อง; (3) การสร้างกลไกความร่วมมือระหว่างประเทศอย่างเป็นระบบ รวมถึงการจัดตั้งหน่วยประสานงาน 24 ชั่วโมง (24/7 Contact Points) เพื่อการประสานข้อมูลแบบทันเหตุการณ์; และ (4) การกำหนดแนวทางในการเก็บ รักษา และแลกเปลี่ยนหลักฐานทางดิจิทัล (Electronic Evidence) ข้ามพรมแดน โดยไม่ขัดต่อหลักอธิปไตยของรัฐผู้ร้องขอหรือรัฐผู้ให้ความร่วมมือ

ความสำคัญของอนุสัญญาดังกล่าวอยู่ที่การยกระดับหลักเกณฑ์ระหว่างประเทศให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศ โดยเสนอแนวทางที่มีผลผูกพันสำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ การสืบสวนข้ามพรมแดน และการคุ้มครองสิทธิของผู้เสียหาย ทั้งนี้ บทบัญญัติมาตรา 34 แห่งอนุสัญญายังเน้นย้ำเรื่องการให้ความช่วยเหลือทางกฎหมายซึ่งกันและกันอย่างมีประสิทธิภาพ พร้อมทั้งกำหนดให้รัฐภาคีจัดให้มีมาตรการเยียวยาแก่ผู้เสียหายจากอาชญากรรมไซเบอร์ รวมถึงการคืนทรัพย์สินหรือผลประโยชน์ที่ได้มาจากการกระทำความผิด

อนุสัญญาฉบับนี้จึงถือเป็นหมุดหมายสำคัญของกฎหมายระหว่างประเทศที่สามารถใช้เป็นต้นแบบในการปรับปรุงกฎหมายภายในของประเทศสมาชิกอาเซียน เพื่อพัฒนาแนวทางการตอบสนองต่ออาชญากรรมข้ามชาติในยุคดิจิทัล โดยเฉพาะในบริบทของแก๊งคอลเซ็นเตอร์ ซึ่งมี

ลักษณะการดำเนินการเชิงเครือข่าย ซ่อนตัวผ่านช่องทางอิเล็กทรอนิกส์ และใช้ประโยชน์จากช่องว่างทางกฎหมายระหว่างรัฐ อาเซียนในฐานะภูมิภาคที่ได้รับผลกระทบอย่างมากจากปรากฏการณ์ดังกล่าว จึงควรพิจารณานำหลักการจากอนุสัญญานี้มาประยุกต์ใช้เพื่อเสริมสร้างความร่วมมือที่มีผลในทางปฏิบัติ ทั้งในด้านการแลกเปลี่ยนหลักฐานดิจิทัล การสื่อสารข้อมูลแบบเร่งด่วน และการคุ้มครองสิทธิของประชาชนผู้ตกเป็นเหยื่ออาชญากรรมไซเบอร์อย่างครอบคลุมและเป็นธรรม

**3.2.2 ระดับภูมิภาค**

3.2.2.1 สหภาพยุโรป

สหภาพยุโรปมีกฎหมายที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์โดยให้ความร่วมมือในด้านความช่วยเหลือทางอาญาซึ่งกันและกันของประเทศในกลุ่ม สหภาพยุโรปมีวัตถุประสงค์เพื่อร่วมกันแก้ไขปัญหาอาชญากรรมในกลุ่มประเทศยุโรป โดยสหภาพยุโรปได้มีการสร้างความสอดคล้องของกฎหมายอาญาของ ประเทศสมาชิกในสหภาพยุโรป (HARMONISATION OF CRIMINAL LAW IN THE EU LEGISLATION - THE CURRENT STATUS AND THE IMPACT OF THE TREATY OF LISBON) เพื่อการปราบปรามอาชญากรรมในทางระหว่างประเทศ กล่าวคือ การสร้างความสอดคล้องของกฎหมายอาญาของประเทศสมาชิกในสหภาพยุโรปเริ่มต้นจากคณะมนตรีแห่งสหภาพยุโรป ได้มีข้อเสนอแนะ (Recommendation) เลขที่ R 89 (9) ปี ค.ศ. 1989[117] ในเรื่องอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ที่เน้นให้ความสำคัญกับความพอเพียงและ การตอบสนองอย่างรวดเร็วต่ออาชญากรรมที่มีลักษณะของการข้ามพรมแดนจึงต้องสร้างความสอดคล้องโดยการลดความแตกต่างระหว่างกฎหมายของประเทศต่าง ๆ รวมทั้งต้องมีวิธีปฏิบัติและการปรับปรุงความร่วมมือทางกฎหมายระหว่างประเทศที่ดีขึ้น นอกจากนี้ ยังเน้นย้ำถึงความต้องการความเห็นพ้องร่วมกันในระดับระหว่างประเทศในเรื่องอาชญากรรมและ การจัดการกับการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์โดยมีเป้าหมายสำคัญของสหภาพยุโรป คือ การประสานความร่วมมือในการสร้างความสอดคล้องของกฎหมายอาญาระหว่างประเทศสมาชิกสหภาพยุโรป การดำเนินการนี้เป็นหนึ่งในเรื่องที่สำคัญที่สุดของความร่วมมือระหว่างประเทศ สมาชิก โดยใช้เวลาหลายสิบปีในการพยายามปรับปรุงพันธกิจร่วมกันระหว่างประเทศสมาชิกให้ดีขึ้น โดยคำนึงถึงความร่วมมือในเรื่องอาชญากรรม ซึ่งนั่นคือการสร้างความสอดคล้องของกฎหมายอาญา (Harmonization of Penal Laws) ระหว่างประเทศสมาชิกในสหภาพยุโรป

---

[117] Council of Europe Committee of Ministers, 'Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime,' <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f1094> accessed May 22 2024.

ในการดำเนินความร่วมมือในเรื่องทางอาญาประเทศสมาชิกมีหน้าที่รับผิดชอบในการทำให้บทบัญญัติที่เกี่ยวข้องกับคำนิยามของความผิดทางอาญาและบทลงโทษมีความคล้ายคลึงหรือใกล้เคียงกัน และต้องสามารถรับรองได้ว่ากฎหมายระดับชาติของตนมีวิธีการ ที่สอดคล้องหรือกลมกลืนกับประเทศสมาชิกอื่น ๆ ในการต่อสู้กับปรากฏการณ์บางอย่าง ซึ่งผลเสีย ของการปฏิบัติตามกรอบการดำเนินการดังกล่าวเกิดจากข้อผูกพันในการที่ประเทศสมาชิกต้อง คำนึงถึงระบบกฎหมายที่แตกต่างกันของประเทศสมาชิกอื่น ๆ ดังนั้นบทบัญญัติกฎหมายรวมถึง ข้อบังคับต่าง ๆ ของประเทศสมาชิกจึงมีลักษณะอย่างกว้างขวางซึ่งเป็นหลักการทั่วๆไป[118] โดยในสหภาพยุโรปได้มีการออกมาตรการในการช่วยเหลือซึ่งกันและกันในทางอาญา ดังนี้

1. สนธิสัญญาสหภาพยุโรปว่าด้วยความร่วมมือในทางอาญา[119] (The European Convention on Mutual Assistance in Criminal Matters) สนธิสัญญาฉบับนี้กำหนดกรอบความร่วมมือในการให้ความช่วยเหลือทางกฎหมายร่วมกันระหว่างประเทศสมาชิก ซึ่งมีพันธกรณีจะให้ความร่วมมืออย่างโดยกำหนดมาตรการใน ระดับกว้างที่สุดที่เป็นไปได้ (Widest measure) เพื่อการสืบสวนสอบสวนดำเนินคดีกับอาชญากรรมโดยมีเงื่อนไขสำคัญคือ ประเทศผู้ร้องขอ (Requesting state) และประเทศผู้รับการร้องขอ (Requested state) ต้องมีความตกลงร่วมกัน ด้วยการส่งคำร้องขอและพิจารณาคำร้อง ตามหลักต่างตอบแทนและตามความตกลงระหว่างกัน[120] อนุสัญญาดังกล่าววางรากฐานให้กับระบบความร่วมมือที่มีความน่าเชื่อถือและมีหลักประกันต่อสิทธิของผู้เกี่ยวข้องในการดำเนินคดีโดยมาตรการสำคัญของอนุสัญญานี้ประกอบด้วยหลักการและกลไกสำคัญ ดังนี้

---

[118] Marcin Rozmus, Ilona Topa, and Marika Walczak, 'Harmonisation of Criminal Law in the EU Legislation - The Current Status and the Impact of the Treaty of Lisbon,' <http://www.ejtn.eu/Documents/Themis/THEMIS%20written%20paper%20-%20Poland%201.pdf> accessed May 22 2024, 6.

[119] อนุสัญญายุโรปว่าด้วยการช่วยเหลือซึ่งกันและกันในเรื่องทางอาญาเป็นสนธิสัญญาความช่วยเหลือทางกฎหมายร่วมกัน ของ สภายุโรป ค.ศ. 1959 ได้รับการรับรองโดย 50 รัฐ รวมทั้ง 46 รัฐสมาชิกของสภายุโรป ซึ่งทุกฝ่ายในอนุสัญญาตกลงที่จะเสนอ "มาตรการช่วยเหลือซึ่งกันและกันที่กว้างที่สุด" ในการสืบสวนอาชญากรรม การจัดหาหลักฐาน และการดำเนินคดีกับผู้ต้องสงสัยทางอาญา อนุสัญญาระบุข้อกำหนดที่การขอความช่วยเหลือทางกฎหมายและจดหมายส่งกลับจาก "รัฐผู้ร้องขอ" ไปยัง "รัฐที่ได้รับการร้องขอ" จะต้องปฏิบัติตาม อนุสัญญายังกำหนดหลักเกณฑ์สำหรับการบังคับใช้จดหมายตอบรับดังกล่าวโดยเจ้าหน้าที่ของรัฐที่ได้รับการร้องขอ

[120] คณาธิป ทองรวีวงศ์, 'การคุ้มครองสิทธิมนุษยชนจากมาตรการความร่วมมือระหว่างประเทศในกรอบของสหประชาชาติว่าด้วยการเข้าถึงข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์ เพื่อการป้องกันและปราบปรามอาชญากรรมไซเบอร์' (วารสารมหาวิทยาลัยหาดใหญ่, 1265).

1. การให้ความช่วยเหลือทางกฎหมายในคดีอาญา อนุสัญญากำหนดให้รัฐภาคีมีพันธกรณีในการให้ความร่วมมือในการรวบรวมและส่งต่อพยานหลักฐานตามคำร้องขอจากรัฐอื่น ทั้งนี้ รวมถึงการสอบปากคำพยาน การส่งเอกสาร การออกหมายเรียก การตรวจค้น การยึดทรัพย์ และมาตรการสอบสวนอื่น ๆ ที่จำเป็นต่อการดำเนินคดี[121] ซึ่งต้องดำเนินการตามขั้นตอนทางกฎหมายของรัฐผู้ถูกร้องขอ เพื่อรักษาความสมดุลระหว่างอำนาจอธิปไตยและความร่วมมือระหว่างประเทศ

2. การถ่ายโอนพยานและหลักฐานข้ามพรมแดน สนธิสัญญาฉบับนี้เปิดโอกาสให้มีการขอความร่วมมือในการนำพยานบุคคลจากรัฐหนึ่งไปยังอีกรัฐหนึ่ง เพื่อการให้ปากคำในกระบวนการยุติธรรม หรือเพื่อยืนยันข้อเท็จจริง รวมถึงการส่งเอกสารทางราชการหรือวัตถุที่เป็นหลักฐาน[122] ทั้งนี้ รัฐภาคีสามารถปฏิเสธการส่งพยานได้หากอาจกระทบต่อความมั่นคงของชาติหรือผลประโยชน์สำคัญของรัฐ

3. หลักการความผิดซ้ำกัน การร้องขอความช่วยเหลือต้องเป็นไปในกรณีที่พฤติการณ์ที่ถูกร้องขอเป็นความผิดอาญาในกฎหมายของทั้งรัฐผู้ร้องขอและรัฐที่ถูกร้องขอ[123] หลักการนี้ทำหน้าที่เป็นกลไกการคัดกรองไม่ให้รัฐภาคีต้องดำเนินการในเรื่องที่ไม่เป็นความผิดในระบบกฎหมายของตน

4. ข้อยกเว้นจากการให้ความช่วยเหลือ แม้จะมีพันธกรณีในการให้ความร่วมมือ แต่อนุสัญญาเปิดช่องให้รัฐภาคีปฏิเสธความร่วมมือในบางกรณี เช่น หากคำร้องมีลักษณะเกี่ยวกับความผิดทางการเมืองหรือเกี่ยวข้องกับความมั่นคงของรัฐ[124] มาตรการนี้จึงสะท้อนความเคารพในอำนาจอธิปไตยของรัฐผู้ถูกร้องขอ

5. การคุ้มครองสิทธิของบุคคลและข้อมูลที่ได้รับ ในการดำเนินการตามอนุสัญญาต้องมีการเคารพสิทธิของบุคคลผู้เกี่ยวข้อง โดยเฉพาะผู้ถูกกล่าวหาในการดำเนินคดี และข้อมูลที่ได้รับจากความร่วมมือดังกล่าวต้องถูกใช้เพื่อวัตถุประสงค์เฉพาะตามที่ร้องขอเท่านั้น[125]เพื่อป้องกันการนำไปใช้ในทางที่อาจละเมิดสิทธิหรือขัดต่อหลักนิติธรรม

6. การจัดตั้งพิธีสารเพิ่มเติม ภายหลังการลงนามในอนุสัญญาหลักได้มีการจัดทำพิธีสารเพิ่มเติมอีกหลายฉบับ เช่น พิธีสารปี ค.ศ. 1978 ว่าด้วยการให้ความร่วมมือด้านการสอบสวน การ

---

[121] Council of Europe. *European Convention on Mutual Assistance in Criminal Matters*, Article 3, ETS No. 030, 1959.

[122] Ibid, Articles 4–7.

[123] Ibid, Articles 5.

[124] Ibid, Articles 2.

[125] Ibid, Articles 21.

ขอข้อมูลเกี่ยวกับบัญชีธนาคาร และการดำเนินการบางอย่างในรูปแบบที่รวดเร็วขึ้น รวมถึงพิธีสารปี ค.ศ. 2001 ซึ่งเปิดทางให้ใช้เทคโนโลยีสมัยใหม่ เช่น การประชุมทางไกลผ่านวิดีโอ (video conferencing) เพื่ออำนวยความสะดวกในการดำเนินคดีและลดภาระการเดินทาง

อีกทั้งความร่วมมือระหว่างประเทศสมาชิกสหภาพยุโรปทางอาญามีเป้าหมายหลักในการป้องกันปัญหาที่อาจเกิดขึ้นหลังจากที่กลุ่มประเทศสหภาพยุโรปได้เปิดพรมแดน ให้มีการผ่านและเข้าออกได้อย่างเสรี โดยความร่วมมือดังกล่าวจะช่วยป้องกันและปราบปรามการผ่านเข้าออกระหว่างประเทศสมาชิกโดยผิดกฎหมายและอาชญากรรมอื่น ๆ ที่เกี่ยวข้อง ทั้งนี้ได้กำหนดมาตรการขึ้นมาที่เรียกว่า "Compensatory Measures" เพื่อช่วยในการให้ความร่วมมือทางอาญาระหว่างประเทศสมาชิกด้วยกัน

2. Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union ซึ่งว่าด้วยการอายัดและริบเครื่องมือและทรัพย์สินที่ได้มาจากการกระทำความผิด โดยมีความสำคัญอย่างยิ่งในการปราบปรามแก๊งคอลเซ็นเตอร์ ซึ่งเป็นอาชญากรรมข้ามชาติประเภทหนึ่งที่เกี่ยวข้องกับการหลอกลวงและฉ้อโกงผ่านโทรศัพท์และเทคโนโลยีสารสนเทศเพื่อป้องกันไม่ให้ผู้กระทำผิดได้ประโยชน์จากกิจกรรมที่ผิดกฎหมาย และเพื่อเสริมสร้างประสิทธิภาพในการปราบปรามอาชญากรรมข้ามชาติ โดยวัตถุประสงค์หลัก คือให้ประเทศสมาชิกของสหภาพยุโรปสามารถดำเนินการอายัดและริบทรัพย์สินที่เกี่ยวข้องกับอาชญากรรม โดยเฉพาะทรัพย์สินที่ใช้เป็นเครื่องมือในการกระทำความผิด หรือได้มาโดยมิชอบ กฎหมายนี้ครอบคลุมทั้งการอายัดทรัพย์สินชั่วคราวก่อนการตัดสินคดี และการริบทรัพย์สินถาวรหลังจากมีคำพิพากษา เน้นการ ประสานความร่วมมือระหว่างประเทศสมาชิก ในการแลกเปลี่ยนข้อมูลและดำเนินการข้ามพรมแดน เพื่อป้องกันไม่ให้ผู้กระทำผิดโยกย้ายทรัพย์สินหนีซึ่ง Directive นี้เป็นเครื่องมือสำคัญในการยับยั้งการฟอกเงินและอาชญากรรมข้ามชาติ เพราะช่วยตัดเส้นทางทางการเงินของแก๊งอาชญากรรม เช่น แก๊งคอลเซ็นเตอร์ที่มีรายได้จากการหลอกลวงข้ามชาติ[126]

3. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters ซึ่งฉบับนี้จัดตั้ง European Investigation Order (EIO) หรือ คำสั่งสอบสวนของยุโรป ซึ่งเป็นเครื่องมือทางกฎหมายสำหรับความร่วมมือด้านกระบวนการยุติธรรมทางอาญาในสหภาพยุโรป โดยมีวัตถุประสงค์

[126] Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union, Official Journal of the European Union, 2014.

เพื่ออำนวยความสะดวกในการรวบรวมหลักฐานข้ามพรมแดนอย่างมีประสิทธิภาพและรวดเร็ว ระหว่างประเทศสมาชิก หนึ่งในจุดแข็งของ EIO คือการกำหนดให้ใช้รูปแบบคำสั่งเดียวกันทั้งสหภาพยุโรป ทำให้ประเทศสมาชิกสามารถร้องขอหรือดำเนินการตามคำสั่งการสืบสวนในคดีอาญาไปยังประเทศสมาชิกอื่นได้โดยไม่ต้องอาศัยกระบวนการข้อตกลงความช่วยเหลือทางกฎหมาย (Mutual Legal Assistance – MLA) แบบเดิมที่มักล่าช้าและซับซ้อน EIO ยังครอบคลุมวิธีการสืบสวนที่หลากหลายและทันสมัย เช่น การตรวจค้นและยึดทรัพย์ การสอบปากคำพยานหรือผู้ต้องหา การดักฟังโทรศัพท์และติดตามพิกัดทางโทรคมนาคม รวมถึงการเข้าถึงข้อมูลบัญชีธนาคารและธุรกรรมทางการเงิน ซึ่งเป็นมาตรการสำคัญในการจัดการกับอาชญากรรมข้ามชาติ โดยเฉพาะอย่างยิ่งในคดีที่เกี่ยวกับการหลอกลวงทางไซเบอร์ นอกจากนี้ EIO ยังมีการกำหนดระยะเวลาในการดำเนินการไว้อย่างชัดเจน โดยรัฐที่ได้รับคำร้องต้องตัดสินใจว่าจะรับหรือปฏิเสธคำสั่งภายใน 30 วัน และดำเนินการตามคำสั่งภายในระยะเวลาไม่เกิน 90 วัน ทั้งนี้เพื่อลดความล่าช้าในการสอบสวนและคุ้มครองสิทธิของผู้เสียหายในคดีอาญา อีกทั้งคำสั่ง EIO จะต้องออกโดยเจ้าหน้าที่ในกระบวนการยุติธรรม ได้แก่ ผู้พิพากษา อัยการ หรือเจ้าหน้าที่ที่มีอำนาจตามกฎหมายเท่านั้น โดยจะต้องคำนึงถึงความสมเหตุสมผลของคำสั่งและไม่ละเมิดสิทธิมนุษยชนขั้นพื้นฐาน อันเป็นหลักการพื้นฐานของกฎหมายในสหภาพยุโรป ด้วยเหตุนี้ EIO จึงเป็นเครื่องมือสำคัญที่ช่วยให้การบังคับใช้กฎหมายระหว่างประเทศสมาชิกมีประสิทธิภาพมากยิ่งขึ้น โดยเฉพาะในยุคที่อาชญากรรมไซเบอร์และการหลอกลวงข้ามพรมแดนมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง การบังคับใช้คำสั่งสอบสวนอย่างทันท่วงทีจึงเป็นปัจจัยสำคัญในการป้องกันและปราบปรามอาชญากรรมในระดับภูมิภาค[127]

4. European Arrest Warrant (EAW) เป็นกลไกทางกฎหมายภายใต้กรอบของสหภาพยุโรปที่ถูกพัฒนาขึ้นเพื่อตอบสนองต่อความจำเป็นในการส่งตัวผู้ร้ายข้ามแดนอย่างรวดเร็วและมีประสิทธิภาพในบริบทของการรวมกลุ่มภูมิภาค โดยมีผลบังคับใช้เมื่อปี ค.ศ. 2004 ตามกรอบของ Framework Decision 2002/584/JHA ซึ่งมีวัตถุประสงค์เพื่อขจัดกระบวนการส่งผู้ร้ายข้ามแดนแบบเดิมที่มักล่าช้าและซับซ้อน ด้วยการวางรากฐานของระบบความเชื่อถือซึ่งกันและกันระหว่างประเทศสมาชิกในด้านคำตัดสินของศาลและกระบวนการยุติธรรม EAW ช่วยให้ประเทศสมาชิกสามารถขอให้ประเทศอื่นในกลุ่ม สหภาพยุโรปจับกุมและส่งตัวบุคคลที่ถูกกล่าวหาหรือถูกตัดสินว่ามีความผิดทางอาญาโดยไม่จำเป็นต้องผ่านกระบวนการทางการทูตหรือคำร้องแบบรัฐต่อรัฐ ซึ่งในอดีตมักก่อให้เกิดความล่าช้าและอุปสรรคทางการเมือง ด้วยระบบนี้ ประเทศที่ได้รับหมายจับสามารถดำเนินการจับกุมและส่งตัวได้ภายในระยะเวลาอันสั้น โดยกำหนดระยะเวลาตามกฎหมายไม่เกิน 60

---

[127] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1 May 2014, 1–36.

วัน[128] นับจากวันจับกุม นอกจากนี้ EAW ยังครอบคลุมความผิดที่มีลักษณะร้ายแรงกว่า 32 ประเภท เช่น การก่อการร้าย การฟอกเงิน การค้ามนุษย์ และอาชญากรรมข้ามชาติ โดยไม่จำเป็นต้องพิสูจน์ว่าการกระทำนั้นเป็นความผิดในทั้งสองประเทศ (principle of dual criminality) หากความผิดนั้นอยู่ในรายการที่กำหนดและมีโทษจำคุกไม่น้อยกว่า 3 ปี[129] สิ่งนี้จึงเป็นเครื่องมือสำคัญที่ทำให้การดำเนินคดีอาชญากรรมข้ามชาติภายในภูมิภาคเป็นไปอย่างคล่องตัวและลดช่องว่างของกฎหมายระหว่างประเทศสมาชิก

ในทางปฏิบัติ EAW ได้รับการใช้อย่างกว้างขวางในยุโรป และได้รับการยอมรับว่าเป็นหนึ่งในกลไกสำคัญที่เสริมสร้างความเป็นหนึ่งเดียวในระบบยุติธรรมของสหภาพยุโรป โดยเฉพาะในยุคที่อาชญากรรมมีความซับซ้อนและข้ามพรมแดนมากขึ้น เช่น กรณีการติดตามตัวกลุ่มผู้ต้องหาคดีอาชญากรรมไซเบอร์หรือเครือข่ายแก๊งคอลเซ็นเตอร์ข้ามชาติ การมีหมายจับกลางเช่นนี้ทำให้หน่วยงานบังคับใช้กฎหมายสามารถทำงานร่วมกันได้อย่างรวดเร็วและมีประสิทธิภาพมากยิ่งขึ้น

ในกรณีแก๊งคอลเซ็นเตอร์ที่เป็นส่วนหนึ่งของอาชญากรรมไซเบอร์ สหภาพยุโรป (EU) ตระหนักถึงความเสี่ยงจากอาชญากรรมข้ามชาติที่พัฒนาอย่างซับซ้อนที่ใช้เทคโนโลยีสื่อสารโทรคมนาคมในการหลอกลวงผู้บริโภคเพื่อโอนเงินหรือข้อมูลส่วนตัวในทางมิชอบ แม่จะไม่ได้ระบุโดยตรงถึงแก๊งคอลเซ็นเตอร์ แต่ได้มีการวางกรอบกฎหมายหลายฉบับที่ใช้ในการป้องกันและปราบปรามพฤติกรรมเหล่านี้ในฐานะ อาชญากรรมข้ามชาติทางอาชญากรรมไซเบอร์และการฉ้อโกงโทรคมนาคม EU จึงได้ดำเนินมาตรการร่วมกันในระดับภูมิภาคเพื่อป้องกันและปราบปรามพฤติกรรมเหล่านี้ ได้แก่

1. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA ได้รับการตราขึ้นเพื่อเสริมสร้างความมั่นคงของระบบสารสนเทศภายในสหภาพยุโรป โดยมุ่งป้องกันและกำหนดโทษทางอาญาต่อการกระทำที่เกี่ยวข้องกับการเข้าถึงระบบโดยมิชอบ การแทรกแซงข้อมูลและการแทรกแซงระบบซึ่งเป็นองค์ประกอบสำคัญของอาชญากรรมไซเบอร์ สาระสำคัญของ Directive ฉบับนี้คือการกำหนดให้การกระทำบางประการ

---

[128] ‘Who does the data protection law apply to?’ (European Commission) <https://ec.europa.eu/info/law/law-topic/dataprotection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en> accessed 11 October 2020.

[129] ‘European Arrest Warrant: Facilitating Judicial Cooperation in Criminal Matters’ (European Commission) <https://commission.europa.eu/law/european-arrest-warrant_en> accessed 16 May 2025.

เป็นความผิดทางอาญาอย่างชัดเจน เช่น การเข้าถึงระบบสารสนเทศโดยมิชอบ (illegal access) ซึ่งรวมถึงกรณีที่แฮกเกอร์ใช้รหัสผ่านหรือโปรแกรมเพื่อเจาะระบบที่ไม่ได้รับอนุญาต, การแทรกแซงระบบ (system interference) อาทิ การส่งไวรัสหรือมัลแวร์เพื่อทำให้ระบบหยุดทำงาน หรือทำงานผิดปกติ, การแทรกแซงข้อมูล (data interference) ซึ่งรวมถึงการเปลี่ยนแปลง ลบ หรือทำลายข้อมูลโดยไม่ได้รับอนุญาต ตลอดจน การสกัดกั้นข้อมูล (illegal interception) เช่น การดักจับข้อมูลส่วนบุคคลหรือข้อมูลสื่อสารผ่านเครือข่าย นอกจากการกำหนดพฤติกรรมต้องห้ามแล้ว Directive นี้ยังได้วางแนวทางการลงโทษทางอาญาที่มีความเหมาะสมและได้สัดส่วน (proportionate sanctions) เพื่อให้การบังคับใช้กฎหมายสามารถป้องปรามและลงโทษผู้กระทำผิดได้อย่างมีประสิทธิภาพ โดยมีข้อกำหนดเกี่ยวกับระดับความรุนแรงของโทษที่แตกต่างกันไปตามลักษณะของความผิดและผลกระทบที่เกิดขึ้น ที่สำคัญคือ Directive 2013/40/EU ยังเน้นการสร้างความร่วมมือในระดับสหภาพยุโรป โดยกำหนดให้ประเทศสมาชิกประสานงานกับหน่วยงานระดับภูมิภาค เช่น Europol ซึ่งเป็นหน่วยงานบังคับใช้กฎหมายของ EU ด้านอาชญากรรมข้ามชาติ และ Eurojust ซึ่งเป็นกลไกความร่วมมือทางตุลาการ เพื่อแลกเปลี่ยนข้อมูล การวางแผนการสอบสวนร่วม และการประสานงานระหว่างประเทศต่าง ๆ เพื่อให้การปราบปรามอาชญากรรมไซเบอร์เป็นไปอย่างมีเอกภาพและมีประสิทธิผล[130]

2. The Directive on security of network and information systems (NIS Directive) หรือ Directive (EU) 2016/1148 สหภาพยุโรปได้มีการตรากฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ชื่อว่า กฎว่าด้วยความปลอดภัยของโครงข่ายและระบบข้อมูลข่าวสารสนเทศ (The Directive on security of network and information systems (the NIS Directive)) บังคับใช้เมื่อวันที่ 6 กรกฎาคม 2016 โดยมีวัตถุประสงค์เพื่อตอบสนองนโยบายในการสร้างความเชื่อมั่นสำหรับการสื่อสาร ให้มีความปลอดภัยมากที่สุด และเพื่อสร้างความเชื่อมั่นว่าพื้นที่ไซเบอร์ในสหภาพยุโรป จะมีความมั่นคงปลอดภัย จึงกำหนดมาตรฐานความปลอดภัยขั้นต่ำที่นำมาใช้กับระบบสื่อสารและ ข้อมูลสารสนเทศทั้งหมด ซึ่งมีการขับเคลื่อนผ่าน 3 ยุทธศาสตร์คือ (1) การสร้างความร่วมมือระหว่างประเทศสมาชิก (2) การสร้างความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์สำหรับประเทศสมาชิก และ (3) การสร้างวัฒนธรรมในเชิงป้องกันและการใช้งานที่ปลอดภัยจากภัย

[130] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Official Journal of the European Union, L 218, 14 August 2013, 8–14, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040> accessed July 6 2025..

คุกคามทางไซเบอร์[131] และล่าสุดได้มีการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (General Data Protection Regulation (GDPR)) เมื่อวันที่ 25 พฤษภาคม 2561 โดยมีวัตถุประสงค์ในการคุ้มครองข้อมูลและข้อมูลส่วนบุคคลของสหภาพยุโรปให้มีความชัดเจนและรัดกุมมากขึ้นกว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับเดิม[132]เพื่อเพิ่มความโปร่งใสและความเป็นมาตรฐานเดียวกันทั่วยุโรป และสิ่งสำคัญ คือ การคุ้มครองข้อมูลส่วนบุคคลของพลเมืองในสหภาพยุโรปไม่ว่าข้อมูลจะเก็บอยู่ที่ใดในโลกก็ตาม โดยมีเนื้อหาสาระที่สำคัญ ดังนี้

มาตรา 3 ได้กำหนดหลักเกณฑ์ Minimum Harmonization ซึ่งเปิดโอกาสให้แต่ละประเทศสมาชิกสามารถตรา หรือคงไว้ซึ่งบทบัญญัติกฎหมายภายในของตนเอง ที่มุ่งให้บรรลุถึงระดับความมั่นคงของระบบเครือข่ายและข้อมูลที่สูงกว่ามาตรฐานขั้นต่ำที่กฎหมายของสหภาพยุโรปกำหนดไว้ได้ ทั้งนี้โดยไม่กระทบต่อพันธกรณีตามกฎหมายของสหภาพยุโรปที่มีอยู่[133]

มาตรา 14 กำหนดให้ผู้ให้บริการโครงสร้างพื้นฐานจำเป็นต้องดำเนินมาตรการด้านความปลอดภัยเพื่อจัดการกับความเสี่ยงที่อาจเกิดขึ้นต่อความมั่นคงของระบบเครือข่ายและข้อมูลที่ใช้ในการดำเนินงานของตนและหากเกิดเหตุการณ์ที่ส่งผลกระทบต่อการให้บริการอย่างมีนัยสำคัญจะต้องแจ้งเหตุการณ์นั้นต่อหน่วยงานที่มีอำนาจ[134]

มาตรา 16 กำหนดข้อผูกพันทางกฎหมายของประเทศสมาชิกสหภาพยุโรปต่อการควบคุมดูแลผู้ให้บริการดิจิทัล (Digital Service Providers) อันได้แก่ ผู้ให้บริการแพลตฟอร์ม

---

[131] 'The Directive on security of network and information systems (NIS Directive)' (Europa) <https://ec.europa.eu/digital-singlemarket/en/network-and-information-security-nis-directive> accessed 22 May 2024.

[132] 'An Overview of the Main Changes under GDPR and How They Differ from the Previous Directive' (EU) <https://www.eugdpr.org/keychanges.html> accessed 23 May 2024.

[133] Directive (EU) 2016/1148

Article 3 Without prejudice to Article 16(10) and to their obligations under Union law, Member States may adopt or maintain provisions with a view to achieving a higher level of security of network and information systems.

[134] Directive (EU) 2016/1148

Article 14 1. Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations

3. Operators of essential services shall notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide.

ออนไลน์ บริการค้นหาออนไลน์ และบริการคลาวด์ โดยในวรรคหนึ่ง กำหนดให้ผู้ให้บริการดิจิทัลต้องดำเนินมาตรการทางเทคนิคและทางองค์กรที่เหมาะสมและได้สัดส่วน เพื่อบริหารจัดการความเสี่ยงที่มีต่อความมั่นคงของระบบเครือข่ายและข้อมูล ซึ่งเป็นการสร้างมาตรฐานขั้นต่ำด้านความมั่นคงไซเบอร์ในระดับภูมิภาค ขณะที่ในวรรคสาม กำหนดให้ผู้ให้บริการดิจิทัลมีหน้าที่แจ้งเหตุการณ์ที่มีผลกระทบอย่างมีนัยสำคัญต่อการให้บริการแก่หน่วยงานผู้มีอำนาจโดยต้องแจ้งโดยไม่ล่าช้า อันสะท้อนถึงกลไกตอบสนองและการแจ้งเตือนภัยไซเบอร์อย่างมีประสิทธิภาพในระดับชาติและภูมิภาค ทั้งนี้ วรรคสิบยังรับรองสิทธิของประเทศสมาชิกในการออกหรือคงไว้ซึ่งมาตรการภายในที่มีความเข้มงวดหรือระดับมาตรฐานที่สูงกว่าเพื่อให้สอดคล้องกับบริบทของแต่ละประเทศ โดยไม่ขัดต่อกรอบข้อผูกพันของกฎหมายสหภาพยุโรป[135]

มาตรา 7 กำหนดให้ประเทศสมาชิกสหภาพยุโรปมีพันธกรณีในการแต่งตั้งหน่วยงานที่มีอำนาจรับผิดชอบด้านความมั่นคงของระบบเครือข่ายและสารสนเทศ (national competent authority) ซึ่งต้องครอบคลุมภาคส่วนสำคัญตามที่ระบุไว้ในภาคผนวกของกฎหมายฉบับนี้ นอกจากนี้

---

[135] Directive (EU) 2016/1148

Article 14 1. Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:

(a) the security of systems and facilities;

(b) incident handling;

(c) business continuity management;

(d) business continuity management;

(e) compliance with international standards.

3. Member States shall ensure that digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability.

10. Without prejudice to Article 1(6), Member States shall not impose any further security or notification requirements on digital service providers.

ประเทศสมาชิกยังต้องแต่งตั้งจุดติดต่อกลางระดับชาติเพื่อเป็นศูนย์กลางประสานงานทั้งภายในและกับประเทศสมาชิกอื่น พร้อมกันนี้ยังต้องจัดตั้งหรือแต่งตั้ง CSIRTs (Computer Security Incident Response Teams) ซึ่งมีบทบาทในการรับมือกับความเสี่ยงและเหตุการณ์ด้านไซเบอร์ในภาคส่วนที่มีความสำคัญ การกำหนดโครงสร้างนี้มีเป้าหมายเพื่อส่งเสริมการตอบสนองต่อภัยคุกคามไซเบอร์อย่างเป็นระบบ มีความต่อเนื่องและสามารถแลกเปลี่ยนข้อมูลระหว่างประเทศสมาชิกได้อย่างมีประสิทธิภาพอันเป็นพื้นฐานสำคัญของการบูรณาการความร่วมมือด้านความมั่นคงทางไซเบอร์ในระดับภูมิภาค[136]

มาตรา 10 กำหนดให้มีการจัดตั้งกลุ่มความร่วมมือซึ่งเป็นกลไกระดับสหภาพยุโรปเพื่อสนับสนุนความร่วมมือเชิงยุทธศาสตร์ระหว่างประเทศสมาชิก โดยมีภารกิจหลักในการส่งเสริมการแลกเปลี่ยนข้อมูล ประสบการณ์ และแนวปฏิบัติที่ดีในการรับมือกับภัยคุกคามไซเบอร์ รวมถึงให้คำแนะนำเกี่ยวกับการดำเนินการตามกฎหมายฉบับนี้ สนับสนุนการพัฒนาศักยภาพของประเทศสมาชิก และการวางแผนยุทธศาสตร์ในระดับชาติ กลุ่มความร่วมมือยังเป็นเวทีสำคัญในการสร้างความไว้วางใจร่วมกันซึ่งเป็นปัจจัยที่จำเป็นต่อการดำเนินมาตรการความมั่นคงในสภาพแวดล้อมดิจิทัลที่เชื่อมโยงกันอย่างซับซ้อน โดยเฉพาะในกรณีของอาชญากรรมไซเบอร์ข้ามพรมแดน[137]

---

[136] Directive (EU) 2016/1148

Article 7 1. Each Member State shall designate one or more national competent authorities on the security of network and information systems covering at least the sectors referred to in Annex II and the services referred to in Annex III.

2. Each Member State shall designate a national single point of contact on the security of network and information systems.

3. Each Member State shall designate one or more CSIRTs (Computer Security Incident Response Teams) responsible for handling risks and incidents for the sectors and services referred to in paragraph 1.

[137] Directive (EU) 2016/1148

Article 10 1. The Cooperation Group shall support and facilitate strategic cooperation and the exchange of information among Member States and shall develop trust and confidence amongst them.

2. To that end, the Cooperation Group shall have the following tasks:

(a) provide guidance on the implementation of this Directive;

(b) assist Member States in building capacity;

(c) exchange best practices on the identification and notification of incidents;

มาตรา 19 สะท้อนหลักการพื้นฐานของการกำกับดูแลด้านความมั่นคงไซเบอร์ในระดับสหภาพยุโรป ซึ่งเน้นย้ำว่าข้อมูลที่ได้จากการแลกเปลี่ยนเพื่อวัตถุประสงค์ในการป้องกันและรับมือกับอาชญากรรมทางไซเบอร์ต้องได้รับการดูแลอย่างเข้มงวด โดยเฉพาะข้อมูลที่อาจส่งผลกระทบต่อความมั่นคงของประเทศหรือสิทธิความเป็นส่วนตัวของบุคคล การรักษาความลับจึงเป็นเครื่องมือสำคัญในการสร้างความไว้วางใจระหว่างประเทศสมาชิก องค์กรเทคนิค และภาคเอกชนที่เกี่ยวข้องในการจัดการภัยคุกคามไซเบอร์[138]

(d) discuss capabilities and preparedness of Member States;

(e) exchange information and cooperate on awareness-raising and training;

(f) exchange information on research and development;

(g) identify emerging risks and threats;

(h) discuss the modalities for reporting incidents;

(i) collect best practices on public-private partnerships;

(j) support Member States in reviewing national strategies;

(k) cooperate with relevant Union institutions, bodies, offices and agencies.

[138] Directive (EU) 2016/1148

Article 19 Member States shall ensure that competent authorities, single points of contact and CSIRTs ensure the confidentiality of the information and data which they receive in the course of carrying out their duties and functions. The obligation of professional secrecy shall apply to all persons who work or have worked for the competent authorities or CSIRTs.

ในปัจจุบันมี NIS2 Directive (Directive (EU) 2022/2555) คือกฎหมายฉบับใหม่ของสหภาพยุโรปที่มีผลบังคับใช้แทน NIS Directive ฉบับเดิม (Directive (EU) 2016/1148) โดยมีวัตถุประสงค์เพื่อยกระดับความมั่นคงปลอดภัยทางไซเบอร์ในสหภาพยุโรปให้ทันสมัย เข้มแข็ง และตอบโจทย์ต่อภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรงและซับซ้อนมากยิ่งขึ้น โดยเหตุผลที่มี NIS2 เนื่องจาก NIS ฉบับแรก (2016) มีช่องว่างหลายประการ เช่น ความไม่สอดคล้องกันของกฎเกณฑ์ระหว่างประเทศสมาชิก ขอบเขตของภาคส่วนที่อยู่ภายใต้การควบคุมมีความจำกัด ทำให้บางภาคส่วนสำคัญไม่ได้อยู่ภายใต้ข้อบังคับและการรายงานเหตุการณ์ไซเบอร์ขาดความสม่ำเสมอ โดยสาระสำคัญของ NIS2 Directive ได้แก่[139]

1) ขยายขอบเขตของผู้มีหน้าที่ปฏิบัติตาม ครอบคลุมทั้ง ภาคบริการจำเป็น (Essential Entities) และ ภาคบริการสำคัญ (Important Entities) เช่น ภาคการเงิน พลังงาน สุขภาพ โครงสร้างพื้นฐานดิจิทัล รวมถึงผู้ให้บริการแพลตฟอร์มดิจิทัลและผู้ให้บริการคลาวด์

2) กำหนดมาตรฐานขั้นต่ำในการบริหารจัดการความเสี่ยง องค์กรที่อยู่ภายใต้ข้อบังคับต้องมีมาตรการจัดการความเสี่ยงทางไซเบอร์ เช่น การประเมินความเสี่ยง การเข้ารหัส การบริหารจัดการเหตุการณ์ และการรายงานเหตุการณ์ภายในเวลาที่กำหนด (ภายใน 24 ชั่วโมงหลังพบเหตุ)

3) บทลงโทษที่เข้มงวดขึ้น NIS2 อนุญาตให้กำหนดบทลงโทษที่มีประสิทธิภาพ เหมาะสม และเป็นการยับยั้ง เช่น การปรับเงิน การห้ามผู้บริหารระดับสูงดำรงตำแหน่งในบางกรณี

4) เพิ่มความร่วมมือระหว่างประเทศสมาชิก มีการจัดตั้ง European Cyber Crises Liaison Organisation Network (EU-CyCLONe) เพื่อเป็นศูนย์กลางในการประสานงานรับมือเหตุการณ์ไซเบอร์ขนาดใหญ่ในระดับสหภาพ

5) บทบาทของ CSIRTs และ Single Points of Contact (SPOCs) ประเทศสมาชิกต้องมีทีมรับมือเหตุการณ์ความปลอดภัยทางไซเบอร์ (CSIRT) และหน่วยงานประสานกลางเพื่อแลกเปลี่ยนข้อมูลและวิเคราะห์ความเสี่ยงอย่างรวดเร็ว

แม้ NIS2 จะไม่ได้ระบุถึงแก๊งคอลเซ็นเตอร์โดยตรง แต่โครงสร้างของกฎหมายมุ่งเน้นไปที่การรับมือกับภัยคุกคามไซเบอร์ที่มีลักษณะเป็น อาชญากรรมข้ามพรมแดน และมีผลกระทบต่อโครงสร้าง

---

[139] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS2 Directive), Official Journal of the European Union, L 333, 27 December 2022, pp. 80–152 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555> accessed 6 July 2025.

พื้นฐานที่สำคัญและประชาชน เช่น การโจมตีระบบเครือข่าย การเข้าถึงข้อมูลส่วนตัวโดยมิชอบ หรือการใช้ระบบโทรคมนาคมในการล่อลวงประชาชน ซึ่งล้วนเป็นลักษณะที่ตรงกับพฤติการณ์ของ แก๊งคอลเซ็นเตอร์

3. General Data Protection Regulation – Regulation (EU) 2016/679 (ระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล)

การป้องกันอาชญากรรมข้ามชาติในยุคดิจิทัลไม่อาจแยกขาดจากการคุ้มครองข้อมูลส่วนบุคคล เนื่องจาก ข้อมูลของเหยื่อ คือทรัพยากรหลักที่อาชญากรใช้ในการดำเนินการ เช่น การแอบอ้างตัวตน หลอกลวงผ่านโทรศัพท์ การส่งลิงก์ฟิชชิ่ง หรือการโทรข่มขู่จากหมายเลขปลอม (spoofed calls) ดังนั้น หากสามารถสกัดกั้นไม่ให้ข้อมูลเหล่านี้รั่วไหลได้ตั้งแต่ต้น ก็ย่อมเป็นการลดความเสี่ยงไม่ให้ประชาชนตกเป็นเหยื่อของเครือข่ายคอลเซ็นเตอร์ โดยสหภาพยุโรปได้กำหนดระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือ GDPR (General Data Protection Regulation – Regulation (EU) 2016/679) ซึ่งมีผลบังคับใช้ตั้งแต่ปี ค.ศ. 2018 โดยกำหนดให้ทั้งหน่วยงานภาครัฐและภาคเอกชนที่เก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลต้องรับผิดชอบต่อการคุ้มครองข้อมูลดังกล่าวอย่างเคร่งครัด โดยมีหลักการสำคัญ เช่น การใช้ข้อมูลเท่าที่จำเป็น ความโปร่งใสในการแจ้งวัตถุประสงค์ของการใช้ข้อมูล และการจัดให้มีมาตรการรักษาความปลอดภัยทั้งในด้านเทคนิคและการบริหารจัดการ[140] นอกจากนี้ หากมีเหตุการณ์ข้อมูลรั่วไหลหรือถูกเจาะระบบ หน่วยงานควบคุม

---

[140] General Data Protection Regulation

Article 5 – Principles relating to processing of personal data Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary (‘storage limitation’);

(f) processed in a manner that ensures appropriate security of the personal data (‘integrity and confidentiality’).

ข้อมูลจะต้องแจ้งเหตุไปยังหน่วยงานกำกับดูแลภายใน 72 ชั่วโมง และต้องแจ้งเจ้าของข้อมูลหากพบว่าเหตุการณ์นั้นอาจส่งผลกระทบร้ายแรง[141]

ภายใต้แนวทางของ GDPR ยังมีการกำหนดให้ผู้ควบคุมข้อมูลต้องดำเนินการประเมินความเสี่ยงล่วงหน้า (Data Protection Impact Assessment: DPIA) โดยเฉพาะในกรณีที่มีการใช้เทคโนโลยีใหม่ หรือมีการประมวลผลข้อมูลในระดับที่อาจสร้างผลกระทบอย่างร้ายแรงต่อสิทธิของบุคคล ข้อกำหนดนี้ทำให้การวางระบบคุ้มครองข้อมูลมีความรอบคอบตั้งแต่ต้นทาง และลดโอกาสที่ข้อมูลจะรั่วไหลไปยังกลุ่มอาชญากรและบทบาทในการป้องกันเหตุการณ์รั่วไหล GDPR ยังมีผลในเชิงการยับยั้ง (deterrence) โดยกำหนดโทษปรับที่รุนแรงต่อองค์กรที่ละเมิด เช่น ปรับสูงสุดไม่เกิน 20 ล้านยูโร หรือ 4% ของรายได้รวมทั่วโลกของบริษัทในปีบัญชีที่ผ่านมา (แล้วแต่จำนวนใดจะสูงกว่า)[3] ทำให้องค์กรต่าง ๆ จำเป็นต้องให้ความสำคัญกับการจัดการข้อมูลอย่างจริงจัง ซึ่งทั้งหมดนี้ส่งผลทางอ้อมต่อการ ลดโอกาสที่ข้อมูลส่วนบุคคลของประชาชนจะรั่วไหลและตกไปอยู่ในมือของเครือข่ายอาชญากรได้อย่างมีนัยสำคัญ[142]

ทั้งนี้ การปราบปรามอาชญากรรมข้ามชาติในรูปแบบของแก๊งคอลเซ็นเตอร์ไม่อาจกระทำได้อย่างมีประสิทธิภาพโดยอาศัยกลไกภาครัฐเพียงฝ่ายเดียว หากแต่จำเป็นต้องอาศัยการบูรณาการระหว่างหน่วยงานรัฐกับภาคเอกชนที่เกี่ยวข้องโดยตรง โดยเฉพาะในสองภาคส่วนหลัก ได้แก่ สถาบันการเงินและผู้ให้บริการโทรคมนาคม ซึ่งเป็นโครงสร้างพื้นฐานที่อาชญากรใช้ในการดำเนินการหลอกลวงและเคลื่อนย้ายเงินผ่านบัญชีม้า หรือส่งสัญญาณโทรศัพท์ผ่านหมายเลขปลอม

สหภาพยุโรปจึงได้กำหนดแนวทางการมีส่วนร่วมของภาคเอกชนอย่างชัดเจนผ่านกฎหมายหลายฉบับ โดยเฉพาะในส่วนของสถาบันการเงินนั้น Directive (EU) 2015/849 หรือที่รู้จักในชื่อ Anti-Money Laundering Directive (AMLD) ได้กำหนดให้ธนาคารต้องมีหน้าที่ตรวจสอบ

---

[141] General Data Protection Regulation

Article 33 – Notification of a personal data breach to the supervisory authority

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority (...), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

[142] General Data Protection Regulation

Article 83 – General conditions for imposing administrative fines

Administrative fines up to €20 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, may be imposed depending on the nature, gravity and duration of the infringement.

ตัวตนลูกค้า (Customer Due Diligence) ติดตามธุรกรรมที่ผิดปกติ และรายงานธุรกรรมต้องสงสัยต่อ Financial Intelligence Unit (FIU) ของรัฐสมาชิก[143] รวมถึง Directive (EU) 2019/1153 ซึ่งให้อำนาจแก่หน่วยงานบังคับใช้กฎหมายในการเข้าถึงข้อมูลบัญชีธนาคารของผู้ต้องสงสัยโดยไม่ต้องผ่านกระบวนการยุติธรรมแบบล่าช้า[144] ซึ่งช่วยให้การติดตามเส้นทางการเงินของแก๊งคอลเซ็นเตอร์สามารถกระทำได้อย่างทันท่วงที ในส่วนของบริษัทโทรคมนาคม สหภาพยุโรปใช้ Directive 2002/58/EC หรือ ePrivacy Directive ซึ่งกำหนดให้ผู้ให้บริการโทรคมนาคมต้องเก็บรักษาข้อมูลการติดต่อสื่อสาร (traffic data) อย่างปลอดภัย[145] และต้องสามารถเปิดเผยข้อมูลต้นทางให้แก่เจ้าหน้าที่เมื่อมีเหตุอันควรสงสัยว่าเกี่ยวข้องกับการกระทำความผิดร้ายแรง[146] นอกจากนี้ ยังเปิดช่องให้รัฐสมาชิกสามารถออกกฎหมายภายในเพื่อบังคับให้เปิดเผยข้อมูลเบอร์โทรศัพท์หรือ IP address ของผู้ใช้ที่อาจเกี่ยวข้องกับอาชญากรรมข้ามชาติภายใต้ข้อยกเว้นด้านความมั่นคง

3.2.2.2 อาเซียน

ปัญหาอาชญากรรมข้ามชาติในภูมิภาคอาเซียนมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง ทั้งในเชิงปริมาณ ความรุนแรง และความซับซ้อนของรูปแบบการกระทำความผิด โดยภูมิภาคอาเซียนได้

---

[143] Directive (EU) 2015/849 — Anti-Money Laundering Directive (AMLD)

Article 13 – Customer Due Diligence Measures

"Member States shall require obliged entities to apply customer due diligence measures… when establishing a business relationship, carrying out occasional transactions above a threshold, or where there is suspicion of money laundering or terrorist financing."

[144] Directive (EU) 2019/1153 — Access to Financial Information

Article 5 – Direct Access to Bank Account Information

"Member States shall ensure that the competent authorities have direct access to bank account information held in the centralised bank account registers."

[145] Directive 2002/58/EC — ePrivacy Directive

Article 5 – Confidentiality of the Communications

"Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network…"

[146] Directive 2002/58/EC — ePrivacy Directive

Article 15 – Exceptions

"Member States may adopt legislative measures to restrict the scope of the rights and obligations… when such restriction constitutes a necessary, appropriate and proportionate measure to safeguard national security… or for the prevention, investigation, detection and prosecution of criminal offences…"

กลายเป็นทั้ง “ต้นทาง” “ทางผ่าน” และ “ปลายทาง” ของการก่ออาชญากรรมลักษณะดังกล่าว แม้ว่าอาเซียนจะมีนโยบายและกลไกความร่วมมือในการป้องกันและปราบปรามอาชญากรรมข้ามชาติระหว่างรัฐสมาชิกเพิ่มมากขึ้น ทว่าอาชญากรรมข้ามชาติก็ยังคงขยายตัวต่อเนื่อง ซึ่งมีสาเหตุสำคัญจากความแตกต่างของระบบกฎหมาย ขั้นตอนกระบวนการยุติธรรม และศักยภาพในการบังคับใช้กฎหมายของแต่ละประเทศสมาชิก จากสถานการณ์ดังกล่าวหน่วยงานผู้บังคับใช้กฎหมายของประเทศสมาชิกอาเซียนจึงจำเป็นต้องเสริมสร้างความร่วมมือทั้งในระดับทวิภาคีและพหุภาคี เพื่อรองรับต่อการเปลี่ยนแปลงและการขยายตัวของอาชญากรรมข้ามชาติ จากการศึกษาพบว่า อาเซียนได้มีความร่วมมือระหว่างประเทศในการจัดการกับแก๊งคอลเซ็นเตอร์ในลักษณะของ มาตรการบูรณาการ ซึ่งครอบคลุมการแบ่งปันข้อมูลข่าวกรอง การร่วมมือด้านการสืบสวนและการจับกุม การส่งผู้ร้ายข้ามแดน และการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง ทั้งนี้ การเสริมสร้างขีดความสามารถด้านดิจิทัลของหน่วยงานบังคับใช้กฎหมาย รวมทั้งการออกแบบกลไกความร่วมมือที่มีลักษณะ “ตอบสนองทันเวลา” (real-time cooperation) จะเป็นปัจจัยสำคัญในการลดช่องว่างที่อาชญากรข้ามชาติเข้าไปแสวงหาประโยชน์จากโครงสร้างทางกฎหมายที่ต่างกันของประเทศสมาชิก โดยอาเซียนได้ดำเนินมาตรการในการให้ความช่วยเหลือกันในทางอาญา ดังนี้

สนธิสัญญาความช่วยเหลือซึ่งกันและกันในทางอาญาของภูมิภาคอาเซียน ( Treaty on Mutual Legal Assistance in Criminal Matters )

เป็นเครื่องมือทางกฎหมายสำคัญระดับภูมิภาคที่ได้กำหนดมาตรการทางกฎหมายสำหรับหน่วยงานบังคับใช้กฎหมายในการให้ความช่วยเหลือและการขอความช่วยเหลือระหว่างรัฐต่อรัฐในภูมิภาคอาเซียนในเรื่องทางอาญาไว้หลายรูปแบบ แต่มีลักษณะที่น่าสนใจกว่าสนธิสัญญาทวิภาคีหรือพหุภาคีทั่วไป กล่าวคือ ได้วางหลักเกณฑ์ความช่วยเหลือระหว่างประเทศอาเซียนไว้มากกว่าสนธิสัญญาสองฝ่ายทั่ว ๆ ไป เช่น การจัดหาให้ซึ่งเอกสารและบันทึกอื่น ๆ ที่ประชาชนใช้ประโยชน์ได้ค่าใช้จ่าย ซึ่งแน่นอนว่าประเทศสมาชิกอาเซียนที่ได้ลงนามรับรองสนธิสัญญาดังกล่าวมีพันธกรณีที่จะต้องนำเอาเงื่อนไขและข้อบทต่าง ๆ ไปกำหนดเป็นกฎหมายภายในเพื่อบังคับใช้ให้เป็นไปในแนวทางเดียวกัน อย่างไรก็ตาม สนธิสัญญาอาเซียนนฉบับนี้มีข้อจำกัดที่คล้ายคลึงกับสนธิสัญญาระหว่างประเทศในเรื่องทางอาญาทั่วไปโดยรัฐผู้รับคำร้องขอสามารถปฏิเสธการให้ความช่วยเหลือได้หากคำร้องขอเข้าข่ายคดีที่เกี่ยวเนื่องกับประเด็นทางการเมือง เชื้อชาติ ศาสนา เพศ ชาติกำเนิด สัญชาติ และความผิดทางทหาร รวมถึงคดีความมั่นคงในลักษณะอื่น ๆ สนธิสัญญาฯ ได้เปิดโอกาสให้ผู้ประสานงานกลางของแต่ละรัฐสามารถส่งคำร้องขอความช่วยเหลือและการติดต่อประสานงานผ่านทางช่องทางตำรวจสากล (INTERPOL) หรือองค์การตำรวจอาเซียน (ASEANAPOL ในสถานการณ์เร่งด่วนได้ จึงทำให้ข้อมูลและพยานหลักฐานที่ได้จากการประสานงานทางคดีผ่านช่องทางดังกล่าว

ได้รับการยอมรับในกระบวนพิจารณาชั้นศาลมากขึ้น ดังนั้น การที่สนธิสัญญาฯได้ระบุถึงกลไกการประสานงานดังกล่าวจึงเท่ากับเป็นการยอมรับถึงความถูกต้องในการประสานความร่วมมือระหว่างประเทศโดยปริยาย[147] โดยสนธิสัญญาดังกล่าวมีสาระสำคัญ ดังนี้

1. มีการกำหนดขอบเขตของความช่วยเหลือที่อยู่ภายใต้สนธิสัญญาฯ รวมถึงกรณีที่ไม่อยู่ภายใต้บังคับของสนธิสัญญา ข้อจำกัดในการให้ความช่วยเหลือของภาคีสมาชิกและการแต่งตั้งผู้ประสานงานกลางของแต่ละประเทศภาคี เพื่อทำหน้าที่จัดทำและรับคำร้องขอความช่วยเหลือ

2. กำหนดรูปแบบและเนื้อหาของคำร้องขอความช่วยเหลือในทางอาญา การดำเนินการตามคำร้องขอ และการรักษาความลับของข้อมูลตามคำร้องของประเทศสมาชิก

3. กำหนดข้อจำกัดในการใช้พยานหลักฐานที่ได้มาจากการให้ความช่วยเหลือ เช่น การได้มาซึ่งคำให้การโดยสมัครใจของผู้ให้การ การได้มาซึ่งพยานหลักฐาน และสิทธิในการปฏิเสธการให้พยานหลักฐานในบางกรณี

4. กำหนดกระบวนการในการจัดหาเอกสารและบันทึกอื่น ๆ ที่ประชาชนใช้ประโยชน์ได้ รวมถึงการปรากฏตัวของบุคคลในประเทศภาคีผู้ร้องขอ และการปรากฏตัวของบุคคลที่ถูกควบคุมตัวในประเทศภาคีผู้ร้องขอด้วย

5. กำหนดหลักประกันในการเดินทางผ่านของบุคคลที่ถูกควบคุมตัว การค้นและยึดพยานหลักฐาน การส่งคืนพยานหลักฐาน การติดตามหาที่อยู่หรือการระบุตัวบุคคล การส่งเอกสารและความช่วยเหลือในการดำเนินการริบทรัพย์สิน

6. กำหนดความสอดคล้องกับข้อตกลงระหว่างประเทศอื่น ๆ การรับรองและการยืนยันความถูกต้องแท้จริงของข้อมูล ค่าใช้จ่ายในการดำเนินการ การปรึกษาหารือ การแก้ไขเพิ่มเติม การระงับข้อพิพาท และการตั้งข้อสงวน

7. กำหนดเงื่อนไขเกี่ยวกับการลงนาม การให้สัตยาบัน การภาคยานุวัติ การเก็บรักษาและการลงทะเบียนสนธิสัญญา การมีผลบังคับใช้ ตลอดจนการบอกเลิกสนธิสัญญา รวมถึงการแต่งตั้งผู้เก็บรักษาสนธิสัญญา

ทั้งนี้ ในกรณีแก๊งคอลเซ็นเอตร์เพื่อเป็นการเสริมสร้างความร่วมมือในการต่อต้านอาชญากรรมทางไซเบอร์ อาเซียนได้มีการจัดทำตราสารความมั่นคงในลักษณะของปฏิญญา (Declaration) โดยที่ประชุมสุดยอดผู้นำอาเซียนครั้งที่ 31 ระหว่างวันที่ 13 พฤศจิกายน 2560

---

[147] ชิตพล กาญจนกิจ, ‘ความร่วมมือระหว่างประเทศว่าด้วยกระบวนการยุติธรรมทางอาญาอาเซียน : ข้อเสนอเชิงยุทธศาสตร์เพื่อการเตรียมความพร้อมเข้าสู่ประชาคมอาเซียน’ (NIDA Development Journal ปีที่ 56 ฉบับที่ 3, 2559) 13–14.

(ASEAN Declaration to Prevent and Combat Cybercrime) ณ กรุงมะนิลา สาธารณรัฐฟิลิปปินส์ คือ

ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ ค.ศ.2017 (ASEAN Declaration to Prevent and Combat Cybercrime)[148] ซึ่งให้ความสำคัญกับการปรับปรุงกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์และหลักฐานทางอิเล็กทรอนิกส์ รวมทั้งสนับสนุนการร่างกรอบการทำงานระดับภูมิภาคเพื่อสร้างความร่วมมือระหว่างประเทศสมาชิกและการกำหนดแผนปฏิบัติการระดับชาติในการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์ รวมถึงการให้ความช่วยเหลือด้านผู้เชี่ยวชาญทางเทคนิคในการป้องกันและต่อต้านอาชญากรรมไซเบอร์ อันเป็นการยกระดับความร่วมมือระหว่างประเทศสมาชิกอาเซียนและประเทศคู่เจรจา รวมทั้งหน่วยงานและองค์กรต่าง ๆ ที่เกี่ยวข้องทั้งในระดับภูมิภาคและนานาชาติ เช่น หัวหน้าตำรวจอาเซียน หัวหน้าตำรวจภาคพื้นยุโรปและองค์การตำรวจสากล นอกจากนี้ปฏิญญาฯยังมีวัตถุประสงค์ในการเสริมสร้างความมั่นคงทางเทคโนโลยี การป้องกัน และความสามารถในการแก้ไขปัญหาเกี่ยวกับอาชญากรรมทางไซเบอร์ เพื่อพัฒนาขีดความสามารถของอาเซียนในการสร้างและพัฒนาศักยภาพในการต่อสู้กับอาชญากรรมทางไซเบอร์อีกด้วย อย่างไรก็ตามปฏิญญาดังกล่าวเป็นการแสดงเจตนารมณ์ร่วมกันระหว่างประเทศสมาชิกในการสร้างความร่วมมือระหว่างกันในการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์ในภูมิภาคอาเซียน โดยในทางกฎหมายระหว่างประเทศการจัดทำปฏิญญาในลักษณะนี้ไม่ก่อให้เกิดพันธกรณีระหว่างประเทศที่ร่วมรับรองปฏิญญา โดยวัตถุประสงค์ของปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ ค.ศ. 2017 (ASEAN Declaration to Prevent and Combat Cybercrime) มีสาระสำคัญ ดังนี้[149]

1. ส่งเสริมความร่วมมือระหว่างประเทศสมาชิกอาเซียน ในการป้องกันและต่อต้านอาชญากรรมไซเบอร์ โดยเน้นการประสานการทำงานทั้งในระดับทวิภาคีและพหุภาคี

2. ส่งเสริมความร่วมมือระหว่างประเทศสมาชิกอาเซียน ในการป้องกันและต่อต้านอาชญากรรมไซเบอร์ โดยเน้นการประสานการทำงานทั้งในระดับทวิภาคีและพหุภาคี

3. สนับสนุนการจัดทำแผนปฏิบัติการระดับชาติ (National Action Plans) ของประเทศสมาชิกเพื่อใช้เป็นแนวทางในการจัดการกับอาชญากรรมทางไซเบอร์อย่างเป็นระบบ

---

[148] Law for ASEAN, อาเซียนกับการจัดการปัญหาอาชญากรรมไซเบอร์ <https://lawforasean.krisdika.go.th/File/files/cybersecurity_dec2.pdf> สืบค้นเมื่อวันที่ 14 พฤศจิกายน 2566.

[149] 'ASEAN Declaration to Prevent and Combat Cybercrime' (ASEAN Secretariat) <https://asean.org> accessed 6 July 2025.

4. เสริมสร้างขีดความสามารถของหน่วยงานภาครัฐและผู้เชี่ยวชาญด้านเทคนิค โดยเฉพาะด้านการป้องกัน ตรวจจับ และตอบโต้ภัยคุกคามจากอาชญากรรมไซเบอร์

5. สร้างกลไกความร่วมมือกับประเทศคู่เจรจาและองค์กรระหว่างประเทศ เช่น INTERPOL, EUROPOL, ASEANAPOL และหน่วยงานอื่น ๆ เพื่อให้สามารถดำเนินงานอย่างมีประสิทธิภาพในระดับภูมิภาคและโลก

อย่างไรก็ดีปฏิญญาฉบับนี้ถือเป็นเพียงการแสดงเจตนารมณ์ทางการเมืองร่วมกันของประเทศสมาชิกอาเซียน ซึ่งไม่ได้มีผลผูกพันทางกฎหมายโดยตรง ตามหลักกฎหมายระหว่างประเทศ แต่อย่างไรก็ตาม ปฏิญญาดังกล่าวถือเป็นก้าวสำคัญในการวางรากฐานของความร่วมมือระหว่างประเทศสมาชิกในประเด็นการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์ในภูมิภาคอาเซียน

**3.2.3 ระดับประเทศ**

3.2.3.1 ประเทศไทย

ประเทศไทยในปัจจุบันประสบปัญหาเกี่ยวกับการประกอบอาชญากรรมที่มีลักษณะเป็นองค์กรอาชญากรรมข้ามชาติทั้งในมิติของการใช้ประเทศไทยเป็นเครือข่ายในการกระทำความผิดและประสบปัญหาทั้งในมิติของการเป็นนผู้เสียหาย ซึ่งส่งผลกระทบต่อความสงบเรียบร้อย และความมั่นคงของประเทศเป็นอย่างมาก โดยในประเทศไทยได้มีกฎหมายที่สามารถนำมาบังคับใช้กับการกระทำผิดของแก๊งคอลเซ็นเตอร์ ดังนี้

1. พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรข้ามชาติ พ.ศ.2556[150]

พระราชบัญญัตินี้ใช้เพื่อจัดการกันอาชญากรรมที่มีการกระทำผิดในลักษณะที่เป็นองค์กรอาชญากรรมข้ามชาติ โดยเฉพาะในกรณีที่มีการทำงานร่วมกันระหว่างสมาชิกในประเทศต่าง ๆ ซึ่งได้ระบุและจำแนกกลุ่มอาชญากรรมที่ทำงานในลักษณะขององค์กรอาชญากรรมข้ามชาติเอาไว้และในพระราชบัญญัตินี้มีมาตรการในการป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ซึ่งสามารถใช้ในการป้องกันการกระทำผิดและการเตรียมการในการจับกุมตัวการ อีกทั้งยังส่งเสริมการร่วมมือระหว่างประเทศในการจัดการกับอาชญากรรมข้ามชาติ โดยการแลกเปลี่ยนข้อมูลและการปฏิบัติการร่วมกันระหว่างหน่วยงานบังคับใช้กฎหมายของประเทศต่าง ๆ โดยสาระสำคัญของพระราชบัญญัตินี้ คือการกำหนดให้การมีส่วนร่วมในองค์กรอาชญากรข้ามชาติไม่ว่าจะในฐานะผู้จัดตั้ง ผู้บริหาร ผู้สนับสนุน หรือผู้สมคบ เป็นความผิดทางอาญา ทั้งนี้แม้ยังมิได้มีการลงมือกระทำความผิดสำเร็จก็ตาม การเตรียมการ หรือการสมคบคิดก็อยู่ในข่ายความผิดเช่นกัน ซึ่งสะท้อนถึงแนวคิดเชิง

---

[150] พัลลภ หริ่งรอด, ‘มาตรการตามกฎหมายในการปราบปรามองค์กรอาชญากรรมข้ามชาติ ศึกษาเฉพาะกลุ่มคอลเซ็นเตอร์’ (การค้นคว้าอิสระนิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2562) 40–47.

ป้องกันที่เน้นการตัดวงจรอาชญากรรมตั้งแต่ต้นทาง[151] โดยเฉพาะในกรณีที่องค์กรอาชญากรรมนั้นมีโครงสร้างแบบเครือข่าย ซึ่งสามารถเปลี่ยนรูปแบบและกระบวนการกระทำผิดได้อย่างยืดหยุ่น

2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

เป็นกฎหมายเฉพาะที่ตราขึ้นเพื่อรับมือกับอาชญากรรมในยุคดิจิทัล โดยเฉพาะความผิดที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์หรือเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือในการกระทำผิด โดยมีวัตถุประสงค์เพื่อคุ้มครองความมั่นคงของระบบคอมพิวเตอร์ ความเชื่อมั่นของสาธารณชนต่อข้อมูลข่าวสารทางดิจิทัล และคุ้มครองสิทธิของประชาชนจากการถูกหลอกลวงผ่านสื่ออิเล็กทรอนิกส์[152] หนึ่งในบทบัญญัติที่สำคัญคือ มาตรา 14 (1)[153] ซึ่งบัญญัติความผิดเกี่ยวกับการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จ โดยมีเจตนาหลอกลวงหรือบิดเบือนข้อเท็จจริง และอาจก่อให้เกิดความเสียหายต่อประชาชนหรือบุคคลอื่น โดยบทบัญญัตินี้มีลักษณะเป็นความผิดฐานหลอกลวงผ่านสื่อเทคโนโลยีที่มิได้กำหนดไว้ในประมวลกฎหมายอาญาโดยตรง แต่มีความจำเป็นอย่างยิ่งในยุคที่การฉ้อโกงมักเกิดขึ้นผ่านระบบดิจิทัล นอกจากนี้ หากเว็บไซต์หรือแอปพลิเคชันที่ใช้หลอกลวงมีระบบเก็บข้อมูลส่วนบุคคลของเหยื่อ เช่น หมายเลขบัตรประชาชน หมายเลขบัญชีธนาคาร หรือ OTP ก็อาจเข้าข่ายละเมิดตาม มาตรา 14 (2)[154] ซึ่งเป็นความผิดในการนำข้อมูลเข้าสู่ระบบโดยประการที่ทำให้เกิดความเสียหายต่อความมั่นคงของประเทศหรือความปลอดภัยสาธารณะ

3. พระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

ให้ความสำคัญและกำหนดมาตรกการการรักษาความมั่นคงปลอดภัยด้านไซเบอร์อย่างมากพร้อมมาตรการด้านกฎหมายและกำหนดประเด็นยุทธศาสตร์ชาติด้านการสร้าง

---

[151] สมศักดิ์ โกศัยสุข, *อาชญากรรมข้ามชาติ: กฎหมายและกลไกการบังคับใช้*, (กรุงเทพฯ: วิญญชน, 2563), 87–89.

[152] ชาญชัย แสวงศักดิ์, *กฎหมายอาชญากรรมทางเทคโนโลยี*, (กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์, 2564), 132–135.

[153] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 14 “ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา”

[154] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 14 “ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน”

ความสามารถในการแข่งขันภายใต้หัวข้ออุตสาหกรรมความมั่นคงของประเทศ โดยการสร้างอุตสาหกรรมที่ส่งเสริมความมั่นคงปลอดภัยไซเบอร์เพื่อลดผลกระทบจากภัยคุกคามไซเบอร์ต่อเศรษฐกิจและสังคมและปกป้องอธิปไตยทางไซเบอร์ เพื่อรักษาผลประโยชน์ของชาติจากการทำธุรกิจดิจิทัลจึงได้มีการบัญญัติพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์พ.ศ. 2562 โดยการนำเสนอร่างของกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคมเพื่อกำหนดหลักเกณฑ์แนวทางและมาตรการต่าง ๆ ที่เกี่ยวข้องอย่างเป็นรูปธรรม ในการป้องกันรับมือและลดความเสี่ยงจากภัยคุมคามทางไซเบอร์ซึ่งมีการประสานความร่วมมือระหว่างผู้เกี่ยวข้องพัฒนาความรู้ความสามารถของบุคลากรและผู้เชี่ยวชาญ รวมถึงการให้ความรู้และความตระหนักถึงภัยไซเบอร์อีกด้วย ซึ่งกฎหมายฉบับนี้ถูกบังคับใช้กับหน่วยงานของรัฐ หรือหน่วยงานเอกชนซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศรวมทั้งสิ้น 8 กลุ่ม ได้แก่ ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคารด้านเทคโนโลยี สารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุขและด้านอื่น ๆ ตามที่คณะกรรมการฯ ประกาศกำหนดเพิ่มเติม[155] พระราชบัญญัตินี้จึงเป็นเครื่องมือสำคัญของภาครัฐในการดำเนินคดีกับขบวนการแก๊งคอลเซ็นเตอร์ที่ใช้เทคโนโลยีในการล่อลวงเหยื่อ และยังสามารถนำมาใช้ในการสั่งปิดเว็บไซต์หรือแพลตฟอร์มที่เกี่ยวข้องกับการกระทำความผิด รวมถึงสามารถยึดอุปกรณ์หรือหลักฐานทางดิจิทัลเพื่อใช้ในกระบวนการสอบสวนและพิจารณาคดี

4. พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542

เป็นการใช้กฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมและรวมไปถึงการกำหนดมาตรการในการดำเนินการเกี่ยวกับทรัพย์สินตามกฎหมายที่เกี่ยวข้องกับการป้องกันและปราบปรามการฟอกเงินประกอบกับหลักการของกฎหมายดังกล่าวที่มีการยึดหรืออายัดทรัพย์สินนั้นเนเพียงมาตรการชั้วคราวเพื่อประกันให้มีการริบทรัพย์หรือใช้เป็นพยานหลักฐานในการพิสูจน์ความผิดในการดำเนินคดีต่าง ๆ[156]

ภายใต้พระราชบัญญัติป้องกันและปราบปรามการ ฟอกเงิน พ.ศ. 2542 มีความเกี่ยวข้องกับความผิดแก๊งคอลเซ็นเตอร์ด้วยกันอยู่ 2 กรณี คือ

1) การฉ้อโกงประชาชนซึ่งถือเป็นความผิดมูลฐาน

---

[155] สุมิตร สีหาฤทธิ์, ปัญหาทางกฎหมายตามพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. 25621, 2-3.

[156] ขวัญชนก ศรีภมร, แนวทางการป้องกันอาชญากรรมที่เกิดจากแก๊งคอลเซ็นเตอร์ออนไลน์โดยมาตรการกำกับดูแลของอุตสาหกรรมโทรคมนาคม (วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต, คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2565) 29.

2) การเปลี่ยนสภาพทรัพย์สินที่เกี่ยวกับการกระทำความผิดโดยการปกปิดซ่อนเร้นทรัพย์สิน ไม่ว่าจะเป็นการปกปิดที่มาของทรัพย์สินหรือมีการอำพราง ลักษณะที่แท้จริงการได้มา รวมถึงการใช้ ครอบครอง โอนซึ่งทรัพย์สินที่เกี่ยวกับการกระทำความผิด

5. ประมวลกฎหมายอาญา

แม้ว่าปัจจุบันจะมีการตรากฎหมายเฉพาะเพื่อจัดการกับอาชญากรรมในโลกยุคดิจิทัล แต่ประมวลกฎหมายอาญายังคงมีบทบาทสำคัญในการบังคับใช้กับพฤติการณ์ของแก๊งคอลเซ็นเตอร์ โดยเฉพาะในความผิดที่มีลักษณะเป็นการฉ้อโกงซึ่งมีรากฐานอยู่บนการหลอกลวงอันเป็นสาระสำคัญของการได้มาซึ่งทรัพย์สินจากเหยื่อ ความผิดดังกล่าวมักเกิดขึ้นโดยอาศัยกลวิธีที่หลากหลาย เช่น การแอบอ้างตัวเป็นเจ้าหน้าที่รัฐ เจ้าหน้าที่ธนาคาร หรือองค์กรผู้มีอำนาจในลักษณะที่น่าเชื่อถือ เพื่อสร้างความหวาดกลัว ความสับสน หรือความเข้าใจผิดให้แก่เหยื่อ[157] ประมวลกฎหมายอาญาจึงทำหน้าที่เป็นกลไกหลักในการดำเนินคดีอาญาต่อผู้กระทำความผิดที่ใช้วิธีการฉ้อโกงดังกล่าว แม้ว่าผู้กระทำความผิดบางรายอาจมิได้ลงมือโดยตรง แต่หากมีส่วนรู้เห็นเป็นผู้สนับสนุนหรือร่วมในกระบวนการดังกล่าว ก็สามารถถูกดำเนินคดีในฐานะผู้ร่วมกระทำความผิดได้เช่นกัน ทั้งนี้ การบังคับใช้บทบัญญัติในประมวลกฎหมายอาญาจำเป็นต้องอาศัยการตีความตามหลักนิติศาสตร์ร่วมกับข้อเท็จจริงในแต่ละกรณีและในคดีที่มีลักษณะข้ามชาติหรือมีการใช้เทคโนโลยีซับซ้อน การประยุกต์ใช้กฎหมายฉบับนี้มักต้องดำเนินควบคู่กับกฎหมายเฉพาะด้านอื่นเพื่อให้เกิดประสิทธิภาพสูงสุดในการบังคับใช้กฎหมาย[158]

6. พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

รัฐบาลไทยได้ประกาศใช้ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 17 มีนาคม 2566 อันเป็นกฎหมายที่มีลักษณะเฉพาะในการตอบสนองต่อภัยคุกคามไซเบอร์อย่างฉับพลัน โดยอาศัยอำนาจตามบทบัญญัติของรัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 172 เพื่อรักษาความปลอดภัยสาธารณะในภาวะเร่งด่วน โดยพระราชกำหนดฉบับนี้มีวัตถุประสงค์สำคัญในการยกระดับกลไกการตอบสนองต่ออาชญากรรมไซเบอร์ในเชิงรุก โดยเฉพาะการจัดวางบทบาทและหน้าที่ให้แก่ผู้ให้บริการทางการเงิน ผู้ให้บริการโทรคมนาคม และหน่วยงานของรัฐที่เกี่ยวข้อง อาทิ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.)

---

[157] สมศักดิ์ โกศัยสุข, *กฎหมายอาญาภาคความผิด ลักษณะความผิดเกี่ยวกับทรัพย์*, (กรุงเทพฯ: วิญญูชน, 2562) 72–74.

[158] อรพรรณ บัวทอง, “การบูรณาการการใช้กฎหมายอาญากับกฎหมายเฉพาะในการปราบปรามอาชญากรรมไซเบอร์,” *วารสารนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย*, ปีที่ 47, ฉบับพิเศษ (2564) 89–91.

สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ธนาคารแห่งประเทศไทย และสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ให้สามารถดำเนินการ “ระงับธุรกรรมต้องสงสัย” หรือ “ปิดใช้งานซิมการ์ด” ได้โดยไม่จำเป็นต้องรอคำสั่งศาลในทันที โดยมีเงื่อนไขว่าต้องได้รับแจ้งจากผู้เสียหาย หรือพบความผิดปกติในการดำเนินการของบัญชีหรือเบอร์โทรศัพท์นั้น ๆ

สาระสำคัญของกฎหมายดังกล่าว ได้แก่ การบัญญัติให้ “หน่วยงานที่เกี่ยวข้องมีหน้าที่แจ้งข้อมูลระหว่างกันภายในระยะเวลาที่กำหนด” เพื่อป้องกันการล่าช้าในการดำเนินคดี ทั้งยังเปิดช่องทางให้ผู้เสียหายสามารถร้องเรียนได้โดยไม่ต้องผ่านกระบวนการศาลตามปกติ และให้อำนาจเจ้าหน้าที่รัฐระงับธุรกรรมหรือระงับการใช้งานอุปกรณ์โทรคมนาคมชั่วคราวสูงสุด 7 วัน หากพบว่ามีเหตุอันควรสงสัยว่ามีการใช้ช่องทางดังกล่าวในการกระทำความผิด นอกจากนี้ พระราชกำหนดยังบัญญัติฐานความผิดใหม่ ได้แก่ การซื้อขายข้อมูลส่วนบุคคลโดยมิชอบ และ การนำข้อมูลของผู้เสียชีวิตไปใช้ในการกระทำผิด ซึ่งถือเป็นการขยายขอบเขตการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยกำหนดโทษทั้งจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ

7. พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568

รัฐบาลไทยได้ตรา พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 เพื่อแก้ไขเพิ่มเติมบทบัญญัติของพระราชกำหนดเดิม และมีผลบังคับใช้ในวันที่ 13 เมษายน 2568 นับเป็นพัฒนาการเชิงนิติบัญญัติที่สำคัญในการรับมือกับภัยคุกคามจากอาชญากรรมไซเบอร์ที่แพร่หลายอย่างต่อเนื่องในประเทศไทย โดยเฉพาะอาชญากรรมในรูปแบบของการหลอกลวงออนไลน์ผ่านบัญชีม้า โทรศัพท์ปลอมแปลง หรือแพลตฟอร์มสื่อสารต่างๆ ที่สร้างความเสียหายทางเศรษฐกิจแก่ประชาชนและบั่นทอนความเชื่อมั่นต่อระบบนิติธรรม โดยสาระสำคัญของพระราชกำหนดฉบับนี้คือ การวางภาระหน้าที่เชิงรุกแก่หน่วยงานรัฐและเอกชนที่เกี่ยวข้อง เช่น สถาบันการเงิน ผู้ให้บริการแก่ผู้ต้องสงสัยว่าใช้ช่องทางดังกล่าวในการกระทำความผิดและต้องรายงานบัญชีต้องสงสัยไปยังหน่วยงานที่มีอำนาจ ศูนย์ปฏิบัติการต่อต้านอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.) หรือสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ภายในเวลาที่กฎหมายกำหนด ซึ่งการวางบทบัญญัติให้มีการระงับบัญชีหรือซิมต้องสงสัยโดยไม่ต้องรอคำสั่งศาล การดำเนินการเช่นนี้มีวัตถุประสงค์เพื่อปกป้องสาธารณประโยชน์และลดความเสียหายที่อาจเกิดขึ้นในทันที อีกหนึ่งความสำคัญคือ บทบัญญัติที่กำหนดให้หน่วยงานผู้ให้บริการมีความรับผิดชอบร่วมกับผู้กระทำความผิด หากพบว่าเพิกเฉยหรือละเลยต่อมาตรการที่รัฐกำหนด เช่น ไม่ตรวจสอบ

ความผิดปกติของธุรกรรม หรือไม่ระงับบัญชีต้องสงสัยภายในเวลาที่กำหนด นอกจากนี้ กฎหมายฉบับนี้ยังวางฐานความผิดทางอาญาใหม่เกี่ยวกับการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบและการใช้ข้อมูลผู้เสียชีวิตในการกระทำความผิด ซึ่งมีโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ โดยสอดคล้องกับเจตนารมณ์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ให้ความคุ้มครองข้อมูลของบุคคลในระดับกว้างขวาง และที่น่าสังเกตอีกประการหนึ่งคือ การกำหนดให้สามารถยื่นคำร้องขอคืนเงินแก่ผู้ให้บริการได้โดยไม่ต้องผ่านกระบวนการฟ้องร้องในศาล อันถือเป็นการเพิ่มประสิทธิภาพของกระบวนการคุ้มครองสิทธิผู้เสียหาย ลดภาระในการเข้าสู่ระบบยุติธรรม และเปิดโอกาสให้เกิดการเยียวยาอย่างรวดเร็ว ในขณะเดียวกัน กฎหมายยังมุ่งยกระดับความปลอดภัยของข้อมูลส่วนบุคคล โดยห้ามมิให้มีการนำข้อมูลส่วนบุคคล รวมถึงข้อมูลของผู้เสียชีวิต ไปใช้เพื่อการกระทำความผิด พร้อมกำหนดโทษอาญาอย่างชัดเจนต่อผู้ฝ่าฝืน

3.2.3.2 ประเทศออสเตรเลีย[159]

รัฐบาลออสเตรเลียได้เล็งเห็นความจำเป็นในการจัดตั้งมาตรการเชิงนโยบายและการบังคับใช้กฎหมายที่มีประสิทธิภาพเพื่อปกป้องประชาชนจากภัยคุกคามไซเบอร์ดังกล่าว โดยมีการดำเนินการทั้งในระดับภายในประเทศผ่านกฎหมายเฉพาะทาง การพัฒนาศักยภาพของหน่วยงานบังคับใช้กฎหมาย โดยหลังจาก ACMA มีการวางแผนปฏิบัติการ The Combating Scams Action Plan ในปี 2019 ที่ได้กล่าวไปข้างต้น ซึ่งประกอบไปด้วย 3 แผนหลักๆ ทำให้เกิดการบังคับใช้กฎหมายและ มาตรฐานอุตสาหกรรมใหม่ขึ้นเพื่อให้เป็นไปตามแผนปฏิบัติการที่ได้วางไว้ ประกอบด้วย

1. Telecommunication (Mobile Number Pre-Porting Additional Identity Verification) เป็นมาตรฐานอุตสาหกรรมด้านการยืนยันตัวตนก่อนการโอนย้ายหมายเลขโทรศัพท์มือถือที่ประกาศใช้เมื่อวันที่ 30 เมษายน ค.ศ. 2020 นั้น ได้รับการจัดทำขึ้นโดยมีพื้นฐานจากมาตรา 125AA(1) แห่งพระราชบัญญัติ Telecommunications Act 1997[160] ของประเทศออสเตรเลีย ซึ่งเป็นบทบัญญัติที่ให้อำนาจแก่หน่วยงานกำกับดูแลด้านโทรคมนาคมในการจัดทำและกำหนดมาตรฐานอุตสาหกรรม (Industry Standard) ที่มีผลบังคับใช้ต่อผู้ให้บริการโทรคมนาคมโดยตรง โดยมาตรฐานดังกล่าวถือเป็นการสืบต่อและพัฒนาจากแนวทางของ Telecommunications (Industry Standard for Mobile Number Pre-Porting Additional Identity Verification)

---

[159] ขวัญชนก ศรีภมร, แนวทางการป้องกันอาชญากรรมที่เกิดจากแก๊งคอลเซ็นเตอร์ออนไลน์โดยมาตรการกำกับดูแลของอุตสาหกรรมโทรคมนาคม (วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต, คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2565) 67-70.

[160] Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020.

Direction 2019 ซึ่งเป็นกฎหมายลำดับรองที่มุ่งเน้นในเรื่องของการเพิ่มความเข้มงวดในการยืนยันตัวตนของผู้ใช้บริการก่อนการอนุญาตให้โอนย้ายหมายเลขโทรศัพท์ วัตถุประสงค์หลักของมาตรฐานอุตสาหกรรมฉบับนี้ คือ การป้องกันการโอนย้ายหมายเลขโทรศัพท์มือถือโดยมิได้รับอนุญาตซึ่งเป็นปัจจัยสำคัญที่ก่อให้เกิดอาชญากรรมทางโทรคมนาคมรูปแบบใหม่ โดยเฉพาะการขโมยตัวตนและการหลอกลวงทางการเงินผ่านการเข้าควบคุมหมายเลขโทรศัพท์ของเหยื่อ[161] มาตรฐานนี้จึงได้กำหนดให้มีการยืนยันตัวตนของผู้ใช้บริการด้วยวิธีการที่สามารถเข้าถึงอุปกรณ์มือถือที่เชื่อมโยงกับหมายเลขนั้นโดยตรงและในทันทีอันเป็นกลไกสำคัญในการสกัดกั้นไม่ให้ผู้ไม่หวังดีสามารถดำเนินการย้ายหมายเลขเพื่อวัตถุประสงค์ในการฉ้อโกงได้ง่าย ข้อกำหนดในมาตรฐานดังกล่าวเน้นที่การยกระดับขั้นตอนการยืนยันตัวตนก่อนอนุญาตให้ย้ายหมายเลข ซึ่งครอบคลุมทั้งในระดับระบบการให้บริการของผู้ให้บริการและการสื่อสารกับลูกค้า ทั้งนี้เพื่อเป็นการเสริมสร้างความมั่นคงให้กับระบบโครงสร้างพื้นฐานโทรคมนาคมและลดความเสี่ยงที่ผู้บริโภคจะได้รับความเสียหายจากพฤติกรรมอาชญากรรมไซเบอร์ในรูปแบบนี้ นอกจากนี้ยังถือเป็น Code of Conduct หรือแนวปฏิบัติที่มีผลผูกพันตามกฎหมายซึ่งผู้ให้บริการทุกรายต้องปฏิบัติตามอย่างเคร่งครัด หากฝ่าฝืนหรือเพิกเฉยต่อมาตรฐานดังกล่าวสำนักงาน ACMA มีอำนาจในการออกคำเตือนอย่างเป็นทางการ[162] รวมทั้งสามารถใช้มาตรการทางกฎหมายในการบังคับให้ผู้ให้บริการปฏิบัติตามได้ ในกรณีที่มีการฝ่าฝืนอย่างชัดแจ้ง ACMA ยังสามารถดำเนินการทางแพ่งตามบทบัญญัติมาตรา 128 แห่งพระราชบัญญัติ Telecommunications Act 1997[163] โดยบทลงโทษในลักษณะนี้จะอยู่ภายใต้กระบวนการพิจารณาของศาล ซึ่งจะพิจารณาองค์ประกอบต่าง ๆ ของการฝ่าฝืน เช่น ความร้ายแรงของพฤติกรรม การละเลยต่อข้อกำหนดอย่างมีนัยสำคัญ และความเสียหายที่เกิดขึ้นกับผู้ใช้บริการ ทั้งนี้เนื่องจากออสเตรเลียใช้ระบบกฎหมายแบบจารีตประเพณีอำนาจในการกำหนดค่าปรับจึงอยู่ภายใต้ดุลพินิจของศาลเป็นสำคัญ ซึ่งสะท้อนให้เห็นถึงการสร้างกลไกการบังคับใช้กฎหมายที่มีความยืดหยุ่นแต่มีประสิทธิภาพในเวลาเดียวกันโดยสรุปมาตรฐานอุตสาหกรรมดังกล่าวไม่เพียงแต่เป็นเครื่องมือสำคัญในการยกระดับความปลอดภัยของระบบโทรคมนาคมในออสเตรเลียเท่านั้น แต่ยังเป็นการแสดงให้เห็นถึงการตอบสนองเชิงนโยบายที่มีการบูรณาการระหว่าง

---

[161] Telecommunications (Industry Standard for Mobile Number Pre-Porting Additional Identity Verification) Direction 2019

[162] The Telecommunication Act 1997, section 129

[163] The Telecommunication Act 1997, subsection 128 (3).

ภาครัฐกับอุตสาหกรรมในการต่อสู้กับภัยคุกคามด้านอาชญากรรมไซเบอร์ที่มีพัฒนาการอย่างต่อเนื่องและซับซ้อนในปัจจุบัน[164]

2. Reducing Scams Call Industry Code ซึ่งหลักเกณฑ์ในการบังคับใช้ภาระผูกพันที่กำหนดให้บริษัทโทรคมนาคมต้องดำเนินการตรวจจับ ติดตาม และปิดกั้นหมายเลขโทรศัพท์ที่เกี่ยวข้องกับการโทรหลอกลวงนั้น ได้รับการจัดทำขึ้นภายใต้กรอบของ Reducing Scam Calls Industry Code ซึ่งถือเป็นเครื่องมือกำกับดูแลที่มีความสำคัญอย่างยิ่งในบริบทของออสเตรเลีย โดยหลักเกณฑ์ดังกล่าวได้รับการพัฒนาและปรับปรุงขึ้นจากข้อเสนอแนะโดยตรงของแผนปฏิบัติการ Combating Scams Action Plan ของสำนักงานสื่อสารและสื่อแห่งออสเตรเลีย (Australian Communications and Media Authority – ACMA) โดยมีวัตถุประสงค์หลักเพื่อควบคุมและลดจำนวนของหมายเลขโทรศัพท์ที่ถูกนำมาใช้ในการหลอกลวงและลดความถี่ของการโทรหลอกลวงที่ส่งผลกระทบต่อประชาชน สาระสำคัญของหลักเกณฑ์นี้อยู่ที่ข้อกำหนดให้ผู้ให้บริการโทรคมนาคมมีหน้าที่ในการตรวจสอบการรับส่งข้อมูลโทรศัพท์บนเครือข่ายของตนอย่างเคร่งครัด โดยเฉพาะการระบุพฤติกรรมต้องสงสัยที่อาจเกี่ยวข้องกับการฉ้อโกงและการแบ่งปันข้อมูลหมายเลขโทรศัพท์ที่พบว่าใช้ในการหลอกลวงให้แก่ผู้ให้บริการรายอื่นรวมถึงหน่วยงานของรัฐที่มีอำนาจเกี่ยวข้อง ทั้งนี้การแบ่งปันข้อมูลดังกล่าวจะไม่ถือเป็นการละเมิดพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1988 (*Privacy Act 1988*) เนื่องจากได้รับการยกเว้นตามบทบัญญัติมาตรา 116A แห่ง Telecommunications Act 1997[165] นอกจากนี้หลักเกณฑ์ยังครอบคลุมถึงหน้าที่ของผู้ให้บริการในการแจ้งเหตุการโทรหลอกลวงต่อหน่วยงานรัฐ รวมถึงให้คำแนะนำและข้อมูลแก่ผู้บริโภคเพื่อสร้างความตระหนักรู้และป้องกันการตกเป็นเหยื่อของกลุ่มมิจฉาชีพ ที่สำคัญคือ *Communications Alliance (CA)* และสมาชิกในอุตสาหกรรมได้แสดงเจตจำนงอย่างชัดเจนในการแสวงหากลยุทธ์ที่มีประสิทธิภาพในการบรรเทาภัยจากแก๊งคอลเซ็นเตอร์ โดยอิงจากบริบทของสภาพแวดล้อมทางสังคมเศรษฐกิจและรูปแบบการฉ้อโกงในออสเตรเลีย ซึ่งสะท้อนถึงกระบวนการพัฒนาอย่างต่อเนื่องของภาคอุตสาหกรรมในการตอบสนองต่อภัยคุกคามทางไซเบอร์ในรูปแบบใหม่นี้ทั้งนี้ แนวทางของ *Reducing Scam Calls Industry Code* มีความสอดคล้องอย่างใกล้ชิดกับแผนปฏิบัติการลำดับที่สองของ *Combating Scams Action Plan* ซึ่งมุ่งเน้นไปที่การตรวจจับและสกัดกั้นกลไกการหลอกลวงทางโทรศัพท์ได้อย่างเป็นรูปธรรม อันเป็นการแสดงให้เห็นถึงพัฒนาการของเครื่องมือกำกับ

---

[164] ขวัญชนก ศรีภมร, แนวทางการป้องกันอาชญากรรมที่เกิดจากแก๊งคอลเซ็นเตอร์ออนไลน์โดยมาตรการกำกับดูแลของอุตสาหกรรมโทรคมนาคม (วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต, คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2565) 71-76.

[165] The Telecommunication Act 1997, section 116A.

ดูแลที่มีพื้นฐานจากนโยบายของรัฐและการประสานงานที่เข้มแข็งระหว่างภาครัฐและเอกชนในการต่อต้านอาชญากรรมโทรคมนาคมอย่างยั่งยืน[166]

แม้ว่าการจัดทำ Industry Code ภายใต้กรอบกฎหมายโทรคมนาคมของออสเตรเลียจะเป็นมาตรการสำคัญในการยกระดับความปลอดภัยของระบบการสื่อสารและการป้องกันอาชญากรรมไซเบอร์รูปแบบใหม่ เช่น การโทรหลอกลวงหรือการฉ้อโกงผ่านหมายเลขโทรศัพท์ แต่ก็ไม่อาจปฏิเสธได้ว่ามาตรการดังกล่าวส่งผลให้ผู้ให้บริการโทรคมนาคมต้องแบกรับภาระเพิ่มเติมในเชิงโครงสร้างและการเงิน โดยเฉพาะอย่างยิ่งในส่วนของการลงทุนเพื่อจัดตั้งและบำรุงรักษาระบบสนับสนุนที่จำเป็นต่อการปฏิบัติตามบทบัญญัติใน Industry Code ตลอดจนการทำข้อตกลงร่วมกับหน่วยงานหรือผู้ให้บริการรายอื่นในระบบโครงข่ายโทรคมนาคม ต้นทุนดังกล่าวมิได้เกิดขึ้นเพียงครั้งเดียวในช่วงต้นของการดำเนินการเท่านั้น หากแต่ยังรวมถึงค่าใช้จ่ายที่ดำเนินอยู่อย่างต่อเนื่อง เช่น การพัฒนาเทคโนโลยีในการตรวจจับพฤติกรรมฉ้อโกง การอัปเดตระบบตรวจสอบข้อมูล การฝึกอบรมบุคลากร และการปรับตัวให้ทันต่อกลยุทธ์ใหม่ของมิจฉาชีพซึ่งมีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว อย่างไรก็ตาม แม้จะมีภาระในเชิงการดำเนินงานและต้นทุนที่เพิ่มขึ้นดังกล่าว แต่การที่ Industry Code มีฐานะเป็นข้อบังคับทางกฎหมาย รวมถึงการที่ ACMA มีอำนาจในการตรวจสอบ ตักเตือน หรือใช้มาตรการบังคับในกรณีที่มีการฝ่าฝืน จึงทำให้ผู้ให้บริการโทรคมนาคมไม่สามารถหลีกเลี่ยงภาระหน้าที่ที่กำหนดไว้ในรหัสข้อปฏิบัติดังกล่าวได้

ในด้านบทลงโทษเมื่อผู้ให้บริการโทรคมนาคมกระทำการฝ่าฝืนหลักปฏิบัติในอุตสาหกรรม (Industry Code) ซึ่งได้รับการจดทะเบียนตามกฎหมายแล้ว สำนักงานสื่อสารและสื่อของออสเตรเลีย (Australian Communications and Media Authority: ACMA) มีอำนาจในการออกคำเตือนอย่างเป็นทางการแก่ผู้ให้บริการที่ฝ่าฝืนข้อกำหนดดังกล่าว[167] อีกทั้งยังสามารถมีคำสั่งให้ผู้ให้บริการดำเนินการให้สอดคล้องกับหลักเกณฑ์ที่กำหนดไว้ใน Industry Code ได้โดยตรง ในกรณีที่การฝ่าฝืนรุนแรงหรือยังคงดำเนินต่อไปแม้มีคำเตือนแล้วอาจมีการกำหนดบทลงโทษทางแพ่งในรูปของค่าปรับทางการเงิน[168] โดยอำนาจในการตัดสินและกำหนดจำนวนค่าปรับนั้นเป็นของศาลซึ่งจะพิจารณาจากปัจจัยหลายประการ ได้แก่ ลักษณะของการฝ่าฝืน ระดับความเสียหายที่เกิดขึ้น และพฤติกรรมของผู้ให้บริการในการปฏิบัติตามหรือเพิกเฉยต่อมาตรฐานอุตสาหกรรม ทั้งนี้มาตรการ

---

[166] ขวัญชนก ศรีภมร, แนวทางการป้องกันอาชญากรรมที่เกิดจากแก๊งคอลเซ็นเตอร์ออนไลน์โดยมาตรการกำกับดูแลของอุตสาหกรรมโทรคมนาคม (วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต, คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2565) 71-76.

[167] The Telecommunication Act 1997, section 122

[168] The Telecommunication Act 1997, section 121.

ดังกล่าวสะท้อนให้เห็นถึงกลไกการกำกับดูแลที่มีประสิทธิภาพและยืดหยุ่นของออสเตรเลียในการควบคุมพฤติกรรมของผู้ให้บริการโทรคมนาคมให้เป็นไปตามมาตรฐานและหลักจริยธรรมของอุตสาหกรรมอย่างเคร่งครัด

3.2.3.3 ประเทศสหราชอาณาจักร

เนื่องจาก Ofcom เป็นหน่วยงานในการกำกับดูแลหมายเลขโทรศัพท์ของประเทศสหราชอาณาจักรโดยเฉพาะอย่างยิ่งการดูแลหมายเลขโทรศัพท์ที่ถูกนำมาใช้อย่างผิดกฎหมาย ไม่ว่าจะเป็นการออกเบอร์ที่ไม่เป็นไปตามข้อกำหนดหรือการนำหมายเลข โทรศัพท์ที่มีการเปิดใช้งานแล้วแต่ไม่มีการใช้งานมาใช้ในทางที่ไม่ชอบ ดังนั้นทาง Ofcom จึงได้ทำการออกข้อกำหนด คือ

The National Telephone Numbering Plan แผนการจัดสรรและกำหนดหมายเลขโทรศัพท์ของสหราชอาณาจักรเป็นส่วนหนึ่งของระบบการกำกับดูแลโทรคมนาคมที่อยู่ภายใต้การดำเนินการของ Ofcom ซึ่งเป็นหน่วยงานกำกับดูแลหลักตามอำนาจที่บัญญัติไว้ใน *The Communications Act 2003* โดยแผนดังกล่าวไม่เพียงแต่กำหนดโครงสร้างของการจัดสรรหมายเลขโทรศัพท์ให้แก่ผู้ให้บริการเท่านั้น หากแต่ยังรวมถึงการกำหนดข้อจำกัดในการใช้งาน[169] การป้องกันการนำหมายเลขไปใช้ในลักษณะที่สร้างความเสียหายหรือสร้างความเข้าใจผิดแก่ผู้บริโภคและการจำกัดการใช้หมายเลขเพื่อวัตถุประสงค์ที่ไม่ชอบด้วยกฎหมาย หมายเลขโทรศัพท์ใดที่ถูกนำไปใช้โดยฝ่าฝืนข้อกำหนดที่กำหนดไว้ในแผนดังกล่าว จะถือว่าเป็นหมายเลขที่ผิดกฎหมาย ซึ่งอาจนำไปสู่การดำเนินคดีหรือการลงโทษตามที่กฎหมายบัญญัติไว้ ในการดำเนินงานตามแผนนี้ Ofcom มีบทบาทสำคัญในการจัดทำและเผยแพร่นโยบายที่เกี่ยวข้องกับการใช้หมายเลขโทรศัพท์ รวมถึงการบังคับใช้นโยบายเหล่านั้นให้เป็นไปตามมาตรฐานที่กำหนดไว้ และที่สำคัญคือสามารถแก้ไขเปลี่ยนแปลงนโยบายได้ตามความเหมาะสม เพื่อให้เท่าทันต่อสถานการณ์ปัจจุบันและวิวัฒนาการของรูปแบบการหลอกลวงหรือพฤติกรรมที่เป็นภัยต่อผู้บริโภค[170] แนวทางในการกำกับดูแลของ Ofcom นั้นตั้งอยู่บนหลักการของการไม่แทรกแซงโดยไม่จำเป็นและให้ความสำคัญกับความยุติธรรมในการตัดสินใจ นอกจากนี้ Ofcom ยังให้ความสำคัญกับความร่วมมือกับหน่วยงานอื่นที่เกี่ยวข้อง ทั้งภาครัฐและภาคเอกชนในการดำเนินมาตรการต่างๆ โดยเฉพาะอย่างยิ่งในประเด็นเกี่ยวกับการควบคุมหมายเลขที่ใช้ในการกระทำความผิด เช่น การโทรหลอกลวง การรบกวนประชาชน หรือการฉ้อโกงทางโทรศัพท์ จากแนวทางการดำเนินงานดังกล่าวจะเห็นได้ว่ากฎหมายของสหราชอาณาจักรมีลักษณะเน้นการควบคุมโดยตรงต่อพฤติกรรมของผู้ใช้หมายเลขโทรศัพท์ ซึ่งรวมถึงบุคคลหรือบริษัทที่ใช้หมายเลขเหล่านั้นในการกระทำความผิด โดยเน้นการลงโทษผู้กระทำผิดเป็นสำคัญ แตกต่างจาก

---

[169] The Telecommunication Act 1997, section 56.

[170] The Telecommunication Act 1997, section 8.

ระบบของออสเตรเลียที่ออกมาตรฐานอุตสาหกรรมที่มีลักษณะเป็นข้อบังคับสำหรับผู้ให้บริการโทรคมนาคมในการวางระบบตรวจสอบและพิสูจน์ตัวตนของผู้ใช้บริการก่อนจะสามารถดำเนินการใดๆ ที่เกี่ยวข้องกับหมายเลขโทรศัพท์ โดยเฉพาะอย่างยิ่งในกรณีของการโอนย้ายหมายเลขโทรศัพท์ ซึ่งออสเตรเลียเน้นย้ำถึงการลดโอกาสของการปลอมแปลงตัวตนและการฉ้อโกงในระดับโครงสร้างของผู้ให้บริการ ในขณะที่สหราชอาณาจักรให้ความสำคัญกับการลงโทษผู้ใช้หมายเลขในทางที่ผิดเป็นหลัก

ในบริบทของการกำกับดูแลการให้บริการโทรคมนาคมในสหราชอาณาจักร หน่วยงานที่มีบทบาทสำคัญอย่าง Ofcom ได้กำหนดให้ผู้ให้บริการโทรคมนาคมต้องดำเนินการตามขั้นตอนที่รัดกุมเพื่อคุ้มครองผู้บริโภค โดยเฉพาะในกระบวนการขอย้ายเครือข่าย (porting) ของผู้ใช้บริการ ซึ่งเป็นช่วงเวลาที่เสี่ยงต่อการถูกหลอกลวงหรือแอบอ้างตัวตน หนึ่งในกลไกสำคัญที่ถูกกำหนดให้ดำเนินการคือการจัดทำ “Record of Consent” หรือบันทึกการให้ความยินยอมของผู้ใช้บริการ เอกสารดังกล่าวถือเป็นหลักฐานแสดงความสมัครใจของผู้ใช้บริการที่ร้องขอการย้ายเครือข่าย และมีหน้าที่สำคัญในการยืนยันความถูกต้องของการดำเนินการ โดยผู้ให้บริการแต่ละรายมีหน้าที่ต้องจัดทำและจัดเก็บเอกสารฉบับนี้เป็นรายกรณี และต้องเก็บรักษาไว้เป็นระยะเวลาไม่น้อยกว่า 12 เดือน[171]และมีเงื่อนไขว่าผู้ให้บริการต้องทำการจัดเก็บสัญญาแม้ว่าสัญญาดังกล่าวจะถูกยกเลิกหรือยุติภายในระยะเวลาสิบสองเดือน[172]

จากที่กล่าวไปข้างต้นตามหลักการกำกับดูแลของ Ofcom หน่วยงานกำกับดูแลกิจการโทรคมนาคมของสหราชอาณาจักร ได้ยึดแนวทางที่ไม่มุ่งเน้นการแทรกแซงโดยไม่จำเป็น แต่เน้นบทบาทในการสนับสนุนการตัดสินใจของผู้ให้บริการโทรคมนาคมภายใต้กรอบของอำนาจหน้าที่ตามกฎหมาย แนวทางดังกล่าวได้สะท้อนผ่าน “A Statement of Ofcom’s General Policy on the Exercise of its Enforcement Powers” ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 1 มีนาคม ค.ศ. 2017 เป็นต้นมา โดยเป็นเอกสารนโยบายที่วางแนวทางการใช้อำนาจของ Ofcom อย่างชัดเจน เพื่อสร้างความโปร่งใส ความสอดคล้อง และประสิทธิผลในการบังคับใช้กฎหมายภายใต้บริบทของการคุ้มครองผู้บริโภคและความมั่นคงของระบบการสื่อสาร ภายใต้กรอบนโยบายดังกล่าว Ofcom ให้ความสำคัญกับการบังคับใช้กฎหมายกับผู้ที่ใช้บริการสื่อสารทางอิเล็กทรอนิกส์หรือเครือข่ายโทรคมนาคมในทางที่ผิด โดยเฉพาะพฤติกรรมที่ก่อให้เกิดหรือมีแนวโน้มที่จะก่อให้เกิดอันตรายแก่ผู้บริโภค ไม่ว่าจะในรูปแบบของการก่อกวน การแอบอ้าง หรือการหลอกลวงทางโทรคมนาคม ซึ่ง Ofcom มีอำนาจในการกำหนดบทลงโทษทางปกครองต่อผู้กระทำผิดได้สูงสุดถึง 2 ล้านปอนด์ ตามที่บัญญัติไว้ใน The

[171] The General Conditions of Entitlement, C7.7

[172] The General Conditions of Entitlement, C7.8

Communications Act 2003[173] ซึ่งเป็นกฎหมายหลักที่ใช้ในการควบคุมดูแลกิจการด้านการสื่อสารของประเทศ นอกจากนี้เพื่อเพิ่มประสิทธิภาพในการบรรลุวัตถุประสงค์เชิงนโยบาย Ofcom ยังได้จัดทำบันทึกความเข้าใจร่วมกับผู้ให้บริการโทรคมนาคมรายใหญ่ของประเทศ โดยบันทึกดังกล่าววางกรอบความร่วมมือในลักษณะสมัครใจระหว่างองค์กรที่เกี่ยวข้องเพื่อกำหนดมาตรการทางเทคนิคในการป้องกันและลดผลกระทบจากการใช้บริการโทรคมนาคมในทางที่ผิดกฎหมาย

เงื่อนไขบังคับที่ผู้ให้บริการโทรคมนาคมต้องปฏิบัติตามหากต้องการให้บริการในสหราชอาณาจักร[174] ที่ในปัจจุบันยังคงมีการปรับปรุงแก้ไขและรวบรวมฉบับล่าสุดยังไม่แล้วเสร็จดี โดยในส่วนที่เกี่ยวเนื่องกับการเกิดอาชญากรรมได้คือส่วนของ การย้ายหมายเลขโดย มีเงื่อนไขที่กำหนดกฎให้ผู้ให้บริการโทรคมนาคมต้องปฏิบัติตามเมื่อผู้ใช้บริการยื่นคำขอการโอนย้ายหมายเลขซึ่ง ณ ปัจจุบัน อยู่ในระหว่างการออกกฎเกณฑ์ใหม่ที่จะมีผลบังคับใช้ปี 2023 โดยการปรับปรุงกฎเกณฑ์ใหม่จะเน้นการปกป้องลูกค้าที่เป็นบุคคลธรรมดาและธุรกิจขนาดเล็ก (SME) ในประเทศที่อยู่ระหว่างกระบวนการเปลี่ยนผู้ให้บริการโทรศัพท์บ้านและ/ หรือบริการบรอดแบรนด์ ไม่ว่าจะเป็นเมื่อย้ายจากผู้ให้บริการโทรคมนาคมรายหนึ่งไปยังอีก ราย หรืออยู่กับผู้ให้บริการโทรคมนาคมรายเดิม เมื่อย้ายตำแหน่ง หรือเปลี่ยนบริการด้วยรายเดียวกัน โดยในปี2023 ผู้ให้บริการสื่อสารจะมีการใช้ “One Touch Switch Process”[175] ซึ่งทำเกิดความรวดเร็วในขั้นตอนการย้ายหมายเลขโทรศัพท์และนำมาแทนที่ขั้นตอนการแจ้งการโอนที่มีอยู่ในปัจจุบัน ในส่วนของโทรศัพท์มือถือจะใช้กระบวนการ Auto-Switch ซึ่งจะมีการบังคับใช้ในปี 2023 โดยกระบวนการใหม่ทั้ง 2 กระบวนการจะมีการแก้ไขเพิ่มเติมใน The General Conditions of Entitlement ซึ่งถือเป็นแนวทางปฏิบัติหลักสำหรับผู้ให้บริการโทรคมนาคมและจะมีผลบังคับใช้วันที่ 3 เมษายน 2023 โดยที่ในปัจจุบันประกาศดังกล่าวอยู่ในระหว่างการแก้ไขและไม่มีผลบังคับใช้ทางกฎหมาย

3.1.3.4 ประเทศฟิลิปปินส์

ประเทศฟิลิปปินส์มีกฎหมายป้องกันและปราบปรามอาชญากรรมข้ามชาติหลายฉบับ ซึ่งออกแบบมาเพื่อต่อสู้กับกิจกรรมอาชญากรรมที่ข้ามพรมแดนและมีผลกระทบระหว่างประเทศ หนึ่งในกฎหมายสำคัญ คือ "Republic Act No. 9208" หรือที่รู้จักในชื่อ "Anti-Trafficking in Persons Act of 2003" กฎหมายนี้มีจุดประสงค์ในการป้องกันและปราบปรามการค้ามนุษย์ นอกจากนี้ยังมีกฎหมายอื่น ๆ ที่เกี่ยวข้องซึ่งฟิลิปปินส์มีหลายกฎหมายและมาตรการที่ใช้ในการป้องกันและ

---

[173] The Communication Act 2003, Section 128, 129, 130

[174] The General Conditions of Entitlement.

[175] Ofcom, Quick easy and reliable switching: Statement on changes to the General Conditions. 17 April 2024.

ปราบปรามอาชญากรรมข้ามชาติ รวมถึงการจัดการกับแก๊งคอลเซ็นเตอร์ที่มักจะก่ออาชญากรรมผ่านการโทรศัพท์และการใช้เทคโนโลยีสื่อสารต่าง ๆ โดยประเทศฟิลิปปินส์ได้ออกกฎหมาย ได้แก่

Cybercrime Prevention Act of 2012 (Republic Act No. 10175) กฎหมายนี้ครอบคลุมถึงอาชญากรรมทางไซเบอร์หลากหลายประเภท เช่น การฉ้อโกงทางอินเทอร์เน็ต การขโมยข้อมูล และการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต กฎหมายนี้ยังมีบทบัญญัติที่ช่วยในการดำเนินการกับอาชญากรรมที่มีลักษณะข้ามชาติอีกด้วย

มาตรา 2 คือการประกาศนโยบาย รัฐตระหนักถึงบทบาทสำคัญของอุตสาหกรรมข้อมูลและการสื่อสาร เช่น การผลิตเนื้อหา โทรคมนาคม การกระจายเสียง พาณิชย์อิเล็กทรอนิกส์ และการประมวลผลข้อมูล ในการพัฒนาสังคมและเศรษฐกิจโดยรวมของประเทศ รัฐยังตระหนักถึงความสำคัญของการสร้างสภาพแวดล้อมที่เอื้อต่อการพัฒนา การเร่งรัด และการประยุกต์ใช้อย่างมีเหตุผลและการใช้ประโยชน์จากเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) เพื่อให้การเข้าถึงการแลกเปลี่ยนและการส่งมอบข้อมูลเป็นไปอย่างอิสระ ง่ายและเข้าใจได้ ความจำเป็นในการปกป้องและรักษาความสมบูรณ์ของคอมพิวเตอร์ ระบบคอมพิวเตอร์และการสื่อสาร เครือข่าย ฐานข้อมูล ความลับ ความสมบูรณ์ ความพร้อมใช้งานของข้อมูลและข้อมูลที่จัดเก็บไว้จากการใช้ในทางที่ผิด การละเมิด และการเข้าถึงโดยผิดกฎหมายในทุกรูปแบบโดยการทำให้พฤติกรรมดังกล่าวเป็นความผิดทางกฎหมาย เพื่อให้บรรลุผลดังกล่าวรัฐจะใช้อำนาจเพียงพอเพื่อป้องกันและต่อสู้กับความผิดดังกล่าวโดยการอำนวยความสะดวกในการตรวจจับ การสืบสวน และการฟ้องร้องในทั้งระดับภายในประเทศและระหว่างประเทศ และโดยการจัดให้มีการจัดการสำหรับความร่วมมือระหว่างประเทศที่รวดเร็วและเชื่อถือได้[176]

---

[176] SEC. 2. *Declaration of Policy*. – The State recognizes the vital role of information and communications industries such as content production, telecommunications, broadcasting, electronic commerce, and data processing, in the nation's overall social and economic development. The State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology (ICT) to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts. ln this light, the State shall adopt sufficient powers to effectively prevent

ในพระราชบัญญัติดังกล่าวได้มีบทบัญญัติที่สำคัญที่กล่าวถึงความผิดที่ครอบคลุมเกี่ยวกับความผิดทางอาชญากรรมทางไซเบอร์ รวมถึงการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (hacking), การดักจับข้อมูลโดยไม่ได้รับอนุญาต, การแทรกแซงข้อมูล, การแทรกแซงระบบ, การใช้เครื่องมือผิดกฎหมาย, การแย่งที่อยู่โดเมน, การปลอมแปลงที่เกี่ยวข้องกับคอมพิวเตอร์, การฉ้อโกงที่เกี่ยวข้องกับคอมพิวเตอร์ และการขโมยข้อมูลส่วนบุคคลทางคอมพิวเตอร์ โดยกำหนดบทลงโทษสำหรับความผิดเหล่านี้มีตั้งแต่การปรับไปจนถึงการจำคุกขึ้นอยู่กับความรุนแรงและลักษณะของอาชญากรรม อีกทั้งกฎหมายนี้กำหนดให้มีการจัดตั้งหน่วยงานพิเศษในหน่วยงานบังคับใช้กฎหมายเพื่อต่อสู้กับอาชญากรรมทางไซเบอร์ หน่วยงานเหล่านี้มีหน้าที่ในการประกันว่ากฎหมายจะถูกบังคับใช้อย่างมีประสิทธิภาพ Cybercrime Prevention Act of 2012 ถือเป็นก้าวสำคัญของรัฐบาลฟิลิปปินส์ในการจัดการกับภัยคุกคามจากอาชญากรรมทางไซเบอร์ แม้ว่าจะมีการวิพากษ์วิจารณ์ โดยเฉพาะในเรื่องเสรีภาพในการพูดและความเป็นส่วนตัวของข้อมูล กฎหมายนี้ได้จัดทำกรอบการทำงานที่ครอบคลุมสำหรับการต่อสู้กับอาชญากรรมทางไซเบอร์และการเสริมสร้างความปลอดภัยทางไซเบอร์ในประเทศ

## 3.3 เปรียบเทียบนโยบายและมาตรการระดับภูมิภาคและระดับประเทศในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

จากการศึกษาและค้นคว้าของผู้วิจัยเกี่ยวกับนโยบายและมาตรการในการป้องกันและปราบปรามอาชญากรรมข้ามชาติแก๊งคอลเซ็นเตอร์ทั้งในระดับภูมิภาคและระดับประเทศ ผู้วิจัยจะทำการวิเคราะห์เปรียบเทียบแยกประเด็นเกี่ยวกับแนวทางการป้องกันที่เป็นสาระสำคัญดังต่อไป

### 3.3.1 เปรียบเทียบนโยบายที่ใช้ในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

3.3.1.1. ระดับภูมิภาค

จากการศึกษาเกี่ยวกับนโยบายในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ทั้งในสหภาพยุโรปและภูมิภาคอาเซียนจะเห็นได้ถึงความแตกต่างเชิงโครงสร้างอย่างชัดเจน ในเรื่องของหน่วยงานระบบหมายจับข้ามประเทศ โดยในด้านยุทธศาสตร์ความมั่นคงทางไซเบอร์ระดับภูมิภาคทั้งสองภูมิภาคต่างตระหนักถึงความสำคัญของภัยคุกคามในโลกดิจิทัล โดยสหภาพ

---

and combat such offenses by facilitating the detection, investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.

ยุโรปมีการกำหนดยุทธศาสตร์ที่ชัดเจนหลายฉบับอย่าง EU Cybersecurity Strategy 2020 ซึ่งกำหนดกรอบแนวทางและมาตรการเชิงรุกเพื่อรับมือกับภัยไซเบอร์แบบบูรณาการ ในขณะที่อาเซียนแม้จะมียุทธศาสตร์ร่วมอย่าง ASEAN Cybersecurity Cooperation Strategy (2021–2025) แต่ยังคงประสบข้อจำกัดในแง่ของกลไกการขับเคลื่อนที่มีลักษณะไม่เป็นบังคับและขาดระบบติดตามผลที่เข้มแข็งและในเรื่องของหน่วยงานกลางสำหรับการบังคับใช้กฎหมาย สหภาพยุโรปมีองค์กรสำคัญอย่าง Europol และ Eurojust ซึ่งเป็นหน่วยงานกลางที่ทำหน้าที่ประสานงานการสืบสวน การวิเคราะห์ข่าวกรอง และการสนับสนุนทางกฎหมายระหว่างประเทศสมาชิกอย่างมีประสิทธิภาพ ในขณะที่อาเซียนยังไม่มีหน่วยงานลักษณะเดียวกันในระดับภูมิภาค การประสานความร่วมมือจึงยังอาศัยกลไกที่ไม่เป็นทางการและขาดอำนาจบังคับในทางกฎหมาย นอกจากนี้สหภาพยุโรปยังมีการจัดตั้งกลไกติดตามและประเมินผลนโยบายอย่างต่อเนื่อง อย่างการจัดตั้งหน่วยงาน ENISA (European Union Agency for Cybersecurity) ที่ทำหน้าที่กำกับดูแลนโยบายความมั่นคงไซเบอร์ รวมถึงระบบประเมินผลที่มีตัวชี้วัดชัดเจน ตรงกันข้ามกับอาเซียนที่ยังขาดกลไกในลักษณะนี้ ทำให้การประเมินประสิทธิภาพของนโยบายเป็นไปอย่างไม่เป็นระบบและยากต่อการปรับปรุงเชิงกลยุทธ์

ในด้านแผนปฏิบัติการระดับภูมิภาคสหภาพยุโรปได้จัดทำแผนเชิงกลยุทธ์ที่สามารถนำไปปฏิบัติได้จริง (EU Strategy to Tackle Organised Crime) ซึ่งกำหนดแนวทางการรับมืออาชญากรรมข้ามชาติอย่างครอบคลุม ทั้งด้านป้องกัน การสืบสวน และการคุ้มครองเหยื่อ ขณะที่อาเซียนยังไม่มีแผนที่มีลักษณะเดียวกันทำให้การดำเนินงานในระดับภูมิภาคยังคงมีลักษณะกระจัดกระจายและไม่ต่อเนื่อง และประเด็นสุดท้าย คือ ระดับความร่วมมือระหว่างประเทศสมาชิกที่ถือเป็นรากฐานของการป้องกันและปราบปรามอาชญากรรมข้ามชาติ สหภาพยุโรปได้วางโครงสร้างความร่วมมือที่มีลักษณะผูกพันทางกฎหมายทำให้สามารถดำเนินการร่วมกันได้อย่างมีประสิทธิภาพ ในขณะที่อาเซียนยังคงยึดหลักฉันทามติและการเจรจาแบบสมัครใจ ซึ่งส่งผลให้กลไกความร่วมมือมีความยืดหยุ่นแต่ขาดประสิทธิผลในด้านการบังคับใช้ ดังนั้น การเปรียบเทียบนโยบายในระดับภูมิภาคระหว่างสหภาพยุโรปและอาเซียนแสดงให้เห็นความแตกต่างในด้านโครงสร้าง กลไก และระดับความเป็นทางการของความร่วมมือ สหภาพยุโรปมีระบบที่เป็นรูปธรรมและมีผลบังคับทางกฎหมายที่เข้มแข็ง ขณะที่อาเซียนยังอยู่ในช่วงพัฒนาแนวทางความร่วมมือ โดยเฉพาะอย่างยิ่งการสร้างกลไกบังคับใช้และระบบติดตามประเมินผลเชิงนโยบาย

**ตารางที่ 3.1** เปรียบเทียบนโยบายที่ใช้ในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ในระดับภูมิภาค

| นโยบาย | สหภาพยุโรป (EU) | อาเซียน (ASEAN) | หมายเหตุ |
|---|---|---|---|
| มียุทธศาสตร์ความมั่นคงทางไซเบอร์ระดับภูมิภาค | ✓ | ✓ | EU มียุทธศาสตร์ไซเบอร์หลายฉบับ เช่น *EU Cybersecurity Strategy 2020* ส่วน ASEAN มียุทธศาสตร์ร่วม เช่น *ASEAN Cybersecurity Cooperation Strategy (2021–2025)* |
| มีหน่วยงานกลางด้านการบังคับใช้กฎหมาย | ✓ | | EU มี *Europol* และ *Eurojust* เป็นศูนย์กลางการประสานงานด้านอาชญากรรมข้ามชาติ ในขณะที่ ASEAN ยังไม่มีหน่วยงานกลางลักษณะนี้ |
| กลไกติดตามและประเมินผลนโยบาย | ✓ | | EU มีการจัดตั้งหน่วยงานติดตาม เช่น *ENISA* และใช้ระบบประเมินผลตามรอบ ส่วน ASEAN ขาดกลไกติดตามที่มีประสิทธิภาพ |
| แผนปฏิบัติการระดับภูมิภาคที่เป็นรูปธรรม | ✓ | | EU จัดทำแผนปฏิบัติการพร้อมกรอบเวลาและตัวชี้วัด เช่น *EU Strategy to tackle Organised Crime* ขณะที่ ASEAN ยังไม่มีแผนที่บังคับใช้ชัดเจน |
| ความร่วมมือระหว่างประเทศสมาชิก | ✓ | ✓ | ทั้งสองภูมิภาคมีความร่วมมือ แต่ EU มีระดับความร่วมมือที่สูงกว่าและมีผลผูกพันทางกฎหมาย ขณะที่ ASEAN อาศัยฉันทามติและการเจรจา |

**ที่มา** สรุปโดยผู้วิจัย

3.3.1.2 ระดับประเทศ

จากการศึกษานโยบายในการป้องกันและปราบปรามอาชญากรรมข้ามชาติในกรณีแก๊งคอลเซ็นเตอร์ พบว่า ประเทศออสเตรเลีย สหราชอาณาจักร และฟิลิปปินส์ ต่างมีการวางมาตรการเชิงรุกในระดับชาติ โดยเฉพาะในสามมิติหลัก ได้แก่ (1) การจัดทำนโยบายและแผนระดับชาติที่มีกรอบเวลาชัดเจน (2) การเสริมสร้างกลไกบังคับใช้กฎหมายที่บูรณาการหลายภาคส่วน และ (3) การพัฒนาระบบการรับแจ้งเหตุและข้อมูลข่าวสารจากประชาชนที่มีประสิทธิภาพ ในกรณีของออสเตรเลีย รัฐบาลได้จัดทำแผนยุทธศาสตร์ความมั่นคงทางไซเบอร์ระดับชาติ (Australia's Cyber Security Strategy 2023–2030) โดยเน้นการปกป้องโครงสร้างพื้นฐาน การป้องกันภัยทางไซเบอร์ในระดับครัวเรือน และการทำงานร่วมกันระหว่างภาครัฐ ภาคเอกชน และประชาชนอย่างเป็นระบบ พร้อมทั้งเปิดช่องทาง Report Cyber ให้ประชาชนสามารถแจ้งเหตุการณ์ต้องสงสัยทางออนไลน์ได้โดยตรงถึงตำรวจและหน่วยงานบังคับใช้กฎหมาย ซึ่งถือเป็นแนวทางเชิงป้องกันที่ส่งเสริมการมีส่วนร่วมของสังคมในวงกว้าง ขณะที่สหราชอาณาจักรได้จัดทำ ยุทธศาสตร์ไซเบอร์แห่งชาติ 2022 (UK National Cyber Strategy 2022) โดยเน้นการสร้างไซเบอร์อัตลักษณ์ ให้กับประเทศในเชิงเศรษฐกิจและความมั่นคง รวมถึงการจัดตั้ง National Cyber Security Centre (NCSC) ภายใต้ GCHQ เพื่อทำหน้าที่ประสานงานกับภาคเอกชนและภาคสังคมในกรณีการฉ้อโกงหรือคุกคามทางไซเบอร์ นอกจากนี้ประชาชนสามารถรายงานการฉ้อโกงทางออนไลน์ได้ผ่านแพลตฟอร์ม *Action Fraud* ซึ่งทำงานร่วมกับตำรวจและศูนย์ประสานงานด้านอาชญากรรมทางเทคโนโลยีของประเทศ สำหรับฟิลิปปินส์แม้จะประสบปัญหาในการเป็นฐานที่ตั้งของกลุ่มอาชญากรรมข้ามชาติประเภทแก๊งคอลเซ็นเตอร์ แต่ก็มีความพยายามในการจัดตั้ง Cybercrime Investigation and Coordinating Center (CICC) ภายใต้ *Republic Act No. 10175: Cybercrime Prevention Act of 2012* เพื่อประสานงานด้านนโยบายและปฏิบัติการเกี่ยวกับอาชญากรรมไซเบอร์ โดยมีการพัฒนาแพลตฟอร์มออนไลน์ให้ประชาชนรายงานพฤติกรรมต้องสงสัย เช่น "Stop Spam" และแอปพลิเคชันของ CICC ที่กำลังพัฒนาในเชิงป้องกัน ทั้งสามประเทศดังกล่าวจึงสะท้อนให้เห็นถึงความสามารถในการบริหารจัดการเชิงนโยบายที่มีลักษณะยืดหยุ่น ทันสมัย และตอบสนองต่อภัยคุกคามรูปแบบใหม่ได้อย่างมีประสิทธิภาพ ไม่ว่าจะเป็นด้านการป้องกันเชิงรุก การตอบสนองฉับไว หรือการปรับปรุงนโยบายโดยอิงกับข้อมูลจริงในระดับชาติ ในทางกลับกัน ประเทศไทยแม้จะมีความพยายามในการจัดตั้งกลไกรับมือกับอาชญากรรมข้ามชาติในช่วงปี 2565 เป็นต้นมา เช่น การจัดตั้งศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (PCT) และการทำงานร่วมกับธนาคารแห่งประเทศไทยและ กสทช. ในการสกัดกั้นบัญชีม้า แต่กลไกเหล่านี้ยังขาด "แผนปฏิบัติการระดับชาติที่มีผลผูกพันทางกฎหมาย" ที่กำหนดบทบาท ความรับผิดชอบ และกระบวนการตรวจสอบของแต่ละหน่วยงานอย่างเป็นรูปธรรม

นอกจากนี้ ระบบการแจ้งเหตุของไทยยังมีข้อจำกัด คือประชาชนมักเข้าแจ้งเหตุกับหน่วยงานรัฐหลังเกิดความเสียหายแล้ว ผ่านทางสถานีตำรวจ หรือเว็บไซต์ของศูนย์ PCT โดยตรง ซึ่งยังไม่เปิดช่องทางในการรับแจ้งเบาะแสหรือพฤติกรรมต้องสงสัยอย่างมีระบบ ทำให้ไม่สามารถใช้ข้อมูลเชิงลึกมาเป็นเครื่องมือกำหนดนโยบายหรือวางแผนป้องกันได้อย่างมีประสิทธิภาพ อีกทั้ง ฐานข้อมูลกลางเกี่ยวกับอาชญากรรมข้ามชาติและการฉ้อโกงทางไซเบอร์ก็ยังไม่เชื่อมโยงระหว่างหน่วยงานในเชิงวิเคราะห์

จากการเปรียบเทียบดังกล่าวสะท้อนให้เห็นว่า ประเทศที่มีกรอบนโยบายที่ชัดเจน มีการจัดตั้งกลไกการประสานงานที่ต่อเนื่องและเปิดพื้นที่ให้ประชาชนมีส่วนร่วมในการรายงานและเฝ้าระวังจะมีความสามารถในการรับมือกับอาชญากรรมข้ามชาติประเภทแก๊งคอลเซ็นเตอร์ได้อย่างรอบด้าน ทั้งในด้านการป้องกัน การตอบสนอง และการประเมินผลนโยบายเพื่อการปรับปรุงอย่างยั่งยืน

**ตารางที่ 3.2** เปรียบเทียบนโยบายที่ใช้ในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ในแต่ละประเทศ

| เรื่อง | ไทย | ออสเตรเลีย | สหราชอาณาจักร | ฟิลิปปินส์ |
|---|---|---|---|---|
| การมีส่วนร่วมขององค์กรภาครัฐและเอกชนรวมไปถึงการวางแผนปฏิบัติการในการป้องกันแก๊งคอลเซ็นเตอร์อย่างเป็นรูปธรรมที่สามารถติดตามผลและวัดผลได้ | ประเทศได้ให้ภาคส่วนที่เกี่ยวข้องได้เข้ามาหารือร่วมกันโดย มีลักษณะเป็นการทำข้อตกลงร่วมกัน (MOU) | The Combating Scams Action Plan เป็นแผนปฏิบัติการเชิงรูปธรรมที่ริเริ่มขึ้นเพื่อเป็นจุดเริ่มต้นในการกำหนดกฎเกณฑ์บังคับใช้กับผู้ให้บริการโทรคมนาคม โดยมีเป้าหมายเพื่อป้องกันและตรวจสอบความผิดปกติของหมายเลขโทรศัพท์ตั้งแต่ต้นทาง | ภาครัฐได้มีการจัดทำแผนปฏิบัติการที่เรียกว่า Nuisance calls and messages Update to ICO - Ofcom joint action plan | ฟิลิปปินส์มีการจัดทำแผนปฏิบัติอย่างเป็นรูปธรรมในการวางแผนการป้องกันเพื่อจัดการกับอันตรายทางอาชญากรรมไซเบอร์คือ Operation against Cybercrime ซึ่งเป็นปฏิบัติการที่ดำเนินการโดยหน่วยงานบังคับใช้กฎหมาย |
| การจัดตั้งหน่วยงานรับเรื่องร้องเรียนแบบ One Stop Service | การเปิดเว็บไซต์ https://www.thaipoliceonline.com/ ให้ประชาชนได้เข้าไป รายงานซึ่งเว็บไซต์ดังกล่าวอยู่ภายใต้การดูแล | มีการจัดทำเว็บไซต์ Scam watch โดยภายในเว็บไซต์ Scam watch จะบอกรายละเอียดของการหลอกลวงแต่ละประเภทเพื่อ | มีการจัดทำเว็บไซต์ที่ใช้รายงานการหลอกลวงรูปแบบต่างๆ คือ Action Fraud โดยประชาชนสามารถศึกษารูปแบบการหลอกลวงรวมไป | รัฐบาลฟิลิปปินส์ได้จัดตั้ง (I-ARC) ขึ้น ศูนย์นี้เป็นศูนย์บริการ 24 ชั่วโมง ที่มีหมายเลขสายด่วน 1326 สำหรับเหยื่อของ |

**ตารางที่ 3.2** (ต่อ)

| เรื่อง | ไทย | ออสเตรเลีย | สหราชอาณาจักร | ฟิลิปปินส์ |
|---|---|---|---|---|
| | ของสำนักงานตำรวจแห่งชาติที่จะทำการรับเรื่องการแจ้งความออนไลน์คดีอาชญากรรมทางเทคโนโลยีไว้ | ส่งเสริมการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับการหลอกลวงของแก๊งมิจฉาชีพรวมถึงด้านอื่นๆ ของการคุ้มครองผู้บริโภคและมีช่องทาง และขั้นตอนการร้องเรียนต่างๆ ซึ่งประชาชนสามารถทำการสอบถามหรือทำการ รายงานได้ตลอด 24 ชั่วโมง | ถึงการแจ้งรายงานได้ทันที | อาชญากรรมทางไซเบอร์รวมถึงการหลอกลวงต่างๆ ที่สามารถรายงานเหตุการณ์ได้ |
| การแบ่งปันข้อมูลระหว่างหน่วยงาน | ประเทศไทยยังไม่มีแนวคิดในการแบ่งปันข้อมูลเบอร์โทรศัพท์ที่ทำการหลอกลวงระหว่างผู้ให้บริการ | ภาครัฐได้เล็งเห็นความสำคัญของการเชื่อมโยงฐานข้อมูลหมายเลขโทรศัพท์ที่กระทำความผิดระหว่างภาครัฐกับ | การแบ่งปันข้อมูลระหว่างผู้ให้บริการโทรคมนาคมด้วยกันรวมไปถึงประเทศพันธมิตรของสหราชอาณาจักรและ | ฟิลิปินส์ได้จัดตั้งศูนย์ตอบสนองระหว่างหน่วยงาน (I-ARC) ในฟิลิปปินส์เป็นบริการสาย |

**ตารางที่ 3.2** (ต่อ)

| เรื่อง | ไทย | ออสเตรเลีย | สหราชอาณาจักร | ฟิลิปปินส์ |
|---|---|---|---|---|
| | โทรคมนาคมด้วยกันเองและยังไม่มีระบบเชื่อมต่อไปยังฐานข้อมูลของภาครัฐมีเพียงแต่การทำงานแยกเป็นหน่วยงานอิสระ | ฐานข้อมูลของภาคเอกชนเพื่อร่วมกันแก้ไขปัญหาอย่างบูรณาการและทันท่วงที | หน่วยงานภาครัฐเพื่อให้การตรวจสอบข้อมูลเป็นไปอย่างรวดเร็วและมีประสิทธิภาพในการจับกุม | ด่วนศูนย์กลางที่จัดตั้งขึ้นเพื่อต่อสู้กับอาชญากรรมทางไซเบอร์หลายรูปแบบ โดยเฉพาะการหลอกลวงทางออนไลน์ ศูนย์ I-ARC |
| การรับเรื่องร้องเรียน | รายงานได้เฉพาะเมื่อถูกหลอกลวงแล้ว | รายงานเหตุการณ์ได้ตั้งแต่พบความผิดปกติจนถึงหลังถูกหลอกลวง | รายงานเหตุการณ์ได้ตั้งแต่พบความผิดปกติจนถึงหลังถูกหลอกลวง | รายงานเหตุการณ์ได้ตั้งแต่พบความผิดปกติจนถึงหลังถูกหลอกลวง |
| กฎหน่วยงานกำกับดูแล | สำนักงาน กสทช. (NBTC) | Australian Communications and Media Authority (ACMA) | Office of Communications (Ofcom) | National Telecommunications Commission (NTC) |

**ที่มา** สรุปโดยผู้วิจัย

**3.3.2 เปรียบเทียบมาตรการที่ใช้ในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์**

3.3.2.1 ระดับภูมิภาค

จากการศึกษามาตรการในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ในระดับภูมิภาคนี้พบว่า สหภาพยุโรปมีการใช้ *European Arrest Warrant (EAW)* ซึ่งเป็นกลไกที่มีผลผูกพันทางกฎหมายใช้สำหรับออกหมายจับผู้ต้องหาข้ามพรมแดนอย่างมีประสิทธิภาพในหมู่ประเทศสมาชิกเป็นการลดอุปสรรคด้านกระบวนการทางกฎหมายและเพิ่มความเร็วในการส่งผู้ร้ายข้ามแดน ในทางตรงกันข้าม ASEAN ยังไม่มีระบบหมายจับส่วนกลางในลักษณะเดียวกัน ซึ่งกลไกที่อาเซียนใช้จะอิงความร่วมมือผ่านกรอบที่ไม่ผูกพันทางกฎหมายอย่าง *ASEAN Mutual Legal Assistance Treaty (MLAT)* ที่แม้จะมีบทบาทด้านการแลกเปลี่ยนข้อมูล แต่ยังขาดกลไกการบังคับใช้ที่มีประสิทธิภาพเทียบเท่า EAW อีกทั้งสหภาพยุโรปได้พัฒนาและบังคับใช้กฎหมายในระดับภูมิภาคที่มีผลผูกพันสูงต่อประเทศสมาชิก เพื่อจัดการกับอาชญากรรมไซเบอร์อย่างมีประสิทธิภาพ โดยเน้นการกำหนดนิยามของความผิด การประสานความร่วมมือข้ามพรมแดน และการสร้างกลไกบังคับใช้ที่เป็นรูปธรรม ได้แก่ Directive 2013/40/EU ว่าด้วยการโจมตีระบบสารสนเทศ ซึ่งกำหนดให้การเข้าถึงระบบโดยมิชอบ การแทรกแซงระบบหรือข้อมูล และการสกัดกั้นข้อมูลเป็นความผิดทางอาญาพร้อมกำหนดบทลงโทษที่สอดคล้องกับหลักความได้สัดส่วนและความเหมาะสม นอกจากนี้ยังมีการส่งเสริมให้รัฐสมาชิกร่วมมือกับหน่วยงานระดับภูมิภาคในการสืบสวนอาชญากรรมไซเบอร์ที่มีมิติระหว่างประเทศ สหภาพยุโรปยังได้ตรา Directive 2014/41/EU ว่าด้วย European Investigation Order (EIO) ซึ่งถือเป็นกลไกสำคัญในการอำนวยความสะดวกแก่กระบวนการสืบสวนและรวบรวมพยานหลักฐานข้ามพรมแดน โดยมีการกำหนดแบบฟอร์มคำสั่งสืบสวนเดียวกันทั่วทั้งสหภาพ กำหนดระยะเวลาที่ชัดเจนในการดำเนินการ ตลอดจนเปิดช่องให้ผู้พิพากษา อัยการ หรือเจ้าหน้าที่ของรัฐที่ได้รับมอบหมายสามารถออกคำสั่งได้ภายใต้หลักความสมเหตุสมผลและไม่ละเมิดสิทธิขั้นพื้นฐานของบุคคล อีกทั้งยังมีเครื่องมือทางกฎหมายเสริมอย่าง Directive 2014/42/EU ว่าด้วยการอายัดและยึดทรัพย์ ซึ่งช่วยให้รัฐสามารถยึดหรือเพิกถอนทรัพย์สินที่ได้จากการกระทำผิด รวมถึงทรัพย์สินที่เกี่ยวข้องกับองค์กรอาชญากรรมข้ามชาติได้อย่างมีประสิทธิภาพ ซึ่งในกรณีของแก๊งคอลเซ็นเตอร์เครื่องมือทางกฎหมายเหล่านี้ช่วยให้สามารถติดตามเส้นทางการเงินที่ซับซ้อนข้ามพรมแดนและยึดทรัพย์กลับคืนได้ในระดับที่กฎหมายภายในประเทศไม่สามารถดำเนินการได้อย่างทันท่วงที สหภาพยุโรปยังให้ความสำคัญกับความมั่นคงของระบบข้อมูลพื้นฐานที่รองรับกิจกรรมทางเศรษฐกิจและการบริหารราชการแผ่นดินผ่านการออก Directive 2016/1148/EU หรือที่เรียกกันว่า NIS Directive ซึ่งต่อมาพัฒนาเป็น NIS2 Directive โดยกำหนดให้ผู้ให้บริการโครงสร้างพื้นฐานสำคัญ

ต้องดำเนินมาตรการทางเทคนิคและการบริหารจัดการที่เหมาะสมเพื่อรับมือกับความเสี่ยงทางไซเบอร์ และมีหน้าที่ต้องรายงานเหตุการณ์ร้ายแรงที่กระทบต่อความต่อเนื่องของบริการให้แก่หน่วยงานที่เกี่ยวข้องโดยไม่ชักช้า กลไกนี้จึงเป็นการสร้างมาตรฐานขั้นต่ำของความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาค และมีบทบาทสำคัญในการลดช่องโหว่ที่อาชญากรไซเบอร์มักอาศัยเป็นจุดโจมตี

ในทางตรงกันข้ามอาเซียนแม้จะตระหนักถึงความรุนแรงของภัยคุกคามไซเบอร์ที่ส่งผลกระทบต่อภูมิภาค แต่การดำเนินการทางกฎหมายส่วนใหญ่ยังอยู่ในลักษณะของความร่วมมือเชิงนโยบายมากกว่าจะเป็นกฎหมายที่มีผลผูกพัน อาเซียนมีการออกปฏิญญาซึ่งเน้นการสร้างกลไกความร่วมมือ การแลกเปลี่ยนข้อมูล และการพัฒนาศักยภาพของประเทศสมาชิก อย่างไรก็ตาม เอกสารเหล่านี้ไม่ได้มีสถานะเป็นกฎหมายที่สามารถบังคับใช้ได้จริงในระดับภูมิภาค และยังขาดกลไกกลางที่มีอำนาจเหมือนกับ Europol หรือ Eurojust ของสหภาพยุโรป โดยจุดอ่อนสำคัญของอาเซียนอยู่ที่โครงสร้างทางกฎหมายที่กระจัดกระจายและไม่มีความกลมกลืนระหว่างประเทศสมาชิก การสืบสวนอาชญากรรมไซเบอร์ข้ามพรมแดนยังต้องอาศัยความร่วมมือแบบกรณีต่อกรณีผ่านช่องทางทวิภาคีหรืออนุสัญญาระหว่างประเทศ เช่น การร้องขอความช่วยเหลือทางกฎหมาย (MLAT) ซึ่งมักมีขั้นตอนซับซ้อนและใช้เวลานาน แตกต่างจากระบบของ EU ที่สามารถดำเนินการตามคำสั่ง EIO ได้อย่างมีประสิทธิภาพและรวดเร็วกว่า นอกจากนี้ ประเทศสมาชิกอาเซียนบางประเทศยังไม่มีการบัญญัติความผิดเกี่ยวกับการแทรกแซงระบบสารสนเทศหรือการฉ้อโกงผ่านระบบดิจิทัลไว้ในกฎหมายภายในอย่างชัดเจนทำให้การบังคับใช้กฎหมายในกรณีแก๊งคอลเซ็นเตอร์ยังคงเผชิญข้อจำกัดหลายประการ

เมื่อพิจารณาจากการเปรียบเทียบจะเห็นได้อย่างชัดเจนว่าสหภาพยุโรปมีความได้เปรียบในการรับมือกับแก๊งคอลเซ็นเตอร์เนื่องจากมีกรอบกฎหมายที่เป็นเอกภาพ มีผลผูกพันในระดับภูมิภาค และสามารถบังคับใช้ได้อย่างมีประสิทธิภาพในทุกประเทศสมาชิก กฎหมายของสหภาพยุโรปไม่เพียงแต่กำหนดนิยามของความผิดทางอาญาที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ไว้อย่างชัดเจน หากยังสร้างกลไกที่เอื้อต่อการสืบสวนร่วม การแลกเปลี่ยนข้อมูลข่าวสาร และการบังคับใช้คำสั่งยึดอายัดทรัพย์ข้ามพรมแดนได้อย่างรวดเร็วและมีประสิทธิภาพ กลไกเหล่านี้มีส่วนสำคัญในการลดช่องว่างของการบังคับใช้กฎหมายระหว่างประเทศสมาชิก และทำให้การจัดการกับอาชญากรรมไซเบอร์ที่มีลักษณะซับซ้อนและไร้พรมแดนเป็นไปอย่างครอบคลุม มีประสิทธิผล และสามารถดำเนินการตอบโต้ได้ทันท่วงทีภายใต้กรอบความร่วมมือทางกฎหมายที่เข้มแข็งและมีมาตรฐานเดียวกันทั้งภูมิภาค

**ตารางที่ 3.3** การเปรียบเทียบมาตรการที่ใช้ในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ในระดับภูมิภาค

| มาตรการทางกฎหมาย | สหภาพยุโรป (EU) | อาเซียน (ASEAN) | หมายเหตุ |
|---|---|---|---|
| กฎหมายกำหนดความผิดไซเบอร์โดยเฉพาะ | ✓ | ✓ | EU มี Directive 2013/40/EU; ASEAN มีปฏิญญา 2017 แต่เป็น soft law ไม่มีผลผูกพันโดยตรง |
| การกำหนดบทลงโทษทางอาญาที่ชัดเจน | ✓ | | EU มีการกำหนดบทลงโทษไว้ใน Directive อย่างชัดเจน; ASEAN ยังไม่มีมาตรฐานร่วม |
| กรอบความร่วมมือในการสืบสวนข้ามพรมแดน | ✓ | ✓ | EU มี EIO และ Eurojust; ASEAN มีความร่วมมือผ่าน AMMTC และ ACTIP แต่ไม่ใช่กลไกบังคับใช้ตรง |
| มาตรการยึดและอายัดทรัพย์ที่ได้จากอาชญากรรม | ✓ | | EU มี Directive 2014/42/EU; ASEAN ยังไม่มีกรอบบังคับใช้ร่วมในเรื่องนี้ |
| กฎหมายว่าด้วยการป้องกันการปลอมแปลง/ฉ้อโกงทางการเงิน | ✓ | | EU มี Directive 2019/713; ASEAN ยังไม่มีข้อตกลงเฉพาะด้านนี้ |
| ข้อกำหนดด้านความปลอดภัยของระบบเครือข่าย | ✓ | | EU มี NIS Directive และ NIS2; ASEAN ยังไม่มีกรอบบังคับใช้ร่วมเช่นเดียวกัน |
| การสร้าง CSIRT ระดับชาติ/ภูมิภาค | ✓ | ✓ | ทั้งสองภูมิภาคมีการส่งเสริมให้จัดตั้ง CSIRT แต่ของ EU มีข้อบังคับที่ชัดเจนกว่า |

**ตารางที่ 3.3** (ต่อ)

| มาตรการทางกฎหมาย | สหภาพยุโรป (EU) | อาเซียน (ASEAN) | หมายเหตุ |
|---|---|---|---|
| การรายงานเหตุการณ์ไซเบอร์โดยผู้ให้บริการสำคัญ | ✓ | | ข้อกำหนดตามมาตรา 14 ของ NIS Directive; ASEAN ไม่มีข้อผูกพันลักษณะนี้ |
| การจัดทำคำสั่งสืบสวนแบบมาตรฐานเดียวกัน (One form EIO) | ✓ | | มีเฉพาะใน EU ภายใต้ Directive 2014/41/EU |

**ที่มา** สรุปโดยผู้วิจัย

3.3.2.2 ระดับประเทศ

จากการศึกษาแต่ละประเทศมีกฎหมายให้อำนาจหน่วยงานกำกับดูแลไว้เพื่อให้องค์กรนั้นทำหน้าที่เป็นหน่วยงานที่มีหน้าที่กำกับดูแลที่เป็นอิสระต่อผู้ให้บริการโทรคมนาคม เนื่องจากกระแสผลักดันที่ทำให้เกิดหน่วยงานกำกับดูแลตาม ข้อกำหนดที่ 5 ในเอกสารอ้างอิงขององค์การการค้าโลก (WTO Reference Paper) ซึ่งระบุให้หน่วยงานกำกับดูแลต้องแยกออกจากผู้ให้บริการโทรคมนาคมพื้นฐานและไม่ต้องมีความรับผิดต่อผู้ให้บริการโทรคมนาคมรายใดรายหนึ่งเป็นพิเศษ รวมถึงการออกกฎเกณฑ์ที่ใช้บังคับกับผู้ให้บริการโทรคมนาคมเหล่านั้น นอกจากนี้การบังคับใช้กฎหมายเพื่อป้องกันการถูกหลอกจากมิจฉาชีพของประเทศไทยมีลักษณะค่อนข้างที่จะคล้ายคลึงกับประเทศออสเตรเลียมากกว่าประเทศสหราชอาณาจักรและประเทศฟิลิปปินส์ เนื่องจากประเทศไทยและประเทศออสเตรเลียมีบทกฎหมายได้ให้อำนาจหน่วยงานไว้ เพื่อออกเป็นกฎเกณฑ์ใช้บังคับกับผู้ให้บริการโทรคมนาคมจะต้องปฏิบัติตามกฎหรือคำสั่งในเรื่องต่าง ๆ ถ้าหากไม่ปฏิบัติตามจะมีบทลงโทษ ซึ่งบทลงโทษดังกล่าวจะมีลักษณะเพื่อเป็นการยับยั้งและป้องกันเนื่องจากต้องการให้ผู้ให้บริการโทรคมนาคมปฏิบัติตามกฎเกณฑ์ อย่างเคร่งครัด แต่ในทางกลับกันการกำกับดูแลของหน่วยงานที่มีอำนาจในการออกกฎเกณฑ์และบังคับใช้กับผู้ให้บริการเครือข่ายของประเทศสหราชอาณาจักรจะเน้นการไม่เข้าไปแทรกแซงเว้นเสียแต่ว่าเรื่องที่ต้องแทรกแซงเป็นเรื่องที่จำเป็นจริง ๆ กล่าวคือ เน้นการขอความร่วมมือและความสมัครใจ เช่น การใช้อำนาจของ Ofcom กับผู้ให้บริการโทรคมนาคม โดยผู้ให้บริการโทรคมนาคมจะต้องดำเนินการตามขั้นตอนที่ เหมาะสมในการตรวจสอบและระบุหมายเลขโทรศัพท์ที่ทำการหลอกลวง แต่ขั้นตอนดังกล่าวให้ขึ้นอยู่กับผู้ให้บริการโทรคมนาคมแต่ละรายในการกำหนด เป็นต้น จึงทำให้ บทลงโทษในแผนปฏิบัติการของประเทศสหราชอาณาจักรจะเน้นไปที่ตัวผู้ที่กระทำการนำหมายเลขโทรศัพท์มาใช้ในการหลอกลวงหรือก่อกวน โดยกำหนดบทลงโทษได้สูงถึง 2 ล้านปอนด์ ซึ่งการลงโทษลักษณะดังกล่าวเป็นการลงโทษที่มุ่งที่จะตอบแทนหรือทดแทน

เนื่องจากทางภาครัฐของประเทศออสเตรเลีย ประเทศสหราชอาณาจักร ประเทศฟิลิปปินส์ได้เล็งเห็นถึงปัญหาที่อาจจะเกิดขึ้นจึงได้ทำการสนับสนุนให้เกิดการเชื่อมโยงกับฐานข้อมูลระหว่างภาครัฐและภาคเอกชน โดยประเทศออสเตรเลียได้เล็งเห็นปัญหาดังกล่าวทำให้เกิดการบังคับใช้ Reducing Scams Call Industry Code ซึ่งเน้นการให้ผู้ให้บริการโทรคมนาคมจะต้องตรวจสอบและตรวจจับการ รับส่งข้อมูลการโทรหลอกลวงบนเครือข่ายของตน โดยเฉพาะอย่างยิ่งเน้นการแบ่งปันข้อมูลของหมายเลขโทรศัพท์ที่ทำการหลอกลวงกับผู้ให้บริการโทรคมนาคมรายอื่นและหน่วยงานภาครัฐที่เกี่ยวข้องรวมไปถึงต้องทำการตรวจสอบ ติดตาม และปิดกั้นการใช้งานหมายเลขโทรศัพท์ที่ทำการหลอกลวงให้ได้อย่างทันท่วงที ซึ่งหลังจากการประกาศใช้ดังกล่าวทางผู้ให้บริการโทรคมนาคมก็สามารถทำการปิดกั้นการใช้งานหมายเลขโทรศัพท์ที่มีความเสี่ยงเป็นมิจฉาชีพได้เป็น

จำนวนมาก ในส่วนของประเทศสหราชอาณาจักรทางภาครัฐมีการทำงานร่วมกับผู้ให้บริการโทรคมนาคม โดยจัดตั้งเป็นคณะทำงาน ซึ่งเป็นหนึ่งในแผนปฏิบัติการเพื่อป้องกันการโทรหลอกลวงที่รบกวนประชาชน โดยมีการแบ่งปันข้อมูลระหว่างกันรวมไปถึงพันธมิตรระหว่างประเทศของสหราชอาณาจักรด้วย แต่ในส่วนของประเทศไทยยังไม่ได้ออกกฎเกณฑ์เกี่ยวกับเรื่องดังกล่าวอย่างชัดเจน ซึ่งจากการเปรียบเทียบดังกล่าวจะเห็นว่าออสเตรเลียและสหราชอาณาจักรมีมาตรการที่เข้มงวดและมีการดำเนินการที่มีประสิทธิภาพกว่า ในขณะที่ฟิลิปปินส์และไทยที่ยังคงต้องพัฒนากลไกและมาตรการเพิ่มเติมเพื่อให้สามารถป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์ได้อย่างมีประสิทธิภาพมากขึ้น

**ตารางที่ 3.4** การเปรียบเทียบมาตรการที่ใช้ในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ในระดับประเทศ

| เรื่อง | ไทย | ออสเตรเลีย | สหราชอาณาจักร | ฟิลิปปินส์ |
|---|---|---|---|---|
| การออกกฎหมายและกฎเกณฑ์ | มีการออกกฎหมายแต่ไม่ครอบคลุม และขาดการวางแผนปฏิบัติการที่เป็นรูปธรรม | มีการออกกฎหมายที่ชัดเจน เช่น Reducing Scams Call Industry Code | มีการออกกฎมายพิเศษเกี่ยวกับการจัดการกับแก๊งคอลเซ็นเตอร์ คือ The National Telephone Numbering Plan | มีการออกกฎหมาย กฎหมายนี้ครอบคลุมถึงอาชญากรรมทางไซเบอร์หลากหลายประเภทแต่มีการปฏิบัติที่ช้ากว่าในบางกรณี |
| บทลงโทษ | มีบทลงโทษ แต่ขาดการบังคับใช้ที่มีประสิทธิภาพ | เน้นการยับยั้งและป้องกัน | ลงโทษสูงถึง 2 ล้านปอนด์ มุ่งที่จะตอบแทนหรือทดแทน | เน้นการยับยั้งและป้องกัน |
| มาตรการเพิ่มเติม | ยังไม่ได้ออกกฎเกณฑ์เกี่ยวกับการตรวจสอบและปิดกั้นหมายเลขโทรศัพท์อย่างชัดเจน | มีการตรวจสอบและปิดกั้นการใช้งานหมายเลขโทรศัพท์ที่ต้องสงสัย | มีการตั้งคณะทำงานร่วมกับผู้ให้บริการและพันธมิตรระหว่างประเทศ | มีการตรวจสอบและปิดกั้นการใช้งานหมายเลขโทรศัพท์ที่ต้องสงสัย |

**ตารางที่ 3.4** (ต่อ)

| เรื่อง | ไทย | ออสเตรเลีย | สหราชอาณาจักร | ฟิลิปปินส์ |
|---|---|---|---|---|
| การออกกฎหมายและกฎเกณฑ์ | การขอความร่วมมือระหว่างประเทศผ่านทางกระทรวงยุติธรรม | มีการความร่วมมือระหว่างประเทศผ่านการทำสนธิสัญญาและข้อตกลง | มีระบบ European Arrest Warrant (EAW) สำหรับการจับกุมผู้กระทำความผิดในยุโรป | มีการประสานงานกับหน่วยงานต่างประเทศ |

**ที่มา** สรุปโดยผู้วิจัย

# บทที่ 4

# สภาพปัญหาในปัจจุบันที่เกี่ยวกับอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ที่เป็นภัยต่อความมั่นคงในภูมิภาคเอเชียตะวันออกฉียงใต้

## 4.1 สถานการณ์ปัญหาอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ที่เกิดขึ้นในภูมิภาคเอเชียตะวันออกเฉียงใต้

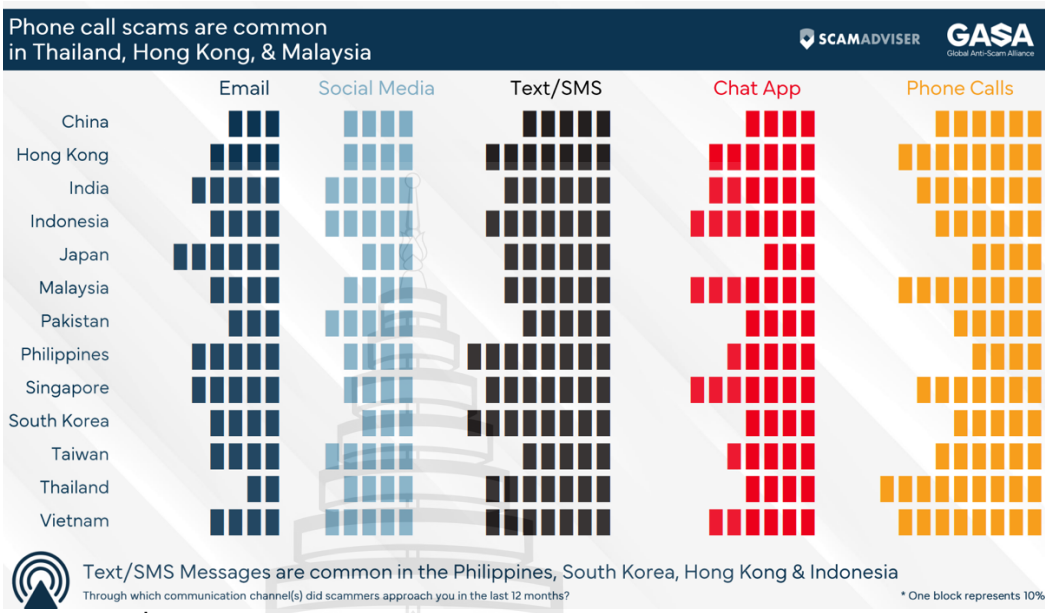
ในช่วงไม่กี่ปีที่ผ่านมาอาชญากรรมข้ามชาติในลักษณะของแก๊งคอลเซ็นเตอร์ได้กลายเป็นปัญหาเร่งด่วนที่ส่งผลกระทบในวงกว้างต่อประเทศสมาชิกอาเซียน โดยเฉพาะในด้านความมั่นคง เศรษฐกิจและสิทธิมนุษยชนของประชาชนในภูมิภาค กลุ่มอาชญากรรมคอลเซ็นเตอร์ในภูมิภาคนี้มักมีลักษณะเป็นเครือข่ายข้ามชาติที่มีการใช้โครงสร้างองค์กรคล้ายธุรกิจแบ่งหน้าที่ชัดเจน อาทิ กลุ่มจัดหาแรงงาน กลุ่มเทคนิคด้านไซเบอร์ กลุ่มพูดหลอกเหยื่อ และกลุ่มฟอกเงิน ซึ่งมักเชื่อมโยงกับขบวนการอาชญากรรมข้ามชาติอื่น โดยรายงานของ *United Nations Office on Drugs and Crime* ระบุว่า ประเทศในเอเชียตะวันออกเฉียงใต้จำนวนมากกลายเป็นทั้ง “ประเทศต้นทาง” ของเหยื่อ ได้แก่ ไทย ฟิลิปปินส์ เวียดนาม และ “ประเทศที่เป็นฐานปฏิบัติการ” ได้แก่ เมียนมา กัมพูชา ลาว ซึ่งกลุ่มเหล่านี้ใช้ในการตั้งศูนย์หลอกลวงผ่านแอปพลิเคชันธนาคารปลอม เว็บไซต์เทียม และการปลอมตัวเป็นเจ้าหน้าที่รัฐ โดยมีเป้าหมายไปที่เหยื่อทั้งในและนอกภูมิภาค[177] อีกทั้งยังมีสถิติที่เผยแพร่โดย Scam Adviser และ Global Anti-Scam Alliance[178] (GASA) ซึ่งเป็นองค์กรที่ทำงานด้านการเฝ้าระวังและรายงานเกี่ยวกับการหลอกลวงออนไลน์ทั่วโลกได้สำรวจและรวบรวมข้อมูลจากประชากรในหลายประเทศในภูมิภาคเอเชียรวมถึงอาเซียน จากข้อมูลสถิติที่เกี่ยวข้องชี้ให้เห็นว่าประเทศไทยประสบปัญหาแก๊งคอลเซ็นเตอร์มากที่สุดในภูมิภาคโดยมีอัตราผู้ที่เคยตกเป็นเหยื่อของการหลอกลวงทางโทรศัพท์สูงถึง 90% ของประชากร ในขณะที่ประเทศสมาชิกอาเซียนอื่น ๆ ได้แก่ มาเลเซียนและเวียดนามพบอัตราเหยื่ออยู่ที่ประมาณ 80% ประเทศสิงคโปร์มีอัตราเหยื่ออยู่ที่ประมาณ 70%

---

[177] ‘Online Scam Centres and Trafficking in Persons in Southeast Asia’ (UNODC, 2023) <https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf> accessed 6 July 2025.

[178] Global Anti-Scam Alliance (GASA), Research <https://www.gasa.org/research> accessed 15 December 2024.

ประเทศอินโดนีเซีย 60% และประเทศฟิลิปปินส์ 40% ซึ่งนับว่าเป็นตัวเลขที่สะท้อนถึงความแพร่หลายและความซับซ้อนของอาชญากรรมประเภทนี้




**ภาพที่ 4.1** ข้อมูลสถิติจาก Scam Adviser และ Global Anti-Scam Alliancce

แม้ว่าแนวโน้มการหลอกลวงทางโทรศัพท์และทางออนไลน์จะเพิ่มสูงขึ้นในหลายประเทศในอาเซียน แต่ในบางประเทศกลับไม่มีรายงานตัวเลขหรือการศึกษาวิจัยที่แสดงถึงขอบเขตของปัญหาอย่างเป็นรูปธรรม ซึ่งการขาดข้อมูลดังกล่าวสะท้อนให้เห็นถึงข้อจำกัดในเชิงระบบของประเทศเหล่านี้

สภาพปัญหาแก๊งคอลเซ็นเตอร์ในประเทศสมาชิกอาเซียนแต่ละประเทศมีความแตกต่างหลากหลายกันไปทั้งในเรื่องของปัจจัยสาเหตุที่เข้าสู่กระบวนการการหลอกลวงของแก๊งคอลเซ็นเตอร์ส่งผลถึงรูปแบบวิธีการและการดำเนินการเพื่อป้องกันและแก้ไขปัญหาของแก๊งคอลเซ็นเตอร์ภายในประเทศต่าง ๆ ดังนี้

### 4.1.1 ประเทศไทย

ในบริบทของประเทศไทยแก๊งคอลเซ็นเตอร์นับว่าเป็นหนึ่งในรูปแบบของอาชญากรรมข้ามชาติที่กำลังทวีความรุนแรงและซับซ้อนมากขึ้น โดยเฉพาะในยุคที่เทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทสำคัญต่อการดำรงชีวิตของประชาชน โดยสภาพสังคมและเศรษฐกิจของไทยเป็นหนึ่งในปัจจัยสำคัญที่เกื้อหนุนให้ประชาชนจำนวนมากตกเป็นเหยื่อของแก๊งคอลเซ็นเตอร์ โดยเฉพาะกลุ่มประชากรสูงอายุ ผู้มีความรู้ด้านเทคโนโลยีต่ำ และประชาชนในพื้นที่ชนบท ซึ่งอาจเข้าถึงข้อมูลข่าวสารที่ถูกต้องได้น้อย ส่งผลให้ขาดทักษะในการระบุและระวังภัยอาชญากรรมออนไลน์ นอกจากนี้ ภายใต้สภาวะทางเศรษฐกิจที่เปราะบางและความเหลื่อมล้ำทางรายได้ ทำให้ประชาชนบางกลุ่มมีแนวโน้มจะหลงเชื่อข้อเสนอที่ให้ผลตอบแทนสูงหรือหลงเชื่อเจ้าหน้าที่ปลอมที่อ้างว่าจะช่วย

แก้ปัญหาทางกฎหมายให้ได้ อีกทั้งการเปลี่ยนผ่านเข้าสู่สังคมดิจิทัลของไทยในขณะที่ยังไม่มีการพัฒนาภูมิคุ้มกันดิจิทัลอย่างทั่วถึง ทั้งในระดับนโยบายและระดับบุคคล ยังเป็นช่องโหว่สำคัญที่ขบวนการอาชญากรสามารถใช้เป็นช่องทางโจมตี โดยเฉพาะจากการเก็บข้อมูลส่วนบุคคลจากช่องทางออนไลน์

รูปแบบและวิธีการหลอกลวง:

รูปแบบของการหลอกลวงโดยแก๊งคอลเซ็นเตอร์ในประเทศไทยมีความหลากหลายและพัฒนาขึ้นอย่างต่อเนื่อง ทั้งในแง่ของกลยุทธ์ เทคนิคการสร้างความน่าเชื่อถือ และเครื่องมือทางเทคโนโลยีที่ใช้สนับสนุนการกระทำความผิด ซึ่งสอดคล้องกับข้อมูลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA)[179] ที่ชี้ว่า ปี 2566 (ค.ศ.2023) ประเทศไทยยังคงเผชิญกับภัยไซเบอร์รูปแบบการหลอกลวงด้วย Social Engineering[180] ในอันดับต้น ๆ ของภัยคุกคาม แก๊งคอลเซ็นเตอร์ใน

---

[179] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA), รายงานภัยคุกคามทางไซเบอร์ประจำปี 2566 (2566) <https://www.etda.or.th> สืบค้นเมื่อ 14 ธันวาคม 2567.

[180] Social Engineering หมายถึง Social Engineering Attacks (วิศวกรรมสังคม) หมายถึง เทคนิคการโจมตีทางไซเบอร์ด้วยวิธีการเข้าถึงข้อมูลหรือบัญชีของเป้าหมายผ่านวิธีการทางจิตวิทยาด้วยการหลอกโน้มน้าวจิตใจให้เป้าหมายหลงเชื่อ เป็นเทคนิคการโจมตีทางไซเบอร์ที่นิยมใช้ในหมู่แฮ็กเกอร์ เรียกได้ว่าเป็นการโจมตีไปที่จิตใจมนุษย์หรือ “การแฮ็กมนุษย์” แต่ไม่ใช่การโจมตีทางเทคนิคไปที่ระบบโดยตรง บางครั้งเป็นการโจมตีทางกายภาพโดยใช้เทคนิคการหลอกให้เป้าหมายหลงเชื่อ โดยมีการหลอกลวงประเภทต่าง ๆ ดังนี้

1. Hybrid warfare เป็นสงครามที่ใช้การผสมผสานกันของเครื่องมือที่มาจากเทคโนโลยีแบบเดิมและเทคโนโลยีในรูปแบบใหม่จะใช้วิธีชักจูงจิตใจมนุษย์ เช่น การปล่อยข่าวปลอม การแทรกแซงการเลือกตั้งโดยอ้างประชาธิปไตยและมักใช้สื่อสังคมออนไลน์เป็นเครื่องมือ

2. Soft Power มาจาก แนวคิดที่พัฒนาโดยโจเซฟ เนย์ (Joseph Nye) แห่งมหาวิทยาลัยฮาร์วาร์ด ใช้ในการเปลี่ยนแปลงและสร้างอิทธิพลต่อความคิดของสังคมและประชาชนในประเทศต่าง ๆ โดยอาศัยทรัพยากรพื้นฐาน 3 ประการ ได้แก่ วัฒนธรรม (culture) ค่านิยมทางการเมือง (political values) และนโยบายต่างประเทศ (foreign policies) เป็นการขยายอิทธิพล การเปลี่ยนแปลงความคิด การทำให้ผู้คนมีส่วนร่วม หรือการเปลี่ยนแปลงพฤติกรรมของผู้อื่น โดยไม่ได้ใช้อำนาจบังคับแบบเดิม (Hard Power)

3. Disinfodemic การบิดเบือนข้อมูลโรคระบาด ข่าวสารทั้งแบบจงใจหรือไม่ได้เจตนา โดยหลักการแล้วข่าวสารช่วยสร้างความเข้มแข็งให้ผู้รับสารมีข้อมูล แต่การบิดเบือนข้อมูลในยุคโรคระบาดกลับทำให้เกิดความอ่อนแอลงได้เช่นกัน ส่งผลต่ออันตรายของชีวิตและความสับสนอลหม่านของผู้คนได้

4. Infodemic ใช้สื่อถึงการระบาดของข้อมูลข่าวสารที่ไม่ถูกต้อง คลาดเคลื่อน หรือบิดเบือนเกี่ยวกับโรคติดเชื้อไวรัสโคโรนา หรือ COVID-19 โดยเกิดจากการรวมคำสองคำเข้าด้วยกันคือ Information (ข่าวสาร) และ Epidemic (การระบาด) การระบาดของข้อมูลข่าวสาร หมายถึง สภาวะความท่วมท้นของข้อมูลที่แพร่กระจายรวดเร็วทั้งจริงบ้างเท็จบ้าง ส่งผลให้ประชาชนไม่สามารถหาแหล่งข้อมูลที่เชื่อถือและไว้ใจได้เมื่อถึงเวลาที่ต้องใช้ข้อมูล ดังนั้น การทำให้มีแหล่งข้อมูลที่เชื่อถือได้ในยุคโรคระบาดข้อมูลข่าวสารจะช่วยต่อสู้กับมายาคติข่าวลือ

ประเทศไทยมีการแบ่งโครงสร้างการปฏิบัติงานที่ชัดเจน โดยมักจะมี “หัวหน้าเครือข่าย” อยู่ต่างประเทศ *(กัมพูชา เมียนมา หรือฟิลิปปินส์)* ซึ่งเป็นสถานที่ตั้งศูนย์ปฏิบัติการ และมี “พนักงานปลายสาย” ซึ่งส่วนใหญ่มักเป็นคนไทยหรือชาวต่างชาติที่พูดภาษาไทยได้คล่องรับหน้าที่โทรศัพท์หาเหยื่อภายในประเทศ และมี “หน้าม้า” ที่เป็นผู้เปิดบัญชีม้า รับโอนเงิน รวมถึง “กลุ่มสนับสนุนด้านเทคโนโลยี” ที่คอยดูแลระบบ Voice over IP (VoIP)[181] หรือแอปพลิเคชันแอบอ้างหน่วยงานรัฐ[182]

**4.1.2 ประเทศฟิลลิปปินส์**

ฟิลิปปินส์เป็นหนึ่งในประเทศสมาชิกอาเซียนที่กำลังเผชิญกับปัญหาอาชญากรรมข้ามชาติในรูปแบบของแก๊งคอลเซ็นเตอร์อย่างเข้มข้น โดยเฉพาะเมื่อพิจารณาถึงบริบทของประเทศที่มีโครงสร้างเศรษฐกิจแบบบริการ (Service-Based Economy) และเป็นศูนย์กลางธุรกิจ BPO (Business Process Outsourcing) ระดับโลก[183] ฟิลิปปินส์มีบุคลากรที่มีความสามารถด้านภาษาอังกฤษและเทคโนโลยีจำนวนมากทำให้กลุ่มอาชญากรใช้จุดแข็งดังกล่าวเป็นเครื่องมือสนับสนุนการจัดตั้ง “ศูนย์หลอกลวง” หรือ call center ปลอมในประเทศ ซึ่งมีทั้งการหลอกลวงพลเมืองของตนเองและชาวต่างชาติ โดยเฉพาะชาวจีน เกาหลีใต้ และญี่ปุ่น ซึ่งในช่วงปีที่ผ่านมาทางการฟิลิปปินส์ได้ดำเนินการตรวจค้นและทลายฐานปฏิบัติการคอลเซ็นเตอร์ผิดกฎหมาย ซึ่งมักตั้งอยู่ในคอนโดมิเนียมหรืออาคารสำนักงานในเขตเศรษฐกิจพิเศษ พบว่ามีการใช้แรงงานต่างด้าวผิดกฎหมาย ซึ่งบางส่วนถูกหลอกลวงหรือล่อลวงให้เข้ามาทำงานภายใต้ระบบบังคับแรงงาน (forced labor) ซึ่งอาจจัดเข้าข่ายการค้ามนุษย์ (human trafficking) อีกด้วย[184]

---

ทั้งหลาย และยังป้องกันไม่ให้ข้อมูลเท็จแพร่กระจายต่อไปวงกว้าง: โปรดดู ACIS PROFESSIONAL, ‘Social engineering (cyber fraud) and attacks’ (ACIS Online, 14 ธันวาคม 2567) <https://www.acisonline.net/?p=10046> สืบค้นเมื่อ 14 ธันวาคม 2567.

[181] Voice over IP (VoIP) เป็นการสื่อสารทางเสียงผ่านโครงข่ายอินเทอร์เน็ต หรือโครงข่ายอื่น ๆ ที่ใช้อินเทอร์เน็ตโพรโทคอล สัญญาณเสียงจะถูกตัดแบ่งเป็นแพ็คเก็ตวิ่งผ่านไปบนโครงข่ายที่ใช้สำหรับการสื่อสารข้อมูลทั่วไป แทนการใช้วงจรเฉพาะตามวิธีการสื่อสารในระบบโทรศัพท์แบบดั้งเดิม เปรียบได้กับการให้รถยนต์วิ่งแทรกกันได้ตามช่องว่างที่มีอยู่ของถนน แทนการให้รถยนต์คันเดียวจองถนนวิ่งแบบผูกขาด ข้อดีของวอยซ์โอเวอร์ไอพีก็คือการสามารถใช้โครงข่ายได้อย่างมีประสิทธิภาพ ทำให้สามารถให้บริการได้ในอัตราค่าบริการที่ถูกลงมาก; โปรดดู: Wikipedia, ‘Voice over IP’ <https://th.wikipedia.org/wiki/วอยซ์โอเวอร์ไอพี> สืบค้นเมื่อ 14 ธันวาคม 2567.

[182] กองบัญชาการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี, สถิติและรูปแบบการหลอกลวงออนไลน์ในประเทศไทย (กรุงเทพฯ: สำนักงานตำรวจแห่งชาติ, 2566).

[183] กรุงเทพธุรกิจ, ‘ฟิลิปปินส์ ผู้นำธุรกิจ Outsourcing’ <https://www.bangkokbiznews.com/tech/552740> สืบค้นเมื่อ 14 ธันวาคม 2567.

[184] Philippine National Police (PNP), Cybercrime Reports and Enforcement Statistics (Manila: PNP Headquarters, 2023).

รูปแบบและวิธีการหลอกลวง:

แก๊งคอลเซ็นเตอร์ในฟิลิปปินส์มีพัฒนาการอย่างซับซ้อนและเป็นระบบ โดยมีลักษณะคล้ายกับองค์กรธุรกิจใต้ดินที่มีการแบ่งหน้าที่ภายในองค์กรจะมีหัวหน้าเครือข่ายซึ่งมักเป็นชาวต่างชาติส่วนมากเป็นชาวจีนหรือไต้หวัน ทำหน้าที่ควบคุมยุทธศาสตร์และเป้าหมายของการดำเนินงาน ต่อมาเป็นระดับผู้จัดการที่ควบคุมทีมหลอกลวง ซึ่งจะรับผิดชอบในภารกิจที่เฉพาะเจาะจงโดยรูปแบบที่พบบ่อยคือการจำลองหน่วยงานรัฐ โดยมิจฉาชีพจะปลอมแปลงหมายเลขโทรศัพท์ให้คล้ายกับหมายเลขทางการและโทรหาเหยื่อโดยอ้างตัวเป็นเจ้าหน้าที่หน่วยงานต่างๆ โดยการประยุกต์ใช้เทคโนโลยีสมัยใหม่ที่เรียกว่า Deep Fake[185] หรือ AI-generated voice ในการจำลองเสียงของเจ้าหน้าที่รัฐเพื่อหลอกลวงได้แนบเนียนยิ่งขึ้น แก๊งบางกลุ่มสามารถสลับการใช้โทรศัพท์ VoIP และโซเชียลมีเดียข้ามแพลตฟอร์มเพื่อหลีกเลี่ยงการตรวจสอบ อีกทั้งยังมีระบบการโอนเงินหลายชั้นผ่านบัญชีม้ารวมถึงคริปโทเคอร์เรนซีเพื่อป้องกันการติดตามเส้นทางทางการเงินของเหยื่อ[186] นอกจากนี้ อีกหนึ่งรูปแบบสำคัญที่พัฒนาในช่วงหลัง คือ Romance Scam[187] หรือการหลอกลวงผ่านความสัมพันธ์ทางออนไลน์ กลุ่มอาชญากรมักใช้รูปโปรไฟล์ปลอมในสื่อสังคมเพื่อสร้างความไว้ใจ จากนั้นค่อย ๆ พาเหยื่อเข้าสู่สถานการณ์หลอกลวงทางการเงิน ตัวอย่างเช่น การขอให้ส่งเงินช่วยค่ารักษา พัสดุติดด่าน หรือการลงทุนร่วมกัน โดยมีรายงานว่ามีเหยื่อชาวต่างชาติและฟิลิปปินส์จำนวนมากที่สูญเสียเงินหลายแสนถึงล้านเปโซ[188]

---

[185] Deepfake หมายถึง เทคโนโลยีที่ใช้ปัญญาประดิษฐ์ (AI) โดยเฉพาะ deep learning ซึ่งเป็นแขนงหนึ่งของ machine learning ในการสร้างหรือปรับเปลี่ยนภาพ วิดีโอ หรือเสียงให้ดูเหมือนจริง โดยมักจะใช้เพื่อปลอมแปลงตัวตนของบุคคล: โปรดดู: Thai PBS, ‘DeepFake คลิปปลอมใบหน้าคนดัง เนียนยิ่งกว่า ‘Fake news’’ International Laboratories Corp., Ltd., 10 ตุลาคม 2565 <https://www.ilc-cosmetic.com/th/deepfake/> สืบค้นเมื่อ 5 ธันวาคม 2567.

[186] Bureau of Immigration, ‘Scam Hubs Abroad with ‘POGO-like’ Operations Continue to Recruit Filipino Victims —BI’ (2024) <https://immigration.gov.ph/scam-hubs-abroad-with-pogo-like-operations-continue-to-recruit-filipino-victims-bi/> accessed 5 December 2024.

[187] Romance Scam หมายถึง การหลอกลวงทางความรัก ผู้กระทำความผิดจะใช้ตัวตนปลอมบนอินเทอร์เน็ตเพื่อเรียกร้องความรักและความไว้วางใจจากเหยื่อ จากนั้นผู้หลอกลวงจะใช้ภาพลวงตาของความสัมพันธ์โรแมนติกหรือความสัมพันธ์ที่ใกล้ชิดเพื่อหลอกลวงและ/หรือขโมยของจากเหยื่อ: โปรดดู: Federal Bureau of Investigation (FBI), Romance Scams, n.d., <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/romance-scams> accessed 5 July 2025.

[188] BBC News. (2024, April 4). *Hundreds rescued from love scam centre in the Philippines*. Retrieved from https://www.bbc.com/news/world-asia-68562643.

**4.1.3 ประเทศมาเลเซีย**

ปัญหาการหลอกลวงจากแก๊งคอลเซ็นเตอร์ยังคงสร้างความเสียหายอย่างรุนแรงทั้งในด้านการเงินและจิตใจแก่ประชาชนมาเลเซียอย่างต่อเนื่อง จากรายงาน *State of Scam Report 2024* ระบุว่า มูลค่าความเสียหายจากการหลอกลวงในปีที่ผ่านมาอยู่ที่ 54.02 พันล้านริงกิต (ประมาณ 12.8 พันล้านดอลลาร์สหรัฐ) คิดเป็นสัดส่วนประมาณ 3% ของผลิตภัณฑ์มวลรวมในประเทศ (GDP) อย่างไรก็ตาม มีเหยื่อเพียงร้อยละ 30 เท่านั้นที่ดำเนินการแจ้งความหรือรายงานเหตุการณ์ที่เกิดขึ้น สะท้อนถึงความไม่เชื่อมั่นในกระบวนการจัดการของภาครัฐและหน่วยงานที่เกี่ยวข้อง[189] ในด้านความเสียหายต่อรายบุคคล พบว่าความสูญเสียเฉลี่ยต่อรายอยู่ที่ประมาณ 2,726 ดอลลาร์สหรัฐ โดยมีเหยื่อเพียงร้อยละ 2 เท่านั้นที่สามารถกู้คืนเงินที่สูญเสียไปได้[190] และในข้อมูลจาก *Whos call Annual Report 2024* ยังระบุด้วยว่า จำนวนสายโทรศัพท์ที่เป็นการหลอกลวงในประเทศมาเลเซียเพิ่มขึ้นอย่างรวดเร็วในปีที่ผ่านมา โดยมีมูลค่าความเสียหายสูงถึง 2.98 ล้านดอลลาร์สหรัฐ เพิ่มขึ้นจากปี ค.ศ.2023 ถึงร้อยละ 82.81 ซึ่งในปีนั้นมีมูลค่าอยู่ที่ 1.63 ล้านดอลลาร์สหรัฐ[191] รวมทั้งทางสำนักงานตำรวจแห่งชาติมาเลเซีย พบว่า จำนวนคดีออนไลน์ที่ได้รับการรายงานในปีค.ศ.2023 เพิ่มขึ้นถึงร้อยละ 35.5 โดยมีจำนวนคดีทั้งหมด 34,532 คดี เพิ่มขึ้นจาก 25,479 คดีในปีก่อนหน้า[192] อีกทั้งประเทศมาเลเซียได้ถูกระบุว่าเป็นหนึ่งในจุดศูนย์กลางสำคัญของเครือข่ายอาชญากรรมทางไซเบอร์ โดยเฉพาะเครือข่ายแก๊งคอลเซ็นเตอร์ข้ามชาติที่กระจายตัวอยู่ในภูมิภาคเอเชียตะวันออกเฉียงใต้ แม้มาเลเซียจะไม่ใช่ประเทศต้นทางหรือแหล่งปฏิบัติการถาวรแต่กลับมีบทบาทในฐานะศูนย์กลางการเคลื่อนย้ายแรงงานผิดกฎหมาย อุปกรณ์เทคโนโลยี และทรัพยากรต่าง ๆ ที่สนับสนุนการหลอกลวงเหล่านี้ โดยพบว่า แก๊งคอลเซ็นเตอร์หลายกลุ่มเลือกใช้คอนโดมิเนียมหรูใจกลางกรุงกัวลาลัมเปอร์เป็นที่ตั้งของสำนักงานหลอกลวง โดยอาศัยฉากหน้าว่าเป็นบริษัททางด้านเทคโนโลยีหรือบริการลูกค้าทั่วไป เพื่อหลีกเลี่ยงความสงสัยจากเจ้าหน้าที่รัฐและประชาชนโดยรอบ ในขณะเดียวกัน เมืองโจโฮร์บาห์รู ซึ่งตั้งอยู่ใกล้พรมแดนประเทศสิงคโปร์ ก็กลายเป็นอีกหนึ่งจุดยุทธศาสตร์ที่แก๊งคอลเซ็นเตอร์ใช้

---

[189] Zainul, E., 'Malaysians lost US$12.8b to scams over the past year, survey reveals' (The Edge Malaysia, 3 October 2024).

[190] Shahrizal, 'Malaysia Loses RM54.02 Billion To Scams, Report Reveals Alarming Rise' (Business Today, 4 October 2024) <https://www.businesstoday.com.my/...> accessed 5 December 2024.

[191] Fam, C., 'Report: Scam Calls in Malaysia Skyrocketed by 82.81% in 2024' (The Star, 3 March 2025) https://www.thestar.com.my/tech/tech-news/2025/03/03/report-scam-calls-in-malaysia-skyrocketed-by-8281-in-2024 accessed 5 December 2025.

[192] Beh, M. T., Combating Scam Syndicates in Malaysia and Southeast Asia (Penang Institute, 2025) <https://penanginstitute.org/publications/issues/combating-scam-syndicates-in-malaysia-and-southeast-asia/> accessed 5 July 2025.

เป็นฐานปฏิบัติการ โดยมุ่งเป้าไปที่พลเมืองของประเทศสิงคโปร์ซึ่งมีอำนาจซื้อสูงและสามารถตกเป็นเหยื่อของการหลอกลวงในรูปแบบต่าง ๆ ได้ง่าย ตำรวจมาเลเซียได้ทำการบุกจับเครือข่ายแก๊งหลอกลวงในพื้นที่ดังกล่าวหลายครั้ง ซึ่งผู้ปฏิบัติงานส่วนใหญ่ไม่ใช่คนมาเลเซีย แต่เป็นชาวต่างชาติที่ลักลอบเข้ามาทำงานผิดกฎหมาย พื้นที่เหล่านี้ถูกออกแบบให้มีระบบสื่อสารครบวงจรซึ่งสามารถรองรับการโทรศัพท์ข้ามประเทศและการโต้ตอบกับเหยื่อจำนวนมากในเวลาเดียวกัน[193]

รูปแบบและวิธีการหลอกลวง:

การดำเนินการของแก๊งเหล่านี้มีลักษณะคล้ายคลึงกับเครือข่ายอาชญากรรมข้ามชาติ โดยมีโครงสร้างการจัดการภายในที่ชัดเจน ทั้งผู้ควบคุมเครือข่าย ผู้ฝึกสอน ผู้โทร (scammers) และฝ่ายเทคนิคที่ดูแลระบบการสื่อสาร ทำให้แก๊งสามารถดำเนินกิจกรรมได้อย่างเป็นระบบและมีประสิทธิภาพ แม้จะมีการจับกุมหรือปิดสำนักงานในบางพื้นที่ แต่ก็พบว่ากลุ่มเหล่านี้สามารถเคลื่อนย้ายฐานปฏิบัติการไปยังที่ใหม่ได้อย่างรวดเร็ว

**4.1.4 ประเทศกัมพูชา**

ประเทศกัมพูชาได้ปรากฏอยู่ในจุดศูนย์กลางของความกังวลในระดับภูมิภาคและระหว่างประเทศ เนื่องจากการกลายเป็นฐานปฏิบัติการสำคัญของเครือข่ายแก๊งคอลเซ็นเตอร์ที่ดำเนินการอย่างเป็นระบบ ซับซ้อน และกว้างขวาง โดยมีเป้าหมายการหลอกลวงผู้คนจากหลากหลายประเทศทั่วเอเชียตะวันออกเฉียงใต้ และแม้กระทั่งในภูมิภาคอื่นของโลก ปัจจัยที่เอื้อให้กัมพูชากลายเป็นศูนย์กลางของอาชญากรรมคอลเซ็นเตอร์นี้มีรากฐานมาจากหลากหลายมิติ ไม่ว่าจะเป็นการเติบโตอย่างรวดเร็วของเขตเศรษฐกิจพิเศษ ได้แก่ สีหนุวิลล์ บาเว็ต ปอยเปต และเมืองชายแดนอื่น ๆ ที่เปิดรับการลงทุนจากกลุ่มทุนต่างชาติ โดยเฉพาะกลุ่มทุนจากจีนซึ่งมีความสัมพันธ์คลุมเครือกับองค์กรอาชญากรรมข้ามชาติ ในพื้นที่เหล่านี้พบว่ามีการจัดตั้งอาคารสำนักงาน อาคารเชิงพาณิชย์ และคาสิโน ซึ่งต่อมาถูกใช้เป็นฐานปฏิบัติการของศูนย์หลอกลวงแบบคอลเซ็นเตอร์อย่างกว้างขวางทำให้กัมพูชากลายเป็นแหล่งกักขังแรงงานบังคับในรูปแบบใหม่ โดยเฉพาะจากประเทศเพื่อนบ้าน เช่น ไทย เวียดนาม อินโดนีเซีย และฟิลิปปินส์[194] จากข้อมูลของสำนักงานตำรวจตรวจคนเข้าเมืองกัมพูชาเปิดเผยเมื่อวันที่ 19 สิงหาคม พ.ศ.2561 (ค.ศ.2018) ว่าเจ้าหน้าที่ได้บุกเข้าจับกุมแก๊งคอลเซ็นเตอร์รายใหญ่จากจีนได้ผู้ต้องหารวม 225 คน พร้อมยึดของกลางเป็นโต๊ะทำงาน เครื่องคอมพิวเตอร์

---

[193] The Star, 'Rich Facade of Scam Call Centres: How Syndicates Exploit High-End Properties in KL' <https://www.thestar.com.my/news/nation/2024/08/21/rich-facade-of-scam-call-centres> accessed 15 December 2024.

[194] 'Trafficked for Scams: Abuse in Southeast Asian Scam Center' (Human Rights Watch) <https://bangkok.ohchr.org/news/2022/online-scam-operations-and-trafficking-forced-criminality-southeast-asia> accessed 15 December 2024.

โน้ตบุ๊กเป็นจำนวนมาก หลังได้รับเบาะแส ระบุว่าคนทั้งหมดซึ่งอาศัยวีซ่าท่องเที่ยวเดินทางเข้าประเทศมาและลงทุนเช่าอาคารอพาร์ตเมนต์ 11 ชั้น ทั้งหลังในย่านตูลกุก ย่านที่พักอาศัยหรูหราในกรุงพนมเปญ ตั้งเป็นศูนย์กลางเพื่อโทรศัพท์หลอกลวงเหยื่อที่ ส่วนใหญ่เป็นข้าราชการและทหารเกษียณอายุในจีน โดยนายอุก ไหเสลา หัวหน้าแผนกสืบสวนสอบสวนของ สำนักงานระบุว่า จากการสอบปากคำผู้ต้องหารายหนึ่งยอมรับว่าทำรายได้จากการโกงได้สูงถึงสัปดาห์ละ 70,000 ดอลลาร์หรือราว 2.34 ล้านบาท โดยชาวบ้านใกล้เคียงเปิดเผยว่าคนในอพาร์ตเมนต์เก็บตัวเงียบ ทำตัวลึกลับจะออกมาซื้อหาอาหารเฉพาะในตอนกลางคืน ตอนแรกเข้าใจว่าคนเหล่านี้เข้ามาเช่าตึกเพื่อตั้งสำนักงานเพราะค่าเช่าสูงถึงเดือนละ 25,000 ดอลลาร์ *(ราว 830,000 บาท)* อันแสดงให้เห็นถึงพฤติกรรมการกระทำผิดของแก๊งคอลเซ็นเตอร์ที่ได้ใช้ประเทศกัมพูชาเป็นฐานสำคัญในการกระทำผิดมาอย่างต่อเนื่อง[195]

รูปแบบและวิธีการหลอกลวง:

กิจกรรมของศูนย์คอลเซ็นเตอร์ในกัมพูชาไม่ได้มีเพียงมิติทางเทคนิค แต่ยังมีโครงสร้างที่ซับซ้อนในลักษณะของบริษัทเถื่อน ซึ่งมีระบบแบ่งงานกันอย่างเป็นลำดับชั้น องค์กรเหล่านี้มีการปรับกลยุทธ์ให้สอดคล้องกับบริบททางสังคม เศรษฐกิจ และจิตวิทยาของเหยื่อ ตัวอย่างเช่น “Pig Butchering Scam” หรือ “กลโกงแบบป้อนหมู” ซึ่งเป็นการสร้างความสัมพันธ์กับเหยื่อทางออนไลน์ในลักษณะที่เหมือนจริง โดยมักใช้ตัวตนปลอม (fake persona) เพื่อสร้างความผูกพันทางอารมณ์ จากนั้นจึงโน้มน้าวให้เหยื่อลงทุนในสินทรัพย์ดิจิทัลหรือแพลตฟอร์มทางการเงินปลอม ซึ่งมักมีการจำลองหน้าเว็บไซต์หรือแอปพลิเคชันให้ดูน่าเชื่อถือ ในบางกรณีเหยื่อยังสามารถถอนเงินได้ในระยะแรกเพื่อสร้างความไว้วางใจก่อนที่การฉ้อโกงจะเกิดขึ้นอย่างเต็มรูปแบบ

**4.1.5 ประเทศสิงคโปร์**

ในปี ค.ศ.2024 ประเทศสิงคโปร์เผชิญกับปัญหาแก๊งคอลเซ็นเตอร์และการหลอกลวงทางออนไลน์ที่เพิ่มขึ้นอย่างมีนัยสำคัญ โดยมีจำนวนคดีที่รายงานทั้งหมด 55,810 คดี เพิ่มขึ้น 10.8% จากปี 2023 ซึ่งในจำนวนนี้ 92.3% เป็นคดีหลอกลวงผ่านแก๊งคอลเซ็นเตอร์[196] และพบว่าเป็นคดีหลอกลวงที่เกี่ยวข้องกับการปลอมแปลงเป็นเจ้าหน้าที่รัฐ (Government Officials Impersonation

---

[195] ‘Annual Report on Cybercrime’ (Cambodian National Police) <https://cnp.gov.kh> accessed 15 December 2024.

[196] Scam Shield, ‘2024 Annual Scams and Cybercrime Brief’ (Singapore: National Crime Prevention Council, 2024) <https://www.scamshield.gov.sg/files/Scams%20and%20Cybercrime%20Briefs/2024_annual_scams_and_cybercrime_brief.pdf> accessed 15 December 2024.

Scams) จำนวนกว่า 1,504 คดี คิดเป็นมูลค่าความเสียหายสูงถึง 151.3 ล้านดอลลาร์สิงคโปร์[197] ซึ่งสูงกว่าการหลอกลวงประเภทอื่น โดยเหยื่อจำนวนมากเชื่อว่าตนกำลังถูกดำเนินคดี หรือมีความผิดทางกฎหมาย จึงตกอยู่ภายใต้แรงกดดันและตัดสินใจโอนเงินให้กับผู้แอบอ้างเพื่อหลีกเลี่ยงความยุ่งยากทางกฎหมาย

รูปแบบและวิธีการหลอกลวง:

เทคนิคที่ใช้ในการโทรหลอกลวงมีการพัฒนาอย่างต่อเนื่อง ไม่เพียงแต่การปลอมหมายเลขโทรศัพท์ (Caller ID Spoofing) แต่ยังรวมถึงการใช้เสียงอัตโนมัติที่ทำให้เหยื่อเข้าใจว่าเป็นระบบของทางการ รวมถึงการให้กดหมายเลขหรือป้อนข้อมูลส่วนตัวผ่านระบบ Interactive Voice Response (IVR) ซึ่งทำให้เป้าหมายตกอยู่ในภาวะที่ยากต่อการคิดวิเคราะห์และตัดสินใจอย่างรอบคอบ โดยเฉพาะเมื่อผู้หลอกลวงอ้างว่าจะดำเนินการจับกุมหากไม่มีการปฏิบัติตาม นอกจากการแอบอ้างเจ้าหน้าที่รัฐแล้ว ยังมีรูปแบบการหลอกลวงอื่นที่แพร่หลายภายในสิงคโปร์ ได้แก่ การหลอกให้ลงทุนผ่านแอปพลิเคชันหรือเว็บไซต์ปลอม (investment scam) ซึ่งอาจเริ่มจากการพูดคุยผ่านโซเชียลมีเดีย เช่น Telegram หรือ Facebook แล้วชักชวนให้ดาวน์โหลดแอปลงทุนปลอมที่มีอินเตอร์เฟซดูน่าเชื่อถือ โดยกลุ่มมิจฉาชีพเหล่านี้จะอ้างผลตอบแทนสูงในช่วงแรกเพื่อให้เหยื่อลงเงินเพิ่มก่อนจะปิดบัญชีและหายตัวไป

**4.1.6 ประเทศบรูไนดารุสซาราม**

ปัญหาแก๊งคอลเซ็นเตอร์ในประเทศบรูไนไม่ได้มีความแพร่หลายหรือรุนแรงเท่ากับบางประเทศในภูมิภาคอาเซียน แต่บรูไนก็ไม่สามารถหลีกเลี่ยงภัยคุกคามนี้ได้อย่างสมบูรณ์ เนื่องจากบรูไนเป็นประเทศที่มีระบบเศรษฐกิจมั่นคงและมีประชากรที่มีฐานะทางการเงินที่ค่อนข้างดี ทำให้ประเทศนี้เป็นเป้าหมายที่ดึงดูดความสนใจของแก๊งคอลเซ็นเตอร์ แม้ว่าแก๊งคอลเซ็นเตอร์อาจไม่ได้ตั้งฐานปฏิบัติการในบรูไนแต่ก็ยังคงสามารถหลอกลวงประชาชนในประเทศนี้ได้ผ่านทางโทรศัพท์หรืออินเทอร์เน็ตและแนวโน้มการหลอกลวงทางโทรศัพท์และออนไลน์เพิ่มขึ้นอย่างต่อเนื่อง ส่งผลให้รัฐบาลและหน่วยงานด้านความมั่นคงไซเบอร์ของประเทศเริ่มแสดงความตื่นตัวและดำเนินมาตรการเชิงรุกเพื่อควบคุมปัญหานี้ จากรายงานของ Cyber Security Brunei (CSB) ในปี 2024 มีการบล็อกเว็บไซต์ปลอมมากกว่า 80 แห่ง และหมายเลขโทรศัพท์ต้องสงสัยมากกว่า 500 หมายเลขที่เกี่ยวข้องกับกิจกรรมฉ้อโกงทางโทรศัพท์และออนไลน์[198] การดำเนินการดังกล่าวเป็นส่วนหนึ่งของความ

---

[197] 'Annual Scams and Cybercrime Brief 2024' (Singapore Police Force) <https://www.police.gov.sg> accessed 15 December 2024.

[198] Cyber Security Brunei, 'Brunei Blocks Over 80 Fake Websites and 500 Suspicious Phone Numbers' The Cyber Express <https://thecyberexpress.com/brunei-strengthens-cybersecurity/amp> accessed 15 December 2024.

พยายามในการจัดการกับการหลอกลวงที่ซับซ้อนขึ้นเรื่อย ๆ และข้อมูลจากธนาคารอิสลามแห่งบรูไน *(Bank Islam Brunei Darussalam - BIBD)* ยังระบุว่า พบกรณีที่มีผู้ไม่หวังดีปลอมตัวเป็นเจ้าหน้าที่ธนาคารโทรศัพท์ไปยังลูกค้าเพื่อขอข้อมูลส่วนบุคคล ซึ่งเป็นช่องทางในการเข้าถึงบัญชีธนาคารของเหยื่อส่งผลให้ธนาคารต้องออกแถลงการณ์เตือนประชาชนให้ระมัดระวังอย่างต่อเนื่อง[199] ทั้งนี้ ยังพบว่าความเสียหายจากการหลอกลวงทางออนไลน์ในบรูไนเพิ่มสูงขึ้นจาก 2.4 ล้านดอลลาร์บรูไนในปี 2023 เป็นกว่า 5 ล้านดอลลาร์บรูไนในปี 2024 ตามรายงานของกองกำลังตำรวจแห่งบรูไน *(Royal Brunei Police Force)*[200]

รูปแบบและวิธีการหลอกลวง:

รูปแบบการหลอกลวงที่ปรากฏในประเทศมีลักษณะคล้ายคลึงกับที่เกิดขึ้นในประเทศอาเซียนอื่น ๆ โดยเฉพาะในรูปแบบการปลอมแปลงตัวตน ซึ่งมักอ้างว่าเป็นเจ้าหน้าที่ของธนาคาร หน่วยงานรัฐ หรือบริษัทเอกชน เพื่อข่มขู่หรือหลอกให้เหยื่อให้ข้อมูลส่วนตัว อีกหนึ่งรูปแบบที่พบคือการส่งลิงก์ปลอมผ่านข้อความหรืออีเมล โดยลิงก์ดังกล่าวมักพาเหยื่อไปยังหน้าเว็บไซต์เลียนแบบของธนาคารหรือบริการสาธารณะ เมื่อผู้ใช้ป้อนข้อมูล คนร้ายจะสามารถนำข้อมูลไปใช้ในการเข้าถึงบัญชีหรือโอนเงินออกจากบัญชีได้ทันที รูปแบบนี้ถือว่าเป็นส่วนหนึ่งของ phishing หรือ social engineering ที่พัฒนาให้แนบเนียนมากขึ้นในปัจจุบัน

**4.1.7 ประเทศอินโดนีเซีย**

ประเทศอินโดนีเซียได้เผชิญกับปัญหาการหลอกลวงผ่านคอลเซ็นเตอร์ที่เพิ่มขึ้นอย่างต่อเนื่อง โดยเฉพาะการหลอกลวงผ่านระบบการชำระเงินแบบเรียลไทม์ ซึ่งมีผู้บริโภคชาวอินโดนีเซียถึง 23% รายงานว่าตกเป็นเหยื่อของการหลอกลวงดังกล่าวในปี 2024 เพิ่มขึ้นจาก 19% ในปี 2023 นอกจากนี้ยังพบว่าการสูญเสียทางการเงินที่มีมูลค่าสูงกว่า 70 ล้านรูเปียห์ (ประมาณ 4,300 ดอลลาร์สหรัฐ) เพิ่มขึ้นจาก 1% ในปี 2023 เป็น 8% ในปี 2024[201] ยังมีรายงานว่าชาวอินโดนีเซียจำนวนมากถูกล่อลวงให้ทำงานในศูนย์หลอกลวง (scam centers) ในประเทศเพื่อนบ้าน เช่น เมียนมา โดยถูกหลอกให้เชื่อว่าจะได้รับงานที่มีรายได้ดี แต่กลับถูกบังคับให้ทำงานในสภาพแวดล้อมที่ไม่เหมาะสม ในเดือน

---

[199] Bank Islam Brunei Darussalam, 'Public Advisory on Scam Calls' (Xinhua News Agency) <https://english.news.cn/20241219/3e4b4af6da724a63a497cdbeebb474ad/c.html> accessed 4 January 2025.

[200] 'Annual Crime Report 2024' (Royal Brunei Police Force) <https://bn.usembassy.gov/2024-trafficking-in-persons-report-brunei/> accessed 4 January 2025.

[201] Stock Titan, 'FICO Survey: 1 in 4 Indonesian Consumers Report Losing Money to Scams' (23 April 2024) <https://www.stocktitan.net/news/FICO/fico-survey-1-in-4-indonesian-consumers-report-losing-money-to-scams-fnj6ol7wggfn.html> accessed 4 January 2025.

กุมภาพันธ์ 2025 มีชาวอินโดนีเซียจำนวน 84 คนที่ถูกช่วยเหลือและส่งกลับประเทศ หลังจากถูกกักขังในศูนย์หลอกลวงในเมืองเมียวดี ประเทศเมียนมา โดยกระทรวงการต่างประเทศอินโดนีเซียระบุว่ามีชาวอินโดนีเซียประมาณ 6,800 คนที่ตกเป็นเหยื่อของการหลอกลวงงานในต่างประเทศในช่วงไม่กี่ปีที่ผ่านมา[202]

รูปแบบและวิธีการหลอกลวง:

ในอินโดนีเซียแก๊งคอลเซ็นเตอร์มีแนวโน้มประยุกต์ใช้รูปแบบการหลอกลวงที่หลากหลาย โดยเฉพาะอย่างยิ่งการหลอกลวงผ่านหมายเลขปลอม ซึ่งมักแสดงเป็นหมายเลขของหน่วยงานรัฐ อีกหนึ่งกลยุทธ์ที่พบมากขึ้น คือ การใช้แอปพลิเคชันปลอมที่ถูกออกแบบให้คล้ายกับแอปธนาคารหรือบริการทางการเงิน โดยแก๊งจะล่อลวงให้เหยื่อดาวน์โหลดแอปผ่านลิงก์ที่ส่งมาทาง SMS หรือโซเชียลมีเดีย

**4.1.8 ประเทศเวียดนาม**

ในปี 2024 ประเทศเวียดนามยังคงเผชิญกับสถานการณ์อาชญากรรมไซเบอร์ในรูปแบบของการหลอกลวงทางออนไลน์ (online fraud) อย่างรุนแรง โดยเฉพาะในกลุ่มผู้ใช้งานสมาร์ตโฟน ซึ่งเป็นกลุ่มเป้าหมายหลักของขบวนการหลอกลวงดังกล่าว สมาคมความมั่นคงทางไซเบอร์แห่งชาติของเวียดนาม (National Cyber Security Association) ได้เปิดเผยรายงานการสำรวจประจำปี พ.ศ. 2567 (ค.ศ.2024) (Cybersecurity Survey Report 2024) ซึ่งระบุว่าความเสียหายทางการเงินที่เกิดจากการหลอกลวงในปีนี้มีมูลค่ารวมสูงถึง 18.9 ล้านล้านด่ง หรือประมาณ 744.3 ล้านดอลลาร์สหรัฐ รายงานฉบับดังกล่าวจัดทำขึ้นโดยอิงจากข้อมูลของผู้เข้าร่วมตอบแบบสอบถามออนไลน์จำนวน 59,000 คน ผลการสำรวจพบว่า ประชาชนชาวเวียดนามจำนวนมากตกเป็นเหยื่อของการหลอกลวง โดยเฉลี่ยแล้วมีผู้ใช้งานสมาร์ตโฟน 1 รายจากทุก ๆ 220 ราย ที่ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ในปี 2024 แม้ว่าร้อยละ 88.98 ของผู้ตอบแบบสอบถามระบุว่าได้แจ้งครอบครัวหรือเพื่อนสนิททันทีหลังจากถูกหลอกลวง แต่มีเพียงร้อยละ 45.69 เท่านั้นที่รายงานเรื่องดังกล่าวต่อหน่วยงานที่เกี่ยวข้อง[203]ปรากฏการณ์นี้แสดงให้เห็นถึงปัญหาในการเข้าถึงกระบวนการยุติธรรมและการขาดความมั่นใจของประชาชนในระบบการจัดการอาชญากรรมไซเบอร์ ซึ่งส่งผลให้การดำเนินการติดตามผู้กระทำผิดและการชดใช้ความเสียหายเป็นไปอย่างล่าช้าและไม่มีประสิทธิภาพ

รูปแบบและวิธีการหลอกลวง:

---

[202] 'Indonesia Rescues Citizens from Scam Centers in Myanmar' (AP News, 21 February 2025) <https://apnews.com/article/57d644b606335eecbd5d3a27a1053e3b> accessed 24 March 2025.

[203] 'Vietnamese Lose $744mn to Online Scams in 2024: Report' (Tuoi Tre News, 17 December 2024) <https://tuoitrenews.vn/news/society/20241217/vietnamese-lose-744mn-to-online-scams-in-2024-report/83436.html> accessed 24 March 2025.

จากข้อมูลของสมาคมฯ รูปแบบการหลอกลวงที่พบมากที่สุดในปี 2024 ได้แก่ การเชิญชวนให้ร่วมลงทุนในโครงการปลอม ร้อยละ 70.72 ของผู้ตอบแบบสอบถามระบุว่าเคยได้รับคำเชิญให้ลงทุนในแพลตฟอร์มการเงินที่ไม่รู้จัก โดยโฆษณาผลตอบแทนที่สูงและปราศจากความเสี่ยง[2] รูปแบบรองลงมา คือ การหลอกลวงโดยแอบอ้างเป็นเจ้าหน้าที่ของรัฐ หน่วยงานภาษี หรือธนาคาร เพื่อเรียกร้องให้เหยื่อโอนเงิน ซึ่งพบในอัตราร้อยละ 62.08 ขณะที่อีกร้อยละ 60.01 ของผู้ตอบแบบสอบถามระบุว่าเคยได้รับข้อความแจ้งว่าตนถูกรางวัลหรือโปรโมชั่นจากบริษัทที่ไม่รู้จัก นอกจากนี้ ขบวนการหลอกลวงในเวียดนามยังได้นำเทคโนโลยีขั้นสูงมาใช้ในการเพิ่มความน่าเชื่อถือของการหลอกลวง โดยเฉพาะการใช้ปัญญาประดิษฐ์ (AI) เพื่อสร้างวิดีโอ Deepfake และการเลียนเสียง เพื่อหลอกลวงในลักษณะที่สมจริงยิ่งขึ้นส่งผลให้เหยื่อยากต่อการแยกแยะเนื้อหาจริงและปลอม ทั้งยังพบการใช้แชตบอตเพื่อสร้างการสื่อสารอย่างต่อเนื่อง และโปรแกรมโทรศัพท์อัตโนมัติที่สามารถติดต่อเหยื่อจำนวนมากในเวลาเดียวกัน[204]

**4.1.9 สาธารณรัฐประชาชนลาว**

ประเทศลาวเผชิญกับปัญหาแก๊งคอลเซ็นเตอร์ที่ทวีความรุนแรงขึ้นอย่างต่อเนื่อง โดยเฉพาะในเขตเศรษฐกิจพิเศษสามเหลี่ยมทองคำ (*Golden Triangle Special Economic Zone - SEZ)* จังหวัดบ่อแก้ว ซึ่งกลายเป็นศูนย์กลางของกิจกรรมผิดกฎหมายที่เกี่ยวข้องกับการหลอกลวงออนไลน์ การค้ามนุษย์ และการบังคับใช้แรงงาน โดยในช่วงครึ่งแรกของปี 2024 ทางการลาวตรวจพบศูนย์ปฏิบัติการคอลเซ็นเตอร์จำนวน 400 แห่งในเขต SEZ ซึ่งเพิ่มขึ้นจาก 305 แห่งในปีก่อนหน้า อุตสาหกรรมหลอกลวงทางไซเบอร์ในลาวมีมูลค่าเกือบ 40 เปอร์เซ็นต์ของเศรษฐกิจลาว[205] ในเดือนสิงหาคม 2024 ทางการลาวได้ดำเนินการปราบปรามศูนย์หลอกลวงในเขต SEZ โดยสามารถจับกุมผู้ต้องสงสัยทั้งสิ้น 1,389 คน การดำเนินการนี้เป็นส่วนหนึ่งของความพยายามในการปราบปรามอาชญากรรมทางไซเบอร์และการหลอกลวงทางการเงินในภูมิภาค[206] แต่ทว่าในปีที่ผ่านมารัฐบาลลาวได้ดำเนินการปราบปรามขบวนการหลอกลวงผ่านคอลเซ็นเตอร์ในเขตเศรษฐกิจพิเศษสามเหลี่ยมทองคำอย่างจริงจัง ตามรายงานของ Laotian Times ระบุว่า เจ้าหน้าที่ลาวสามารถยึดอุปกรณ์ที่ใช้ในการหลอกลวงได้มากมาย รวมถึงคอมพิวเตอร์และโทรศัพท์มือถือหลายพัน

---

[204] Ibid.

[205] Prachatai, 'เขตเศรษฐกิจพิเศษสามเหลี่ยมทองคำ: อุตสาหกรรมหลอกลวงในลาว' (ธันวาคม 2567) <https://prachatai.com/journal/2024/12/111689> สืบค้นเมื่อ 4 มกราคม 2568.

[206] 'ลาวเร่งปราบปรามขบวนการแก๊งคอลเซ็นเตอร์ ยึดทรัพย์สินและควบคุมตัวชาวต่างชาติหลายพันคน' (Intsharing, 14 สิงหาคม 2567) <https://intsharing.co/2024/08/14/ลาวเร่งปราบปรามขบวนการ/> สืบค้นเมื่อ 4 มกราคม 2568.

เครื่อง[207] อีกทั้ง รัฐบาลลาวได้สั่งปิดศูนย์หลอกลวงทั้งหมดในพื้นที่ดังกล่าวภายในวันที่ 25 สิงหาคม 2024 และได้ดำเนินการร่วมกับทางการจีนในการจับกุมและส่งตัวผู้กระทำผิดกลับประเทศ[208]

รูปแบบและวิธีการหลอกลวง:

รูปแบบการหลอกลวงที่ใช้ในลาวมีลักษณะคล้ายกับประเทศสมาชิกอาเซียนโดยการหลอกว่าเป็นเจ้าหน้าที่จากธนาคารหรือเจ้าหน้าที่รัฐ โดยจะโทรศัพท์หรือส่งข้อความผ่านแอปพลิเคชันเพื่อลวงเหยื่อให้เปิดเผยข้อมูลส่วนตัว เลขบัตรเครดิต หรือรหัสผ่าน รวมถึงการหลอกให้โอนเงินเพื่อหลีกเลี่ยงคดีความหรือภาษีย้อนหลัง นอกจากนี้ยังพบการใช้เทคนิคทางเทคโนโลยีเพื่อให้การหลอกลวงดูน่าเชื่อถือมากยิ่งขึ้น

**4.1.10 ประเทศเมียนมา**

ประเทศเมียนมาได้กลายเป็นหนึ่งในศูนย์กลางที่สำคัญของกิจกรรมอาชญากรรมทางไซเบอร์ โดยเฉพาะในรูปแบบของแก๊งคอลเซ็นเตอร์ ซึ่งมีการดำเนินงานในลักษณะที่เป็นระบบ มีการจัดโครงสร้างภายในคล้ายกับบริษัทที่ถูกต้องตามกฎหมายและใช้เทคโนโลยีสารสนเทศขั้นสูงในการหลอกลวงเหยื่อจากหลากหลายประเทศ ทั้งในภูมิภาคเอเชียตะวันออกเฉียงใต้และภูมิภาคอื่นของโลก สถานการณ์นี้มีต้นตอมาจากความไม่มั่นคงทางการเมืองของประเทศหลังการรัฐประหารเมื่อปี ค.ศ. 2021 ซึ่งได้เปิดช่องว่างให้กลุ่มอาชญากรข้ามชาติเข้ามาหลบซ่อนและจัดตั้งฐานปฏิบัติการในพื้นที่ชายแดนของเมียนมา อาทิ เมืองเมียวดี *(Myawaddy)*, เขตพิเศษ *Shwe Kokko* และ *KK Park* ซึ่งอยู่ภายใต้การควบคุมของกองกำลังติดอาวุธท้องถิ่นและกลุ่มทุนต่างชาติ โดยเฉพาะกลุ่มทุนจากประเทศจีนที่มีสายสัมพันธ์อันคลุมเครือกับองค์กรอาชญากรรมข้ามชาติ[209] ศูนย์ปฏิบัติการของแก๊งคอลเซ็นเตอร์ในเมียนมาไม่เพียงแต่มีบทบาทในด้านเทคนิคหรือการหลอกลวงผ่านโทรศัพท์หรืออินเทอร์เน็ตเท่านั้นแต่ยังรวมถึงมิติด้านแรงงาน ซึ่งกลายเป็นประเด็นด้านสิทธิมนุษยชนที่รุนแรงอย่างยิ่ง กล่าวคือ มีการล่อลวงหรือค้ามนุษย์แรงงานจากประเทศเพื่อนบ้านและประเทศในแอฟริกาให้เข้ามาทำงานในตำแหน่งที่อ้างว่าเกี่ยวข้องกับเทคโนโลยีสารสนเทศหรือการตลาด เมื่อบุคคลเหล่านั้น

---

[207] ‘Lao Police Bust Nine Fraud Rings, Seize Thousands of Devices in 2024’ 2 January 2025) <https://laotiantimes.com/2025/01/02/lao-police-bust-nine-fraud-rings-seize-thousands-of-devices-in-2024/> accessed 4 January 2025.

[208] 'Laos Orders ‘Scam Centers’ in Golden Triangle SEZ to Be Completely Shut Down' (Business & Human Rights Resource Centre, 12 August 2024) https://www.business-humanrights.org/en/latest-news/laos-orders-scam-centres-in-golden-triangle-sez-to-be-completely-shut-down/ accessed 8 January 2025.

[209] ‘How Myanmar Became a Global Center for Cyber Scams’ (Council on Foreign Relations 2024) <https://www.cfr.org/in-brief/how-myanmar-became-global-center-cyber-scams> accessed 8 January 2025.

เดินทางมาถึง กลับถูกยึดหนังสือเดินทางและบังคับให้ปฏิบัติงานในลักษณะหลอกลวงออนไลน์ หากไม่สามารถทำตามเป้าหมายที่กำหนดไว้ได้จะถูกทำร้าย ถูกข่มขู่ และในบางกรณีมีการขายแรงงานไปยังกลุ่มอาชญากรอื่นหรือแม้แต่การขายอวัยวะ[210] ตามรายงานของตำรวจไทยในปี 2025 มีแรงงานมากถึง 100,000 คนที่อาจถูกกักขังอยู่ในศูนย์หลอกลวงเหล่านี้บริเวณชายแดนไทย-เมียนมา ซึ่งถือเป็นตัวเลขที่สะท้อนให้เห็นถึงขนาดและความซับซ้อนของเครือข่ายดังกล่าวได้อย่างชัดเจน[211]

รูปแบบและวิธีการหลอกลวง:

ในเชิงโครงสร้างองค์กรอาชญากรรมเมียนมายังแสดงลักษณะร่วมกับประเทศอย่างกัมพูชาและลาว คือ การจัดตั้งศูนย์คอลเซ็นเตอร์ในรูปแบบของบริษัทเถื่อนหรือคอมเพล็กซ์ขนาดใหญ่ ซึ่งแบ่งงานกันอย่างชัดเจนระหว่างเจ้าหน้าที่โทรศัพท์ ฝ่ายสอนงาน ฝ่ายควบคุม และผู้บริหารระดับสูง โดยในแต่ละศูนย์จะมีการคัดเลือกแรงงานที่มาจากหลากหลายประเทศในภูมิภาค โดยรูปแบบการหลอกลวงของแก๊งคอลเซ็นเตอร์ในเมียนมานั้นคล้ายคลึงกับประเทศเพื่อนบ้านในอาเซียน ไม่ว่าจะเป็นการแอบอ้างเป็นเจ้าหน้าที่รัฐเพื่อข่มขู่เหยื่อ การหลอกให้ลงทุนในแพลตฟอร์มดิจิทัลปลอม ทั้งหมดนี้เป็นรูปแบบที่ถูกผลิตซ้ำผ่านระบบฝึกฝนที่คล้ายคลึงกัน โดยเฉพาะการใช้สคริปต์ที่มีการออกแบบมาอย่างแยบยลและสามารถปรับเปลี่ยนตามบริบทของแต่ละประเทศเป้าหมาย

## 4.2 สภาพปัญหาทางด้านนโยบายของอาเซียนที่เกี่ยวกับอาชญากรรมข้ามชาติ กรณีแก๊งคอลเซ็นเตอร์

แม้ว่าอาเซียนจะมีนโยบายและแถลงการณ์เกี่ยวกับความร่วมมือด้านความมั่นคงและการต่อต้านอาชญากรรมข้ามชาติหลายฉบับ แต่การขาดนโยบายที่มีลักษณะเป็นกลไกบังคับใช้ร่วมกันและความแตกต่างในเชิงระบบกฎหมายของประเทศสมาชิก กลับกลายเป็นอุปสรรคสำคัญต่อการดำเนินการในทางปฏิบัติ ทำให้ไม่สามารถตอบสนองต่อสถานการณ์อาชญากรรมที่มีการเปลี่ยนแปลงรวดเร็วได้อย่างทันท่วงที การวิเคราะห์สภาพปัญหาทางด้านนโยบายจึงมีความจำเป็นอย่างยิ่งในการทำความเข้าใจรากฐานของความไร้ประสิทธิภาพในการจัดการกับอาชญากรรมคอลเซ็นเตอร์ เพื่อ

---

[210] Reuters, ‘Scam Hubs on Thai-Myanmar Border Still Have Up to 100,000 People’ (Thai Police Says 2025) <https://www.reuters.com/world/asia-pacific/scam-hubs-thai-myanmar-border-still-have-up-100000-people-thai-police-says-2025-03-18/> accessed 8 January 2025.

[211] Ratcliffe Rebecca, ‘Tens of thousands could be held in illegal scam compounds in Myanmar’ (Thai police general says, 21 February 2025)<https://www.theguardian.com/world/2025/feb/21/myanmar-scam-call-centre-compounds>/> accessed 8 January 2025.

เสนอแนวทางในการปรับปรุงกฎหมายและกลไกความร่วมมือของประเทศสมาชิกอาเซียนให้สามารถรับมือกับภัยคุกคามที่มีความซับซ้อนและมีการเปลี่ยนแปลงอย่างรวดเร็วนี้ได้อย่างมีประสิทธิภาพและยั่งยืน โดยในหัวข้อนี้จะทำการวิเคราะห์ถึงสภาพปัญหาของนโยบายของอาเซียนที่เกี่ยวข้องในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ ดังนี้

**4.2.1 แผนปฏิบัติการของอาเซียนในการต่อสู้กับอาชญากรรมข้ามชาติ ASEAN Plan of Action in Combating Transnational Crime (ASEAN POA-TC)**

เป็นกรอบความร่วมมือระดับภูมิภาคที่จัดตั้งขึ้นเพื่อให้ประเทศสมาชิกอาเซียนสามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ[212]มีเป้าหมายเพื่อจัดการกับปัญหาอาชญากรรมข้ามชาติที่เป็นภัยต่อภูมิภาค โดยเฉพาะกลุ่มอาชญากรรมที่มีการดำเนินงานข้ามพรมแดน ซึ่งอาเซียนพยายามเน้นความร่วมมือระดับภูมิภาคเพื่อเสริมสร้างความเข้มแข็งในการบังคับใช้กฎหมายและป้องกันอาชญากรรมเหล่านี้ ซึ่งรวมถึงการค้ามนุษย์ ยาเสพติด การฟอกเงิน อาชญากรรมทางเทคโนโลยีสารสนเทศ (Cybercrime) และรวมถึงการจัดการกับแก๊งคอลเซ็นเตอร์ที่เน้นการสร้างกลไกการแลกเปลี่ยนข้อมูลข่าวสาร การประสานงานระหว่างหน่วยงานและการแบ่งปันทรัพยากร สร้างแนวทางและมาตรฐานให้กับกฎหมายในประเทศสมาชิกอาเซียนเพื่อรองรับการปราบปรามอาชญากรรมข้ามชาติ ถึงแม้แผนดังกล่าวจะมีความครอบคลุมในประเด็นที่เกี่ยวข้องกับ “อาชญากรรมทางไซเบอร์” ในฐานะหนึ่งในอาชญากรรมที่ได้รับการระบุให้เป็นวาระสำคัญของภูมิภาค แต่ในบริบทของอาชญากรรมไซเบอร์สมัยใหม่ โดยเฉพาะกรณีแก๊งคอลเซ็นเตอร์ซึ่งเป็นอาชญากรรมที่อาศัยเทคโนโลยีและการจัดตั้งข้ามพรมแดน การนำแผนปฏิบัติการดังกล่าวมาประยุกต์ใช้กลับยังเผชิญข้อจำกัดทั้งในระดับโครงสร้าง กฎหมาย และการประสานงานระหว่างประเทศสมาชิก โดยจากการวิเคราะห์มีสภาพปัญหาดังนี้

1. สถานะของแผนที่ไม่ผูกพันตามกฎหมายระหว่างประเทศ แผน POA-TC เป็นเพียงกรอบความร่วมมือเชิงนโยบาย (soft law) มิใช่สนธิสัญญาที่มีผลผูกพันทางกฎหมาย (binding treaty) ส่งผลให้รัฐสมาชิกสามารถเลือกปฏิบัติตามหรือไม่ก็ได้ ทั้งยังไม่มีบทบัญญัติที่กำหนดกรอบเวลา หรือกลไกการกำกับติดตาม (monitoring mechanism) อย่างชัดเจน สิ่งนี้จึงทำให้แผนดังกล่าวไม่มีพลังในการขับเคลื่อนอย่างแท้จริง โดยเฉพาะในกรณีที่ประเทศสมาชิกมีระดับความพร้อมหรือเจตจำนงทางการเมืองที่แตกต่างกัน การปฏิบัติการร่วมในการปราบปรามแก๊งคอลเซ็นเตอร์จึงขาดความสม่ำเสมอและมีแนวโน้มล้มเหลวในการตอบสนองภัยคุกคามที่รวดเร็วและซับซ้อน

2. แผนฯ ยังคงยึดโยงกับกรอบความเข้าใจแบบดั้งเดิมของอาชญากรรมข้ามชาติ เช่น การค้ามนุษย์ การก่อการร้าย หรือการค้ายาเสพติด ซึ่งมีรูปแบบชัดเจนและกระทำในโลกทางกายภาพ

---

[212] ASEAN Secretariat, ASEAN Plan of Action in Combating Transnational Crime (Jakarta: ASEAN Secretariat, 2016).

ในขณะที่ “แก๊งคอลเซ็นเตอร์” ใช้เทคโนโลยีซับซ้อน เช่น การ spoofing สัญญาณโทรศัพท์ การปลอมแอปพลิเคชันธนาคาร และการเคลื่อนย้ายทรัพย์สินผ่านคริปโทเคอร์เรนซี ซึ่งเป็นมิติใหม่ของอาชญากรรมที่ไม่ได้รับการกล่าวถึงอย่างชัดเจนในแผนยุทธศาสตร์ของอาเซียน ความไม่เท่าทันของแผนดังกล่าวจึงเป็นอุปสรรคสำคัญต่อการนำไปปรับใช้จริง

3. ความไม่สอดคล้องกันของกฎหมายและการบังคับใช้ระหว่างประเทศสมาชิก แม้แผนฯ จะเรียกร้องให้ประเทศสมาชิกพัฒนากฎหมายและสร้างมาตรฐานร่วมกันในการจัดการอาชญากรรมข้ามชาติ (legal harmonization) แต่ในความเป็นจริงระบบกฎหมายของประเทศสมาชิกมีความแตกต่างกันอย่างมาก โดยบางประเทศยังไม่มีกฎหมายเฉพาะเกี่ยวกับอาชญากรรมไซเบอร์ ขณะที่บางประเทศมีข้อจำกัดด้านสิทธิมนุษยชนหรือขาดทรัพยากรในการบังคับใช้ ส่งผลให้กระบวนการสอบสวนและดำเนินคดีข้ามพรมแดนต่อกลุ่มแก๊งคอลเซ็นเตอร์เป็นไปได้ยาก

แผนปฏิบัติการของอาเซียนในการต่อสู้กับอาชญากรรมข้ามชาติเป็นความพยายามที่สำคัญของภูมิภาคในการส่งเสริมความร่วมมือด้านความมั่นคง อย่างไรก็ดี ในบริบทของการปราบปรามแก๊งคอลเซ็นเตอร์ ซึ่งมีลักษณะเป็นอาชญากรรมไซเบอร์ที่มีพลวัตสูง แผนดังกล่าวยังไม่สามารถตอบสนองต่อความท้าทายเหล่านี้ได้อย่างเพียงพอ ทั้งในด้านกฎหมาย การบังคับใช้ กลไกความร่วมมือ และความทันสมัยของมาตรการ

**4.2.2 แผนยุทธศาสตร์ความร่วมมืออาเซียนด้านความมั่นคงทางไซเบอร์ (ASEAN Cybersecurity Cooperation Strategy)**

แผนยุทธศาสตร์ความร่วมมืออาเซียนด้านความมั่นคงทางไซเบอร์เป็นกรอบความร่วมมือระดับภูมิภาคที่จัดทำขึ้นเพื่อเสริมสร้างความมั่นคงทางไซเบอร์ในกลุ่มประเทศสมาชิกอาเซียน โดยมีเป้าหมายหลักเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ส่งเสริมการแลกเปลี่ยนข้อมูล พัฒนาขีดความสามารถ และยกระดับความตระหนักรู้ในประเด็นไซเบอร์ ทั้งในระดับนโยบาย เทคโนโลยี และกำลังคน อย่างไรก็ตามเมื่อพิจารณาในเชิงปฏิบัติการนำแผนยุทธศาสตร์นี้ไปใช้ในการต่อสู้กับอาชญากรรมไซเบอร์รูปแบบเฉพาะอย่าง แก๊งคอลเซ็นเตอร์ซึ่งมีลักษณะเป็นอาชญากรรมข้ามชาติที่ใช้เทคโนโลยีเป็นเครื่องมือหลัก ยังคงเผชิญกับสภาพปัญหาหลายประการ ดังนี้

1. ลักษณะของแผนที่ไม่ผูกพันทางกฎหมาย

แผนยุทธศาสตร์ความร่วมมืออาเซียนด้านความมั่นคงทางไซเบอร์ (ASEAN Cybersecurity Cooperation Strategy) มีลักษณะเป็นเอกสารซึ่งหมายความว่า ไม่มีผลผูกพันทางกฎหมายต่อรัฐสมาชิกอาเซียนในระดับที่เทียบเท่ากับสนธิสัญญา (treaty) หรือข้อตกลงระหว่างประเทศ (international convention) ตามกฎหมายระหว่างประเทศ การที่แผนดังกล่าวไม่มีผลผูกพันตามกฎหมายส่งผลให้รัฐสมาชิกสามารถเลือกปฏิบัติตามหรือไม่ปฏิบัติตามก็ได้ โดยไม่ต้องรับผลทางกฎหมายหรือการลงโทษใด ๆ จากกลไกของอาเซียน นอกจากนี้ยังไม่มีบทบัญญัติที่กำหนดให้

ต้องรายงานผลหรือแสดงความรับผิดชอบต่อความล้มเหลวในการดำเนินการตามแผน ทำให้มาตรการที่กำหนดไว้ในแผนไม่สามารถแปรเปลี่ยนเป็น “พันธกรณี” ในเชิงกฎหมายได้จริง ด้วยลักษณะที่ไม่ผูกพันนี้เอง ทำให้แผนยุทธศาสตร์ฯ กลายเป็นเพียงแนวทางหรือกรอบความร่วมมือทั่วไปที่ ขาดพลังในการผลักดันให้เกิด “การปฏิบัติจริง” โดยเฉพาะในสถานการณ์ที่ต้องการการตอบสนองแบบเร่งด่วน เช่น การติดตามเส้นทางธุรกรรมทางการเงินของแก๊งคอลเซ็นเตอร์ การแบ่งปันข้อมูลผู้ต้องสงสัยหรือการดำเนินคดีข้ามพรมแดน ทำให้การดำเนินงานที่ไม่สอดคล้องกันในภูมิภาคและไม่มีเครื่องมือในการกำกับติดตามหรือบังคับใช้ จึงกลายเป็นเพียงแนวทางที่ดีในหลักการแต่อ่อนในทางปฏิบัติโดยเฉพาะเมื่อเทียบกับความเร็วและความรุนแรงของภัยไซเบอร์ในปัจจุบัน

2. ขาดกลไกประสานความร่วมมือด้านการบังคับใช้กฎหมาย

แม้แผนจะส่งเสริมความร่วมมือด้านนโยบายและการสร้างขีดความสามารถทางเทคนิค แต่กลับไม่มีกลไกเฉพาะที่รองรับการ “บังคับใช้กฎหมายร่วมกัน” หรือ “การปฏิบัติการข้ามพรมแดน” ต่ออาชญากรรมไซเบอร์ เช่น การตั้งศูนย์ปฏิบัติการร่วม (Joint Cybercrime Task Force) หรือการแลกเปลี่ยนฐานข้อมูลผู้กระทำผิดแบบเรียลไทม์กรณีแก๊งคอลเซ็นเตอร์ที่ผู้กระทำผิดอยู่ต่างประเทศ ใช้เครือข่าย VPN ปลอม IP และรับเงินผ่านบัญชีในประเทศที่สาม จำเป็นต้องใช้ความร่วมมือในเชิงลึกจากหลายประเทศทั้งในการสืบสวน ติดตามทรัพย์ และจับกุม แต่แผนยุทธศาสตร์ไม่ได้ระบุเครื่องมือหรือกลไกดังกล่าวอย่างเป็นรูปธรรม ทำให้การประยุกต์ใช้ในทางคดีจริงยังขาดประสิทธิภาพ

3. การพึ่งพาการฝึกอบรมและการเสริมสร้างศักยภาพมากกว่าการสร้างโครงสร้างถาวร

แผนยุทธศาสตร์เน้นการจัดอบรม ประชุมเชิงปฏิบัติการ และสร้างความตระหนักรู้ในหมู่เจ้าหน้าที่และประชาชน ซึ่งแม้จะมีความสำคัญในการยกระดับความเข้าใจ แต่ก็เป็นมาตรการในเชิง *capacity-building* มากกว่าการสร้างโครงสร้างถาวร เช่น กฎหมายไซเบอร์ที่สอดคล้องกันทั่วภูมิภาค ระบบการตรวจจับภัยคุกคามแบบร่วม หรือแพลตฟอร์มสำหรับรายงานอาชญากรรมทางไซเบอร์แบบอาเซียน การพึ่งพาการฝึกอบรมอย่างเดียวโดยไม่เสริมสร้างโครงสร้างทางกฎหมายและระบบปฏิบัติการร่วม ส่งผลให้แผนไม่สามารถรองรับการปฏิบัติจริงในสถานการณ์วิกฤต เช่น การจัดการกรณีแก๊งคอลเซ็นเตอร์ที่ต้องการความเร็ว ความแม่นยำ และการประสานข้ามประเทศ

ท้ายที่สุดแม้แผนยุทธศาสตร์ฯ ได้เสนอให้จัดตั้ง ASEAN Cybersecurity Centre of Excellence (ACoE) และโครงการฝึกอบรมเพื่อเสริมสร้างความสามารถของประเทศสมาชิก แต่ยังขาดแผนงานระยะยาวที่ชัดเจนเกี่ยวกับการปฏิบัติการร่วม (joint operations) หรือระบบเตือนภัยล่วงหน้า (early warning systems) ที่จำเพาะต่อการปราบปรามอาชญากรรมไซเบอร์ข้ามชาติ ซึ่งเป็นสิ่งจำเป็นในการรับมือกับรูปแบบของแก๊งคอลเซ็นเตอร์ที่ดำเนินการอย่างเป็นเครือข่ายและมีการแปรรูปกลยุทธ์อย่างต่อเนื่อง ดังนั้น แม้แผนยุทธศาสตร์ความร่วมมืออาเซียนด้านความมั่นคงทางไซ

เบอร์ จะถือเป็นก้าวสำคัญในการยกระดับการรับมือภัยคุกคามทางไซเบอร์ในภูมิภาค แต่เมื่อพิจารณาในมิติเฉพาะของการปราบปรามแก๊งคอลเซ็นเตอร์ ยังพบข้อจำกัดในเชิงโครงสร้าง ความไม่เท่าเทียมด้านขีดความสามารถ และการขาดพันธกรณีเชิงกฎหมายที่ชัดเจน

## 4.3 สภาพปัญหาทางด้านกฎหมายของอาเซียนที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

### 4.3.1 สภาพปัญหาทางด้านกฎหมายระดับภูมิภาคอาเซียนที่เกี่ยวกับอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

แก๊งคอลเซ็นเตอร์เป็นปัญหาอาชญากรรมข้ามชาติอย่างที่แพร่หลายไปทั่วในภูมิภาคเอเชียตะวันออกเฉียงใต้ เนื่องจากภูมิภาคนี้เป็นแหล่งฐานปฏิบัติการ เป็นพื้นที่ที่พลเมืองอาเซียนทั้งหลายได้รับผลกระทบจากแก๊งคอลเซ็นเตอร์ ขัดต่อกฎบัตรอาเซียนในข้อ 1 (ความมุ่งประสงค์ของอาเซียน) (11) “เพื่อเพิ่มพูนความเป็นอยู่ที่ดีและการดำรงชีวิตของประชาชนอาเซียนด้วยการให้ประชาชนมีโอกาสที่ทัดเทียมกันในการเข้าถึงการพัฒนามนุษย์ สวัสดิการสังคม และ ความยุติธรรม” และ (12) “เพื่อเสริมสร้างความร่วมมือในการสร้างสภาพแวดล้อมที่ปลอดภัย มั่นคง และ ปราศจากยาเสพติดสำหรับประชาชนของอาเซียน” โดยแก๊งคอลเซ็นเตอร์ ถือว่าเป็นอาชญากรรมข้ามชาติที่ส่งผลกระทบในวงกว้างต่อความมั่นคงและความสงบเรียบร้อยในสังคม แต่ข้อเท็จจริงจริงปรากฏว่าการจัดการกับปัญหาแก๊งคอลเซ็นเตอร์นี้ในระดับภูมิภาคอาเซียนยังไม่ประสบความสำเร็จ เนื่องจากต้องเผชิญกับปัญหาและอุปสรรคทางกฎหมายหลายประการ ซึ่งจากการศึกษาพบว่าความร่วมมือระหว่างประเทศของอาเซียนในการจัดการกับปัญหาอาชญากรรมข้ามชาติแก๊งคอลเซ็นเตอร์มีมาตรการสำหรับการจัดการ โดยในบทนี้จะวิเคราะห์ถึงสภาพปัญหาของมาตรการของอาเซียนที่เกี่ยวข้องในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ ดังนี้

4.3.1.1 กฎบัตรอาเซียน (ASEAN Charter)

จากการศึกษาเหตุผลและหลักการของการจัดทำกฎบัตรอาเซียน เห็นได้ว่าอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์นี้ได้อาศัยช่องโหว่ของหลักเกณฑ์ โดยอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์นี้ได้อาศัยช่องโหว่ของหลักเกณฑ์ทางกฎหมายของอาเซียนหรือวิถีอาเซียน (ASEAN Ways) ตามที่กำหนดไว้ในข้อ 2 ของกฎบัตรอาเซียน[213] เช่น หลักการเคารพเอกราช อธิปไตย ความ

[213] CHARTER OF THE ASSOCIATION OF SOUTHEAST ASIAN NATIONS
ARTICLE 2 “PRINCIPLES 2. ASEAN and its Member States shall act in accordance with the following Principles:

เสมอภาค บูรณภาพแห่งดินแดน และอัตลักษณ์ แห่งชาติของรัฐสมาชิกอาเซียนทั้งปวง และ หลักการไม่แทรกแซงกิจการภายในของรัฐสมาชิกอาเซียน เป็นต้น ก่อการกระทำความผิดต่อพลเมืองอาเซียนที่เป็นกรณีเกี่ยวข้องกับการกระทำผิดที่ครอบคลุมหลายประเทศ

4.3.1.2 สนธิสัญญาความช่วยเหลือซึ่งกันและกันในทางอาญาของภูมิภาคอาเซียน (Treaty on Mutual Legal Assistance in Criminal Matters - ASEAN MLAT)[214] ซึ่งลงนามเมื่อปี พ.ศ. 2547 (ค.ศ.2004) และมีผลบังคับใช้เมื่อ พ.ศ. 2552 (ค.ศ.2009) โดย ASEAN MLAT มีวัตถุประสงค์เพื่อส่งเสริมความร่วมมือระหว่างรัฐสมาชิกในการสอบสวน การฟ้องร้อง และการดำเนินคดีทางอาญา ซึ่งในบริบทของการปราบปรามแก๊งคอลเซ็นเตอร์มักประกอบด้วยขบวนการที่มีลักษณะเป็นเครือข่ายอาชญากรรมข้ามชาติ การดำเนินคดีจำเป็นต้องอาศัยความร่วมมือระหว่างประเทศทั้งในด้านการรวบรวมพยานหลักฐาน การติดตามเส้นทางการเงิน และการขอส่งผู้ต้องหาให้ดำเนินคดีในประเทศที่ได้รับความเสียหาย สนธิสัญญา ASEAN MLAT จึงมีบทบาทสำคัญในฐานะกลไกทางกฎหมายที่อำนวยความสะดวกให้รัฐภาคีสามารถร้องขอความช่วยเหลือซึ่งกันและกันได้โดยมีกรอบกฎหมายรองรับอย่างเป็นทางการ ตัวอย่างเช่น หากเจ้าหน้าที่ไทยต้องการข้อมูลจากผู้ให้บริการอินเทอร์เน็ตในฟิลิปปินส์ ซึ่งเป็นที่ตั้งของเซิร์ฟเวอร์ที่แก๊งคอลเซ็นเตอร์ใช้ในการโทรหลอกลวง สามารถใช้ช่องทาง MLAT เพื่อร้องขอข้อมูลจากทางการฟิลิปปินส์โดยผ่านกระบวนการที่ได้รับการรับรองตามกฎหมาย ซึ่งจะมีน้ำหนักมากกว่าการประสานงานแบบไม่เป็นทางการ หรือหากมีผู้กระทำผิดที่หลบหนีไปยังประเทศภาคีอื่น การขอความร่วมมือเพื่อระบุตัวบุคคล การสอบสวน และการส่งผู้ร้ายข้ามแดนก็สามารถดำเนินการผ่านช่องทาง MLAT ได้อย่างถูกต้องตามกระบวนการ อย่างไรก็ตาม แม้ ASEAN MLAT จะมีศักยภาพในเชิงหลักการ แต่การใช้งานจริงในบริบทของแก๊งคอลเซ็นเตอร์ยังต้องพึ่งพาความรวดเร็ว ความเชื่อมั่นซึ่งกันและกัน และความพร้อมทางเทคโนโลยีของแต่ละประเทศ ซึ่งยังคงเป็นข้อจำกัดหลักที่ทำให้การใช้สนธิสัญญานี้ในทางปฏิบัติเพื่อปราบปรามแก๊งคอลเซ็นเตอร์ยังไม่สามารถเกิดผลสัมฤทธิ์ได้อย่างเต็มที่ เมื่อพิจารณาถึงการประยุกต์ใช้ในกรณีของ แก๊งคอลเซ็นเตอร์ กลับพบว่ายังมีข้อจำกัดและสภาพปัญหาหลายประการที่ทำให้ไม่สามารถตอบสนองต่อภัยคุกคามลักษณะนี้ได้อย่างมีประสิทธิภาพ โดยสภาพปัญหาหลักได้แก่

1. ปัญหาข้อจำกัดด้านการตีความคำว่า “ความช่วยเหลือในทางอาญา”

---

(a) respect for the independence, sovereignty, equality, territorial integrity and national identity of all ASEAN Member States

(e) non-interference in the internal affairs of ASEAN Member States;”

[214] 'ASEAN Treaty on Mutual Legal Assistance in Criminal Matters (MLAT)' (Jakarta: ASEAN Secretariat, 2004) https://asean.org accessed 4 March 2025.

การตีความคำว่า “ความช่วยเหลือในทางอาญา” ภายใต้สนธิสัญญานี้ในทางปฏิบัติมักจำกัดเฉพาะการให้ความร่วมมือแบบดั้งเดิม เช่น การส่งมอบพยาน การร้องขอเอกสาร การสอบสวนในประเทศปลายทาง เป็นต้น โดยขาดการตีความขยายให้ครอบคลุมถึงการสืบค้นข้อมูลทางดิจิทัล การระงับบัญชีธุรกรรมออนไลน์ การเข้าถึงข้อมูลจากผู้ให้บริการอินเทอร์เน็ต หรือการแลกเปลี่ยนข้อมูลเรียลไทม์เกี่ยวกับการเคลื่อนไหวของเครือข่ายอาชญากรรมไซเบอร์ ซึ่งเป็นหัวใจในการจัดการแก๊งคอลเซ็นเตอร์ ในกรณีของแก๊งคอลเซ็นเตอร์ ซึ่งพฤติกรรมการกระทำผิดส่วนใหญ่เกิดขึ้นผ่านเครือข่ายโทรคมนาคมและแพลตฟอร์มดิจิทัล การร้องขอความช่วยเหลือจำเป็นต้องมีลักษณะรวดเร็วและเฉพาะทาง การตีความความช่วยเหลือในแบบเดิมกลับทำให้หน่วยงานที่รับคำขอในบางประเทศปฏิเสธการดำเนินการ เนื่องจากไม่เห็นว่าเป็นความผิดทางอาญาตามมาตรฐานของประเทศตน หรือเห็นว่าไม่อยู่ในขอบเขตของ MLAT ซึ่งกลายเป็นข้อจำกัดในการบังคับใช้

ปัญหานี้สะท้อนให้เห็นถึงความไม่สอดคล้องกันระหว่างกรอบความร่วมมือทางกฎหมายที่ออกแบบขึ้นในบริบทแบบอนาล็อก กับลักษณะของอาชญากรรมในยุคดิจิทัลที่มีพลวัตสูงและข้ามพรมแดนอย่างรวดเร็ว โดยเฉพาะอย่างยิ่งเมื่อระบบ MLAT ดั้งเดิมถูกวิพากษ์วิจารณ์ว่าไม่สามารถตอบสนองต่อการร้องขอหลักฐานทางดิจิทัลได้ทันเวลา ทั้งยังไม่มีเครื่องมือในการเข้าถึงหรือบังคับใช้กับข้อมูลที่อยู่ในต่างเขตอำนาจ[215] ดังนั้นชี้ให้เห็นว่า ระบบความร่วมมือแบบ MLAT ที่มีอยู่ในปัจจุบันนั้น ถูกออกแบบขึ้นก่อนยุคอินเทอร์เน็ต และไม่เหมาะสมต่อการจัดการกับหลักฐานดิจิทัลข้ามเขตอำนาจ อีกทั้งยังทำงานช้าและไม่เพียงพอต่อความต้องการในทางปฏิบัติสำหรับการสอบสวนอาชญากรรมไซเบอร์[216]

2. ปัญหาความล่าช้าในกระบวนการขอความช่วยเหลือ

สนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันในทางอาญาในภูมิภาคอาเซียน (ASEAN MLAT) มีวัตถุประสงค์ในการส่งเสริมความร่วมมือทางกฎหมายระหว่างรัฐภาคีในการสอบสวน ดำเนินคดี หรือดำเนินการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรมข้ามชาติ โดยสามารถร้องขอความช่วยเหลือได้ในรูปแบบต่าง ๆ เช่น การจัดหาพยาน การจัดส่งเอกสารหรือหลักฐาน การบังคับใช้คำสั่งศาล รวมถึงการดำเนินการอื่นที่จำเป็นต่อกระบวนการยุติธรรมภายในประเทศ อย่างไรก็ตามกลไกของสนธิสัญญาดังกล่าวยังคงอิงอยู่กับระบบการประสานงานแบบรัฐต่อรัฐ (State-to-State Mechanism) ผ่านหน่วยงานกลาง (Central Authority) ซึ่งในทางปฏิบัติมักเป็นกระทรวงยุติธรรม

---

[215] Anna Maria Osula, *Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorial Evidence* (NATO CCDCOE, 2015) <https://ccdcoe.org/uploads/2018/10/Research_A-M.Osula_2015.pdf > accessed 5 March 2025.

[216] Jennifer Daskal, ‘The Digital Unfitness of Mutual Legal Assistance’ (Security and Human Rights 28, no. 1–4 (2017)) <https://doi.org/10.1163/18750230-02801011> accessed 5 March 2025.

หรือสำนักงานอัยการสูงสุดของแต่ละประเทศ ทำให้ขั้นตอนการดำเนินงานมีลักษณะเป็นทางการ ใช้เวลานาน และไม่สามารถตอบสนองต่อเหตุการณ์ที่มีลักษณะเร่งด่วน โดยเฉพาะในกรณีของอาชญากรรมข้ามชาติที่อาศัยเทคโนโลยีขั้นสูง เช่น แก๊งคอลเซ็นเตอร์ ซึ่งมีความสามารถในการหลบเลี่ยงร่องรอยทางดิจิทัล เคลื่อนย้ายข้ามพรมแดนได้รวดเร็ว และก่ออาชญากรรมในเวลาเพียงไม่กี่นาที ในบริบทนี้ การขอความช่วยเหลือผ่าน ASEAN MLAT เช่น การขอข้อมูลการสื่อสาร ข้อมูลบัญชีธุรกรรมทางการเงิน หรือการตรวจค้นเซิร์ฟเวอร์ในต่างประเทศ ไม่สามารถดำเนินการได้ทันท่วงที ส่งผลให้อาชญากรสามารถถอนเงินหรือโอนทรัพย์สินได้ภายในเวลาอันสั้น ในขณะที่คำร้องขอ MLAT อาจต้องใช้เวลาหลายสัปดาห์ หรือแม้กระทั่งหลายเดือน กว่าจะได้รับการตอบสนองอย่างเป็นทางการ ปัญหาความล่าช้าดังกล่าวเป็นผลจากหลายปัจจัย ได้แก่ ความแตกต่างของระบบกฎหมายภายในที่อาจต้องมีคำสั่งศาลก่อนการตอบสนองคำขอ ข้อจำกัดด้านทรัพยากรบุคลากรหรืองบประมาณ ขั้นตอนอนุมัติที่ซับซ้อน และการไม่มีระบบติดตามหรือกลไกเร่งรัดคำร้องภายในสนธิสัญญา

แม้ยังไม่มีรายงานอย่างเป็นทางการที่ประเมินระยะเวลาเฉลี่ยของคำร้อง ASEAN MLAT โดยเฉพาะ แต่เมื่อพิจารณาจากแนวโน้มของระบบ MLAT ทั่วโลกจะพบว่ากระบวนการดังกล่าวมักเผชิญกับความล่าช้าเป็นระบบ จากการศึกษาโดย Stanford Center for Internet and Society[217] รายงานว่าคำร้องขอข้อมูลการสื่อสารผ่าน MLA ในสหราชอาณาจักรอาจใช้เวลานานถึง 10-13 เดือนในการดำเนินการ นอกจากนี้ รายงานของ Council of Europe T-CY (2013–2014) ยังระบุว่าโดยทั่วไป คำร้อง MLA สำหรับข้อมูลอิเล็กทรอนิกส์ใช้เวลาระหว่าง 6 ถึง 24 เดือนจึงจะได้รับการตอบสนอง[218]

อีกทั้ง สนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันในทางอาญาในภูมิภาคอาเซียน (ASEAN MLAT) ได้ถูกออกแบบมาเพื่อส่งเสริมความร่วมมือข้ามพรมแดนในด้านกระบวนการยุติธรรมทางอาญา ทว่าบทบัญญัติใน มาตรา 3[219] ซึ่งบัญญัติถึงเหตุแห่งการปฏิเสธความช่วยเหลือยังคงเป็น

---

[217] 'The Mutual Legal Assistance Problem Explained' (Stanford Center for Internet and Society, 2015) <https://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained> accessed 5 March 2025.

[218] Council of Europe, Assessment Report on Mutual Legal Assistance and Electronic Evidence, T-CY (2013–2014).

[219] Treaty on Mutual Legal Assistance in Criminal Matters

ARTICLE 3 LIMITATIONS ON ASSISTANCE

1. The Requested Party shall refuse assistance if, in its opinion –

(a) the request relates to the investigation, prosecution or punishment of a person for an offence that is, or is by reason of the circumstances in which it is alleged to have been committed or was committed, an offence of a political nature;

(b) the request relates to the investigation, prosecution or punishment of a person in respect of an act or omission that, if it had occurred in the Requested Party, would have constituted a military offence under the laws of the Requested Party which is not also an offence under the ordinary criminal law of the Requested Party;

(c) there are substantial grounds for believing that the request was made for the purpose of investigating, prosecuting, punishing or otherwise causing prejudice to a person on account of the person's race, religion, sex, ethnic origin, nationality or political opinions;

(d) the request relates to the investigation, prosecution or punishment of a person for an offence in a case where the person - (i) has been convicted, acquitted or pardoned by a competent court or other authority in the Requesting or Requested Party; or (ii) has undergone the punishment provided by the law of that Requesting or Requested Party, in respect of that offence or of another offence constituted by the same act or omission as the first-mentioned offence; (e) the request relates to the investigation, prosecution or punishment of a person in respect of an act or omission that, if it had occurred in the Requested Party, would not have constituted an offence against the laws of the Requested Party except that the Requested Party may provide assistance in the absence of dual criminality if permitted by its domestic laws;

(f) the provision of the assistance would affect the sovereignty, security, public order, public interest or essential interests of the Requested Party;

(g) the Requesting Party fails to undertake that it will be able to comply with a future request of a similar nature by the Requested Party for assistance in a criminal matter;

(h) the Requesting Party fails to undertake that the item requested for will not be used for a matter other than the criminal matter in respect of which the request was made and the Requested Party has not consented to waive such undertaking;

(i) the Requesting Party fails to undertake to return to the Requested Party, upon its request, any item obtained pursuant to the request upon completion of the criminal matter in respect of which the request was made;

(j) the provision of the assistance could prejudice a criminal matter in the Requested Party; or

(k) the provision of the assistance would require steps to be taken that would be contrary to the laws of the Requested Party. 2. The Requested Party may refuse assistance if, in its opinion –

จุดอ่อนสำคัญที่ส่งผลกระทบต่อประสิทธิภาพในการปราบปรามอาชญากรรมข้ามชาติ โดยเฉพาะในบริบทของ แก๊งคอลเซ็นเตอร์ ซึ่งมีลักษณะซับซ้อนและแทรกซ้อนกับผลประโยชน์ของรัฐ มาตรา 3 ให้

---

(a) the Requesting Party has, in respect of that request, failed to comply with any material terms of this Treaty or other relevant arrangements;

(b) the provision of the assistance would, or would be likely to prejudice the safety of any person, whether that person is within or outside the territory of the Requested Party; or (c) the provision of the assistance would impose an excessive burden on the resources of the Requested Party.

3. For the purposes of subparagraph 1

(a), the following offences shall not be held to be offences of a political nature: (a) an offence against the life or person of a Head of State or a member of the immediate family of a Head of State;

(b) an offence against the life or person of a Head of a central Government, or of a Minister of a central Government;

(c) an offence within the scope of any international convention to which both the Requesting and Requested Parties are parties to and which imposes on the Parties thereto an obligation either to extradite or prosecute a person accused of the commission of that offence; and

(d) any attempt, abetment or conspiracy to commit any of the offences referred to in subparagraphs (a) to (c)

4. The Requested Party may restrict the application of any of the provisions made under paragraph 3 according to whether the Requesting Party has made similar provision in its laws.

5. Assistance shall not be refused solely on the ground of secrecy of banks and similar financial institutions or that the offence is also considered to involve fiscal matters.

6. The Requested Party may postpone the execution of the request if its immediate execution would interfere with any ongoing criminal matters in the Requested Party.

7. Before refusing a request or postponing its execution pursuant to this Article, the Requested Party shall consider whether assistance may be granted subject to certain conditions.

8. If the Requesting Party accepts assistance subject to the terms and conditions imposed under paragraph 7, it shall comply with such terms and conditions.

9. If the Requested Party refuses or postpones assistance, it shall promptly inform the Requesting Party of the grounds of refusal or postponement.

10. The Parties shall, subject to their respective domestic laws, reciprocate any assistance granted in respect of an equivalent offence irrespective of the applicable penalty.

อำนาจแก่รัฐที่ได้รับคำร้อง (Requested State) ในการปฏิเสธความช่วยเหลือหากเห็นว่าคดีเกี่ยวข้องกับความมั่นคง ความสงบเรียบร้อย หรือผลประโยชน์อันเป็นสาระสำคัญของรัฐ นอกจากนี้ยังมีข้อที่เปิดช่องให้รัฐสามารถอ้างเรื่องความไม่สอดคล้องกับกฎหมายภายในในการปฏิเสธได้ แม้ในทางทฤษฎีเหตุแห่งการปฏิเสธเหล่านี้จะเป็นมาตรฐานทั่วไปที่พบในความตกลงทวิภาคีหรือพหุภาคีในลักษณะเดียวกัน ทว่า ในบริบทของอาเซียนซึ่งมีลักษณะทางการเมืองและกฎหมายที่หลากหลาย ข้อบทเหล่านี้อาจถูกตีความอย่างกว้างเกินสมควร ส่งผลให้ รัฐภาคีสามารถใช้เป็นข้ออ้างในการหลีกเลี่ยงไม่ให้ความร่วมมือในคดีที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ โดยอ้างว่าเป็นการกระทบต่อ “ผลประโยชน์แห่งชาติ” หรือขัดต่อกฎหมายในประเทศของตน

สภาพปัญหาดังกล่าวชี้ให้เห็นว่า มาตรา 3 ของสนธิสัญญาฯ แม้จะมีความตั้งใจดีในการเคารพสิทธิสากลของรัฐภาคีแต่ในทางปฏิบัติกลับกลายเป็นอุปสรรคต่อความร่วมมือข้ามพรมแดนในกรณีเร่งด่วนและซับซ้อนอย่างอาชญากรรมไซเบอร์ ดังนั้น การปฏิรูปหรือเสนอแนะแนวทางในการปรับปรุงการตีความมาตรา 3 จึงควรเป็นวาระสำคัญในกระบวนการเสริมสร้างความร่วมมือด้านกฎหมายของอาเซียนให้สอดรับกับภัยคุกคามยุคใหม่อย่างแท้จริง

4.3.1.2 ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ ค.ศ.2017 (ASEAN Declaration to Prevent and Combat Cybercrime)[220] ในยุคที่ภัยคุกคามจากอาชญากรรมไซเบอร์ขยายตัวอย่างรวดเร็ว โดยเฉพาะในรูปแบบของ แก๊งคอลเซ็นเตอร์ ที่ดำเนินการข้ามพรมแดนและใช้เทคโนโลยีเป็นเครื่องมือในการหลอกลวงและฉ้อโกงประชาชนในภูมิภาคเอเชียตะวันออกเฉียงใต้ อาเซียนจึงตระหนักถึงความจำเป็นในการร่วมมือกันอย่างใกล้ชิดในระดับภูมิภาคเพื่อต่อกรกับภัยคุกคามดังกล่าว ซึ่งนำไปสู่การรับรอง ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ (ASEAN Declaration to Prevent and Combat Cybercrime) เมื่อปี ค.ศ. 2017 ในการประชุมรัฐมนตรีว่าการกระทรวงมหาดไทยอาเซียน ครั้งที่ 11 ณ กรุงมะนิลา ประเทศ

---

[220] ASEAN Declaration to Prevent and Combat Cybercrime คือ ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ให้ความสำคัญกับการปรับปรุงกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์และหลักฐานทางอิเล็กทรอนิกส์ รวมทั้งสนับสนุนการร่างกรอบการทำงานระดับภูมิภาคเพื่อสร้างความร่วมมือระหว่างประเทศสมาชิกและการกำหนดแผนปฏิบัติการระดับชาติในการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์ รวมถึงการให้ความช่วยเหลือด้านผู้เชี่ยวชาญทางเทคนิคในการป้องกันและต่อต้านอาชญากรรมไซเบอร์ อันเป็นการยกระดับความร่วมมือระหว่างประเทศสมาชิกอาเซียนและประเทศคู่เจรจา รวมทั้งหน่วยงานและองค์กรต่าง ๆ ที่เกี่ยวข้องทั้งใน ระดับภูมิภาคและนานาชาติ นอกจากนี้ ปฏิญญาฯ ยังมีวัตถุประสงค์ในการเสริมสร้างความมั่นคงทางเทคโนโลยี การป้องกัน และความสามารถในการแก้ไขปัญหาเกี่ยวกับอาชญากรรมทางไซเบอร์ เพื่อพัฒนาขีดความสามารถของอาเซียนในการสร้างและพัฒนาศักยภาพในการต่อสู้กับอาชญากรรมทางไซเบอร์. โปรดดู: ‘อาเซียนกับการจัดการปัญหาอาชญากรรมไซเบอร์’ (Law for ASEAN) <https://lawforasean.krisdika.go.th/File/files/cybersecurity_dec2.pdf> สืบค้นเมื่อ 14 พฤศจิกายน 2566.

ฟิลิปปินส์ ปฏิญญาฉบับนี้มีเป้าหมายหลักเพื่อส่งเสริมความร่วมมือระหว่างรัฐสมาชิกในการป้องกัน ตรวจจับ และดำเนินคดีกับอาชญากรรมไซเบอร์ โดยเน้นการแลกเปลี่ยนข้อมูล เสริมสร้างขีดความสามารถทางเทคนิค และสนับสนุนการฝึกอบรมบุคลากร อย่างไรก็ตามแม้ปฏิญญาจะเป็นการแสดงเจตจำนงทางการเมืองที่ชัดเจน แต่ลักษณะของปฏิญญาซึ่งไม่ใช่ตราสารผูกพันทางกฎหมาย (non-binding instrument) ทำให้เกิดข้อจำกัดในการนำไปสู่การปฏิบัติที่เป็นรูปธรรมในระดับประเทศอย่างแท้จริง ยิ่งไปกว่านั้น ข้อความในปฏิญญายังมีลักษณะทั่วไป (generic) และไม่ได้กำหนดกลไกความร่วมมือเฉพาะด้าน เช่น หน่วยประสานงานกลาง การแบ่งปันฐานข้อมูลอาชญากร หรือแนวทางร่วมในการวิเคราะห์พฤติกรรมไซเบอร์ ที่จะช่วยให้สามารถรับมือกับรูปแบบอาชญากรรมเฉพาะอย่างแก๊งคอลเซ็นเตอร์ได้อย่างมีประสิทธิภาพ นอกจากนี้ปฏิญญาฯ ไม่ได้เชื่อมโยงหรืออ้างอิงกับสนธิสัญญาระหว่างประเทศสำคัญ เช่น อนุสัญญาบูดาเปสต์ว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Budapest Convention) หรือแนวปฏิบัติของ INTERPOL ในการสืบสวนอาชญากรรมไซเบอร์ข้ามชาติ ทำให้ขาดความเชื่อมโยงกับมาตรฐานสากล

อีกประเด็นที่ควรพิจารณา คือ การไม่มีการจัดตั้งกรอบประเมินผลและติดตามความคืบหน้า (Monitoring and Evaluation Framework) สำหรับการดำเนินงานตามปฏิญญา ซึ่งนำไปสู่ความไม่แน่นอนในประสิทธิภาพของมาตรการต่าง ๆ ที่แต่ละประเทศดำเนินการภายใต้เจตจำนงของปฏิญญาฉบับนี้ แม้ปฏิญญาจะมีจุดแข็งในแง่ของการเปิดพื้นที่ให้ประเทศสมาชิกพัฒนาแนวทางป้องกันอาชญากรรมไซเบอร์ในบริบทของตนเองและส่งเสริมแนวคิดเรื่องความมั่นคงทางไซเบอร์ในระดับภูมิภาค แต่ในทางปฏิบัติการขาดกลไกบังคับใช้ที่มีผลผูกพัน การไม่มีบทลงโทษ และการขาดกลไกติดตามผล ทำให้ไม่สามารถผลักดันการบูรณาการเชิงยุทธศาสตร์ระหว่างประเทศสมาชิกได้อย่างแท้จริง โดยเฉพาะเมื่อเผชิญกับภัยคุกคามที่เคลื่อนไหวรวดเร็วและซับซ้อนเช่นเครือข่ายแก๊งคอลเซ็นเตอร์ ซึ่งมักใช้โครงสร้างองค์กรที่กระจายตัวในหลายประเทศอาเซียน ดังนั้น แม้ปฏิญญาจะเป็นก้าวแรกของอาเซียนในการแสดงเจตนารมณ์ร่วมกันในการต่อสู้กับอาชญากรรมไซเบอร์ แต่หากต้องการให้เกิดผลในทางปฏิบัติอย่างแท้จริง จำเป็นต้องมีการยกระดับจากปฏิญญาทางการเมือง ไปสู่ความตกลงระหว่างรัฐที่มีผลผูกพันทางกฎหมายและมีกลไกความร่วมมือที่มีโครงสร้างรองรับอย่างชัดเจน อาทิ ศูนย์ข้อมูลไซเบอร์อาเซียน (ASEAN Cybercrime Information Hub) หรือการจัดตั้งหน่วยปฏิบัติการสอบสวนร่วมด้านไซเบอร์ (Joint Cybercrime Taskforce) เพื่อรับมือกับอาชญากรรมอย่างแก๊งคอลเซ็นเตอร์ที่กระทบต่อประชาชนในภูมิภาคอย่างลึกซึ้ง

**4.3.2 สภาพปัญหาทางด้านกฎหมายที่เกี่ยวกับอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ในแต่ละประเทศของสมาชิกอาเซียน**

ในทุก ๆ ประเทศของสมาชิกอาเซียนต่างก็ได้รับผลกระทบจากแก๊งคอลเซ็นเตอร์ โดยได้สร้างปัญหาใหญ่ให้กับประเทศสมาชิกในภูมิภาคอาเซียน โดยเฉพาะในด้านความมั่นคงทางสังคมและเศรษฐกิจ แต่ละประเทศได้ดำเนินมาตรการต่าง ๆ เพื่อป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์ ดังนี้

4.3.2.1 ประเทศไทย

ประเทศไทยได้บัญญัติกฎหมายหลายฉบับเพื่อรับมือกับอาชญากรรมที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์ ซึ่งมักมีลักษณะเป็นอาชญากรรมทางเทคโนโลยีและข้ามชาติ ได้แก่

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (แก้ไขเพิ่มเติม พ.ศ. 2560) พระราชบัญญัตินี้เป็นกฎหมายหลักที่ใช้ในการรับมือกับอาชญากรรมที่ใช้เทคโนโลยีเป็นเครื่องมือ โดยเฉพาะกรณีที่คนร้ายติดต่อผู้เสียหายผ่านโทรศัพท์หรือแพลตฟอร์มออนไลน์

มาตรา 14[221] (1) ห้ามการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ หากมีลักษณะหลอกลวงและก่อให้เกิดความเสียหายแก่ประชาชน

---

[221] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (แก้ไขเพิ่มเติม พ.ศ. 2560) มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(1) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ (4)

มาตรา 5-10[222] บัญญัติความผิดเกี่ยวกับการเข้าถึงระบบโดยมิชอบ การดักข้อมูล การรบกวนระบบ ซึ่งใช้เอาผิดกับผู้ที่ล้วงข้อมูลหรือแฮ็กระบบของเหยื่อ

2. ประมวลกฎหมายอาญา ใช้ในการเอาผิดผู้กระทำผิดฐานทั่วไป โดยเฉพาะการฉ้อโกงและการแอบอ้างบุคคลอื่น

มาตรา 341[223] ใช้ในกรณีที่แก๊งคอลเซ็นเตอร์แอบอ้างเป็นเจ้าหน้าที่รัฐหรือธนาคารเพื่อหลอกลวงเหยื่อให้โอนเงิน

---

[222] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (แก้ไขเพิ่มเติม พ.ศ. 2560)

มาตรา 5 ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 6 ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 8 ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะ หรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 9 ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 10 ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

[223] ประมวลกฎหมายอาญา มาตรา 341 ผู้ใดโดยทุจริตหลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดความจริงที่ควรบอกแล้วได้ไปซึ่งทรัพย์สินของบุคคลนั้นหรือบุคคลที่สามหรือทำให้บุคคลนั้นหรือบุคคลที่สามเสียทรัพย์สินผู้นั้นกระทำความผิดฐานฉ้อโกง ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกพันบาท หรือทั้งจำทั้งปรับ

มาตรา 267-269[224] การปลอมแปลงเอกสารและใช้เอกสารปลอมใช้กับการปลอมหนังสือราชการ แจ้งบัญชีธนาคารปลอม หรือสำเนาหนังสือแจ้งความเท็จ

มาตรา 343[225] ความผิดฐานฉ้อโกงประชาชนเพิ่มโทษในกรณีที่ผู้กระทำความผิดกระทำต่อประชาชนจำนวนมาก

3. พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 แก๊งคอลเซ็นเตอร์มักมีการเคลื่อนย้ายเงินอย่างซับซ้อน ทั้งในและนอกประเทศ โดยใช้บัญชีม้าหรือผู้รับโอนเงินแทน ดังนั้น พ.ร.บ. นี้จึงถูกใช้ในการตรวจสอบเส้นทางการเงินและดำเนินคดีฟอกเงิน

มาตรา 3 และ 5[226] กำหนดความผิดฐานฟอกเงิน รวมถึงการแปลงสภาพทรัพย์สินที่ได้จากการกระทำความผิดอาญา เช่น การโอนเงินระหว่างบัญชี การถอนเงินเพื่อโอนไปต่างประเทศ

---

[224] ประมวลกฎหมายอาญา มาตรา 267 ผู้ใดแสดงข้อความอันเป็นเท็จต่อเจ้าพนักงาน ซึ่งอาจทำให้ผู้อื่นหรือประชาชนเสียหายหรือเพื่อให้เจ้าพนักงานกระทำหรืองดเว้นการกระทำอย่างใดในหน้าที่ต้องระวาง โทษจำคุกไม่เกินหกเดือนหรือปรับไม่เกินหนึ่งพันบาทหรือทั้งจำทั้งปรับ

มาตรา 269 ผู้ใดยื่นเอกสารหรือหลักฐานอันเป็นเท็จต่อเจ้าพนักงานต้องระวาง โทษเช่นเดียวกับมาตรา 267

มาตรา 269 ผู้ใดทำปลอมเอกสารราชการหรือเอกสารอื่นใดที่เจ้าพนักงานออกให้หรือใช้ในการปฏิบัติราชการ หรือใช้เอกสารปลอมนั้น ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งหมื่นบาทหรือทั้งจำทั้งปรับ

[225] ประมวลกฎหมายอาญา มาตรา 343 ถ้าการกระทำความผิดตามมาตรา 341 ได้กระทำโดย

(1) แสดงตนเป็นบุคคลอื่น

(2) อาศัยเหตุที่ประชาชนหลงเชื่อว่าผู้กระทำเป็นบุคคลอื่น

ผู้กระทำต้องระวางโทษ จำคุกไม่เกินห้าปี และปรับไม่เกินหนึ่งแสนบาท

[226] พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 3 ในพระราชบัญญัตินี้ “ความผิดมูลฐาน” หมายความว่า

(1) ความผิดเกี่ยวกับยาเสพติด ตามกฎหมายว่าด้วยการป้องกันและปราบปรามยาเสพติด หรือกฎหมายว่าด้วยมาตรการในการปราบปรามผู้กระทำความผิดเกี่ยวกับยาเสพติด

(2) ความผิดเกี่ยวกับการค้ามนุษย์ ตามกฎหมายว่าด้วยการป้องกันและปราบปรามการค้ามนุษย์ หรือความผิดตามประมวลกฎหมายอาญาในความผิดเกี่ยวกับเพศ เฉพาะที่เกี่ยวกับการเป็นธุระจัดหา ล่อไป พาไป หรือรับไว้เพื่อการอนาจาร ซึ่งชายหรือหญิง เพื่อสนองความใคร่ของผู้อื่น หรือความผิดฐานพรากเด็กและผู้เยาว์ เฉพาะที่เกี่ยวกับการกระทำเพื่อหากำไรหรือเพื่ออนาจาร หรือโดยทุจริต ซื้อจำหน่าย หรือรับตัวเด็กหรือผู้เยาว์ซึ่งถูกพรากนั้น หรือความผิดตามกฎหมายว่าด้วยการป้องกันและปราบปรามการค้าประเวณี เฉพาะที่เกี่ยวกับการเป็นธุระจัดหา ล่อไป หรือชักพาไปเพื่อให้บุคคลนั้นกระทำการค้าประเวณี หรือที่เกี่ยวกับการเป็นเจ้าของกิจการการค้าประเวณี ผู้ดูแลหรือผู้จัดการกิจการค้าประเวณี หรือสถานการค้าประเวณี หรือเป็นผู้ควบคุมผู้กระทำการค้าประเวณีในสถานการค้าประเวณี

(3) ความผิดเกี่ยวกับการฉ้อโกงประชาชน ตามประมวลกฎหมายอาญา หรือความผิดตามกฎหมายว่าด้วยการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน

(4) ความผิดเกี่ยวกับการยักยอกหรือฉ้อโกงหรือประทุษร้ายต่อทรัพย์ หรือกระทำโดยทุจริตตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน หรือกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์ ซึ่งกระทำโดยกรรมการ หรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบหรือมีประโยชน์เกี่ยวข้องในการดำเนินงานของสถาบันการเงินนั้น

(5) ความผิดต่อตำแหน่งหน้าที่ราชการ หรือความผิดต่อตำแหน่งหน้าที่ในการยุติธรรม ตามประมวลกฎหมายอาญา ความผิดตามกฎหมายว่าด้วยความผิดของพนักงานในองค์การหรือหน่วยงานของรัฐ หรือความผิดต่อตำแหน่งหน้าที่หรือทุจริตต่อหน้าที่ตามกฎหมายอื่น

(6) ความผิดเกี่ยวกับการกรรโชก หรือรีดเอาทรัพย์ ที่กระทำโดยอ้างอำนาจอั้งยี่หรือซ่องโจร ตามประมวลกฎหมายอาญา

(7) ความผิดเกี่ยวกับการลักลอบหนีศุลกากร ตามกฎหมายว่าด้วยศุลกากร

(8) ความผิดเกี่ยวกับการก่อการร้าย ตามประมวลกฎหมายอาญา

(9) ความผิดเกี่ยวกับการพนัน ตามกฎหมายว่าด้วยการพนัน เฉพาะความผิดเกี่ยวกับการเป็นผู้จัดให้มีการเล่นการพนันโดยไม่ได้รับอนุญาต โดยมีวงเงินในการกระทำความผิดรวมกันมีมูลค่าตั้งแต่ห้าล้านบาทขึ้นไป หรือเป็นการจัดให้มีการเล่นการพนันทางสื่ออิเล็กทรอนิกส์

(10) ความผิดเกี่ยวกับการเป็นสมาชิกอั้งยี่ ตามประมวลกฎหมายอาญา หรือการมีส่วนร่วมในองค์กรอาชญากรรม ที่มีกฎหมายกำหนดเป็นความผิด

(11) ความผิดเกี่ยวกับการรับของโจร ตามประมวลกฎหมายอาญา เฉพาะที่เกี่ยวกับการช่วยจำหน่าย ซื้อ รับจำนำ หรือรับไว้ด้วยประการใดซึ่งทรัพย์ที่ได้มาโดยการกระทำความผิดอันมีลักษณะเป็นการค้า

(12) ความผิดเกี่ยวกับการปลอมหรือการแปลงเงินตรา ดวงตรา แสตมป์ และตั๋ว ตามประมวลกฎหมายอาญา อันมีลักษณะเป็นการค้า

(13) ความผิดเกี่ยวกับการค้าตามประมวลกฎหมายอาญา เฉพาะที่เกี่ยวกับการปลอม หรือการละเมิดทรัพย์สินทางปัญญาของสินค้า หรือความผิดตามกฎหมายที่เกี่ยวกับการคุ้มครองทรัพย์สินทางปัญญาอันมีลักษณะเป็นการค้า

(14) ความผิดเกี่ยวกับการปลอมเอกสารสิทธิ บัตรอิเล็กทรอนิกส์ หรือหนังสือเดินทาง ตามประมวลกฎหมายอาญา อันมีลักษณะเป็นปกติธุระหรือเพื่อการค้า

(15) ความผิดเกี่ยวกับทรัพยากรธรรมชาติหรือสิ่งแวดล้อม โดยการใช้ ยึดถือ หรือครอบครองทรัพยากรธรรมชาติ หรือกระบวนการแสวงหาประโยชน์จากทรัพยากรธรรมชาติโดยมิชอบด้วยกฎหมาย อันมีลักษณะเป็นการค้า

(16) ความผิดเกี่ยวกับการประทุษร้ายต่อชีวิตหรือร่างกายจนเป็นเหตุให้เกิดอันตรายสาหัส ตามประมวลกฎหมายอาญา เพื่อให้ได้ประโยชน์ซึ่งทรัพย์สิน

(17) ความผิดเกี่ยวกับการหน่วงเหนี่ยวหรือกักขังผู้อื่น ตามประมวลกฎหมายอาญา เฉพาะกรณีเพื่อเรียกหรือรับผลประโยชน์ หรือเพื่อต่อรองให้ได้รับผลประโยชน์อย่างใดอย่างหนึ่ง

*(ทั้งนี้ “การฉ้อโกงประชาชน” ซึ่งเกี่ยวข้องกับแก๊งคอลเซ็นเตอร์ ถือเป็นหนึ่งในความผิดมูลฐานตามภาคผนวกของ พ.ร.บ. นี้)*

มาตรา 21 และ 40[227] ให้อำนาจสำนักงาน ปปง. ในการตรวจสอบ บล็อกบัญชี หรือยึดทรัพย์ที่เกี่ยวข้องกับอาชญากรรมได้

4. พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

มาตรา 4[228] กำหนดให้ สถาบันการเงิน, ผู้ให้บริการชำระเงิน และผู้ให้บริการโทรคมนาคม ต้องจัดให้มีระบบแลกเปลี่ยนข้อมูลบัญชีและธุรกรรมทันทีเมื่อมีเหตุสงสัยด้านอาชญากรรมทางเทคโนโลยี

---

มาตรา 5 ผู้ใด

(1) โอน รับโอน หรือเปลี่ยนสภาพทรัพย์สินที่เกี่ยวกับการกระทำความผิด เพื่อซุกซ่อนหรือปกปิดแหล่งที่มาของทรัพย์สินนั้น หรือเพื่อช่วยเหลือผู้อื่นไม่ว่าก่อน ขณะ หรือหลังการกระทำความผิด มิให้ต้องรับโทษหรือรับโทษน้อยลงในความผิดมูลฐาน หรือ

(2) กระทำด้วยประการใด ๆ เพื่อปกปิดหรืออำพรางลักษณะที่แท้จริง การได้มา แหล่งที่ตั้ง การจำหน่าย การโอน หรือการได้สิทธิใด ๆ ซึ่งทรัพย์สินที่เกี่ยวกับการกระทำความผิด หรือ

(3) ได้มา ครอบครอง หรือใช้ทรัพย์สิน โดยรู้ในขณะที่ได้มา ครอบครอง หรือใช้ทรัพย์สินนั้นว่าเป็นทรัพย์สินที่เกี่ยวกับการกระทำความผิด

ผู้นั้นกระทำความผิดฐานฟอกเงิน

[227] พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 21 ในกรณีที่มีเหตุอันควรสงสัยว่าทรัพย์สินใดเป็นทรัพย์สินที่เกี่ยวกับการกระทำความผิด หรือเป็นทรัพย์สินที่เกี่ยวกับการกระทำความผิดมูลฐาน ให้พนักงานเจ้าหน้าที่มีอำนาจยึดหรืออายัดทรัพย์สินนั้นไว้ชั่วคราวได้ไม่เกินเก้าสิบวัน และให้รายงานต่อคณะกรรมการธุรกรรมโดยไม่ชักช้า เพื่อพิจารณาดำเนินการตามมาตรา 48 ต่อไป

มาตรา 40 ในกรณีที่คณะกรรมการธุรกรรมมีคำสั่งให้ยึดหรืออายัดทรัพย์สินตามมาตรา 48 วรรคหนึ่ง และพนักงานอัยการได้ยื่นคำร้องต่อศาลเพื่อขอให้ทรัพย์สินนั้นตกเป็นของแผ่นดินตามมาตรา 49 แล้ว หากศาลมีคำสั่งให้ทรัพย์สินตกเป็นของแผ่นดิน ให้สำนักงานดำเนินการตามคำสั่งศาลนั้น และหากมีผู้เสียหายจากการกระทำความผิดมูลฐาน ให้สำนักงานแจ้งให้ผู้เสียหายทราบถึงสิทธิในการยื่นคำร้องขอรับชดใช้ค่าเสียหายจากทรัพย์สินที่ตกเป็นของแผ่นดินนั้นภายในระยะเวลาที่กำหนดโดยกฎหมาย

[228] พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาตรา 4 เพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ในกรณีที่มีเหตุอันควรสงสัยว่า มีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยี ให้สถาบันการเงินและผู้ประกอบธุรกิจ มีหน้าที่เปิดเผยหรือแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้าที่เกี่ยวข้องในระหว่าง สถาบันการเงินและผู้ประกอบธุรกิจนั้นผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูล ที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน และธนาคารแห่งประเทศไทย เห็นชอบร่วมกัน

มาตรา 6 วรรคหนึ่ง[229] ให้อำนาจแก่สถาบันการเงินและผู้ให้บริการทางการเงินในการระงับการใช้บัญชีชั่วคราว หากมีเหตุอันควรเชื่อว่าบัญชีนั้นเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี เช่น บัญชีม้า โดยไม่ต้องรอคำสั่งศาล ถือเป็นมาตรการเชิงป้องกันเพื่อสกัดกั้นการโอนเงินไปยังเครือข่ายอาชญากรรมก่อนทันเวลา

มาตรา 7[230] ผู้เสียหายสามารถแจ้งร้องขอให้ธนาคารระงับบัญชีภายใน 72 ชั่วโมง และธนาคารต้องแจ้งความกับเจ้าหน้าที่ภายใน 7 วัน

---

เพื่อดำเนินการตามวัตถุประสงค์ตามวรรคหนึ่ง ให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการ โทรคมนาคมอื่น หรือผู้ให้บริการอื่นที่เกี่ยวข้องมีหน้าที่เปิดเผยหรือแลกเปลี่ยนข้อมูลการให้บริการ ที่เกี่ยวข้องระหว่างกันผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลที่กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคมและสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เห็นชอบร่วมกัน

เมื่อมีการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามวรรคหนึ่งหรือวรรคสองแล้ว ให้ผู้เปิดเผย หรือแลกเปลี่ยนข้อมูลแจ้งให้สำนักงานตำรวจแห่งชาติหรือกรมสอบสวนคดีพิเศษแล้วแต่กรณี และสำนักงานป้องกันและปราบปรามการฟอกเงิน ทราบโดยทันที และเมื่อได้รับแจ้งแล้ว ให้สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ หรือสำนักงานป้องกันและปราบปรามการฟอกเงิน แล้วแต่กรณี มีอำนาจนำข้อมูลดังกล่าวไปใช้ประโยชน์เพื่อป้องกันปราบปราม หรือระงับอาชญากรรมทางเทคโนโลยีได้

[229] มาตรา 6 วรรคหนึ่ง ในกรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจพบเหตุอันควรสงสัยเองหรือได้รับข้อมูลจากระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามมาตรา 4 ว่าบัญชีเงินฝากหรือ บัญชีเงินอิเล็กทรอนิกส์ใดถูกใช้หรืออาจถูกใช้ทำธุรกรรมที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี หรือการกระท าความผิดมูลฐานหรือความผิดฐานฟอกเงินตามกฎหมายว่าด้วยการป้องกันและปราบปราม การฟอกเงิน ให้สถาบันการเงินหรือผู้ประกอบธุรกิจมีหน้าที่ระงับการทeธุรกรรมและแจ้งสถาบันการเงิน หรือผู้ประกอบธุรกิจที่รับโอนถัดไป พร้อมทั้งนำข้อมูลเข้าสู่ระบบหรือกระบวนการเปิดเผยหรือ แลกเปลี่ยนข้อมูลตามมาตรา 4 เพื่อให้สถาบันการเงินและผู้ประกอบธุรกิจผู้รับโอนทุกทอดทราบ และระงับการทำธุรกรรมดังกล่าวไว้ทันทีเป็นการชั่วคราวไม่เกินเจ็ดวันนับแต่วันที่พบเหตุอันควรสงสัย หรือได้รับแจ้ง แล้วแต่กรณี เพื่อตรวจสอบความถูกต้องแท้จริงและแจ้งให้เจ้าพนักงานผู้มีอำนาจ

[230] มาตรา 7 ในกรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจได้รับแจ้งจากผู้เสียหาย ซึ่งเป็นผู้ถือบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ว่า ได้มีการทำธุรกรรมโดยบัญชีเงินฝากหรือ บัญชีเงินอิเล็กทรอนิกส์ดังกล่าวและเข้าข่ายเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี ให้สถาบันการเงิน หรือผู้ประกอบธุรกิจดังกล่าวมีหน้าที่ระงับการทำธุรกรรมนั้นไว้ชั่วคราว พร้อมทั้งนำข้อมูลเข้าสู่ระบบ หรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามมาตรา 4 เพื่อให้สถาบันการเงินและผู้ประกอบธุรกิจ ผู้รับโอนทุกทอดทราบและระงับการทำธุรกรรมดังกล่าวไว้ทันที และแจ้งให้ผู้เสียหายไปร้องทุกข์ ต่อพนักงานสอบสวนภายในเจ็ดสิบสองชั่วโมง เมื่อมีการร้องทุกข์แล้ว ให้พนักงานสอบสวนแจ้งให้ สถาบันการเงินหรือผู้ประกอบธุรกิจที่ได้รับการทำธุรกรรมไว้ทราบ และให้พนักงานสอบสวนพิจารณาดำเนินการเกี่ยวกับบัญชีเงินฝากและบัญชีเงินอิเล็กทรอนิกส์ดังกล่าวภายในเจ็ดวันนับแต่วันที่ได้รับ แจ้งความร้องทุกข์ หากไม่มีคำสั่งให้ระงับการทำธุรกรรมไว้ต่อไปภายในเวลาดังกล่าว ให้สถาบันการเงิน หรือผู้ประกอบธุรกิจยกเลิกการระงับการทำธุรกรรมนั้น

มาตรา 8[231] การแจ้งเหตุผ่านโทรศัพท์หรือระบบอิเล็กทรอนิกส์มีผลเทียบเท่าการแจ้งเป็นหนังสือ เพื่ออำนวยความสะดวกรวดเร็วในการดำเนินการ

5. พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 เป็นการแก้ไขเพิ่มเติมจากฉบับปี 2566 โดยมีเจตนารมณ์เพื่อขยายขอบเขตการคุ้มครองผู้เสียหายให้มากขึ้น เพิ่มความชัดเจนในภาระหน้าที่ของผู้ให้บริการทางการเงิน และเร่งรัดกระบวนการในการอายัด ปิดกั้น และคืนเงิน ให้ผู้เสียหายจากอาชญากรรมทางเทคโนโลยี โดยมีประเด็นสำคัญดังนี้

มาตรา 6/1 (เพิ่มเติมใหม่) กำหนดให้ธนาคารและผู้ให้บริการทางการเงินต้องดำเนินการตรวจสอบและ “ดึงเงินคืน” ให้ผู้เสียหายภายใน 3 วันทำการ นับแต่วันที่ได้รับแจ้งหากมีหลักฐานเพียงพอว่าเงินดังกล่าวเป็นผลจากการกระทำความผิด เช่น การหลอกลวงออนไลน์หรือการโอนเข้า “บัญชีม้า”

มาตรา 6/2 และ 6/3 เพิ่มเติมกลไกการร้องขอคืนเงินผ่านระบบกลางซึ่งเชื่อมโยงข้อมูลกับหน่วยงานรัฐ เช่น สำนักงานตำรวจแห่งชาติ และสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) เพื่อให้สามารถดำเนินการคืนเงินอย่างมีประสิทธิภาพ โดยไม่ต้องรอคำพิพากษาของศาลในทุกกรณี

แม้ประเทศไทยจะมีกฎหมายหลายฉบับที่สามารถนำมาใช้ในการดำเนินคดีกับขบวนการแก๊งคอลเซ็นเตอร์ ไม่ว่าจะเป็นประมวลกฎหมายอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (แก้ไขเพิ่มเติม พ.ศ. 2560) และพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 แต่ในทางปฏิบัติยังปรากฏข้อจำกัดหลายประการที่สะท้อนถึงปัญหาเชิงโครงสร้างและการบังคับใช้กฎหมายที่ยังไม่สอดรับกับลักษณะเฉพาะของอาชญากรรมข้ามชาติในยุคดิจิทัล ปัญหาสำคัญประการหนึ่ง คือ การบังคับใช้กฎหมายยังไม่สามารถครอบคลุมพฤติกรรมของแก๊งคอลเซ็นเตอร์ที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว โดยเฉพาะการใช้

---

[231] มาตรา 8 การแจ้งข้อมูลหรือหลักฐานตามมาตรา 6 และมาตรา 7 จะกระทำทางโทรศัพท์ หรือวิธีการทางอิเล็กทรอนิกส์ก็ได้ ในกรณีที่กระทำทางโทรศัพท์ ให้ผู้ได้รับแจ้งบันทึกไว้เป็นลายลักษณ์อักษร ลงลายมือชื่อผู้รับแจ้งและวันเวลาที่ได้รับไว้เป็นหลักฐาน พร้อมทั้งส่งสำเนาให้ผู้แจ้งเก็บไว้เป็นหลักฐานด้วย

การร้องทุกข์ในความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีจะกระทำต่อพนักงานสอบสวน ณ สถานีตำรวจแห่งใดในราชอาณาจักรหรือต่อกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรม ทางเทคโนโลยีก็ได้ และจะร้องทุกข์โดยวิธีการทางอิเล็กทรอนิกส์ก็ได้ โดยให้ถือว่าเป็นการร้องทุกข์ โดยชอบด้วยประมวลกฎหมายวิธีพิจารณาความอาญา และในการสอบสวนหรือดำเนินการเกี่ยวกับการกระทำความผิดดังกล่าว ให้พนักงานสอบสวนที่รับคำร้องทุกข์ไม่ว่าประจำอยู่ที่ใดหรือพนักงานสอบสวน ที่ผู้บัญชาการตำรวจแห่งชาติกำหนดเป็นพนักงานสอบสวนผู้รับผิดชอบมีอำนาจสอบสวนและดำเนินการเกี่ยวกับการกระทำความผิดดังกล่าวได้ไม่ว่าความผิดนั้นจะเกิดขึ้น ณ ที่ใดในราชอาณาจักร

เทคโนโลยีสมัยใหม่เป็นเครื่องมือในการหลอกลวงผู้เสียหาย กฎหมายที่มีอยู่ในปัจจุบัน เช่น มาตรา 341 แห่งประมวลกฎหมายอาญา ซึ่งบัญญัติความผิดฐานฉ้อโกง รวมถึงมาตรา 343 ที่เกี่ยวกับการฉ้อโกงประชาชน ยังมีขอบเขตที่จำกัดและไม่สามารถอธิบายพฤติกรรมใหม่ ๆ ได้อย่างครอบคลุมโดยชัดแจ้ง ยิ่งไปกว่านั้น การแยกบทบัญญัติกฎหมายออกจากกันตามลักษณะความผิด เช่น การกระทำความผิดทางเทคโนโลยีใน พ.ร.บ.คอมพิวเตอร์และการฟอกเงินใน พ.ร.บ.ฟอกเงิน ทำให้กระบวนการดำเนินคดีในแต่ละกรณีขาดความเชื่อมโยงกันและซับซ้อนในการบูรณาการข้อมูล ซึ่งไม่เอื้อต่อการแกะรอยเส้นทางของผู้กระทำความผิดที่มักมีลักษณะเป็นเครือข่ายข้ามประเทศ นอกจากนี้ กฎหมายไทยยังขาดกลไกทางกฎหมายที่รองรับการดำเนินคดีต่อองค์กรอาชญากรรมข้ามชาติอย่างชัดเจน แม้ประเทศไทยจะเป็นภาคีของอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมข้ามชาติ (United Nations Convention against Transnational Organized Crime - UNTOC) แต่ยังไม่มีการตรากฎหมายภายในที่นิยาม “องค์กรอาชญากรรมข้ามชาติ” และวางมาตรการในการเอาผิดกับผู้นำหรือผู้มีส่วนร่วมในเครือข่ายอาชญากรรมดังกล่าวโดยตรง ซึ่งเป็นข้อจำกัดสำคัญในการติดตามและดำเนินคดีกับ “ผู้อยู่เบื้องหลัง” ที่มักไม่ปรากฏตัวในประเทศไทย อีกประเด็นที่เป็นปัญหาสำคัญคือข้อจำกัดของอำนาจศาลในคดีที่ผู้กระทำผิดอาศัยอยู่ในต่างประเทศแต่มีการกระทำความผิดต่อผู้เสียหายที่อยู่ในประเทศไทย แม้ว่าจะมีหลักเขตอำนาจศาลตามสถานที่ที่ผลเกิดแต่อำนาจในการดำเนินคดีอาญาข้ามเขตแดนของรัฐยังเป็นข้อจำกัดตามหลักอธิปไตยของแต่ละประเทศ การที่กฎหมายไทยยังไม่มีบทบัญญัติที่รองรับการขยายเขตอำนาจศาลสำหรับอาชญากรรมไซเบอร์ที่เกิดจากต่างประเทศอย่างชัดเจน ส่งผลให้การดำเนินคดีต้องพึ่งพากระบวนการส่งผู้ร้ายข้ามแดนหรือความร่วมมือระหว่างรัฐ ซึ่งใช้เวลานานและมีข้อจำกัดในเชิงปฏิบัติอย่างมาก สุดท้าย แม้พระราชบัญญัติป้องกันและปราบปรามการฟอกเงินจะให้ความสำคัญกับการยึดและอายัดทรัพย์สินที่ได้มาจากการกระทำผิด แต่มาตรการดังกล่าวยังไม่สามารถนำมาใช้ได้อย่างมีประสิทธิภาพในกรณีที่ผู้กระทำผิดใช้เทคนิคซับซ้อน เช่น การใช้บัญชีม้า (บัญชีผู้อื่น) หรือการเคลื่อนย้ายเงินผ่านสินทรัพย์ดิจิทัล (cryptocurrency) ซึ่งยังไม่อยู่ภายใต้การกำกับดูแลอย่างเข้มงวด ยิ่งไปกว่านั้น การคืนทรัพย์สินให้กับผู้เสียหายยังคงเป็นไปได้ยาก เนื่องจากกระบวนการพิสูจน์และการบริหารจัดการทรัพย์ที่มีความซับซ้อน จากสภาพปัญหาดังกล่าวสะท้อนให้เห็นว่ากฎหมายของไทยแม้จะมีอยู่ในหลากหลายฉบับ แต่ยังไม่มีความพร้อมอย่างเป็นระบบในการเผชิญกับลักษณะของอาชญากรรมข้ามชาติในยุคปัจจุบัน

4.3.2.2 ประเทศฟิลลิปปินส์

ประเทศฟิลิปปินส์มีบทบัญญัติกฎหมายหลายฉบับที่เกี่ยวข้องกับการปราบปรามอาชญากรรมคอลเซ็นเตอร์ ซึ่งส่วนใหญ่อยู่ในกลุ่มของกฎหมายอาญาและกฎหมายว่าด้วยอาชญากรรมทางไซเบอร์ โดยกฎหมายหลักที่เกี่ยวข้อง ได้แก่

Republic Act No. 10175 หรือ Cybercrime Prevention Act of 2012 ซึ่งเป็นกฎหมายที่กำหนดความผิดเกี่ยวกับการเข้าถึงระบบโดยมิชอบ การฉ้อโกงทางอิเล็กทรอนิกส์ (Computer-related Fraud) การขโมยข้อมูลประจำตัว (Identity Theft) และการดักฟังหรือเข้าถึงการติดต่อสื่อสารโดยไม่ได้รับอนุญาต (Cyber Espionage)

มาตรา 4[232] กำหนดความผิดทางอาญาทางไซเบอร์ที่เกี่ยวข้องกับพฤติกรรมของแก๊งคอลเซ็นเตอร์

---

[232] Republic Act No. 10175

Article 4. *Cybercrime Offenses.* — The following acts constitute the offense of cybercrime punishable under this Act:

(a) Offenses against the confidentiality, integrity and availability of computer data and systems:

(1) Illegal Access. – The access to the whole or any part of a computer system without right.

(2) Illegal Interception. – The interception made by technical means without right of any non-public transmission of computer data to, from, or within a computer system including electromagnetic emissions from a computer system carrying such computer data.

(3) Data Interference. — The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses.

(4) System Interference. — The intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses.

(5) Misuse of Devices.

(i) The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:

(aa) A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this Act; or

(bb) A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under this Act.

(ii) The possession of an item referred to in paragraphs 5(i)(aa) or (bb) above with intent to use said devices for the purpose of committing any of the offenses under this section.

(6) Cyber-squatting. – The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:

(i) Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration:

(ii) Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and

(iii) Acquired without right or with intellectual property interests in it.

(b) Computer-related Offenses:

(1) Computer-related Forgery. —

(i) The input, alteration, or deletion of any computer data without right resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible; or

(ii) The act of knowingly using computer data which is the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design.

(2) Computer-related Fraud. — The unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent: *Provided,* That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

(3) Computer-related Identity Theft. – The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right: *Provided,* That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

(c) Content-related Offenses:

(1) Cybersex. — The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.

( 2) Child Pornography. — The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system: Provided, That the penalty to be imposed shall be (1) one degree higher than that provided for in Republic Act No. 9775.*1âwphi1*

(3) Unsolicited Commercial Communications. — The transmission of commercial electronic communication with the use of computer system which seek to advertise, sell, or offer for sale products and services are prohibited unless:

มาตรา 6[233] มาตรานี้ระบุว่า ความผิดใด ๆ ที่กำหนดไว้ในประมวลกฎหมายอาญา หรือกฎหมายพิเศษอื่น ๆ หากกระทำผ่านเทคโนโลยีสารสนเทศและการสื่อสาร จะอยู่ภายใต้บทบัญญัติของกฎหมายนี้ด้วย ดังนั้น หากแก๊งคอลเซ็นเตอร์กระทำความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญา แต่ใช้เทคโนโลยีในการกระทำความผิดก็จะถูกดำเนินคดีภายใต้กฎหมายนี้เช่นกัน

มาตรา 7 [234]ระบุว่า การดำเนินคดีภายใต้กฎหมายนี้ ไม่ขัดขวางการดำเนินคดีภายใต้กฎหมายอื่น ๆ ที่เกี่ยวข้อง ซึ่งหมายความว่า ผู้กระทำความผิดสามารถถูกดำเนินคดีภายใต้หลายกฎหมายพร้อมกันได้ หากการกระทำของเขาเข้าข่ายความผิดตามกฎหมายเหล่านั้น

---

(i) There is prior affirmative consent from the recipient; or

(ii) The primary intent of the communication is for service and/or administrative announcements from the sender to its existing users, subscribers or customers; or

(iii) The following conditions are present:

(aa) The commercial electronic communication contains a simple, valid, and reliable way for the recipient to reject. receipt of further commercial electronic messages (opt-out) from the same source;

(bb) The commercial electronic communication does not purposely disguise the source of the electronic message; and

(cc) The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

(4) Libel. — The unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future.

[233] Article 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act: *Provided,* That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

[234] Article 7. *Liability under Other Laws.* — A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws.

มาตรา 12[235] มาตรานี้ให้อำนาจแก่เจ้าหน้าที่ในการเก็บรวบรวมข้อมูลการจราจรทางคอมพิวเตอร์แบบเรียลไทม์ เพื่อใช้ในการสืบสวนและดำเนินคดี ซึ่งเป็นเครื่องมือสำคัญในการติดตามและจับกุมแก๊งคอลเซ็นเตอร์ที่ใช้เทคโนโลยีในการกระทำความผิด

แม้ว่า Republic Act No. 10175 จะถือเป็นกฎหมายลำดับต้น ๆ ในภูมิภาคเอเชียตะวันออกเฉียงใต้ที่ออกมาเพื่อรับมือกับภัยคุกคามจากโลกไซเบอร์โดยตรง และมีบทบัญญัติที่ครอบคลุมการกระทำความผิดไซเบอร์หลากหลายประเภท เช่น การเข้าถึงระบบโดยมิชอบ (Illegal Access), การฉ้อโกงผ่านคอมพิวเตอร์ (Computer-related Fraud), และการขโมยข้อมูลระบุตัวตน (Identity Theft) ซึ่งมีความเกี่ยวข้องโดยตรงกับการดำเนินงานของแก๊งคอลเซ็นเตอร์ ทว่าในทางปฏิบัติกลับพบว่าประเทศฟิลิปปินส์ยังคงเผชิญกับอุปสรรคสำคัญในการบังคับใช้กฎหมายดังกล่าวอย่างมีประสิทธิภาพ หนึ่งในปัญหาหลักที่สังเกตได้ชัด คือ ความไม่ชัดเจนของนิยามบางประการในกฎหมาย โดยเฉพาะในมาตรา 4 ที่ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งระบุพฤติการณ์แบบกว้างมากเกินไป ทำให้เกิดช่องว่างในการตีความและบังคับใช้ เช่น การกำหนดความผิดฐาน “Computer-related Fraud” แม้จะครอบคลุมการหลอกลวงในลักษณะเดียวกับการฉ้อโกงผ่านโทรศัพท์หรือสื่ออิเล็กทรอนิกส์ แต่กลับไม่ได้ระบุลักษณะเฉพาะของการหลอกลวงเชิงองค์กรข้ามชาติอย่าง “แก๊งคอลเซ็นเตอร์” ไว้อย่างชัดเจน ส่งผลให้เจ้าหน้าที่รัฐอาจไม่สามารถเชื่อมโยงการกระทำของผู้กระทำผิดกับบทบัญญัติของกฎหมายนี้ได้อย่างตรงประเด็นหรือทำให้การตั้งข้อกล่าวหาในทางคดีต้องพึ่งพากฎหมายอาญาทั่วไป ซึ่งไม่สอดคล้องกับรูปแบบอาชญากรรมยุคใหม่ที่ใช้เทคโนโลยีเป็น

---

[235] Article 12. *Real-Time Collection of Traffic Data.* — Law enforcement authorities, with due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system.

Traffic data refer only to the communication’s origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities.

All other data to be collected or seized or disclosed will require a court warrant.

Service providers are required to cooperate and assist law enforcement authorities in the collection or recording of the above-stated information.

The court warrant required under this section shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce and the showing: (1) that there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, or is being committed, or is about to be committed: (2) that there are reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and (3) that there are no other means readily available for obtaining such evidence.

เครื่องมือหลัก อีกประเด็นที่ควรวิพากษ์ คือ การที่กฎหมายไซเบอร์ของฟิลิปปินส์ยังคงให้ความสำคัญกับการควบคุม “เนื้อหา” (content-based control) มากกว่าการจัดการกับ “องค์กรอาชญากรรม” ที่อยู่เบื้องหลังการกระทำผิด เช่น การควบคุมการหมิ่นประมาททางออนไลน์ (Cyber Libel) ซึ่งแม้จะมีความสำคัญในแง่สิทธิมนุษยชนและศักดิ์ศรีบุคคล แต่กลับทำให้ทรัพยากรในการบังคับใช้กฎหมายถูกเบี่ยงเบนไปจากเป้าหมายหลักในการปราบปรามอาชญากรรมไซเบอร์เชิงเศรษฐกิจอย่างกรณีแก๊งคอลเซ็นเตอร์ นอกจากนี้ แม้ในมาตรา 6 จะระบุว่า หากมีการกระทำผิดตามประมวลกฎหมายอาญาหรือกฎหมายอื่น ๆ ผ่านช่องทางเทคโนโลยีก็จะถูกพิจารณาเป็นความผิดตามกฎหมายฉบับนี้ด้วย ทว่ากระบวนการนำความผิดอื่น ๆ เข้ามาผูกโยงกับการกระทำความผิดไซเบอร์ในทางคดี ยังขาดแนวปฏิบัติที่ชัดเจน ส่งผลให้การดำเนินคดีล่าช้าและทำให้ผู้กระทำผิดบางรายหลุดพ้นจากกระบวนการยุติธรรม

4.3.2.3 ประเทศมาเลเซีย

ในช่วงไม่กี่ปีที่ผ่านมา มาเลเซียได้เผชิญกับการเพิ่มขึ้นของอาชญากรรมไซเบอร์อย่างมีนัยสำคัญ โดยเฉพาะอย่างยิ่งการหลอกลวงทางโทรศัพท์หรือที่เรียกว่า “แก๊งคอลเซ็นเตอร์” ซึ่งมักแฝงตัวอยู่ในประเทศเพื่อนบ้านและใช้เทคโนโลยีสื่อสารในการหลอกลวงประชาชน[236] เพื่อตอบสนองอาชญากรรมดังกล่าวรัฐมาเลเซียได้มีการออกกฎหมายหลายฉบับที่เกี่ยวข้อง แม้จะไม่ได้บัญญัติเฉพาะเจาะจงว่าเป็นแก๊งคอลเซ็นเตอร์ แต่มีบทบัญญัติที่สามารถนำมาใช้จัดการกับพฤติกรรมเหล่านี้ได้โดยตรงหรือโดยอ้อม ดังนี้

1. Communications and Multimedia Act 1998 (CMA 1998) เป็นกฎหมายหลักที่ใช้ควบคุมพฤติกรรมบนระบบสื่อสารและอินเทอร์เน็ตในประเทศมาเลเซีย

มาตรา 233[237] ห้ามไม่ให้บุคคลใช้บริการเครือข่ายเพื่อวัตถุประสงค์ที่ไม่เหมาะสม รวมถึงการสื่อสารที่หลอกลวง ข่มขู่ คุกคาม หรือสร้างความเดือดร้อนโดยไม่มีเหตุอันควร โดยมีโทษ

---

[236] ‘Understanding Malaysia’s Cyber Threat Landscape: A 2025 Outlook’ (Security Quotient, 20 February 2025) <https://securityquotient.io/understanding-malaysias-cyber-threat-landscape-a-2025-outlook/> accessed 10 March 2025.

[237] Communications and Multimedia Act 1998

Article 233

(1) A person who—

(a) by means of any network facilities or network service or applications service knowingly—

(i) makes, creates or solicits; and

จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 50,000 ริงกิต หรือทั้งจำทั้งปรับ และปรับเพิ่มเติมอีกไม่เกิน 1,000 ริงกิตต่อวัน หากยังไม่หยุดกระทำ ซึ่งมาตรานี้มักถูกนำมาใช้จัดการกับกลุ่มผู้กระทำความผิดที่ส่งข้อความหลอกลวงทางโทรศัพท์หรือออนไลน์ เช่น การแอบอ้างเป็นเจ้าหน้าที่รัฐ แจ้งเหยื่อให้โอนเงิน ฯลฯ

2. Computer Crimes Act 1997 (CCA 1997) เป็นกฎหมายหลักในการควบคุมการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบและการกระทำความผิดที่เกี่ยวข้องกับระบบข้อมูล

มาตรา 3[238] ผู้ใดเข้าถึงข้อมูลในระบบคอมพิวเตอร์โดยไม่มีสิทธิถือว่ามีความผิด

---

(ii) initiates the transmission of, any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person; or

(b) initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address, commits an offence.

(2) A person who knowingly—

(a) by means of a network service or applications service provides any obscene communication for commercial purposes to any person; or

(b) permits a network service or applications service under the person's control to be used for an activity described in paragraph (a), commits an offence.

(3) A person who commits an offence under this section shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of one thousand ringgit for every day during which the offence is continued after conviction.

[238] Computer Crimes Act 1997

Article 3 (1) A person shall be guilty of an offence if— (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer; (b) the access he intends to secure is unauthorized; and (c) he knows at the time when he causes the computer to perform the function that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at— (a) any particular program or data; (b) a program or data of any particular kind; or (c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding five years or to both.

มาตรา 5[239] ห้ามแก้ไข ดัดแปลง หรือลบข้อมูลในระบบโดยไม่ได้รับอนุญาต มาตรานี้เกี่ยวข้องโดยตรงกับกลุ่มอาชญากรที่แฮกข้อมูล สร้างเว็บไซต์ปลอม หรือเจาะระบบข้อมูลเพื่อใช้ในกิจกรรมหลอกลวง

3. Cyber Security Act 2024 เพื่อตอบสนองต่อภัยคุกคามดังกล่าว รัฐบาลมาเลเซียได้ออกกฎหมาย Cyber Security Act 2024 (Act 854) ซึ่งมีวัตถุประสงค์เพื่อเสริมสร้างความมั่นคงทางไซเบอร์ของประเทศ โดยการจัดตั้งคณะกรรมการความมั่นคงไซเบอร์แห่งชาติ (National Cyber Security Committee - NCSC) และกำหนดบทบาทหน้าที่ของหน่วยงานที่เกี่ยวข้อง รวมถึงการควบคุมผู้ให้บริการด้านความมั่นคงไซเบอร์ผ่านระบบการออกใบอนุญาต

อย่างไรก็ตาม เมื่อพิจารณาเชิงลึกแล้วพบว่ากฎหมายเหล่านี้ยังมีข้อจำกัดทั้งในเชิงโครงสร้าง เนื้อหา และการบังคับใช้ ซึ่งสะท้อนให้เห็นถึงความท้าทายของระบบกฎหมายภายในในการรับมือกับอาชญากรรมข้ามชาติที่มีพลวัตสูงเช่นนี้ ปัญหาแรกที่สะท้อนอย่างชัดเจนคือการขาดกฎหมายเฉพาะที่กำหนดนิยามและองค์ประกอบของ “แก๊งคอลเซ็นเตอร์” ในฐานะความผิดโดยตรง ทำให้การบังคับใช้กฎหมายต้องอาศัยการตีความตามกฎหมายทั่วไป เช่น ความผิดฐานฉ้อโกงตาม *Penal Code* มาตรา 415 หรือการใช้ระบบเครือข่ายในทางที่ผิดตาม *Communications and Multimedia Act 1998* มาตรา 233 ซึ่งแม้จะครอบคลุมพฤติกรรมบางส่วนของกลุ่มอาชญากรเหล่านี้ แต่ก็ยังไม่สามารถสะท้อนถึงลักษณะเฉพาะของขบวนการที่มีโครงสร้างเป็นเครือข่าย ใช้เทคนิคทางไซเบอร์ขั้นสูงและดำเนินการอย่างเป็นระบบในระดับระหว่างประเทศ ปัญหาแรกที่สะท้อนอย่างชัดเจน คือ การขาดกฎหมายเฉพาะที่กำหนดนิยามและองค์ประกอบของแก๊งคอลเซ็นเตอร์ในฐานะความผิดโดยตรง ทำให้การบังคับใช้กฎหมายต้องอาศัยการตีความตามกฎหมายทั่วไป เช่น

---

[239] Computer Crimes Act 1997

Article 5 (1) A person shall be guilty of an offence if he does any act which he knows will cause unauthorized modification of the contents of any computer.

(2) For the purposes of this section, it is immaterial that the act in question is not directed at— (a) any program or data; (b) a program or data of any kind; or (c) a program or data held in any particular computer.

(3) For the purposes of this section, it is immaterial whether an unauthorized modification is, or is intended to be, permanent or merely temporary.

(4) A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding seven years or to both; or be liable to a fine not exceeding one hundred and fifty thousand ringgit or to imprisonment for a term not exceeding ten years or to both, if the act is done with the intention of causing injury as defined in the Penal Code.

ความผิดฐานฉ้อโกงตาม *Penal Code* มาตรา 415 หรือการใช้ระบบเครือข่ายในทางที่ผิดตาม *Communications and Multimedia Act 1998* มาตรา 233 ซึ่งแม้จะครอบคลุมพฤติกรรมบางส่วนของกลุ่มอาชญากรเหล่านี้ แต่ก็ยังไม่สามารถสะท้อนถึงลักษณะเฉพาะของขบวนการที่มีโครงสร้างเป็นเครือข่าย ใช้เทคนิคทางไซเบอร์ขั้นสูง และดำเนินการอย่างเป็นระบบในระดับระหว่างประเทศ ในแง่ของการควบคุมพฤติกรรมผ่านระบบไซเบอร์ *Computer Crimes Act 1997* ถือเป็นกฎหมายที่สำคัญในการรับมือกับการเข้าถึงระบบหรือข้อมูลโดยมิชอบ อย่างไรก็ตาม ตัวบทกฎหมายฉบับนี้มีข้อจำกัดในการอธิบายพฤติกรรมการหลอกลวงที่ซ่อนอยู่ใน “รูปแบบทางสังคม” (social engineering) เช่น การปลอมเป็นเจ้าหน้าที่รัฐหรือธนาคารโทรศัพท์มาหลอกให้เหยื่อโอนเงิน ซึ่งมิได้ใช้การเจาะระบบหรือเทคนิค hacking แต่ใช้ความหลอกลวงผ่านเสียงและคำพูดแทน จึงไม่ตกอยู่ภายใต้ความผิดของกฎหมายนี้โดยตรง ทั้งนี้ยังไม่รวมถึงกรณีที่ระบบบัญชีธนาคารและธุรกรรมถูกใช้เป็นเครื่องมือรองรับเงินที่หลอกลวงมาจากเหยื่อ ซึ่งหากไม่มีการเชื่อมโยงอย่างเป็นระบบระหว่างกฎหมายอาชญากรรมทางคอมพิวเตอร์กับกฎหมายการฟอกเงิน (*Anti-Money Laundering Act*) ก็อาจเกิดช่องว่างในการดำเนินคดีต่อผู้มีส่วนเกี่ยวข้องโดยเฉพาะ “บัญชีม้า” ที่เป็นกลไกสำคัญในการกระจายเงินให้เครือข่ายอาชญากร อีกทั้งการบังคับใช้กฎหมายของมาเลเซียยังขาดเทคโนโลยีสนับสนุนและทรัพยากรที่เพียงพอสำหรับการติดตาม ตรวจสอบ วิเคราะห์เส้นทางการเงินและกิจกรรมบนโลกดิจิทัลของกลุ่มอาชญากร โดยเฉพาะอย่างยิ่งในบริบทของธุรกรรมทางการเงินที่เคลื่อนย้ายรวดเร็วผ่านระบบออนไลน์ หรือการใช้สกุลเงินดิจิทัล (cryptocurrency) ที่ยากต่อการตรวจสอบ นอกจากนี้ เจ้าหน้าที่ผู้บังคับใช้กฎหมายยังต้องพัฒนาทักษะในด้าน digital forensics และการสืบสวนไซเบอร์อย่างเป็นระบบ เพื่อให้สามารถตอบโต้กับกลยุทธ์อาชญากรรมที่เปลี่ยนแปลงอย่างรวดเร็วและมีเทคโนโลยีสนับสนุนในระดับสูง แม้จะมีการร่างกฎหมายใหม่อย่าง *Cyber Security Bill 2024* ซึ่งมีเป้าหมายในการเสริมสร้างความมั่นคงทางไซเบอร์และกำหนดอำนาจของหน่วยงานอย่าง *National Cyber Security Agency (NACSA)* ให้สามารถประสานการป้องกันและตอบโต้ภัยคุกคามไซเบอร์ในระดับประเทศ แต่ในทางปฏิบัติ ความสำเร็จของกฎหมายฉบับนี้จะต้องพึ่งพาทั้งความชัดเจนของบทบัญญัติ การจัดสรรงบประมาณอย่างเพียงพอและการสร้างความร่วมมือกับประเทศต่าง ๆ ในภูมิภาคผ่านกรอบกฎหมายระหว่างประเทศ ไม่เช่นนั้นกฎหมายดังกล่าวอาจกลายเป็นเพียงกรอบนโยบายที่ขาดพลังในการขับเคลื่อนจริงในทางปฏิบัติ

4.2.3.4 ประเทศกัมพูชา

ในประเทศกัมพูชา การต่อสู้กับอาชญากรรมที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์และอาชญากรรมทางไซเบอร์ได้รับการพัฒนาอย่างต่อเนื่องผ่านการออกกฎหมายและร่างกฎหมายหลายฉบับ ดังนี้

1. ประมวลกฎหมายอาญาแห่งราชอาณาจักรกัมพูชา ประมวลกฎหมายอาญาของกัมพูชามีบทบัญญัติที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์และการฉ้อโกง ซึ่งสามารถนำมาใช้ในการดำเนินคดีกับพฤติกรรมของแก๊งคอลเซ็นเตอร์ได้ เช่น

มาตรา 427-432[240] เป็นมาตราที่ว่าด้วยการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต การแทรกแซงระบบ และการแทรกแซงข้อมูล

---

[240] Cambodian Penal Code

Article 427: Unauthorized access to or remaining in automated data processing system Fraudulently accessing or remaining within an automated data processing system shall be punishable by imprisonment from one month to one year and a fine from one hundred thousand to two million Riels.

Where the act causes the destruction or modification of data contained in that system, or any alteration of the functioning of that system, the sentence is imprisonment from one to two years and a fine from two million to four million a u Riels.

Article 428: Obstructing the functioning of an automated data processing system shall be punishable by imprisonment from one to years and a fine from two million to four million Riels.

Article 429: The fraudulent introduction of data into an automated data processing system or the fraudulent deletion or modification of the that it contains shall be punishable by imprisonment from one to two years and a fine from two million to four million Riels.

Article 430: Participating in a group or a conspiracy established with a view to the planning of one or more offences defined in this Section shall be punishable by imprisonment from one to two years and a fine from two million to four million Riels.

Article 431: An attempt to commit the misdemeanours defined in this Section shall be punishable by the same penalties.

Article 432: The following additional penalties may be imposed in respect of the misdemeanours detined in this Section:

(1) forfeiture of certain rights. either rim permanently or for a period not exceeding five years;

(2) prohibition from practising a profession in the practice of or in connection with which the offence was committed, either permanently or for a period not exceeding five years;

(3) confiscation of any instruments, materials or items which were used or intended to be used to commit the offence;

2. ร่างกฎหมายว่าด้วยอาชญากรรมทางไซเบอร์เป็นความพยายามของรัฐบาลกัมพูชาในการวางกรอบทางกฎหมายเพื่อจัดการกับภัยคุกคามทางไซเบอร์ ซึ่งรวมถึงการกระทำผิดที่เกี่ยวข้องกับการแฮ็กข้อมูล การฉ้อโกงออนไลน์ การละเมิดข้อมูลส่วนบุคคล และการเผยแพร่ข้อมูลที่ถูกมองว่าเป็นภัยต่อความมั่นคงของรัฐ อย่างไรก็ตาม ร่างกฎหมายนี้ได้รับเสียงวิพากษ์วิจารณ์จากองค์กรสิทธิมนุษยชน เนื่องจากมีบทบัญญัติที่คลุมเครือและอาจถูกนำมาใช้เพื่อจำกัดเสรีภาพในการแสดงความคิดเห็นอย่างไม่เป็นธรรม ร่างกฎหมายฉบับนี้ประกอบด้วยบทบัญญัติจำนวน 8 หมวด รวม 48 มาตรา โดยครอบคลุมประเด็นสำคัญ เช่น ความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ ความผิดฐานฉ้อโกงโดยใช้คอมพิวเตอร์ ความผิดฐานปลอมแปลงข้อมูลและความผิดเกี่ยวกับเนื้อหาต้องห้าม

แม้ว่ารัฐบาลกัมพูชาจะได้ริเริ่มร่างกฎหมายว่าด้วยอาชญากรรมทางไซเบอร์ (Draft Law on Cybercrime) มาตั้งแต่ช่วงปี พ.ศ. 2557 (ค.ศ. 2014) แต่จนถึงปัจจุบัน ร่างกฎหมายดังกล่าวยังไม่ผ่านการบังคับใช้อย่างเป็นทางการ ซึ่งแสดงถึงความล่าช้าในการจัดวางโครงสร้างทางกฎหมายเพื่อตอบสนองต่อภัยคุกคามในโลกดิจิทัล อันเป็นผลให้ประเทศขาดเครื่องมือทางกฎหมายที่จำเป็นต่อการสืบสวน ดำเนินคดี และป้องกันอาชญากรรมในรูปแบบใหม่เหล่านี้อย่างมีประสิทธิภาพ นอกจากความล่าช้าในการตรากฎหมายแล้ว เนื้อหาของร่างกฎหมายเองก็เป็นประเด็นที่ก่อให้เกิดข้อวิพากษ์วิจารณ์ในระดับนานาชาติ โดยเฉพาะจากองค์กรสิทธิมนุษยชน หลายบทบัญญัติในร่างกฎหมายมีลักษณะคลุมเครือ ขาดความชัดเจนในด้านคำจำกัดความและอาจถูกใช้เป็นเครื่องมือในการจำกัดเสรีภาพของประชาชนในการแสดงออกบนโลกออนไลน์ มากกว่าจะเน้นไปที่การควบคุมหรือปราบปรามอาชญากรรมไซเบอร์โดยแท้จริง ประเด็นที่น่าวิตกยิ่งไปกว่านั้น คือ ร่างกฎหมายฉบับนี้ให้ดุลพินิจอย่างกว้างขวางแก่เจ้าหน้าที่รัฐในการตีความพฤติกรรมทางอินเทอร์เน็ตว่าเป็นภัยต่อ “ความมั่นคง” หรือ “ความสงบเรียบร้อย” โดยไม่ต้องมีหลักฐานเชิงเทคนิคหรือกระบวนการพิจารณาอย่างโปร่งใส ด้วยเหตุนี้จึงมีความเสี่ยงที่ร่างกฎหมายจะกลายเป็นกลไกควบคุมความคิดเห็นในโลกไซเบอร์ มากกว่า

---

(4) confiscation of the items or funds which I \@PI were the subject of the offence;

(5) confiscation of the proceeds or property arising out of the offence;

(6) confiscation of the utensils, materials and firnishings in the premises in which the offence was committed;

(7) confiscation of one or more vehicles belonging to the convicted person;

(8) publication of sentencing decision for a period not exceeding two months;

(9) publication of sentencing decision in the print media;

(10) broadcasting of sentencing decision any audio-visual communication for a period not exceeding eight days.

จะเป็นกรอบการควบคุมพฤติกรรมที่เป็นอาชญากรรมจริง ๆ ยิ่งไปกว่านั้น ความร่วมมือระหว่างประเทศในกระบวนการส่งผู้ร้ายข้ามแดน การแลกเปลี่ยนข้อมูลข่าวกรองทางไซเบอร์ หรือการพิสูจน์หลักฐานดิจิทัล ยังมีข้อจำกัดอย่างมากในกัมพูชา โดยเฉพาะอย่างยิ่งเมื่อเปรียบเทียบกับประเทศเพื่อนบ้านในสมาชิกอาเซียนที่มีกฎหมายว่าด้วยอาชญากรรมไซเบอร์ที่ครอบคลุมและมีผลใช้บังคับแล้ว ทำให้ความสามารถในการมีส่วนร่วมในความร่วมมือระดับภูมิภาคของกัมพูชายังอยู่ในระดับต่ำ ดังนั้น ระบบกฎหมายของกัมพูชายังคงประสบกับข้อจำกัดเชิงโครงสร้างในการต่อสู้กับอาชญากรรมคอลเซ็นเตอร์และไซเบอร์ที่มีความซับซ้อนและแพร่หลายมากขึ้น ร่างกฎหมายว่าด้วยอาชญากรรมไซเบอร์แม้จะเป็นก้าวแรกที่สำคัญ แต่หากไม่มีการปรับปรุงเนื้อหาให้มีความชัดเจน เคารพสิทธิมนุษยชนและมีผลใช้บังคับในทางปฏิบัติ ย่อมไม่สามารถเป็นเครื่องมือที่มีประสิทธิภาพในการปราบปรามอาชญากรรมสมัยใหม่ได้อย่างแท้จริง

4.3.2.5 ประเทศสิงคโปร์

ประเทศสิงคโปร์เป็นหนึ่งในประเทศสมาชิกอาเซียนที่มีระบบกฎหมายและการบังคับใช้ที่มีประสิทธิภาพสูง โดยเฉพาะในด้านการจัดการกับอาชญากรรมไซเบอร์ ซึ่งรวมถึงปัญหาแก๊งคอลเซ็นเตอร์ที่มีลักษณะเป็นอาชญากรรมข้ามชาติและใช้เทคโนโลยีเป็นเครื่องมือหลักในการกระทำความผิด สิงคโปร์ได้วางรากฐานทางกฎหมายที่มั่นคงผ่านกฎหมายสำคัญหลายฉบับ ดังนี้

1.Computer Misuse Act (CMA) 1993[241] ซึ่งต่อมาได้รับการแก้ไขเพิ่มเติมจนกลายเป็น Computer Misuse and Cybersecurity Act (CMCA) ภายใต้ CMCA สิงคโปร์ได้บัญญัติความผิดที่เกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต การแทรกแซงหรือทำลายข้อมูล และการใช้ระบบคอมพิวเตอร์เพื่อวัตถุประสงค์ที่ผิดกฎหมาย โดยครอบคลุมทั้งความผิดที่เกิดขึ้นภายในประเทศและที่เกิดจากต่างประเทศแต่ส่งผลกระทบต่อระบบหรือประชาชนของสิงคโปร์ กฎหมายดังกล่าวจึงมีลักษณะข้ามพรมแดน (extraterritorial effect) ซึ่งถือเป็นจุดแข็งในการรับมือกับกลุ่มอาชญากรรมอย่างแก๊งคอลเซ็นเตอร์ที่มีเครือข่ายข้ามชาติ

2. Cybersecurity Act 2018[242] ได้เสริมความเข้มแข็งให้กับระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยเน้นการกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure – CII) และกำหนดให้หน่วยงานภาครัฐและเอกชนที่เกี่ยวข้องต้องรายงานเหตุการณ์ด้านไซเบอร์ที่มีผลกระทบ พร้อมทั้งให้สำนักงานความมั่นคงไซเบอร์ (Cyber

---

[241] ‘Computer Misuse Act 1993’ (Singapore Statutes Online, 1993) <https://sso.agc.gov.sg/Act/CMA1993> accessed 10 March 2025.

[242] ‘Singapore, Cybersecurity Act 2018’ (Singapore Statutes Online, 2018) <https://sso.agc.gov.sg/Act/CA2018> accessed 10 March 2025.

Security Agency – CSA) มีอำนาจเข้าตรวจสอบและออกคำสั่งเพื่อควบคุมสถานการณ์อย่างทันท่วงที

แม้ว่าสิงคโปร์จะถือเป็นหนึ่งในประเทศที่มีกรอบกฎหมายทางไซเบอร์ที่เข้มแข็งและมีประสิทธิภาพมากที่สุดในภูมิภาคอาเซียน โดยเฉพาะการตรากฎหมายสำคัญอย่าง *Computer Misuse Act 1993* และ *Cybersecurity Act 2018* ที่ครอบคลุมทั้งมาตรการลงโทษเชิงอาญาและกลไกในการป้องกันภัยไซเบอร์ แต่เมื่อพิจารณาเชิงลึกในบริบทของการปราบปรามแก๊งคอลเซ็นเตอร์ในลักษณะของอาชญากรรมข้ามชาติ กลับพบว่ายังมีข้อจำกัดทางกฎหมายที่น่าห่วงอยู่หลายประการ ประการแรก ปัญหาอยู่ที่ “อำนาจข้ามเขตแดน” ของกฎหมายสิงคโปร์ซึ่งยังไม่สามารถบังคับใช้ได้อย่างมีประสิทธิภาพเมื่อการกระทำความผิดเกิดขึ้นนอกราชอาณาจักร เช่น ในกรณีที่กลุ่มแก๊งคอลเซ็นเตอร์ตั้งศูนย์ปฏิบัติการในประเทศที่มีช่องว่างทางกฎหมายหรือมีรัฐที่ล้มเหลวในการบังคับใช้กฎหมายไซเบอร์ สิงคโปร์เองแม้จะสามารถติดตามการโอนเงินหรือสัญญาณดิจิทัลที่เข้ามาในประเทศได้ดี แต่กลับไม่สามารถดำเนินคดีเอาผิดกับผู้กระทำผิดที่อยู่นอกเขตแดนได้อย่างเป็นรูปธรรม หากไม่มีความร่วมมือในทางสนธิสัญญาหรือความตกลงระหว่างประเทศ

ประการที่สอง กฎหมายไซเบอร์ของสิงคโปร์ยังมีลักษณะเน้นลงโทษผู้กระทำผิดในพื้นที่มากกว่าการขยายอำนาจไปยังเครือข่ายที่อยู่เบื้องหลังของขบวนการ โดยเฉพาะการเชื่อมโยงกับอาชญากรรมทางการเงิน เช่น การฟอกเงินผ่านบัญชีม้าหรือการเปิดบัญชีหลอกลวงด้วยบัตรประชาชนปลอม กฎหมายอย่าง *Computer Misuse Act* แม้จะกำหนดโทษอย่างชัดเจนในเรื่องการเข้าถึงและเปลี่ยนแปลงข้อมูลในระบบคอมพิวเตอร์โดยมิชอบ แต่ก็ยังไม่สามารถเชื่อมโยงอย่างมีประสิทธิภาพกับระบบการสืบสวนทางการเงินหรือการติดตามเส้นทางการเงินที่ซับซ้อนได้โดยลำพัง อีกทั้ง แม้ *Cybersecurity Act 2018* จะให้อำนาจหน่วยงานรัฐเข้าแทรกแซงระบบสำคัญเพื่อป้องกันการโจมตีไซเบอร์ แต่ก็มีข้อวิจารณ์จากนักกฎหมายและภาคประชาสังคมว่าการกำหนดขอบเขตของ “Critical Information Infrastructure (CII)” ยังแคบเกินไปและไม่รวมโครงสร้างที่เกี่ยวข้องกับระบบการชำระเงินของภาคประชาชนทั่วไป ซึ่งเป็นเป้าหมายหลักของกลุ่มคอลเซ็นเตอร์ส่งผลให้ระบบป้องกันเชิงโครงสร้างยังไม่ครอบคลุมเป้าหมายที่แท้จริงของอาชญากรในโลกดิจิทัล นอกจากนี้ปัญหาที่ซับซ้อนอีกประการหนึ่ง คือ การบังคับใช้กฎหมายกับ “เหยื่อที่ไม่รู้ตัวว่าตนมีส่วนร่วมในการกระทำผิด” เช่น กรณีบุคคลในสิงคโปร์ถูกว่าจ้างให้เปิดบัญชีธนาคารโดยไม่ทราบว่าเป็นบัญชีม้า กฎหมายในปัจจุบันยังไม่สามารถแยกแยะเจตนาได้อย่างชัดเจนและอาจทำให้ผู้บริสุทธิ์ตกเป็นผู้ต้องหาโดยไม่สมควร ซึ่งเป็นจุดเปราะบางทางนโยบายที่ต้องได้รับการทบทวนโดยด่วน ในภาพรวม แม้สิงคโปร์จะมีเจตจำนงทางนโยบายและเครื่องมือทางกฎหมายที่ทันสมัย แต่ก็ยังเผชิญข้อจำกัดที่เป็นผลจากลักษณะของอาชญากรรมไซเบอร์สมัยใหม่ที่ไร้พรมแดน มีเครือข่ายข้ามชาติ และใช้เทคโนโลยีลวงตาเหนือการตรวจจับของระบบกฎหมายแบบดั้งเดิม

4.3.2.6 บรูไนดารุสซาลาม

ประเทศบรูไนแม้จะเป็นประเทศขนาดเล็กในภูมิภาคอาเซียน แต่ก็ให้ความสำคัญกับการป้องกันอาชญากรรมทางไซเบอร์และภัยคุกคามดิจิทัลอย่างต่อเนื่อง โดยเฉพาะในบริบทของความมั่นคงและความเป็นระเบียบเรียบร้อยของสังคมตามหลักการของรัฐอิสลาม บรูไนมีกฎหมายและนโยบายที่เกี่ยวข้องกับการจัดการอาชญากรรมไซเบอร์ รวมถึงปราบปรามแก๊งคอลเซ็นเตอร์ ดังนี้

1. Computer Misuse Act (Chapter 194)[243], revised edition 2007 เป็นกฎหมายหลักในการจัดการกับอาชญากรรมทางคอมพิวเตอร์ เช่น การเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต การดักฟังข้อมูล การทำลายข้อมูล และการใช้คอมพิวเตอร์เพื่อการฉ้อโกง กฎหมายนี้มีบทลงโทษที่ชัดเจน โดยเฉพาะกับผู้ที่กระทำความผิดโดยเจตนาในการหลอกลวงหรือสร้างความเสียหายแก่บุคคลหรือระบบสารสนเทศของรัฐ

2. Telecommunications Order 2001[244] เป็นกฎหมายที่ควบคุมการใช้ระบบโทรคมนาคม รวมถึงการใช้เครือข่ายโทรศัพท์หรืออินเทอร์เน็ตเพื่อจุดประสงค์ในการฉ้อโกง หลอกลวง หรือส่งข้อความที่ผิดกฎหมาย และมีความเกี่ยวข้องกับพฤติกรรมของแก๊งคอลเซ็นเตอร์ที่ใช้โทรศัพท์เป็นเครื่องมือในการล่อลวงเหยื่อ

3. Sedition Act (Chapter 24) และ Penal Code (Chapter 22) แม้จะไม่ใช่กฎหมายเฉพาะด้านไซเบอร์ แต่ก็ถูกนำมาใช้ร่วมในการเอาผิดผู้กระทำผิดที่ใช้เทคโนโลยีสื่อสารเพื่อจุดประสงค์ผิดกฎหมาย เช่น การข่มขู่ ข่มเหง หรือหลอกลวงประชาชนผ่านช่องทางดิจิทัล

แม้ว่าบรูไนจะมีกรอบกฎหมายที่เข้มงวดและวางอยู่บนหลักของระบบกฎหมายอังกฤษผสมกับหลักศาสนาอิสลาม แต่เมื่อพิจารณาในบริบทของการเผชิญกับแก๊งคอลเซ็นเตอร์และอาชญากรรมไซเบอร์ พบว่ายังมีข้อจำกัดหลายประการที่สะท้อนถึงสภาพปัญหาทางกฎหมายที่ควรได้รับการแก้ไขอย่างเป็นระบบ บรูไนยังไม่มีกฎหมายว่าด้วยอาชญากรรมทางไซเบอร์ (Cybercrime Act) ที่ครอบคลุมและทันสมัยในระดับเดียวกับประเทศพัฒนาแล้ว โดยแม้ว่าประมวลกฎหมายอาญา (Penal Code, Chapter 22) และกฎหมายบางฉบับ เช่น Sedition Act (Chapter 24) และ Public Order Act จะสามารถตีความเพื่อครอบคลุมพฤติกรรมผิดกฎหมายบางอย่างในโลกออนไลน์ได้ แต่ข้อจำกัดในการบัญญัติโดยตรงเกี่ยวกับอาชญากรรมไซเบอร์ เช่น การฉ้อโกงผ่านเทคโนโลยี การโจมตีระบบคอมพิวเตอร์ หรือการแพร่กระจายข้อมูลหลอกลวงทางอินเทอร์เน็ต ยังคงเป็นจุดอ่อนสำคัญ กรณีของแก๊งคอลเซ็นเตอร์ที่ใช้เทคโนโลยีเพื่อหลอกลวงประชาชนข้ามพรมแดนจึงอาจหลุดรอดจาก

---

[243] 'Computer Misuse Act (Chapter 194)' (Attorney General's Chambers Brunei, 2007) <https://www.agc.gov.bn/AGC%20Site%20Pages/LOV.aspx> accessed 10 March 2025.

[244] 'Telecommunications Order 2001' (Attorney General's Chambers Brunei, 2001) <https://www.agc.gov.bn/AGC%20Site%20Pages/LOV.aspx> accessed 10 March 2025.

บทบัญญัติที่มีอยู่ในกฎหมายปัจจุบัน แม้ว่า Sedition Act (Chapter 24) จะมีเจตนารมณ์เพื่อรักษาความสงบเรียบร้อยของรัฐ แต่ในทางปฏิบัติพบว่า บทบัญญัติของกฎหมายดังกล่าวมีลักษณะทั่วไปและอาจนำไปสู่การตีความในลักษณะที่เป็นการควบคุมการแสดงออกของประชาชนมากกว่าการปราบปรามอาชญากรรมข้ามชาติ ส่งผลให้กลไกกฎหมายของบรูไนยังไม่สามารถแยกแยะระหว่างพฤติกรรมผิดกฎหมายในโลกไซเบอร์กับการใช้เสรีภาพบนโลกออนไลน์ได้อย่างมีประสิทธิภาพ โดยเฉพาะในกรณีของการแอบอ้างหน่วยงานรัฐเพื่อหลอกลวงประชาชน ซึ่งปรากฏชัดในหลายกรณีของแก๊งคอลเซ็นเตอร์ในภูมิภาคอาเซียน แม้ว่า Sedition Act (Chapter 24) จะมีเจตนารมณ์เพื่อรักษาความสงบเรียบร้อยของรัฐ แต่ในทางปฏิบัติพบว่า บทบัญญัติของกฎหมายดังกล่าวมีลักษณะทั่วไปและอาจนำไปสู่การตีความในลักษณะที่เป็นการควบคุมการแสดงออกของประชาชนมากกว่าการปราบปรามอาชญากรรมข้ามชาติ ส่งผลให้กลไกกฎหมายของบรูไนยังไม่สามารถแยกแยะระหว่างพฤติกรรมผิดกฎหมายในโลกไซเบอร์กับการใช้เสรีภาพบนโลกออนไลน์ได้อย่างมีประสิทธิภาพ โดยเฉพาะในกรณีของการแอบอ้างหน่วยงานรัฐเพื่อหลอกลวงประชาชน ซึ่งปรากฏชัดในหลายกรณีของแก๊งคอลเซ็นเตอร์ในภูมิภาคอาเซียน จากการวิเคราะห์สภาพปัญหาทางกฎหมายของบรูไนจะเห็นได้ว่า แม้จะมีกฎหมายอาญาที่เข้มงวด แต่การเผชิญกับภัยคุกคามแบบใหม่ในรูปแบบของอาชญากรรมข้ามชาติ โดยเฉพาะอย่างยิ่งในกรณีของแก๊งคอลเซ็นเตอร์ ยังขาดความพร้อมทั้งในแง่ของกรอบกฎหมายเฉพาะทาง การคุ้มครองข้อมูล การตีความกฎหมาย และกลไกความร่วมมือระหว่างประเทศ

4.3.2.7 ประเทศอินโดนีเซีย

ประเทศอินโดนีเซียมีกฎหมายที่เกี่ยวข้องกับการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์ ซึ่งมักจัดอยู่ภายใต้กรอบของอาชญากรรมไซเบอร์และการฉ้อโกง โดยกฎหมายที่ใช้ในการจัดการกับพฤติกรรมของแก๊งคอลเซ็นเตอร์ คือ Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law) หรือที่รู้จักกันในชื่อ Undang-Undang Informasi dan Transaksi Elektronik *(ฉบับแก้ไขล่าสุด: Law No. 19 of 2016)* กฎหมายฉบับนี้เป็นกฎหมายหลักที่ใช้ในการจัดการกับอาชญากรรมไซเบอร์ในอินโดนีเซีย โดยกำหนดบทลงโทษสำหรับการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต การปลอมแปลงข้อมูลอิเล็กทรอนิกส์ และการโจมตีระบบคอมพิวเตอร์ เช่น

มาตรา 28 (1)[245] ระบุว่าบุคคลใดที่มีเจตนาและ/หรือโดยมิชอบกระจายข่าวปลอมและทำให้ผู้บริโภคได้รับความเสียหายในการทำธุรกรรมทางอิเล็กทรอนิกส์จะต้องรับโทษตามที่กฎหมายกำหนด

[245] Electronic Information and Transactions

มาตรา 35 และ 36[246] กล่าวถึง การปลอมแปลงหรือบิดเบือนข้อมูลอิเล็กทรอนิกส์ โดยมีเจตนาให้ผู้อื่นหลงเชื่อ ซึ่งสอดคล้องกับพฤติกรรมของแก๊งคอลเซ็นเตอร์ที่หลอกให้โอนเงินหรือเปิดเผยข้อมูลส่วนตัว

กฎหมายหลักที่อินโดนีเซียใช้ในการควบคุมและลงโทษอาชญากรรมเหล่านี้ คือ พระราชบัญญัติว่าด้วยข้อมูลและธุรกรรมอิเล็กทรอนิกส์ (Electronic Information and Transactions Law หรือ EIT Law) ปี ค.ศ. 2008 ซึ่งได้รับการแก้ไขเพิ่มเติมในปี ค.ศ. 2016 และ 2024 อย่างไรก็ตาม แม้จะมีกฎหมายดังกล่าว แต่การบังคับใช้กฎหมายและโครงสร้างทางกฎหมายโดยรวมของประเทศก็ยังคงเผชิญกับข้อจำกัดหลายประการ EIT Law ของอินโดนีเซีย แม้จะเป็นกฎหมายสำคัญที่มีบทบัญญัติเกี่ยวกับการฉ้อโกงผ่านระบบอิเล็กทรอนิกส์ (มาตรา 28 วรรค 1 และมาตรา 35) และการเข้าถึงข้อมูลโดยมิชอบ (มาตรา 30) แต่กฎหมายฉบับนี้ยังคงมีปัญหาด้านการตีความที่คลุมเครือ การบัญญัติที่ไม่ครอบคลุมกลวิธีใหม่ ๆ ที่อาชญากรไซเบอร์ใช้ และการเชื่อมโยงกับกฎหมายอื่น ๆ ที่อาจยังไม่สอดรับกันโดยสมบูรณ์ ตัวอย่างเช่น กฎหมายดังกล่าวไม่สามารถครอบคลุมกรณีที่มีการหลอกลวงโดยใช้บุคคลสวมรอยเป็นเจ้าหน้าที่รัฐหรือการใช้ระบบการโอนเงินที่เกี่ยวพันกับธนาคารต่างประเทศ ซึ่งเป็นพฤติกรรมที่พบได้บ่อยในคดีแก๊งคอลเซ็นเตอร์ในทางปฏิบัติ ยังมีปัญหาเรื่องสิทธิมนุษยชนและการใช้อำนาจเกินขอบเขต ซึ่งถูกวิจารณ์โดยองค์กรสิทธิมนุษยชนภายในประเทศและระหว่างประเทศ เช่น Human Rights Watch ว่าบางมาตราของกฎหมาย EIT ถูกใช้เป็นเครื่องมือในการจำกัดเสรีภาพในการแสดงออกมากกว่าการจัดการกับอาชญากรรมไซเบอร์อย่างแท้จริง ปัญหานี้ทำให้เกิดข้อกังวลว่าหากไม่มีการปรับปรุงโครงสร้างทางกฎหมายให้สมดุลระหว่างการบังคับใช้และการคุ้มครองสิทธิของประชาชน อาจเกิดความไม่เชื่อมั่นในระบบยุติธรรมและเปิดช่องว่างให้กลุ่มอาชญากรรมดำเนินการได้ง่ายยิ่งขึ้น แม้อินโดนีเซียจะมีกฎหมายที่ตั้งใจ

---

Article 28 (1) Any Person who knowingly and without authority disseminates false and misleading information resulting in consumer loss in Electronic Transactions.

(2) Any Person who knowingly and without authority disseminates information aimed at inflicting hatred or dissension on individuals and/or certain groups of community based on ethnic groups, religions, races, and inter-groups (SARA).

[246] Electronic Information and Transactions

Article 35 Any Person who knowingly and without authority or unlawfully manipulates, creates, alters, deletes, tampers with Electronic Information and/or Electronic Documents with the intent that such Electronic Information and/or Electronic Documents would seem to be authentic data.

Article 36 Any Person who knowingly and without authority or unlawfully commits acts as intended by Article 27 through Article 34 to other Persons' detriment.

ออกแบบมาเพื่อควบคุมอาชญากรรมไซเบอร์โดยเฉพาะ แต่การรับมือกับปรากฏการณ์ที่ซับซ้อนอย่างแก๊งคอลเซ็นเตอร์ยังคงเผชิญกับข้อจำกัดทางกฎหมาย โครงสร้างการบังคับใช้และความร่วมมือข้ามชาติอย่างมีนัยสำคัญ การปฏิรูปในระดับนโยบาย การพัฒนาศักยภาพเจ้าหน้าที่ และการสร้างระบบความร่วมมือเชิงลึกกับประเทศเพื่อนบ้านคือแนวทางสำคัญในการลดภัยคุกคามจากอาชญากรรมข้ามชาติในยุคดิจิทัล

4.3.2.8 ประเทศเวียดนาม

ประเทศเวียดนามได้กำหนดกรอบกฎหมายหลายฉบับที่เกี่ยวข้องกับการควบคุมและจัดการกับอาชญากรรมไซเบอร์ รวมถึงการกระทำผิดของแก๊งคอลเซ็นเตอร์ ซึ่งส่วนใหญ่ดำเนินการผ่านช่องทางออนไลน์หรือโทรคมนาคม โดยกฎหมายหลักที่ใช้บังคับได้แก่

1. Law on Cybersecurity, 2018 เป็นกฎหมายหลักที่มีเป้าหมายเพื่อปกป้องความมั่นคงของรัฐ ความสงบเรียบร้อย และสิทธิของประชาชนบนโลกออนไลน์ โดยกำหนดให้บริษัทเทคโนโลยีต้องจัดเก็บข้อมูลผู้ใช้ภายในประเทศและสามารถบังคับให้ลบเนื้อหาหรือข้อมูลที่ถูกพิจารณาว่าคุกคามความมั่นคงได้

2. Criminal Code of Vietnam 2015 *(amended 2017)* กำหนดโทษสำหรับความผิดเกี่ยวกับการฉ้อโกงโดยใช้เทคโนโลยี เช่น มาตรา 174[247] ความผิดฐานฉ้อโกงทรัพย์สิน

---

[247] Criminal Code of Vietnam 2015

Article 174 1. A person who uses deception to obtain another person's property which is assessed at from VND 2,000,000 to under VND 50,000,000 or property assessed at under VND 2,000,000 in any of the following cases shall face a penalty of up to 03 years' community sentence or 06 - 36 months' imprisonment:

a) The offender previously incurred a civil penalty for appropriation of property;

b) The offender has a previous conviction for theft or any of the criminal offences specified in Article 168, 169, 170, 171, 172, 173, 175 and 290 hereof which has not been expunged;

c) The offence has a negative impact on social safety, order, and security;

d) The property obtained is the primary means of livelihood of the victim and the victim's family; the property obtained is a souvenir, memento, or religious item that has a spiritual value to the victim.

2. This offence committed in any of the following cases shall carry a penalty of 02 - 07 years' imprisonment:

a) The offence is committed by an organized group;

b) The offence is committed in a professional manner;

มาตรา 285-290[248] ความผิดเกี่ยวกับการใช้ระบบคอมพิวเตอร์หรือเครือข่ายข้อมูลโดยมิชอบ เช่น การแฮ็ก เข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือการแพร่ไวรัส

3. Law on Cyber Information Security, 2015 มุ่งเน้นการรักษาความมั่นคงของข้อมูล การจัดการความเสี่ยงด้านไซเบอร์ และการป้องกันการละเมิดข้อมูลส่วนบุคคล

---

c) The property obtained is assessed at from VND 50,000,000 to under VND 200,000,000;

d) Dangerous recidivism;

dd) The offence involves abuse of the offender's position or power or committed in the name of an agency or organization;

e) The offender employs deceitful methods to commit the offence;

g) The property obtained is assessed at from VND 2,000,000 to under VND 50,000,000 or but the offender commits the offence in any of the cases specified in Point a through d Clause 1 of this Article.

3. This offence committed in any of the following cases shall carry a penalty of 07 - 15 years' imprisonment:

a) The property obtained is assessed at from VND 200,000,000 to under VND 500,000,000;

b) The property obtained is assessed at from VND 50,000,000 to under VND 200,000,000 or but the offender commits the offence in any of the cases specified in Point a through d Clause 1 of this Article.

c) The offender takes advantage of a natural disaster or epidemic to commit the offence.

4. This offence committed in any of the following cases shall carry a penalty of 12 - 20 years' imprisonment or life imprisonment:

a) The property stolen is VND 500,000,000 or over;

b) The property obtained is assessed at from VND 200,000,000 to under VND 500,000,000 or but the offender commits the offence in any of the cases specified in Point a through d Clause 1 of this Article.

c) The offender takes advantage of a war or state of emergency to commit the offence.

5. The offender might also be liable to a fine of from VND 50,000,000 to VND 200,000,000, be prohibited from holding certain positions or doing certain works for 01 - 05 years, or have all or part of his/her property confiscated.

[248] National Assembly of the Socialist Republic of Vietnam, Criminal Code (No. 100/2015/QH13 of November 27, 2015) <https://www.policinglaw.info/assets/downloads/2015_Criminal_Code_of_Vietnam_(English_translation).pdf> accessed 10 March 2025.

4. Decree No. 15/2020/ND-CP กำหนดบทลงโทษทางปกครองเกี่ยวกับการละเมิดในด้านเทคโนโลยีสารสนเทศ การสื่อสารโทรคมนาคม และกิจกรรมบนอินเทอร์เน็ต รวมถึงพฤติกรรมหลอกลวงประชาชนทางออนไลน์

เวียดนามถือเป็นหนึ่งในประเทศที่เผชิญความท้าทายทางกฎหมายในการปราบปรามอาชญากรรมรูปแบบใหม่นี้ แม้รัฐบาลเวียดนามจะได้ดำเนินการตรากฎหมายหลายฉบับที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ แต่ยังปรากฏสภาพปัญหาทางกฎหมายที่สำคัญหลายประการซึ่งส่งผลต่อประสิทธิภาพในการบังคับใช้กฎหมายต่ออาชญากรรมข้ามชาติที่มีลักษณะซับซ้อน ประการแรก คือ ปัญหาเชิงนิยามและเขตอำนาจในกฎหมาย แม้ในประมวลกฎหมายอาญาเวียดนามปี 2015 จะมีบทบัญญัติที่เกี่ยวกับการฉ้อโกงผ่านเทคโนโลยีสารสนเทศ (เช่น มาตรา 290 ว่าด้วยการใช้เครือข่ายคอมพิวเตอร์เพื่อยักยอกทรัพย์) แต่บทบัญญัติเหล่านี้ยังไม่ครอบคลุมถึงลักษณะเฉพาะของกลุ่มอาชญากรรมที่มีความเป็นระบบ เช่น เครือข่ายคอลเซ็นเตอร์ที่มีการแบ่งหน้าที่ชัดเจน การทำงานข้ามพรมแดน และการใช้เทคโนโลยีขั้นสูง ซึ่งยากต่อการสืบสวนภายในประเทศเพียงลำพัง

ประการที่สอง คือ ความทับซ้อนและไม่สอดคล้องกันของกฎหมายด้านไซเบอร์ ในขณะที่ Cybersecurity Law 2018 ให้อำนาจอย่างกว้างขวางแก่หน่วยงานรัฐในการควบคุมข้อมูลและการสื่อสารบนอินเทอร์เน็ต แต่กฎหมายฉบับนี้มักถูกวิพากษ์วิจารณ์ในแง่การละเมิดสิทธิเสรีภาพ และขาดกลไกการกำกับดูแลที่โปร่งใส ส่งผลให้การบังคับใช้กฎหมายในทางปฏิบัติไม่สามารถสร้างความสมดุลระหว่างความมั่นคงกับสิทธิของประชาชน อีกทั้งยังไม่มีบทบัญญัติที่เน้นการคุ้มครองเหยื่ออาชญากรรมไซเบอร์โดยตรง

ประการที่สาม คือ ข้อจำกัดด้านความร่วมมือระหว่างประเทศ แม้เวียดนามจะเป็นภาคีของอนุสัญญาระหว่างประเทศบางฉบับ และมีความร่วมมือกับ INTERPOL และอาเซียนแต่ยังไม่มีการให้สัตยาบันต่อ Budapest Convention on Cybercrime ซึ่งเป็นกรอบความร่วมมือสำคัญระดับสากลที่ใช้ในการประสานงานและรวบรวมพยานหลักฐานข้ามพรมแดน การไม่เข้าร่วมในข้อตกลงดังกล่าวส่งผลให้เวียดนามมีข้อจำกัดในการแลกเปลี่ยนข้อมูลกับประเทศอื่นที่ร่วมมือในการสืบสวนเครือข่ายแก๊งคอลเซ็นเตอร์

อีกทั้งในเชิงโครงสร้างของกระบวนการยุติธรรม ยังพบปัญหาในด้านขีดความสามารถของเจ้าหน้าที่ในการตรวจสอบและวิเคราะห์หลักฐานดิจิทัล รวมถึงการฝึกอบรมเจ้าหน้าที่สอบสวนและอัยการที่ยังไม่เพียงพอ ส่งผลให้การดำเนินคดีอาญากับผู้กระทำผิดในโลก ไซเบอร์เป็นไปอย่างล่าช้าและไม่ทั่วถึง นอกจากนี้ การที่ผู้กระทำผิดส่วนใหญ่อยู่ในต่างประเทศหรือใช้โครงข่ายอาชญากรรมที่ซับซ้อน ยังทำให้เกิดปัญหาในการติดตามตัวผู้ต้องหาและบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพ กล่าวโดยสรุป แม้เวียดนามจะมีความพยายามอย่างต่อเนื่องในการจัดการกับอาชญากรรมไซเบอร์และกลุ่มแก๊งคอลเซ็นเตอร์ผ่านการออกกฎหมายและจัดตั้งหน่วยงานเฉพาะ แต่

ยังคงมีช่องว่างด้านกฎหมายและการบังคับใช้ที่ต้องได้รับการแก้ไขในเชิงระบบ โดยเฉพาะการปรับปรุงบทบัญญัติกฎหมายให้ทันสมัยมากขึ้น การยกระดับความร่วมมือระหว่างประเทศ และการลงทุนในการพัฒนาศักยภาพบุคลากรในกระบวนการยุติธรรม ซึ่งจะเป็นรากฐานสำคัญในการป้องกันและปราบปรามอาชญากรรมไซเบอร์ข้ามชาติได้อย่างยั่งยืน

4.3.2.9 สาธารณรัฐประชาชนลาว

สปป.ลาวได้ออกกฎหมายหลายฉบับเพื่อรับมือกับอาชญากรรมไซเบอร์ ได้แก่

1. Law on Prevention and Combating Cyber Crime, 2015[249] กฎหมายฉบับนี้เป็นกฎหมายเฉพาะของลาวในการควบคุมอาชญากรรมไซเบอร์ โดยมีเนื้อหาเกี่ยวกับความผิดเกี่ยวกับการเข้าถึงระบบโดยไม่ได้รับอนุญาต การแทรกแซงข้อมูล การกระทำผ่านเทคโนโลยีเพื่อฉ้อโกงหรือหลอกลวง การเผยแพร่ข้อมูลเท็จหรือผิดศีลธรรม การใช้เทคโนโลยีเพื่อวัตถุประสงค์ที่ผิดกฎหมาย เช่น การข่มขู่ ล่อลวง ฉ้อโกง

2. Law on Electronic Data Protection, 2017[250] มุ่งเน้นการคุ้มครองข้อมูลส่วนบุคคลและข้อมูลอิเล็กทรอนิกส์อื่น ๆ โดยกำหนดข้อบังคับเกี่ยวกับการเก็บรวบรวม การประมวลผล และการถ่ายโอนข้อมูล

3. Penal Code of Lao PDR (2017)[251] รวมบทบัญญัติที่เกี่ยวข้องกับการกระทำผิดทางอาญา รวมถึงอาชญากรรมไซเบอร์และการฉ้อโกง

แม้ว่าสาธารณรัฐประชาธิปไตยประชาชนลาว (สปป.ลาว) จะได้ประกาศใช้ กฎหมายว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ พ.ศ. 2558 (2015) และปรับปรุงประมวลกฎหมายอาญาฉบับใหม่ในปี พ.ศ. 2560 (ค.ศ.2017) ซึ่งครอบคลุมถึงพฤติกรรมอาชญากรรมไซเบอร์ในรูปแบบต่าง ๆ แล้ว แต่การบังคับใช้กฎหมายเหล่านี้ในการจัดการกับปัญหา “แก๊งคอลเซ็นเตอร์” ที่มีลักษณะเป็นอาชญากรรมข้ามชาตินั้นยังประสบกับข้อจำกัดหลายประการทั้งในเชิงกฎหมาย สถาบัน และโครงสร้างพื้นฐานทางเทคโนโลยี กฎหมายว่าด้วยอาชญากรรมไซเบอร์ของลาวแม้จะระบุถึงพฤติกรรม “การใช้เทคโนโลยีเพื่อฉ้อโกงหรือหลอกลวง” ไว้ในมาตรา 7–9 แต่ยังขาดรายละเอียดด้าน

---

[249] 'Law on Prevention and Combating Cyber Crime (Unofficial Translation)' (International Telecommunication Union, 2015) <https://dig.watch/resource/laos-law-on-prevention-and-combating-cyber-crime-2015> accessed 10 March 2025.

[250] 'Data Protection Laws of the World: Laos' (DLA Piper) <https://www.dlapiperdataprotection.com/index.html?c=LA> accessed 10 March 2025.

[251] 'Penal Code' (Lao PDR Official Gazette, 2017) <https://laoofficialgazette.gov.la/kcfinder/upload/files/1Oct2020_Lao%20Penal%20Code_English%20version.pdf> accessed 10 March 2025.

ขั้นตอนทางกฎหมายในการสืบสวน รวบรวมพยานหลักฐานดิจิทัล และความร่วมมือระหว่างประเทศ ซึ่งล้วนเป็นกลไกสำคัญในการปราบปรามขบวนการข้ามชาติอย่างแก๊งคอลเซ็นเตอร์ที่มักเปลี่ยนสถานที่ตั้งหรือใช้คนต่างชาติในการปฏิบัติการ อีกทั้งปัญหาด้านโครงสร้างพื้นฐานทางเทคโนโลยีของลาว ยังเป็นอุปสรรคต่อการติดตามเส้นทางการกระทำผิด เช่น การติดตามหมายเลขโทรศัพท์ปลอม (spoofing) หรือการตรวจสอบบัญชีธนาคารที่รับโอนเงินจากเหยื่อ โดยเฉพาะเมื่อผู้กระทำความผิดใช้ระบบที่อยู่ในต่างประเทศ นอกจากนี้ ระบบการธนาคารและโทรคมนาคมของลาวยังไม่มีการพัฒนาเกณฑ์ควบคุมหรือตรวจจับพฤติกรรมที่น่าสงสัยอย่างเพียงพอ ในด้านการบังคับใช้กฎหมาย แม้จะมีการตั้งคณะกรรมการไซเบอร์หรือหน่วยงานที่เกี่ยวข้อง แต่เจ้าหน้าที่รัฐของลาวยัง ขาดความรู้ความเข้าใจเชิงเทคนิคในระดับลึกเกี่ยวกับอาชญากรรมดิจิทัล ประกอบกับทรัพยากรที่จำกัดทั้งบุคลากรและงบประมาณ จึงทำให้การดำเนินคดีกับขบวนการเหล่านี้เป็นไปได้ยาก โดยเฉพาะในกรณีที่ต้องมีการขอความร่วมมือกับต่างประเทศ เช่น การส่งผู้ร้ายข้ามแดน หรือการตรวจสอบทรัพย์สินข้ามพรมแดน สุดท้าย การที่ลาวยังไม่ได้เข้าเป็นภาคีของอนุสัญญาระหว่างประเทศว่าด้วยอาชญากรรมทางไซเบอร์ Budapest Convention on Cybercrime ทำให้ขาดกลไกความร่วมมืออย่างเป็นระบบกับประเทศอื่น ๆ ทั้งในและนอกภูมิภาค ซึ่งส่งผลให้การประสานงานในการติดตามกลุ่มแก๊งคอลเซ็นเตอร์ที่มักย้ายฐานปฏิบัติการเป็นไปอย่างล่าช้า

4.3.2.10 ประเทศเมียนมา

สำหรับประเทศเมียนมามีความพยายามในการจัดการกับอาชญากรรมไซเบอร์และแก๊งคอลเซ็นเตอร์ผ่านกฎหมายต่าง ๆ ดังนี้

1. Cybersecurity Law 2024 กฎหมายฉบับนี้มีบทบัญญัติที่เกี่ยวข้องกับการควบคุมกิจกรรมออนไลน์และการป้องกันอาชญากรรมไซเบอร์ เช่น การห้ามใช้ VPN โดยไม่ได้รับอนุญาต โดยมีโทษจำคุก 1–6 เดือน หรือปรับระหว่าง 1–10 ล้านจ๊าต การควบคุมและปิดกั้นแพลตฟอร์มดิจิทัลที่เผยแพร่ข้อมูลที่ถูกมองว่าเป็น “ข่าวปลอม” หรือ “ข่าวลือ” ซึ่งอาจส่งผลต่อความมั่นคงของรัฐ การกำหนดให้ผู้ให้บริการแพลตฟอร์มดิจิทัลต้องเก็บข้อมูลผู้ใช้เป็นเวลา 3 ปี และเปิดเผยต่อเจ้าหน้าที่ เมื่อมีการร้องขอและการลงโทษผู้ที่ให้บริการการพนันออนไลน์โดยไม่ได้รับอนุญาต ซึ่งอาจเกี่ยวข้องกับกิจกรรมของแก๊งคอลเซ็นเตอร์

2. Myanmar Penal Code ประมวลกฎหมายอาญาของเมียนมา ซึ่งมีรากฐานมาจากประมวลกฎหมายอาญาของอินเดียในยุคอาณานิคม มีบทบัญญัติที่เกี่ยวข้องกับการฉ้อโกงและการหลอกลวง

3. Telecommunications Law 2013 กฎหมายฉบับนี้มีบทบัญญัติที่เกี่ยวข้องกับการใช้เครือข่ายโทรคมนาคมในทางที่ผิด เช่น

มาตรา 66 (c) การขโมยเงินหรือทรัพย์สินใด ๆ การฉ้อโกง การยักยอก หรือการกระทำความผิดโดยใช้เครือข่ายการสื่อสารโทรคมนาคม

มาตรา 66(d) การขู่กรรโชก บีบบังคับ การจำกัดเสรีภาพโดยมิชอบ การหมิ่นประมาท การรบกวน การใช้อิทธิพลโดยมิชอบ หรือการข่มขู่บุคคลใดโดยใช้เครือข่ายการสื่อสารโทรคมนาคม[252]

แม้ว่าเมียนมาจะพยายามออกกฎหมายและระเบียบเพื่อควบคุมการใช้งานเทคโนโลยีสารสนเทศ รวมถึงความผิดที่เกิดขึ้นในโลกออนไลน์ เช่น พ.ร.บ.โทรคมนาคม ปี 2013 (Telecommunications Law), ร่างกฎหมายความมั่นคงทางไซเบอร์ (Cybersecurity Law Draft ปี 2024) และประมวลกฎหมายอาญาที่สืบทอดจากยุคอาณานิคม แต่ก็ยังประสบกับข้อจำกัดอย่างชัดเจนในการจัดการกับอาชญากรรมไซเบอร์สมัยใหม่อย่าง “แก๊งคอลเซ็นเตอร์” ที่มีลักษณะข้ามพรมแดน ซับซ้อน และเปลี่ยนแปลงรูปแบบอย่างรวดเร็ว ปัญหาประการแรก คือ กรอบกฎหมายที่ล้าหลังและไม่เฉพาะเจาะจง โดยบทบัญญัติในประมวลกฎหมายอาญา เช่น มาตรา 415 และ 420 ว่าด้วยการฉ้อโกงและหลอกลวงนั้น อาจมีเนื้อหากว้างเกินไป ไม่ครอบคลุมลักษณะเฉพาะของอาชญากรรมไซเบอร์ที่ดำเนินการผ่านโครงข่ายดิจิทัล เช่น การ spoof เบอร์โทร, การ phishing หรือการเข้าถึงระบบโดยมิชอบผ่านเทคโนโลยีอินเทอร์เน็ต นอกจากนี้ร่างกฎหมายความมั่นคงทางไซเบอร์ซึ่งร่างขึ้นภายใต้บริบทของรัฐบาลทหารกลับถูกวิพากษ์วิจารณ์ว่าเน้นควบคุมการแสดงออกทางออนไลน์และการเซ็นเซอร์ มากกว่าการป้องกันอาชญากรรมไซเบอร์อย่างแท้จริง ส่งผลให้ขาดความสมดุลระหว่างเสรีภาพและความมั่นคง

ประการที่สอง คือ ข้อจำกัดด้านโครงสร้างสถาบันและการบังคับใช้กฎหมาย เมียนมายังขาดหน่วยงานเฉพาะทางด้านอาชญากรรมไซเบอร์ที่มีอำนาจและทรัพยากรเพียงพอในการสืบสวนสอบสวนคดีข้ามชาติ อีกทั้งการบังคับใช้กฎหมายยังเผชิญกับข้อจำกัดทางการเมือง โดยเฉพาะหลัง

---

[252] Telecommunications Law 2013

Article 66. Whoever is found guilty of any of the following offences shall be liable to be punished with imprisonment for a term not exceeding 3 years or with fine or with both:

(a) disturbing, altering the specified standard or original position of, or destroying a communication network without the permission of the owner or authorized administrator;

(b) using a virus or other means for the purpose of destroying a telecommunication network;

(c) stealing money or any property, fraud, misappropriation or mischief using any communication network,

(d) extortion of any person, coercion, unlawful restriction, defamation, interfering, undue influence, or intimidation using a telecommunication network.

การรัฐประหารในปี 2021 ทำให้กลไกของรัฐและระบบยุติธรรมถูกตั้งคำถามถึงความเป็นอิสระและความโปร่งใส ยิ่งไปกว่านั้น เมียนมายังไม่มีความร่วมมือทางกฎหมายกับประเทศเพื่อนบ้านอย่างเป็นระบบ เช่น ข้อตกลงส่งผู้ร้ายข้ามแดนหรือกลไกการแบ่งปันข่าวกรองแบบเรียลไทม์ ทำให้ยากต่อการสืบสวนจับกุมแก๊งคอลเซ็นเตอร์ที่มีฐานปฏิบัติการอยู่ในประเทศแต่เหยื่ออยู่ต่างประเทศ

ประการที่สาม คือ ความไม่ชัดเจนของกฎหมายในระดับปฏิบัติ โดยเฉพาะในร่างกฎหมายความมั่นคงทางไซเบอร์ที่ยังไม่ผ่านการรับรองอย่างเป็นทางการ ส่งผลให้เกิดสุญญากาศทางกฎหมายในหลายกรณี และเปิดช่องให้เจ้าหน้าที่ตีความตามดุลพินิจ ซึ่งเสี่ยงต่อการลิดรอนสิทธิประชาชนโดยไม่จำเป็น มากกว่าการแก้ปัญหาเชิงนโยบายด้านอาชญากรรมข้ามชาติอย่างเป็นระบบด้วยข้อจำกัดทั้งในเชิงเนื้อหากฎหมาย กลไกสถาบัน และการบังคับใช้ ทำให้เมียนมายังคงเป็นจุดอ่อนสำคัญในภูมิภาคอาเซียนต่อการต่อต้านแก๊งคอลเซ็นเตอร์ ซึ่งมักใช้ประเทศที่มีกฎหมายหย่อนยานและการควบคุมอ่อนแอเป็นฐานปฏิบัติการ หากไม่มีการปฏิรูปกฎหมายและสร้างความร่วมมือระหว่างประเทศอย่างเข้มแข็ง เมียนมาจะยังคงเผชิญกับความเสี่ยงในการตกเป็น “Safe Haven” ของอาชญากรไซเบอร์ข้ามชาติอย่างต่อเนื่อง

ดังนั้น จากการศึกษากฎหมายที่เกี่ยวข้องของประเทศสมาชิกอาเซียน 10 ประเทศ พบว่าสภาพปัญหาทางกฎหมายที่เกี่ยวข้องมีลักษณะร่วมกันและมีประเด็นเฉพาะที่น่าพิจารณา ประเทศส่วนใหญ่ของอาเซียนมีความพยายามในการออกกฎหมายเฉพาะด้านอาชญากรรมไซเบอร์หรือแก้ไขกฎหมายอาญาเดิมให้ครอบคลุมความผิดสมัยใหม่ ตัวอย่างเช่น ไทยใช้พระราชบัญญัติป้องกันและปราบปรามการฟอกเงินและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในการเอาผิดกับแก๊งคอลเซ็นเตอร์ ขณะที่ฟิลิปปินส์ มีกฎหมาย Cybercrime Prevention Act of 2012 ที่มีโครงสร้างใกล้เคียงสากล แต่ยังขาดกลไกความร่วมมือเชิงปฏิบัติ ส่วนอินโดนีเซีย มี Electronic Information and Transactions Law (EIT Law) ซึ่งถูกวิจารณ์ว่ามีเนื้อหากำกวมและเปิดช่องให้เจ้าหน้าที่ใช้อำนาจเกินขอบเขต ในบางประเทศ เช่น กัมพูชาและเมียนมา แม้จะมีร่างกฎหมายเกี่ยวกับอาชญากรรมไซเบอร์ แต่ยังไม่ผ่านความเห็นชอบหรือมีเจตนาเพื่อควบคุมการแสดงออกมากกว่าการป้องกันอาชญากรรม ส่งผลให้ยังไม่มีพื้นฐานทางกฎหมายที่มั่นคงพอในการสืบสวนจับกุมเครือข่ายแก๊งคอลเซ็นเตอร์ ขณะที่ลาวแม้จะมีบทบัญญัติเกี่ยวกับอาชญากรรมไซเบอร์ในระดับหลักการ แต่การบังคับใช้ยังอยู่ในขั้นเริ่มต้น โดยขาดทั้งบุคลากรและระบบสนับสนุนทางเทคนิค ในทางตรงกันข้ามสิงคโปร์และมาเลเซียถือเป็นประเทศที่มีกฎหมายไซเบอร์ที่พัฒนาแล้ว เช่น Cybersecurity Act 2018 และ Computer Crimes Act 1997 ของมาเลเซีย รวมถึงแผนยุทธศาสตร์ความมั่นคงดิจิทัลระดับชาติ กลับกันปัญหาในประเทศเหล่านี้อยู่ที่ความท้าทายเชิงเทคโนโลยีและความร่วมมือข้ามประเทศ และบรูไนแม้จะมีกฎหมายทั่วไปเกี่ยวกับการฉ้อโกงและความผิดคอมพิวเตอร์ แต่ยังไม่มีกรอบกฎหมายเฉพาะเจาะจงด้านไซเบอร์ หรือการประสานงานเชิง

เทคนิคกับนานาชาติอย่างชัดเจน ขณะที่เวียดนามแม้มีกฎหมายหลายฉบับ เช่น Law on Cybersecurity 2018 และประมวลกฎหมายอาญา 2015 ที่ครอบคลุมความผิดไซเบอร์ แต่กลับถูกตั้งคำถามในด้านการลิดรอนเสรีภาพและการตีความกฎหมายในทางอำนาจรัฐมากกว่าการอุดช่องโหว่ในเชิงการบังคับใช้

**ตารางที่ 4.1** ตารางสรุปกฎหมายและปัญหาที่เกี่ยวข้องในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ของประเทศสมาชิกอาเซียน

| ประเทศ | มีกฎหมายไซเบอร์เฉพาะ | มีบทบัญญัติต่อต้านแก๊งคอลเซ็นเตอร์ | ระบบบังคับใช้มีประสิทธิภาพ | มีกลไกความร่วมมือข้ามชาติ | หมายเหตุ |
|---|---|---|---|---|---|
| ไทย | ✓ | ✓ | ขาดการบังคับใช้แบบเชิงรุก | ความร่วมมือยังจำกัด | มีกฎหมายหลายฉบับ เช่น พ.ร.บ.คอมพิวเตอร์, ประมวลกฎหมายอาญา, พ.ร.บ.ฟอกเงิน แต่กฎหมายกระจายหลายฉบับ ซึ่งบางมาตราล้าสมัยและการบังคับใช้ข้ามแดนยาก |
| ฟิลิปปินส์ | ✓ | ✓ | ศักยภาพทางเทคนิคต่ำ | ประสานงานยังช้า | มีกฎหมาย Cybercrime Prevention Act (RA 10175), Anti-Wiretapping Act, Anti-Fraud แต่การบังคับใช้ไม่ทั่วถึง |
| มาเลเซีย | ✓ | ✓ | ✓ | ✓ | มีกฎหมาย Computer Crimes Act, Communications and Multimedia Act, Penal Code แต่การบังคับใช้ยังไม่ทันต่อเทคโนโลยีใหม่ |
| สิงคโปร์ | ✓ | ✓ | ✓ | ✓ | มีกฎหมาย Cybersecurity Act, Computer Misuse Act, Penal Code มีการบังคับใช้เข้มงวดและใช้เทคโนโลยีสูง |
| บรูไน | มีกฎหมายทั่วไปเท่านั้น | ยังไม่ชัดเจนเรื่องพฤติกรรมเฉพาะ | ยังพึ่งกฎหมายอาญาทั่วไป | | มีกฎหมาย Penal Code, Sedition Act, Telecommunications Order ขาดกฎหมายเฉพาะด้านไซเบอร์โดยตรง และกรอบการสืบสวนจำกัด |
| เวียดนาม | ✓ | ✓ | ใช้เพื่อควบคุมข้อมูลมากกว่า | | มีกฎหมาย Cybersecurity Law (2018), Penal Code 2015 ถูกวิจารณ์ว่าละเมิดสิทธิพลเมือง และควบคุมเนื้อหาออนไลน์มากกว่าความปลอดภัยไซเบอร์ |

**ตารางที่ 4.1** (ต่อ)

| ประเทศ | มีกฎหมายไซเบอร์เฉพาะ | บทบัญญัติต่อต้านแก๊งคอลเซ็นเตอร์ | ระบบบังคับใช้มีประสิทธิภาพ | มีกลไกความร่วมมือข้ามชาติ | หมายเหตุ |
|---|---|---|---|---|---|
| กัมพูชา | อยู่ระหว่างร่างกฎหมาย | ใช้กฎหมายอาญา/คอมฯ ทั่วไป | | | ยังไม่มีกฎหมายไซเบอร์ฉบับสมบูรณ์ (อยู่ระหว่างร่าง: Draft Law on Cybercrime) ช่องว่างทางกฎหมายสูง ขาดกรอบควบคุมการดำเนินคดีออนไลน์ |
| เมียนมา | มีเพียงกฎหมายสื่อ/โทรคมนาคม | | | | มี Electronic Transactions Law และร่าง Cybersecurity Law ร่างกฎหมายขัดสิทธิมนุษยชน และยังไม่มีระบบการดำเนินการที่มีประสิทธิภาพ |
| ลาว | ✓ | ยังไม่ครอบคลุมความผิดยุคใหม่ | | | มีบางกฎหมาย เช่น Law on Prevention and Combating Cybercrime (2015) แต่ยังจำกัด และขาดบุคลากร-เครื่องมือ และการบังคับใช้ยังอ่อน |
| อินโดนีเซีย | ✓ | ✓ | ปัญหาตีความกฎหมาย | ความร่วมมือยังไม่สมบูรณ์ | มีกฎหมาย: Electronic Information and Transactions Law (ITE Law), Criminal Code แต่การตีความกฎหมายไม่ชัด การใช้กฎหมายบางครั้งกระทบสิทธิเสรีภาพ |

**ที่มา** สรุปโดยผู้วิจัย

## 4.4 สภาพปัญหาในทางปฏิบัติที่เกี่ยวกับอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

อาชญากรรมข้ามชาติที่เกิดจากแก๊งคอลเซ็นเตอร์เป็นปัญหาที่ซับซ้อนและมีผลกระทบอย่างกว้างขวางในภูมิภาคอาเซียน ด้วยการใช้เทคโนโลยีสื่อสารที่ทันสมัยและช่องโหว่ทางด้านกฎหมายทำให้แก๊งคอลเซ็นเตอร์สามารถขยายการก่ออาชญากรรมข้ามพรมแดนได้ง่ายขึ้น อีกทั้งการรับมือกับปัญหานี้ในทางปฏิบัติยังคงเต็มไปด้วยอุปสรรคและความท้าทายที่หลากหลาย เนื่องจากในปัจจุบันอาเซียนยังไม่มีหน่วยงานที่เฉพาะเจาะจงสำหรับการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์โดยตรง มีเพียงแต่หน่วยงานที่ดูแลและรับผิดชอบในด้านการจัดการกับอาชญากรรมข้ามชาติและความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งสามารถครอบคลุมการรับมือกับการกระทำผิดของแก๊งคอลเซ็นเตอร์ที่ใช้เทคโนโลยีและกลวิธีการหลอกลวงข้ามพรมแดนในการก่ออาชญากรรม หน่วยงานหลักที่มีบทบาทสำคัญในด้านนี้ ได้แก่

ASEANAPOL (ASEAN Chiefs of National Police) เป็นองค์กรที่ประกอบด้วยหน่วยงานตำรวจระดับสูงสุดจาก 10 ประเทศสมาชิกอาเซียน มีบทบาทในการส่งเสริมความร่วมมือด้านการบังคับใช้กฎหมายระหว่างประเทศสมาชิกอาเซียน เพื่อป้องกันและปราบปรามอาชญากรรมข้ามชาติที่ส่งผลกระทบต่อความมั่นคงและความสงบเรียบร้อยในภูมิภาค ASEANAPOL ทำหน้าที่เป็นเวทีในการแลกเปลี่ยนข้อมูลข่าวกรองและการประสานงานระหว่างหน่วยงานตำรวจของประเทศสมาชิก ครอบคลุมการจัดการกับอาชญากรรมข้ามชาติรูปแบบต่าง ๆ เช่น การค้ามนุษย์ การก่อการร้าย การค้ายาเสพติด การฟอกเงิน การลักลอบค้าอาวุธ การโจรกรรมรถยนต์ และอาชญากรรมทางเศรษฐกิจ รวมถึงอาชญากรรมทางไซเบอร์[253]

ASEAN Cybercrime Operations Desk (ACOD) เป็นหน่วยงานภายใต้การสนับสนุนของ INTERPOL ที่ที่จัดตั้งขึ้น เพื่อเสริมสร้างความสามารถในการรับมือกับอาชญากรรมทางไซเบอร์ที่ข้ามพรมแดนในภูมิภาคอาเซียน ACOD มีบทบาทสำคัญในการประสานงานและสนับสนุนการสืบสวนที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ โดยเฉพาะอย่างยิ่งการหลอกลวงทางออนไลน์และการฉ้อโกงที่เกิดขึ้นจากแก๊งคอลเซ็นเตอร์ซึ่งเป็นภัยคุกคามที่เพิ่มขึ้นอย่างต่อเนื่องในภูมิภาคนี้ บทบาทของ ACOD มุ่งเน้นไปที่การรวบรวม วิเคราะห์ และแลกเปลี่ยนข้อมูลข่าวกรองที่เกี่ยวข้องกับการก่ออาชญากรรมไซเบอร์ระหว่างหน่วยงานตำรวจของประเทศสมาชิกอาเซียน ACOD ช่วยอำนวยความสะดวกในการประสานงานระหว่างประเทศ ทำให้การติดตามอาชญากรข้ามพรมแดนและการดำเนินคดีเป็นไปได้

---

[253] 'ASEANAPOL' (ASEANAPOL Secretariat) <http://www.aseanapol.org/>accessed 10 December 2024.

อย่างมีประสิทธิภาพมากขึ้น นอกจากนี้ ACOD ยังมีส่วนช่วยในการวางแผนปฏิบัติการร่วมเพื่อจับกุมกลุ่มอาชญากรและรื้อถอนเครือข่ายการกระทำผิดทางไซเบอร์[254]

ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) หน่วยงานของอาเซียนที่มีบทบาทในการประสานงานและกำหนดยุทธศาสตร์เพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ในภูมิภาคอาเซียน โดยมุ่งเน้นการจัดการและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในระดับภูมิภาค การสร้างความร่วมมือระหว่างประเทศสมาชิกอาเซียน และการพัฒนาความสามารถทางไซเบอร์ของประเทศสมาชิกเพื่อให้สามารถรับมือกับอาชญากรรมทางไซเบอร์

ซึ่งจากการศึกษาถึงการทำงานของหน่วยงานดังกล่าวพบว่า ในทางปฏิบัติยังคงเต็มไปด้วยอุปสรรคและความท้าทายที่หลากหลาย ซึ่งสามารถวิเคราะห์ถึงสภาพปัญหาในทางปฏิบัติ ดังนี้

**4.4.1 ปัญหาความร่วมมือด้านการแลกเปลี่ยนข้อมูลและข่าวกรอง**

การแลกเปลี่ยนข้อมูลข่าวกรองถือเป็นกลไกสำคัญในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีของแก๊งคอลเซ็นเตอร์ซึ่งมีลักษณะการดำเนินงานเป็นเครือข่ายข้ามพรมแดนที่ซับซ้อน การเฝ้าระวัง การติดตาม และการสกัดกั้นอาชญากรรมเหล่านี้ไม่สามารถพึ่งพาเพียงกลไกภายในประเทศได้ จำเป็นต้องมีการแลกเปลี่ยนข้อมูลอย่างทันท่วงทีระหว่างประเทศสมาชิก อย่างไรก็ดี จากการศึกษาพบว่า ความร่วมมือด้านการแลกเปลี่ยนข้อมูลในภูมิภาคอาเซียนยังคงประสบปัญหาเชิงโครงสร้างและข้อจำกัดในหลายมิติ

1. การขาดกลไกกลางที่มีลักษณะถาวรและมีอำนาจบังคับใช้ในระดับภูมิภาค แม้อาเซียนจะมีหน่วยงาน เช่น ASEANAPOL และ INTERPOL ASEAN Cybercrime Operations Desk ที่มีบทบาทในการประสานงานระหว่างตำรวจในภูมิภาค แต่การแลกเปลี่ยนข้อมูลยังคงอยู่ในลักษณะสมัครใจ ไม่มีกรอบข้อผูกพันทางกฎหมายที่ชัดเจน ส่งผลให้ประเทศสมาชิกบางรายลังเลที่จะส่งต่อข้อมูลที่ละเอียดอ่อน โดยเฉพาะในคดีที่อาจเกี่ยวข้องกับความมั่นคงหรือผลประโยชน์ระดับชาติ ซึ่งสะท้อนถึงข้อจำกัดเชิงสถาบันในระดับภูมิภาคที่ยังไม่มีการพัฒนากลไกบังคับที่เทียบเท่ากับโครงสร้างของ Europol หรือ SIENA ของสหภาพยุโรป[255]

2. ความแตกต่างของกฎหมายภายในประเทศสมาชิกอาเซียน ซึ่งเป็นอุปสรรคต่อการแลกเปลี่ยนข้อมูลอย่างมีประสิทธิภาพ กล่าวคือ แต่ละประเทศมีนิยาม ความเข้าใจ และระดับการคุ้มครองข้อมูลที่แตกต่างกัน เช่น ข้อมูลผู้ต้องสงสัยที่ยังไม่ถูกตั้งข้อหาหรือยังอยู่ในกระบวนการ

---

[254] 'ASEAN's Cyber Initiatives: A Select List' (Center for Strategic and International Studies) <http://www.csis.org/blogs/strategic-technologies-blog/aseans-cyber-initiatives-select-list> accessed 10 December 2024.

[255] Helena Carrapico and André Barrinha, "European Union Cyber Diplomacy: A Coherent Actor?" *Journal of Common Market Studies* 56, no. 5 (2018): 1250–1266.

สืบสวน อาจถูกมองว่าเป็นข้อมูลลับที่ไม่สามารถเปิดเผยได้ในบางประเทศ ขณะที่อีกประเทศอาจอนุญาตให้มีการแชร์ข้อมูลเพื่อป้องกันอาชญากรรมล่วงหน้า ความไม่สอดคล้องเช่นนี้สะท้อนถึงการขาดกฎหมายระดับภูมิภาคที่กำหนดมาตรฐานร่วมด้านการปกป้องและการแบ่งปันข่าวกรองอย่างชัดเจน หนึ่งในความท้าทายของอาเซียนคือการขาด harmonisation ด้านกฎหมายไซเบอร์และการแบ่งปันข้อมูลข่าวกรองระหว่างประเทศสมาชิก

3. ปัจจัยทางการเมืองและภูมิรัฐศาสตร์ ที่บั่นทอนระดับความไว้วางใจระหว่างประเทศสมาชิก ความสัมพันธ์ทางการทูตที่ไม่แน่นแฟ้น หรือความขัดแย้งเชิงผลประโยชน์ในด้านเศรษฐกิจและความมั่นคง[256] อาจทำให้บางประเทศเลือกที่จะจำกัดการส่งต่อข้อมูลให้เฉพาะพันธมิตรที่ใกล้ชิดเท่านั้น ซึ่งในอาเซียนยังคงมีความรอบคอบสูงในการแบ่งปันข้อมูลข่าวกรองที่เกี่ยวข้องกับความมั่นคงภายในประเทศทำให้กระบวนการแลกเปลี่ยนข้อมูลเป็นไปอย่างจำกัดทั้งในเชิงปริมาณและความลึกของเนื้อหา

**4.4.2 ปัญหาการขาดทรัพยากรและขีดความสามารถในการปฏิบัติการ**

ปัญหาการขาดทรัพยากรและขีดความสามารถในการปฏิบัติการของหน่วยงานบังคับใช้กฎหมายในภูมิภาคอาเซียน เป็นอุปสรรคสำคัญที่ทำให้การรับมือกับอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์มีประสิทธิภาพต่ำกว่าที่ควรจะเป็น แม้จะมีความพยายามในการสร้างความร่วมมือระดับภูมิภาคแต่ยังคงมีความเหลื่อมล้ำด้านศักยภาพและทรัพยากรระหว่างประเทศสมาชิกส่งผลให้การประสานงานมีประสิทธิภาพจำกัด ซึ่งจากการศึกษาพบว่า กลุ่มประเทศสมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ (อาเซียน) ได้ริเริ่มดำเนินมาตรการหลายประการในการเสริมสร้างความสามารถด้านความมั่นคงทางไซเบอร์ของภูมิภาค โดยครอบคลุมทั้งการพัฒนาขีดความสามารถ การสร้างองค์ความรู้ และการแลกเปลี่ยนข้อมูลข่าวสารเกี่ยวกับอาชญากรรมไซเบอร์ระหว่างประเทศสมาชิก อาเซียนประกอบด้วยประเทศสมาชิก 10 ประเทศและมีผลิตภัณฑ์มวลรวมภายในประเทศ (GDP) รวมกันราว 3.2 ล้านล้านดอลลาร์สหรัฐ โดยตำแหน่งประธานหมุนเวียนประจำปี ซึ่งในปี ค.ศ. 2024 ประเทศลาวได้รับหน้าที่ดังกล่าว[257] แม้ว่าอาเซียนจะมีการขับเคลื่อนความร่วมมือทางไซเบอร์เพิ่มขึ้น แต่ขีดความสามารถของประเทศสมาชิกกลับมีความแตกต่างกันอย่างมีนัยสำคัญ ตัวอย่างเช่น ประเทศที่มีความก้าวหน้าอย่างสิงคโปร์และมาเลเซีย มีโครงสร้างพื้นฐานด้านความมั่นคงไซเบอร์ระดับชาติ และมีระบบนิเวศด้านเทคโนโลยีที่เข้มแข็ง ในขณะที่ประเทศที่มีทรัพยากรจำกัด เช่น เมียน

---

[256] United Nations Office on Drugs and Crime (UNODC), *Enhancing International Cooperation in Criminal Matters in ASEAN: Barriers and Good Practices* (2024) 17–18.

[257] 'ASEAN's Cyber Initiatives: A Select List' (Center for Strategic and International Studies) https://www.csis.org/blogs/strategic-technologies-blog/aseans-cyber-initiatives-select-list accessed 29 June 2025.

มา กัมพูชา และลาว ยังขาดแคลนโครงสร้างพื้นฐานและบุคลากร ซึ่งจำกัดขีดความสามารถของประเทศเหล่านี้ในการตอบสนองต่อภัยคุกคามทางไซเบอร์[258] รายงานดัชนีการบูรณาการทางดิจิทัลของอาเซียน (ASEAN Digital Integration Index) สะท้อนความเหลื่อมล้ำดังกล่าวอย่างชัดเจน โดยสิงคโปร์มีคะแนนเฉลี่ยสูงสุดอยู่ที่ 80.70 ขณะที่เมียนมามีคะแนนเฉลี่ยต่ำที่สุดเพียง 30.11 คะแนน จากข้อมูลดังกล่าวเห็นได้ถึงความเหลื่อมล้ำในด้านขีดความสามารถไซเบอร์ของประเทศสมาชิกอาเซียน ซึ่งบ่งชี้ถึงระดับความพร้อมในการบริหารจัดการภัยคุกคามทางไซเบอร์ที่ไม่เท่าเทียมกันระหว่างประเทศสมาชิก ซึ่งส่งผลโดยตรงต่อประสิทธิภาพของความร่วมมือระดับภูมิภาคในด้านการป้องกันและปราบปรามอาชญากรรมไซเบอร์ก่อให้เกิดปัญหาทั้งในเชิงโครงสร้างและการปฏิบัติจริง โดยประเทศที่มีระบบความมั่นคงทางไซเบอร์เข้มแข็งมักจะสามารถรับมือกับภัยคุกคามใหม่ ๆ ได้อย่างรวดเร็วและแม่นยำ ทั้งในด้านการวิเคราะห์ การสืบสวน และการตอบโต้ ขณะที่ประเทศที่มีทรัพยากรจำกัดจำเป็นต้องพึ่งพาความช่วยเหลือจากภายนอกและอาจไม่สามารถตรวจจับภัยคุกคามได้ทันท่วงที ซึ่งช่องว่างดังกล่าวกลายเป็นจุดอ่อนทางยุทธศาสตร์ที่อาชญากรข้ามชาติสามารถใช้เป็นช่องทางโจมตีได้ง่ายกว่า

อีกทั้งยังมีในเรื่องของการขาดแคลนบุคลากรที่มีความเชี่ยวชาญเฉพาะทางซึ่งแก๊งคอลเซ็นเตอร์มีรูปแบบการกระทำผิดซับซ้อนและข้ามพรมแดน เจ้าหน้าที่ผู้ปฏิบัติงานจึงจำเป็นต้องมีทักษะทางเทคนิคหลายด้าน ไม่ว่าจะเป็นการสืบสวนในเชิงดิจิทัล (digital forensics), การถอดรหัสข้อมูลทางไซเบอร์ (cyber decoding), การตรวจสอบเส้นทางการเงินผ่านระบบอิเล็กทรอนิกส์ (digital financial tracking), และการวิเคราะห์ข่าวกรองที่ได้จากการสกัดข้อมูลบนเครือข่ายออนไลน์ (cyber intelligence analysis) รายงานโดย ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) ระบุว่า กัมพูชา ลาว และเมียนมา มีเจ้าหน้าที่ผู้ปฏิบัติงานด้านไซเบอร์ในภาครัฐในระดับต่ำกว่าเกณฑ์ที่จำเป็น และขาดโปรแกรมการฝึกอบรมอย่างเป็นระบบหรือหลักสูตรประจำปีที่ใช้พัฒนาเจ้าหน้าที่เหล่านี้ให้ทันต่อเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว[259] ส่วนประเทศที่มีความก้าวหน้าในด้านนี้ ได้แก่ สิงคโปร์และมาเลเซีย ก็ต้องเผชิญกับความต้องการบุคลากรที่เกินกว่ากำลังผลิตของสถาบันการศึกษาและระบบฝึกอบรมภายในประเทศ เช่น ในสิงคโปร์เอง รัฐบาลถึงกับต้องออกโครงการ Cybersecurity Talent Development Fund และ Cybersecurity Associates and Technologists Programmed เพื่อเร่งสร้างบุคลากรในระยะสั้นและระยะยาวให้เพียงพอกับ

---

[258] Ibid.

[259] 'Annual Report on Cybersecurity Training in ASEAN' (ASEAN-Japan Cybersecurity Capacity Building Centre) <https://ajccbc.dga.or.th> accessed 29 June 2025.

ภัยคุกคามที่เพิ่มขึ้น[260] และในหลายกรณีหน่วยงานในประเทศกำลังพัฒนาในอาเซียนต้องพึ่งพาผู้เชี่ยวชาญจากต่างประเทศ เช่น หน่วยงาน FBI ของสหรัฐฯ, INTERPOL, หรือองค์กรพัฒนาเทคโนโลยีจากญี่ปุ่นและเกาหลีใต้ เพื่อถอดรหัสข้อมูลที่ถูกเข้ารหัสหรือช่วยสอบสวนเส้นทางการเงินที่ซับซ้อน แม้จะเป็นประโยชน์ในระยะสั้นแต่การพึ่งพาบุคคลภายนอกอย่างต่อเนื่องอาจทำให้ประเทศเหล่านี้ขาดความสามารถในการดำเนินการด้วยตนเองและยังอาจก่อให้เกิดข้อกังวลด้านความมั่นคงและอธิปไตย โดยเฉพาะในเรื่องของการเปิดเผยข้อมูลที่มีความอ่อนไหวทางความมั่นคงให้แก่บุคคลหรือองค์กรภายนอก ดังนั้น ปัญหาการขาดทรัพยากรและขีดความสามารถในการปฏิบัติการของอาเซียนเป็นมากกว่าประเด็นเชิงงบประมาณ แต่ครอบคลุมตั้งแต่โครงสร้างพื้นฐาน เทคโนโลยี บุคลากร ไปจนถึงวัฒนธรรมการบริหารงานและความสามารถในการบูรณาการข้อมูลและความร่วมมือ ซึ่งล้วนเป็นข้อจำกัดสำคัญที่ทำให้อาเซียนยังไม่สามารถดำเนินการเชิงรุกและตอบสนองต่อภัยคุกคามจากแก๊งคอลเซ็นเตอร์ข้ามชาติได้อย่างเต็มประสิทธิภาพ

**4.4.3 ปัญหาการขาดหน่วยงานเฉพาะเจาะจงในการรับมือกับแก๊งคอลเซ็นเตอร์ในภูมิภาคอาเซียน**

ลักษณะเฉพาะของแก๊งคอลเซ็นเตอร์ คือ การใช้เทคโนโลยีระดับสูง การแฝงตัวในระบบออนไลน์ และการเคลื่อนย้ายข้ามพรมแดนอย่างรวดเร็ว ซึ่งต้องการหน่วยงานที่มีความเชี่ยวชาญเฉพาะทางในด้านไซเบอร์ การวิเคราะห์ข้อมูลข่าวกรอง การตรวจสอบเส้นทางการเงิน และการทำงานร่วมกับหน่วยงานในต่างประเทศ แต่ในหลายประเทศยังคงดำเนินการภายใต้โครงสร้างระบบราชการแบบดั้งเดิม ทำให้การประสานงานภายในประเทศล่าช้า ไม่มีศูนย์กลางข้อมูลหรือฐานข้อมูลกลางที่ใช้ติดตามพฤติกรรมและเส้นทางของกลุ่มอาชญากร หนึ่งในสาเหตุสำคัญที่ทำให้ความพยายามในการปราบปรามแก๊งคอลเซ็นเตอร์ในภูมิภาคอาเซียนยังไม่มีประสิทธิภาพเท่าที่ควร คือ การขาดหน่วยงานเฉพาะทางหรือหน่วยงานกลางที่รับผิดชอบโดยตรงในการติดตาม ป้องกัน และดำเนินคดีกับอาชญากรรมข้ามชาติประเภทนี้โดยเฉพาะ แม้ว่าแต่ละประเทศจะมีหน่วยงานบังคับใช้กฎหมายอยู่แล้ว เช่น สำนักงานตำรวจแห่งชาติหรือหน่วยงานปราบปรามอาชญากรรมทางเศรษฐกิจ แต่หน่วยงานเหล่านี้มักมีภารกิจหลากหลายและขาดการจัดสรรทรัพยากรที่เพียงพอให้สามารถมุ่งเน้นที่แก๊งคอลเซ็นเตอร์โดยตรง

ตัวอย่างเช่น ในประเทศไทย แม้จะมีการจัดตั้งศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.) แต่หน่วยงานนี้ยังไม่มีฐานะเป็นหน่วยงานถาวรตามกฎหมาย และยังต้องพึ่งพางบประมาณหรือคำสั่งชั่วคราวจากผู้บังคับบัญชาเป็นหลัก ซึ่งส่งผลต่อความต่อเนื่องในการปฏิบัติภารกิจและการพัฒนาขีดความสามารถอย่างเป็นระบบ ในขณะที่ประเทศเพื่อนบ้านอย่างเมียน

---

[260] ‘Cybersecurity Talent Development Initiatives’ (Cyber Security Agency of Singapore) <https://www.csa.gov.sg/programmes/talent> accessed 29 June 2025.

มา ลาว และกัมพูชา ยิ่งมีข้อจำกัดมากกว่า เพราะขาดโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ และยังไม่มีการจัดตั้งหน่วยงานเฉพาะทางที่มีบุคลากรหรืออำนาจหน้าที่ที่ชัดเจนในการรับมือกับคดีลักษณะนี้ ในระดับอาเซียนแม้จะมีกลไกหลายประการที่เกี่ยวข้องกับการปราบปรามอาชญากรรมข้ามชาติ เช่น

1. การประชุมรัฐมนตรีอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Ministerial Meeting on Transnational Crime - AMMTC)

2. การประชุมเจ้าหน้าที่อาวุโสด้านอาชญากรรมข้ามชาติ (Senior Officials Meeting on Transnational Crime - SOMTC)

3. ความร่วมมือระหว่างสำนักงานตำรวจแห่งชาติ (ASEANAPOL)

4. หน่วยงาน ASEAN Desk ของ INTERPOL

5. ศูนย์พัฒนาศักยภาพด้านความมั่นคงไซเบอร์อาเซียน-ญี่ปุ่น (ASEAN-Japan Cybersecurity Capacity Building Centre - AJCCBC)

แต่กลไกเหล่านี้ส่วนใหญ่ยังอยู่ในลักษณะเชิงนโยบาย หรือเน้นการฝึกอบรมมากกว่าการดำเนินการเชิงปฏิบัติการจริง ไม่มีหน่วยงานระดับภูมิภาคที่ทำหน้าที่เป็นศูนย์กลางในการรวบรวม วิเคราะห์ และแบ่งปันข้อมูลข่าวกรองเกี่ยวกับแก๊งคอลเซ็นเตอร์โดยเฉพาะ อีกทั้งยังไม่มีฐานข้อมูลร่วมที่สามารถเชื่อมโยงแบบเรียลไทม์ระหว่างประเทศสมาชิก และไม่มีเจ้าหน้าที่ปฏิบัติการระดับภูมิภาคที่สามารถทำงานร่วมกันในลักษณะข้ามพรมแดนได้อย่างมีประสิทธิภาพ เช่นเดียวกับที่สหภาพยุโรป (EU) จัดตั้งหน่วยงาน Europol Cybercrime Centre[261] (EC3) ที่ทำหน้าที่เป็นศูนย์กลางด้านอาชญากรรมไซเบอร์ในยุโรป ซึ่งมีทั้งอำนาจในการประสานงาน วิเคราะห์ข้อมูลเชิงลึก และสนับสนุนการดำเนินการร่วมของประเทศสมาชิกผ่านโครงการ Joint Cybercrime Action Taskforce (J-CAT) และการบริหารจัดการฐานข้อมูลอาชญากรรมไซเบอร์ที่เป็นระบบและต่อเนื่อง ในขณะที่กลไกของอาเซียนยังขาดความสามารถเหล่านี้อย่างมีนัยสำคัญ เมื่อไม่มีหน่วยงานที่มีอำนาจเฉพาะเจาะจงและทรัพยากรพร้อมในการติดตามและปราบปรามแก๊งคอลเซ็นเตอร์โดยตรง ส่งผลให้การดำเนินการในหลายประเทศมักเป็นเพียงการ “ดับไฟเฉพาะหน้า” หรือเน้นการจับกุมเมื่อได้รับ

---

[261] ศูนย์ยุโรปเพื่อการต่อต้านอาชญากรรมไซเบอร์ (European Cybercrime Centre - EC3) เป็นหน่วยงานเฉพาะทางภายใต้สำนักงานตำรวจยุโรป (Europol) ที่ก่อตั้งขึ้นในวันที่ 11 มกราคม 2013 ณ กรุงเฮก ประเทศเนเธอร์แลนด์ โดยมีวัตถุประสงค์หลักเพื่อเสริมสร้างขีดความสามารถของหน่วยงานบังคับใช้กฎหมายของสหภาพยุโรป (EU) ในการรับมือกับอาชญากรรมไซเบอร์ที่มีความซับซ้อนและข้ามพรมแดน; โปรดดู: ‘European Cybercrime Centre (EC3)’ (Europol) https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 accessed 3 May 2025.

แจ้งความเท่านั้น โดยไม่มีระบบการวิเคราะห์ข้อมูลเชิงลึก หรือการดำเนินมาตรการป้องกันในเชิงโครงสร้าง

**ตารางที่ 4.2** สรุปสภาพปัญหาในปัจจุบันที่เกี่ยวกับอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ที่เป็นภัยต่อความมั่นคงในภูมิภาคเอเชียตะวันออกฉียงใต้

| สภาพปัญหา | | ปัญหา/ประเด็น |
|---|---|---|
| สภาพปัญหาทางด้านนโยบาย | นโยบายหลัก | ASEAN Plan of Action to Combat Transnational Crime (2016-2025)<br>- ไม่ได้มุ่งเป้าเฉพาะอาชญากรรมไซเบอร์ หรืออาชญากรรมในรูปแบบใหม่<br>- เน้นความร่วมมือในภาพรวมโดยไม่มีกลไกบังคับใช้ หรือระบบประเมินผลการดำเนินงาน<br>- ขาดความชัดเจนในบทบาทของหน่วยงานกลางที่มีอำนาจประสานงานระหว่างประเทศในกรณีที่ต้องดำเนินการเร่งด่วน |
| | นโยบายเฉพาะด้าน | ASEAN Cybersecurity Cooperation Strategy (ACCS)<br>- ไม่ใช่กฎหมายที่มีผลผูกพัน รัฐสมาชิกจึงสามารถปฏิบัติหรือไม่ปฏิบัติได้ตามความสมัครใจ<br>- ข้อเสนอส่วนใหญ่ยังเป็นระดับแนวทาง เช่น การส่งเสริมความร่วมมือ การแบ่งปันข้อมูล หรือการพัฒนาศักยภาพ ซึ่งยังไม่ตอบโจทย์การจัดการภัยคุกคามเฉพาะทางอย่างแก๊งคอลเซ็นเตอร์<br>- ขาดการกำกับติดตามผลและการวัดประสิทธิภาพ อย่างจริงจัง |
| สภาพปัญหาทางด้านกฎหมาย | | 1. มาตรการที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ในภูมิภาคอาเซียนที่มีสภาพบังคับทางกฎหมาย<br>สนธิสัญญาความช่วยเหลือซึ่งกันและกันในทางอาญาของภูมิภาคอาเซียน (Treaty on Mutual Legal Assistance in Criminal Matters - ASEAN MLAT)<br>- มีความล่าช้าในกระบวนการขอความช่วยเหลือ จากขั้นตอนราชการที่ซับซ้อนและไม่มีระบบอิเล็กทรอนิกส์ |

**ตารางที่ 4.2** (ต่อ)

| สภาพปัญหา | ปัญหา/ประเด็น |
|---|---|
| | - ข้อจำกัดในการตีความคำว่าความช่วยเหลือทางอาญา ซึ่งอาจไม่ครอบคลุมรูปแบบอาชญากรรมไซเบอร์สมัยใหม่<br>- เหตุแห่งการปฏิเสธคำร้อง ตามมาตรา 3 ของสนธิสัญญาฯ ที่ให้อำนาจแก่รัฐภาคีปฏิเสธได้หากเห็นว่าขัดต่อกฎหมายภายในหรือผลประโยชน์แห่งรัฐ อาจถูกตีความกว้างเกินไปจนกระทบการร่วมมือจริง<br>2. มาตรการที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ในภูมิภาคอาเซียนที่ยังไม่มีสภาพบังคับทางกฎหมาย<br>ปฏิญญาอาเซียนว่าด้วยการป้องกันและปราบปรามอาชญากรรมไซเบอร์ (ASEAN Declaration to Prevent and Combat Cybercrime)<br>- ขาดผลผูกพันทางกฎหมาย<br>- ขาดกลไกการติดตามหรือบังคับให้รัฐสมาชิกดำเนินการตาม<br>- ข้อเสนอหลายอย่างยังอยู่ในระดับเจตนารมณ์ เช่น “การส่งเสริมการฝึกอบรมและการแลกเปลี่ยนข้อมูล” โดยไม่มีรายละเอียดการดำเนินการที่ชัดเจน ผลคือ การรับมือกับปัญหาที่เกิดขึ้นจริง เช่น แก๊งคอลเซ็นเตอร์ข้ามพรมแดน จึงยังไม่มีท่าทีที่เป็นรูปธรรม |

**ตารางที่ 4.2** (ต่อ)

| สภาพปัญหา | ปัญหา/ประเด็น |
|---|---|
| สภาพปัญหาในทางปฏิบัติ | 1. ปัญหาความร่วมมือด้านการแลกเปลี่ยนข้อมูลและข่าวกรอง<br>ความร่วมมือยังไม่มีความเป็นระบบและไม่มีกลไกกลางที่มีสภาพบังคับ ส่งผลให้การแลกเปลี่ยนข้อมูลเกิดความล่าช้าและไม่ทั่วถึง นอกจากนี้ ยังมีอุปสรรคจากความแตกต่างของกฎหมายภายใน ความไว้วางใจระหว่างรัฐ และความเหลื่อมล้ำด้านศักยภาพของหน่วยงานบังคับใช้กฎหมายในแต่ละประเทศ ทำให้การสกัดกั้นแก๊งคอลเซ็นเตอร์ไม่มีประสิทธิภาพเท่าที่ควร<br>2. ปัญหาการขาดทรัพยากรและขีดความสามารถในการปฏิบัติการ<br>อาเซียนยังมีความเหลื่อมล้ำด้านโครงสร้างพื้นฐาน บุคลากร และเทคโนโลยีในการรับมือภัยคุกคามไซเบอร์ โดยเฉพาะในประเทศที่มีทรัพยากรจำกัด ทำให้ไม่สามารถตอบสนองภัยจากแก๊งคอลเซ็นเตอร์ได้อย่างมีประสิทธิภาพ<br>3. ปัญหาการขาดหน่วยงานเฉพาะเจาะจงในการรับมือกับแก๊งคอลเซ็นเตอร์ในภูมิภาคอาเซียน<br>แม้แก๊งคอลเซ็นเตอร์จะใช้เทคโนโลยีและข้ามพรมแดนได้รวดเร็ว แต่หลายประเทศในอาเซียนยังขาดหน่วยงานเฉพาะทางที่มีขีดความสามารถในการติดตาม ป้องกัน และดำเนินคดีโดยตรง ทำให้การประสานงานล่าช้า ไม่มีศูนย์กลางข้อมูลกลางหรือกลไกความร่วมมือระดับภูมิภาคแบบที่สหภาพยุโรปมี จึงส่งผลให้การจัดการแก๊งคอลเซ็นเตอร์ยังคงเป็นลักษณะ “แก้ปัญหาเฉพาะหน้า” มากกว่าการดำเนินการเชิงรุกอย่างยั่งยืน |

**ที่มา** สรุปโดยผู้วิจัย

# บทที่ 5

# วิเคราะห์ผลกระทบ แนวทาง และมาตรการของอาเซียนในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ โดยเฉพาะกรณีแก๊งคอลเซ็นเตอร์

## 5.1 วิเคราะห์ผลกระทบของปัญหาอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้

แก๊งคอลเซ็นเตอร์นั้นนอกจากเป็นอาชญากรรมที่กระทำลงและส่งผลกระทบโดยตรงต่อสิทธิในร่างกาย อนามัยและเสรีภาพของเหยื่อยังส่งผลกระทบต่อชุมชนและสังคมอีกด้วย โดยการกระทำเหล่านี้ล้วนเป็นตัวการสำคัญในการบ่อนทำลายกระบวนการบังคับใช้กฎหมายและกระบวนการยุติธรรม จากการศึกษาค้นพบว่า ปัญหาแก๊งคอลเซ็นเตอร์ได้ส่งผลกระทบโดยตรงต่อประเทศชาติรวมไปถึงส่งผลกระทบต่อภูมิภาคอาเซียนหลายประการ ดังนี้

### 5.1.1 ผลกระทบต่อบุคคล

ปัญหาแก๊งคอลเซ็นเตอร์ที่แพร่กระจายในภูมิภาคอาเซียนได้สร้างผลกระทบร้ายแรงต่อบุคคลในหลายมิติ โดยเฉพาะในด้านการเงิน สุขภาพจิต และความมั่นคงส่วนบุคคล การหลอกลวงที่มีรูปแบบซับซ้อน เช่น การแอบอ้างเป็นเจ้าหน้าที่รัฐหรือบริษัทที่น่าเชื่อถือ ทำให้เหยื่อตกอยู่ในสถานการณ์ที่ไม่ทันตั้งตัว ส่งผลให้สูญเสียเงินจำนวนมากบางรายถึงขั้นสูญเสียเงินเก็บทั้งชีวิตหรือถูกหลอกให้กู้ยืมเงินมาชำระค่าใช้จ่ายที่ไม่มีอยู่จริง สถานการณ์เหล่านี้ทำให้เหยื่อต้องเผชิญกับปัญหาทางการเงินอย่างหนักจนบางคนไม่สามารถฟื้นตัวได้ในระยะเวลาอันสั้น นอกจากผลกระทบทางการเงินแล้ว แก๊งคอลเซ็นเตอร์ยังส่งผลต่อสุขภาพจิตของเหยื่ออย่างรุนแรง ความเครียดจากการถูกหลอกลวง ความโกรธต่อตนเองที่พลาดท่าให้กับกลโกง และความกังวลเกี่ยวกับความปลอดภัยของข้อมูลส่วนตัว ล้วนทำให้เหยื่อต้องเผชิญกับปัญหาทางจิตใจ บางคนเกิดภาวะซึมเศร้าหรือวิตกกังวลจนส่งผลกระทบต่อคุณภาพชีวิตในระยะยาว ยิ่งไปกว่านั้นการตกเป็นเหยื่อของการขโมยข้อมูลส่วนตัวยังทำให้ผู้เสียหายเผชิญความเสี่ยงต่อการถูกนำข้อมูลไปใช้ในทางที่ผิดหรือถูกหลอกซ้ำอีก[262]

### 5.1.2 ผลกระทบต่อเศรษฐกิจ

[262] ‘ภัยอาชญากรรมแก๊งคอลเซ็นเตอร์’ (สำนักหอสมุดแห่งชาติ) <https://dl.parliament.go.th/handle/lirt/600738> สืบค้น 19 มกราคม 2568.

ปัญหาแก๊งคอลเซ็นเตอร์ที่เกิดขึ้นในภูมิภาคเอเชียตะวันออกเฉียงใต้ได้ส่งผลกระทบต่อเศรษฐกิจในหลายด้านทั้งในระดับบุคคล องค์กร และระดับประเทศ โดยความเสียหายที่เกิดขึ้นไม่เพียงแค่จำกัดในมูลค่าเงินที่สูญเสีย แต่ยังส่งผลต่อระบบเศรษฐกิจโดยรวมอย่างกว้างขวาง หนึ่งในผลกระทบที่ชัดเจนที่สุด คือ การสูญเสียเงินทุนในระบบเศรษฐกิจ เมื่อประชาชนถูกหลอกให้โอนเงินหรือทำธุรกรรมที่ผิดกฎหมาย เงินเหล่านี้มักถูกส่งไปยังบัญชีในต่างประเทศหรือถูกเปลี่ยนมือเข้าสู่เครือข่ายอาชญากรรมทำให้เงินทุนที่ควรหมุนเวียนอยู่ในระบบเศรษฐกิจของประเทศหายไปส่งผลให้การใช้จ่ายภายในประเทศลดลงซึ่งอาจส่งผลต่อการเติบโตทางเศรษฐกิจในระยะยาว[263]

โดยในระดับองค์กร ผลกระทบไม่ได้เกิดกับเหยื่อโดยตรงเท่านั้น แต่ยังแผ่ขยายไปถึงผู้ให้บริการทางการเงินและธุรกิจเอกชน โดยเฉพาะบริษัทที่ถูกแอบอ้างชื่อในการกระทำความผิด เช่น ธนาคาร บริษัทโทรคมนาคม หรือแพลตฟอร์มโซเชียลมีเดีย บริษัทเหล่านี้มักต้องแบกรับต้นทุนด้านความเสียหายต่อชื่อเสียง (reputational damage) การรับมือกับข้อร้องเรียน การตรวจสอบภายในและภาระค่าใช้จ่ายในการป้องกันซ้ำในอนาคต ทั้งยังมีความเสี่ยงต่อการถูกดำเนินคดีความรับผิดร่วม (vicarious liability) หากไม่สามารถพิสูจน์ได้ว่าได้ใช้ความระมัดระวังตามสมควรในการป้องกันอาชญากรรมผ่านระบบของตน ความเสียหายเหล่านี้มีผลต่อความสามารถในการแข่งขันและความน่าเชื่อถือของบริษัทในตลาดโลกโดยตรง[264]

ในระดับประเทศ ปัญหานี้ก่อให้เกิดต้นทุนทางตรงและทางอ้อมในระบบเศรษฐกิจของรัฐอย่างมีนัยสำคัญ โดยต้นทุนทางตรงได้แก่ งบประมาณที่รัฐต้องใช้ในการป้องกันและปราบปรามอาชญากรรม เช่น การพัฒนาระบบตรวจสอบ การสร้างแพลตฟอร์มฐานข้อมูลร่วมระหว่างหน่วยงาน การฝึกอบรมเจ้าหน้าที่เฉพาะทาง และการลงทุนในโครงสร้างพื้นฐานด้านไซเบอร์ซิเคียวริตี้ ซึ่งส่วนใหญ่มักเป็นงบประมาณที่ต้องเบียดบังจากภาคส่วนอื่น เช่น การศึกษา สาธารณสุข หรือการพัฒนาท้องถิ่น ส่วนต้นทุนทางอ้อมนั้นรวมถึงการสูญเสียโอกาสในการดึงดูดการลงทุนโดยตรงจากต่างประเทศ (FDI) ความแพร่หลายของแก๊งคอลเซ็นเตอร์สะท้อนให้เห็นถึงช่องโหว่ในระบบกฎหมาย

---

[263] สักกรินทร์ นิยมศิลป์, ‘อาชญากรรมข้ามชาติ: ภัยคุกคามไทยและอาเซียน’ (การประชุมวิชาการระดับชาติ ครั้งที่ 11 ความหลากหลายทางประชากรและสังคมในประเทศไทย, มหาวิทยาลัยมหิดล, 2558), 236.

[264] ‘คนไทยถูกหลอกลวงทางออนไลน์ 36 ล้านคน ความเสียหายเกือบ 50,000 ล้านบาท’ (สำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ (สสส.) และคณะเศรษฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย) <https://www.the101.world/tossapon-tassanapan-interview/> สืบค้น 9 กุมภาพันธ์ 2567.

และการบังคับใช้ของรัฐ ซึ่งบ่อนทำลาย “ความเชื่อมั่นของนักลงทุน” และอาจทำให้นักลงทุนประเมินความเสี่ยงของประเทศในกลุ่มอาเซียนไว้ในระดับสูง[265]

นอกจากนี้ ยังมีผลกระทบเชิงระบบที่มักถูกมองข้าม นั่นคือ ความเสียหายต่อความน่าเชื่อถือของโครงสร้างพื้นฐานทางเศรษฐกิจในภาพรวม เช่น ระบบการชำระเงินผ่านธนาคาร ระบบโอนเงินระหว่างประเทศ หรือแม้กระทั่งการใช้เทคโนโลยี Blockchain ในอนาคต หากประชาชนรู้สึกว่าไม่สามารถไว้วางใจโครงสร้างเหล่านี้ได้ ย่อมส่งผลให้การเปลี่ยนผ่านไปสู่ระบบเศรษฐกิจดิจิทัลเกิดขึ้นได้ช้าลง ซึ่งจะเป็นการฉุดรั้งขีดความสามารถในการแข่งขันของประเทศในระยะยาว

**5.1.3 ผลกระทบต่อความมั่นคงของภูมิภาค**

ปัญหาแก๊งคอลเซ็นเตอร์ที่แพร่กระจายในภูมิภาคเอเชียตะวันออกเฉียงใต้ไม่เพียงส่งผลในระดับปัจเจกบุคคลหรือเศรษฐกิจเท่านั้น หากแต่ยังเป็นภัยคุกคามต่อ “ความมั่นคงของภูมิภาค” ในลักษณะเชิงโครงสร้าง โดยก่อให้เกิดแรงสั่นสะเทือนต่อทั้งระบบความปลอดภัยของประชาชน ความสามารถของรัฐในการบังคับใช้กฎหมาย และกลไกความร่วมมือในระดับภูมิภาค ในระดับแรก แก๊งคอลเซ็นเตอร์ได้สร้างความเปราะบางต่อ “ความมั่นคงมนุษย์” (human security) ซึ่งเป็นแนวคิดที่เน้นการคุ้มครองบุคคลมากกว่ารัฐ โดยองค์การสหประชาชาติได้กำหนดองค์ประกอบของความมั่นคงมนุษย์ไว้ 7 ด้าน หนึ่งในนั้นคือความมั่นคงทางเศรษฐกิจและความมั่นคงของบุคคล ซึ่งล้วนได้รับผลกระทบโดยตรงจากการฉ้อโกงและการหลอกลวงออนไลน์ลักษณะนี้[266] ความสามารถของกลุ่มอาชญากรในการเจาะข้อมูลส่วนบุคคลและสวมรอยหน่วยงานรัฐได้อย่างแนบเนียน นำไปสู่ความรู้สึกไม่ปลอดภัยในชีวิตประจำวัน การขาดความเชื่อมั่นในระบบ และความไม่ไว้วางใจในบุคคลรอบข้าง

ในระดับรัฐ รายได้ที่เกิดจากอาชญากรรมมักถูกส่งต่อไปยังเครือข่ายอาชญากรรมข้ามชาติ ซึ่งอาจเชื่อมโยงกับการค้ามนุษย์ อาวุธ และยาเสพติด[267] ก่อให้เกิดการบั่นทอนอธิปไตยของรัฐในการควบคุมความสงบเรียบร้อยภายในประเทศ อาชญากรรมที่ไม่สามารถตรวจสอบได้และไร้พรมแดนยังทำให้เจ้าหน้าที่รัฐสูญเสียศักยภาพในการดำเนินการบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพ โดยเฉพาะในรัฐที่มีทรัพยากรจำกัด ยิ่งไปกว่านั้น การบังคับใช้กฎหมายที่ล่าช้าหรือไร้ประสิทธิภาพยังส่งผลกระทบต่อระบบความยุติธรรมโดยรวม เช่น ภาระงานที่เพิ่มขึ้นของตำรวจ หน่วยงานดิจิทัล และ

---

[265] ‘ผลกระทบของแก๊งคอลเซ็นเตอร์ต่อเศรษฐกิจไทย’ (ธนาคารแห่งประเทศไทย, 2566) <https://sustainability.ais.co.th/th/update/aunjai-cyber/789/gang-call-center-scam> สืบค้น 9 กุมภาพันธ์ 2567.

[266] United Nations Development Programme, Human Development Report 1994: New Dimensions of Human Security (New York: Oxford University Press, 1994) 23–25.

[267] Peter Andreas and Ethan Nadelmann, Policing the Globe: Criminalization and Crime Control in International Relations (New York: Oxford University Press, 2006) 5–6.

ศาล ซึ่งอาจทำให้เกิดปัญหาความล่าช้าในการพิจารณาคดี ความเหลื่อมล้ำในการเข้าถึงความยุติธรรม และลดทอนความไว้วางใจของประชาชนต่อรัฐ ความหวาดระแวงที่ฝังรากอยู่ในสังคมอาจนำไปสู่ความแตกแยกและลดทอนทุนทางสังคมอย่างมีนัยสำคัญซึ่งเป็นรากฐานสำคัญของเสถียรภาพทางการเมืองและความร่วมมือภายในประเทศ

**5.1.4 ผลกระทบต่อความสัมพันธ์ระหว่างประเทศ**

ปัญหาแก๊งคอลเซ็นเตอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้ได้ส่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศอย่างมีนัยสำคัญ ทั้งในมิติของความร่วมมือ ความตึงเครียด และภาพลักษณ์ในเวทีระหว่างประเทศ โดยเฉพาะอย่างยิ่งในบริบทของอาเซียน ซึ่งพยายามผลักดันแนวคิด “ประชาคมการเมืองและความมั่นคงอาเซียน” (ASEAN Political-Security Community) ที่เน้นความร่วมมือด้านความมั่นคงข้ามพรมแดน แต่กรณีแก๊งคอลเซ็นเตอร์กลับสะท้อนถึงข้อจำกัดเชิงโครงสร้างในความร่วมมือระหว่างประเทศสมาชิกอย่างชัดเจน

1. การที่แต่ละประเทศมีกฎหมายภายในและกลไกทางกฎหมายที่แตกต่างกันมาก เช่น ความแตกต่างในกระบวนการส่งผู้ร้ายข้ามแดน หรือข้อจำกัดด้านการรับพยานหลักฐานจากต่างประเทศ เป็นอุปสรรคสำคัญต่อการทำงานร่วมกัน[268]โดยเฉพาะเมื่อต้องจัดการกับอาชญากรที่โยกย้ายข้ามแดนอย่างรวดเร็ว การที่ประเทศหนึ่งอาจมีขั้นตอนที่ล่าช้า หรือไม่ยอมรับคำขอความร่วมมือในทางกฎหมายจากอีกประเทศหนึ่งย่อมทำให้เกิดความล่าช้าและความไม่พึงพอใจในการบังคับใช้กฎหมายร่วมกันซึ่งในบางกรณีถึงขั้นนำไปสู่ความตึงเครียดทางการทูต เช่น การกล่าวโทษกันในสื่อสาธารณะ หรือความลังเลใจในการส่งเจ้าหน้าที่หรือข้อมูลข้ามประเทศ

2. ประเทศที่ถูกระบุว่าเป็น “แหล่งต้นตอ” หรือ “ฐานปฏิบัติการ” ของแก๊งคอลเซ็นเตอร์ ย่อมตกอยู่ภายใต้แรงกดดันจากประชาคมระหว่างประเทศ ทั้งจากรัฐบาลประเทศคู่เจรจา องค์กรความร่วมมือระดับภูมิภาค และสื่อมวลชนระหว่างประเทศ ซึ่งอาจทำให้ประเทศดังกล่าวต้องเร่งดำเนินการในเชิงสัญลักษณ์ เช่น การจับกุมครั้งใหญ่ หรือการจัดสัมมนาระหว่างประเทศเพื่อแสดงความตั้งใจในการแก้ไขปัญหา แต่ในเชิงโครงสร้างแล้ว กลับยังไม่สามารถจัดการกับปัญหาได้อย่างยั่งยืน นอกจากนี้ หากประเทศใดถูกมองว่าไม่สามารถควบคุมภัยคุกคามทางไซเบอร์หรืออาชญากรรมข้ามชาติได้ ก็อาจสูญเสียความน่าเชื่อถือในการเป็นหุ้นส่วนความมั่นคงในสายตาขององค์กรระหว่างประเทศหรือนักลงทุน

3. แม้ว่าปัญหาแก๊งคอลเซ็นเตอร์จะผลักดันให้เกิดความร่วมมือด้านการสืบสวนข้ามพรมแดนในบางกรณี เช่น การตั้ง “ศูนย์ประสานงานร่วม” ระหว่างไทย-จีน หรือโครงการอบรมจาก

---

[268] United Nations Office on Drugs and Crime (UNODC), Manual on Mutual Legal Assistance and Extradition (2012).

INTERPOL หรือ UNODC แต่ความร่วมมือเหล่านี้ยังอยู่ในลักษณะเฉพาะกิจ (ad hoc) และไม่มีหน่วยงานกลางระดับภูมิภาคที่มีอำนาจชัดเจนในการประสานงานด้านอาชญากรรมไซเบอร์หรือคดีลักษณะพิเศษอย่างคอลเซ็นเตอร์โดยตรง อาเซียนยังมาตรการแบบบูรณาการที่สามารถเชื่อมโยงกฎหมายภายในของประเทศสมาชิกเข้ากับกลไกความร่วมมือระหว่างประเทศได้อย่างแท้จริง

ด้วยเหตุนี้ ปัญหาแก๊งคอลเซ็นเตอร์จึงไม่ได้เพียงก่อให้เกิดความเสียหายทางเศรษฐกิจหรือสังคมภายในประเทศเท่านั้น แต่ยังสร้างผลกระทบเชิงโครงสร้างต่อความสัมพันธ์ระหว่างประเทศในภูมิภาค และสะท้อนถึงความเปราะบางของระบบความร่วมมือในกรอบอาเซียนที่จำเป็นต้องได้รับการทบทวนและเสริมสร้างให้แข็งแรงยิ่งขึ้น

**5.1.5 ผลกระทบทางด้านวัฒนธรรม**

ปัญหาแก๊งคอลเซ็นเตอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้ไม่เพียงส่งผลกระทบต่อเศรษฐกิจความมั่นคง หรือกฎหมายเท่านั้น แต่ยังแทรกซึมสู่ระดับวัฒนธรรมของสังคมอาเซียนอย่างลึกซึ้ง โดยเฉพาะในมิติของ ความไว้วางใจในระหว่างบุคคลและโครงสร้างทางสังคม ซึ่งถือเป็นรากฐานของวัฒนธรรมชุมชนในหลายประเทศอาเซียน เช่น ไทย ลาว เมียนมา หรือฟิลิปปินส์ ที่ให้ความสำคัญกับค่านิยมเอื้อเฟื้อเผื่อแผ่และการไว้เนื้อเชื่อใจระหว่างกัน แก๊งคอลเซ็นเตอร์มักอาศัยการแอบอ้างหน่วยงานของรัฐหรือสถาบันที่มีความน่าเชื่อถือเป็นเครื่องมือในการหลอกลวงเหยื่อ ทำให้ประชาชนเริ่มไม่เชื่อถือแม้กระทั่งการติดต่อจากหน่วยงานรัฐจริง ๆ หรือหลีกเลี่ยงการมีปฏิสัมพันธ์กับผู้อื่นที่ไม่รู้จัก ผลที่เกิดขึ้นคือ การเปลี่ยนแปลงวัฒนธรรมทางสังคมในระดับจุลภาค โดยความไม่ไว้วางใจกลายเป็นกลไกป้องกันตนเองของปัจเจกบุคคล แทนที่จะเป็นความร่วมมือเชิงชุมชนตามแบบแผนวัฒนธรรมดั้งเดิม ความระแวงนี้ยังส่งผลให้เกิดความเฉื่อยชาทางสังคมกล่าวคือ ประชาชนเลือกที่จะไม่เข้าไปมีส่วนร่วมกับสังคม เพราะกลัวตกเป็นเหยื่อหรือถูกหลอก

อีกประเด็นที่สำคัญคือ ปรากฏการณ์แก๊งคอลเซ็นเตอร์ที่แทรกซึมในพื้นที่เศรษฐกิจระดับล่างอาจส่งผลให้เกิดการ สั่นคลอนของค่านิยมทางศีลธรรม โดยเฉพาะในกลุ่มเยาวชนหรือประชาชนที่ประสบปัญหาเศรษฐกิจอย่างต่อเนื่อง ในบางกรณีมีการเข้าร่วมกับเครือข่ายอาชญากรรมอย่างไม่รู้เท่าทัน หรือยอมรับพฤติกรรมดังกล่าวในฐานะโอกาส แทนที่จะมองว่าเป็นการละเมิดสิทธิผู้อื่นและผิดจริยธรรม กรณีดังกล่าวชี้ให้เห็นว่าแก๊งคอลเซ็นเตอร์ไม่เพียงแต่ก่อความเสียหายทางตรง แต่ยังสร้างความเคลื่อนคลาดในโครงสร้างคุณค่าทางวัฒนธรรมในระยะยาว[269] ยิ่งไปกว่านั้นการที่อาเซียนถูกเชื่อมโยงกับปัญหาอาชญากรรมไซเบอร์และการหลอกลวงทางออนไลน์ในระดับโลก ได้ส่งผลต่อภาพลักษณ์ของวัฒนธรรมภูมิภาค ในสายตาประชาคมระหว่างประเทศ สื่อมวลชนและรายงานข่าวต่างประเทศหลายแห่งรายงานถึงเอเชียตะวันออกเฉียงใต้ว่าเป็นแหล่งกบดาน หรือศูนย์กลางของการ

---

[269] ทศพล ทรรศนพรรณ, ‘วิกฤต “มิจฉาชีพออนไลน์” รัฐไทยทำอะไรได้ไหม (2566)<https://www.the101.world/tossapon-tassanapan-interview/> สืบค้น 9 กุมภาพันธ์ 2567.

ก่ออาชญากรรมคอลเซ็นเตอร์ ซึ่งไม่เพียงส่งผลกระทบต่อการท่องเที่ยวและการลงทุนแต่ยังลดทอนทุนทางวัฒนธรรมของประเทศสมาชิกอาเซียนในเวทีระหว่างประเทศ

## 5.2 วิเคราะห์แนวทางของอาเซียนในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

ปัญหาแก๊งคอลเซ็นเตอร์ในภูมิภาคอาเซียนได้กลายเป็นภัยคุกคามที่ส่งผลกระทบต่อเศรษฐกิจ สังคม และความปลอดภัยของประชาชนในหลายประเทศ ด้วยโครงสร้างเครือข่ายที่ซับซ้อนและการดำเนินงานข้ามพรมแดน ทำให้การจัดการกับอาชญากรรมรูปแบบนี้ไม่สามารถพึ่งพาการดำเนินงานของแต่ละประเทศได้โดยลำพัง ความจำเป็นในการแก้ปัญหาจึงต้องอาศัยแนวทางที่บูรณาการ ทั้งในระดับประเทศและภูมิภาค เนื่องจากความร่วมมือระหว่างประเทศในภูมิภาคอาเซียนเป็นอีกหนึ่งแนวทางที่หลีกเลี่ยงไม่ได้ เนื่องจากแก๊งคอลเซ็นเตอร์มักใช้ประโยชน์จากความเชื่อมโยงของพรมแดนและการดำเนินงานที่ไม่ถูกตรวจสอบอย่างทั่วถึง โดยจะทำการวิเคราะห์ถึงแนวทางของอาเซียนในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ ซึ่งมีผลการศึกษาดังนี้

5.2.1 การบูรณาการแผนยุทธศาสตร์ความร่วมมือด้านความมั่นคงทางอาชญากรรมไซเบอร์

โดยในแนวทางนี้ได้พัฒนามาจากแผนยุทธศาสตร์ความร่วมมืออาเซียนด้านความมั่นคงทางไซเบอร์[270] (ASEAN Cybersecurity Cooperation Strategy) ที่มีอยู่แต่เดิมที่ได้รับการออกแบบมาเพื่อจัดการกับภัยคุกคามเหล่านี้ โดยแผนยุทธศาสตร์ความร่วมมือด้านความมั่นคงทางอาชญากรรมไซเบอร์ของอาเซียน (ASEAN Cybersecurity Cooperation Strategy) จัดทำขึ้นภายใต้กรอบความร่วมมือของ*คณะมนตรีประชาคมการเมืองและความมั่นคงอาเซียน* (ASEAN Political-Security Community Council: APSC Council) และดำเนินการภายใต้ความรับผิดชอบของ *คณะทำงานอาเซียนด้านความมั่นคงทางไซเบอร์* (ASEAN Cybersecurity Working Group: ACGWG) ซึ่งเป็นกลไกระดับนโยบายที่จัดตั้งขึ้นโดยมติของที่ประชุมรัฐมนตรีอาเซียนด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ASEAN Ministers Meeting on Telecommunications and Information Technology – TELMIN) ภายใต้กรอบ*ประชาคมเศรษฐกิจอาเซียน* (ASEAN Economic

[270] แผนยุทธศาสตร์ความร่วมมืออาเซียนด้านความมั่นคงทางไซเบอร์ (ASEAN Cybersecurity Cooperation Strategy) คือ แผนการที่ออกแบบมาเพื่อส่งเสริมความร่วมมือและการประสานงานระหว่างประเทศสมาชิกอาเซียนในการเสริมสร้างความมั่นคงทางไซเบอร์ในภูมิภาคอาเซียน โดยมีเป้าหมายเพื่อให้ประเทศสมาชิกสามารถร่วมมือกันในการรับมือกับภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและหลากหลาย

Community: AEC) ที่มีอำนาจในการกำหนดแนวนโยบายระดับภูมิภาคด้านดิจิทัลและไซเบอร์ โดยเฉพาะ แผนดังกล่าวเป็นผลสืบเนื่องจากการลงนามใน “ASEAN Digital Masterplan 2025 (ADM 2025)” ซึ่งได้รับการรับรองโดย TELMIN และ APSC Council ในปี 2021 โดยมีสิงคโปร์ทำหน้าที่ประธานฝ่ายเทคนิคหลักในกระบวนการจัดทำแผนยุทธศาสตร์และได้รับการสนับสนุนเชิงวิชาการจากองค์การระหว่างประเทศ ได้แก่ สหภาพโทรคมนาคมระหว่างประเทศ (ITU), องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) และองค์กรภาคเอกชนชั้นนำในเอเชียตะวันออกเฉียงใต้ แต่จากการวิเคราะห์ถึงสภาพปัญหาของนโยบายดังกล่าว *(ในหัวข้อที่ 4.2.1)* ที่แม้ว่าอาเซียนจะมีแผนยุทธศาสตร์ด้านความมั่นคงไซเบอร์แต่ในทางปฏิบัติกลับพบว่ายังขาดความเป็นเอกภาพและแนวทางที่เป็นรูปธรรมในการดำเนินงานร่วมกัน เนื่องจากไม่สอดคล้องกันของนโยบาย ยุทธศาสตร์และความสามารถในการดำเนินงานของแต่ละประเทศสมาชิก แม้จะมีเป้าหมายร่วมกันในระดับอาเซียนแต่แต่ละประเทศสมาชิกอาเซียนยังคงวางนโยบายความมั่นคงทางไซเบอร์ตามบริบทและทรัพยากรของตน ส่งผลให้เกิดความเหลื่อมล้ำทางมาตรการและขาดความต่อเนื่องของกลไกปฏิบัติ ซึ่งแนวทางนี้ได้นำแนวคิดความร่วมมือระหว่างประเทศ[271] (International Cooperation) มาวิเคราะห์ โดยการสร้างเครือข่ายความร่วมมือระหว่างประเทศจะทำให้เกิดการแลกเปลี่ยนข้อมูลที่มีคุณค่าเกี่ยวกับแนวทางการป้องกันและปราบปรามอาชญากรรมไซเบอร์ การสร้างความสัมพันธ์ที่แน่นแฟ้นระหว่างหน่วยงานที่เกี่ยวข้องในแต่ละประเทศจะช่วยเสริมสร้างการรับรู้ถึงปัญหาที่เกิดขึ้น รวมถึงการพัฒนามาตรการที่เหมาะสมในการตอบสนองต่อปัญหา นอกจากนี้ ความร่วมมือระหว่างประเทศยังสามารถทำให้การประสานงานในระดับสากลเกิดขึ้นได้อย่างมีประสิทธิภาพ โดยประเทศต่าง ๆ สามารถสนับสนุนกันในด้านทรัพยากร

การบูรณาการแผนให้มีประสิทธิภาพ ต้องเริ่มจากการยกระดับสถานะของแผนจากเอกสารนโยบายทั่วไปไปสู่รูปแบบ ปฏิญญาร่วมรัฐมนตรี (Ministerial Declaration) หรือจัดทำเป็นบันทึกความเข้าใจระหว่างรัฐ (Memorandum of Understanding: MoU) ที่กำหนดกรอบความร่วมมือ

---

[271] แนวคิดความร่วมมือระหว่างประเทศมีพื้นฐานอยู่บนหลักความสัมพันธ์ระหว่างประเทศที่มองว่าเวทีระหว่างประเทศไม่มีรัฐใดที่มีอำนาจอธิปไตยอันสมบูรณ์ หากแต่ต้องเอื้ออาทรช่วยเหลือซึ่งกันและกันเพื่อลดความขัดแย้งและแบ่งปันผลประโยชน์ร่วมกันจึงจะทำให้แต่ละประเทศดำรงอยู่ได้อย่างสงบสุข โดยแนวคิดนี้ถือได้ว่าเป็นแนวคิดตามสำนักเสรีนิยมสมัยใหม่ (Neo Liberalism) ซึ่งความร่วมมือระหว่างประเทศสามารถเกิดขึ้นเมื่อรัฐ ได้ปรับพฤติกรรมให้สอดคล้องกับความต้องการของรัฐอื่น ๆ ผ่านกระบวนการประสานงานเชิงนโยบายที่เรียกว่า วิถีปฏิบัติระหว่างประเทศ ด้วยเหตุนี้หากรัฐใดประสบกับภัยคุกคามที่เหมือนหรือคล้ายคลึงกัน รัฐเหล่านั้นต้องหันหน้าเข้าหากันและร่วมมือกันทั้งในระดับรัฐบาลและระดับเจ้าหน้าที่ผู้ปฏิบัติการเพื่อขจัดภัยคุกคามนั้น หรือสร้างเงื่อนไขให้มีโอกาสเกิดขึ้นได้น้อยที่สุด แนวความคิดนี้ เห็นเป็นที่ประจักษ์ผ่านกรอบความร่วมมือระหว่างประเทศ ทั้งในระดับทวิภาคีและพหุภาคี เช่น การประชุมต่าง ๆ และความร่วมมือในระดับปฏิบัติการของหน่วยงานบังคับใช้ กฎหมาย ทั้งในรูปแบบที่เป็นทางการและไม่เป็นทางการ

อย่างชัดเจน ทั้งในเชิงโครงสร้าง (การตั้งกลไกร่วมระดับภูมิภาค) เชิงภารกิจ (การแบ่งปันข้อมูลข่าวกรองไซเบอร์) และเชิงเวลา (กำหนดแผนปฏิบัติการเป็นระยะ 3-5 ปี) กลไกหลักที่ควรเป็นผู้ดำเนินการบูรณาการ คือ คณะมนตรีประชาคมการเมืองและความมั่นคงอาเซียน (APSC Council) ซึ่งเป็นหน่วยงานที่มีอำนาจกำหนดทิศทางเชิงนโยบายของอาเซียนในประเด็นด้านความมั่นคง โดยเฉพาะประเด็นที่เกี่ยวข้องกับอาชญากรรมข้ามชาติและไซเบอร์ รวมถึงการกำหนดให้ ASEAN Secretariat (สำนักงานเลขาธิการอาเซียน) ทำหน้าที่ติดตามประเมินผล และเป็นศูนย์กลางข้อมูล (clearing house) สำหรับการแลกเปลี่ยนข่าวกรองหรือคำร้องขอความร่วมมือด้านการสืบสวนสอบสวน ในทางปฏิบัติการบูรณาการควรยึดแนวทาง Multi-layered Coordination คือ จัดให้มีแผนร่วมในระดับภูมิภาค (Regional Plan) เชื่อมโยงกับแผนระดับชาติ (National Plan) และขับเคลื่อนผ่านศูนย์ฝึกอบรมหรือหน่วยปฏิบัติการร่วม ดังนั้น แม้ว่าอาเซียนจะมีแนวทางในระดับยุทธศาสตร์ที่ชัดเจนเกี่ยวกับการสร้างความมั่นคงทางอาชญากรรมไซเบอร์ แต่หากไม่มีการบูรณาการอย่างเป็นระบบในระดับประเทศและไม่มีมาตรการสนับสนุนให้เกิดการดำเนินงานร่วมกันอย่างแท้จริง แผนดังกล่าวก็จะไม่สามารถตอบสนองต่อภัยคุกคามในรูปแบบใหม่ได้อย่างมีประสิทธิภาพ การบูรณาการจึงต้องไม่ใช่เพียงการกำหนดเป้าหมายร่วมกันในเอกสารนโยบายเท่านั้น หากแต่ต้องแปรสภาพเป็น “กลไกปฏิบัติการร่วม” ที่สามารถยกระดับการดำเนินการจริงในภูมิภาคได้อย่างยั่งยืน กล่าวโดยสรุป อาเซียนควรจึงบูรณาการแผนยุทธศาสตร์ความร่วมมือด้านความมั่นคงทางอาชญากรรมไซเบอร์อย่างจริงจังและเป็นรูปธรรมมากขึ้น

5.1.2 การเสริมสร้างกลไกการแลกเปลี่ยนข้อมูลข่าวกรองระหว่างประเทศสมาชิกอาเซียน

แนวทางการพัฒนากลไกการแบ่งปันข้อมูลข่าวกรองในระดับอาเซียนเกิดขึ้นจากปัญหาหลักที่ทำให้การป้องกันและปราบปรามอาชญากรรมข้ามชาติแก๊งคอลเซ็นเตอร์ไม่มีประสิทธิภาพเท่าที่ควร การเสนอแนวทางนี้เกิดจากการวิเคราะห์สภาพปัญหาที่ปรากฏชัดในหลายกรณีจริง นั้นก็คือ การดำเนินการจับกุมเครือข่ายแก๊งคอลเซ็นเตอร์ซึ่งพบว่าข้อมูลจากประเทศหนึ่งไม่สามารถส่งถึงอีกประเทศได้ทันเวลา ทำให้ผู้ต้องหาหลบหนีได้ก่อนหรือในบางกรณีที่ข้อมูลการเงินและเส้นทางการโอนเงินไม่สามารถตรวจสอบข้ามพรมแดนได้ทัน เนื่องจากไม่มีข้อตกลงหรือกลไกในการแลกเปลี่ยนข้อมูลอย่างเป็นทางการ ทั้งนี้ ความล่าช้าและความไม่สมบูรณ์ของข้อมูลที่ถูกส่งข้ามประเทศ ไม่เพียงเป็นอุปสรรคต่อการดำเนินคดี แต่ยังสร้างช่องว่างให้เครือข่ายอาชญากรรมสามารถขยายกิจการได้โดยไร้การขัดขวางจากภาครัฐ ควรเริ่มต้นจากการพัฒนาและปรับปรุง Memorandum of Understanding (MOU) หรือข้อตกลงด้านการแลกเปลี่ยนข่าวกรองระหว่างประเทศสมาชิกให้มีรูปแบบที่เป็นระบบมากขึ้นและครอบคลุมถึงประเด็นการรักษาความลับของข้อมูล (data confidentiality), ความปลอดภัยในการส่งผ่านข้อมูล (data security) และขั้นตอนการนำข้อมูลไปใช้เพื่อการสืบสวนสอบสวน รวมถึงต้องพัฒนากลไกทางเทคนิค เช่น ระบบฐานข้อมูลกลาง (centralized intelligence

platform) ที่แต่ละประเทศสามารถเข้าถึงได้ภายใต้การควบคุมร่วมกัน องค์ประกอบหนึ่งที่ควรได้รับการพัฒนา คือ การใช้เทคโนโลยีสนับสนุนการแลกเปลี่ยนข้อมูลข่าวกรอง ได้แก่ การนำมาตรฐาน Structured Threat Information Expression[272] (STIX) และ Trusted Automated Exchange of Indicator Information[273] (TAXII) ซึ่งเป็นโปรโตคอลที่ใช้ในการแลกเปลี่ยนข้อมูลภัยคุกคามในระดับสากลเพื่อให้ข่าวกรองสามารถถูกรวบรวม วิเคราะห์ และนำไปใช้อย่างมีประสิทธิภาพ

ซึ่งแนวทางนี้พัฒนามาจากแนวคิดว่าด้วยความร่วมมือระหว่างประเทศ (International Co – Operation) เป็นแนวคิดในความสัมพันธ์ระหว่างประเทศที่หมายถึงการที่รัฐต่าง ๆ หรือองค์กรระหว่างประเทศทำงานร่วมกันเพื่อบรรลุเป้าหมายที่มีผลประโยชน์ร่วมกัน ไม่ว่าจะเป็นด้านเศรษฐกิจ ความมั่นคง สิ่งแวดล้อม หรือสังคม โดยแนวคิดนี้ถือได้ว่าเป็นแนวคิดตามสำนักเสรีนิยมสมัยใหม่ (Neo Liberalism) ซึ่งความร่วมมือระหว่างประเทศสามารถเกิดขึ้นเมื่อรัฐ ได้ปรับพฤติกรรมให้สอดคล้องกับความต้องการของรัฐ อื่น ๆ ผ่านกระบวนการประสานงานเชิงนโยบายที่เรียกว่าวิถีปฏิบัติระหว่างประเทศ[274] ด้วยเหตุนี้หากรัฐใดประสบกับภัยคุกคามที่เหมือนหรือคล้ายคลึงกัน รัฐเหล่านั้นต้องหันหน้าเข้าหากันและร่วมมือกันทั้งในระดับรัฐบาลและระดับเจ้าหน้าที่ผู้ปฏิบัติการเพื่อขจัดภัยคุกคามนั้นหรือสร้างเงื่อนไขให้มีโอกาสเกิดขึ้นได้น้อยที่สุด เมื่อนำมาปรับใช้กับการพัฒนากลไกการแบ่งปันข้อมูลข่าวกรองแบบเรียลไทม์จะเห็นได้ว่า การแบ่งปันข้อมูลข่าวกรองแบบเรียลไทม์จะช่วยให้การประสานงานและการดำเนินการระหว่างประเทศในเครือข่ายเดียวกันเป็นไปอย่างมีประสิทธิภาพ ส่งเสริมการแลกเปลี่ยนข้อมูล และการตอบสนองต่อภัยคุกคามข้ามชาติอย่างรวดเร็ว การมีข้อมูลที่ทันสมัยจะทำให้ประเทศต่างๆ สามารถจับตาและป้องกันการกระทำผิดได้ดีขึ้น อีกทั้งควรมีการจัดตั้งระบบกลางสำหรับการแบ่งปันข้อมูลข่าวกรองระหว่างประเทศสมาชิก ระบบนี้ควรออกแบบมาให้มีความปลอดภัยสูง รองรับการส่งข้อมูลที่รวดเร็ว และสามารถจัดเก็บข้อมูลที่จำเป็นสำหรับการสืบสวนและปราบปรามได้ การพัฒนากลไกการแบ่งปันข้อมูลข่าวกรองแบบเรียลไทม์ในอาเซียนเป็นสิ่งจำเป็นเพื่อรับมือกับอาชญากรรมข้ามชาติอย่างมีประสิทธิภาพ การวางรากฐานที่มั่นคงด้วยระบบกลาง มาตรฐานข้อมูล ความไว้วางใจระหว่างประเทศ และการสนับสนุนด้านเทคโนโลยี จะช่วยให้อาเซียนก้าวข้ามความท้าทายและเสริมสร้างความมั่นคงในยุคดิจิทัลได้อย่างยั่งยืน

---

[272] STIX (Structured Threat Information Expression) เป็นภาษาที่ใช้สำหรับแสดงข้อมูลข่าวกรองด้านภัยคุกคามไซเบอร์ในรูปแบบที่เป็นโครงสร้าง (structured format) โดยมุ่งเน้นให้ข้อมูลสามารถถูกรวบรวม วิเคราะห์ และนำไปใช้งานต่อได้อย่างอัตโนมัติ

[273] TAXII (Trusted Automated Exchange of Indicator Information) เป็นโปรโตคอลหรือมาตรฐานสำหรับการ *รับส่งข้อมูล STIX* อย่างปลอดภัยระหว่างหน่วยงานหรือระบบต่าง ๆ โดยอัตโนมัติ

[274] Keohane, O. After hegemony: Cooperation and discord in the world political economy, (New Jersey: Princeton University Press,2005), 103-104.

5.2.3 การพัฒนากลไกความร่วมมือระหว่างประเทศในระดับปฏิบัติการ

โดยแนวทางนี้วิเคราะห์มาจากสภาพปัญหาทางด้านปฏิบัติ (ในหัวข้อที่ 4.4) ที่หน่วยงานบังคับใช้กฎหมายของแต่ละประเทศมักทำงานแยกกันและใช้กระบวนการที่แตกต่างกัน แสดงให้เห็นถึงช่องว่างสำคัญในการประสานความร่วมมือระหว่างประเทศสมาชิกในระดับปฏิบัติการ ทั้งในเรื่องของโครงสร้างหน่วยงานและการปฏิบัติการร่วมแบบเฉพาะกิจที่ยังขาดกลไกสนับสนุนอย่างเป็นระบบ แนวทางในการพัฒนากลไกความร่วมมือระหว่างประเทศในระดับปฏิบัติการของอาเซียนควรถูกออกแบบโดยตั้งอยู่บนพื้นฐานของความเข้าใจเชิงลึกถึงข้อจำกัดที่แท้จริงของประเทศสมาชิก ทั้งในด้านโครงสร้างสถาบัน ความเหลื่อมล้ำทางทรัพยากร และความแตกต่างในระดับความพร้อมด้านเทคโนโลยีสารสนเทศ โดยการดำเนินแนวทางนี้ไม่ควรมุ่งเน้นเพียงแค่การนำระบบหรือเครื่องมือจากภายนอกเข้ามาประยุกต์ใช้ แต่ควรเริ่มต้นจากการสร้างกรอบความเข้าใจร่วมกันระหว่างประเทศสมาชิกอาเซียน ซึ่งหมายถึงการตกลงกันในหลักการพื้นฐานของการแบ่งปันข้อมูล การประสานงาน และการดำเนินปฏิบัติการร่วมที่คำนึงถึงหลักอธิปไตย ความปลอดภัยทางข้อมูลและความไว้วางใจระหว่างกัน หนึ่งในหัวใจสำคัญของแนวทางนี้ คือ การส่งเสริมความไว้วางใจเชิงสถาบันระหว่างหน่วยงานของรัฐสมาชิก ซึ่งเป็นสิ่งที่ยังคงขาดอยู่ในโครงสร้างความร่วมมือปัจจุบันของอาเซียน เนื่องจากไม่มีกรอบพันธกรณีที่มีผลบังคับในระดับภูมิภาค ทำให้หลายประเทศยังลังเลในการแบ่งปันข้อมูลที่เกี่ยวข้องกับความมั่นคง ซึ่งสอดคล้องกับการศึกษาโดย UNODC ที่ระบุว่าความไม่ไว้วางใจและข้อจำกัดด้านกฎหมายระหว่างประเทศเป็นอุปสรรคสำคัญของความร่วมมือในเอเชียตะวันออกเฉียงใต้ในประเด็นอาชญากรรมข้ามชาติ[275] ซึ่งถ้าวิเคราะห์จากแนวความคิดในการช่วยเหลือระหว่างประเทศในทางอาญา (International Mutual Assistance in Criminal Matters) ที่กล่าวไว้ว่าการให้ความช่วยเหลือซึ่งกันและกันในทางเรื่องอาญามีรูปแบบของการให้ความช่วยเหลือระหว่างประเทศในทางอาญาที่สามารถแบ่งออกได้เป็น 3 ระดับ[276] ได้แก่ (1) ความช่วยเหลือซึ่งกันและกันทางอาญา

---

[275] United Nations Office on Drugs and Crime. *Enhancing Cross-border Cooperation in Southeast Asia to Combat Transnational Organized Crime*. UNODC Regional Report, 2020.

[276] รูปแบบของการให้ความช่วยเหลือระหว่างประเทศในทางอาญาที่สามารถแบ่งออกได้เป็น 3 ระดับ ได้แก่

1. ความช่วยเหลือซึ่งกันและกันทางอาญาในรูปแบบไม่เป็นทางการ เป็นการให้ความร่วมมือกันในระดับเจ้าหน้าที่รัฐกันเองโดยอาศัยความสัมพันธ์ระหว่างบุคคล ซึ่งการให้ความช่วยเหลือแบบไม่เป็นทางการนี้มักจะเป็นเรื่องเล็กน้อยไม่จำเป็นต้องอาศัยหลักเกณฑ์ในการพิจารณารายละเอียดมากนัก

2. ความช่วยเหลือซึ่งกันและกันทางอาญาในรูปแบบกึ่งทางการ จะเป็นการให้ความช่วยเหลือซึ่งกันและกันซึ่งเป็นไปตามความตกลงหรือความตกลงหรือความร่วมมือของหน่วยงานระหว่างประเทศที่มีหน้าที่รับผิดชอบเกี่ยวกับกระบวนการทางอาญาต่างๆ

ในรูปแบบไม่เป็นทางการ (2) ความช่วยเหลือซึ่งกันและกันทางอาญาในรูปแบบกึ่งทางการ และ (3) ความช่วยเหลือซึ่งกันและกันทางอาญาในรูปแบบอย่างเป็นทางการ โดยแนวทางการพัฒนากลไกความร่วมมือระหว่างประเทศในระดับปฏิบัติการในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์นั้นจำเป็นต้องอาศัยแนวคิดการให้ความช่วยเหลือซึ่งกันและกันทางอาญาในรูปแบบกึ่งทางการ (Semi-Formal Mutual Legal Assistance) ที่มีความยืดหยุ่นและเหมาะสมกับลักษณะของอาชญากรรมที่เปลี่ยนแปลงเร็ว อาศัยเทคโนโลยี และไม่สามารถรอความร่วมมือที่ต้องใช้ระยะเวลานานผ่านช่องทางทางการทูตได้ โดยสามารถวิเคราะห์เปรียบเทียบได้จากสหภาพยุโรปได้จัดตั้งหน่วยงานเฉพาะที่เรียกว่า Europol (European Union Agency for Law Enforcement Cooperation) ซึ่งมีบทบาทในการประสานข้อมูลข่าวกรองด้านอาชญากรรม การสนับสนุนการสืบสวนข้ามประเทศ การจัดตั้งศูนย์แลกเปลี่ยนข้อมูลแบบเรียลไทม์ รวมถึงการสนับสนุนการฝึกอบรมและเทคโนโลยีให้แก่หน่วยงานบังคับใช้กฎหมายของประเทศสมาชิก ทั้งนี้ Europol ยังได้พัฒนาโครงสร้างภายในที่สำคัญอย่าง European Cybercrime Centre (EC3) และ Europol Intelligence Centre (EIC) ซึ่งทำหน้าที่เป็นศูนย์กลางในการจัดเก็บ วิเคราะห์ และเผยแพร่ข้อมูลข่าวกรองด้านอาชญากรรมไซเบอร์ข้ามชาติ ในระดับปฏิบัติการ Europol ยังมี แพลตฟอร์มการสื่อสารที่ปลอดภัย นั้นก็คือ SIENA: Secure Information Exchange Network Application[277] ซึ่งทำให้หน่วยงาน

---

3. ความช่วยเหลือซึ่งกันและกันทางอาญาในรูปแบบอย่างเป็นทางการ สามารถแบ่งออกได้เป็น 2 รูปแบบ ได้แก่

1) ความช่วยเหลือซึ่งกันและกันทางอาญาโดยไม่มีข้อตกลงต่อกันสำหรับหลักต่างตอบแทนหรือหลักถ้อยทีถ้อยปฏิบัติ (Reciprocity) การที่รัฐหนึ่งยอมรับในการบังคับให้ตามคำร้องขอของรัฐอื่นภายใต้เงื่อนไขว่าหากรัฐตนได้ร้องขอให้รัฐอื่นนั้นดำเนินการเช่นเดียวกันแล้ว รัฐนั้นจะยอมปฏิบัติตามเช่นเดียวกัน ซึ่งเป็นข้อผูกมัด ตามกฎหมาย (Legal obligation) หลักต่างตอบแทนหรือหลักถ้อยทีถ้อยปฏิบัตินี้ท้าให้รัฐทังสองต่างมีความ ผูกพันตามกฎหมายระหว่างประเทศมากกว่าหลักไมตรีจิต (Comity) ซึ่งรัฐจะไม่มีข้อผูกมัดทางกฎหมายมาเป็นตัวบังคับ

2) ความช่วยเหลือซึ่งกันและกันทางอาญาโดยมีข้อตกลงต่อกัน เช่น อนุสัญญาสหประชาชาติว่าด้วยการต่อต้านองค์กรอาชญากรรมข้ามชาติที่จัดตังในลักษณะองค์กร ค.ศ. 2000 พิธีสารเพื่อป้องกันปราบปรามและลงโทษการค้ามนุษย์โดยเฉพาะผู้หญิงและเด็ก

[277] In an organization like Europol, which facilitates and relies on the exchange of information, the secure and swift transmission of sensitive and restricted data is essential. The Secure Information Exchange Network Application (SIENA) is a state-of-the-art platform that meets the communication needs of EU law enforcement. The platform enables the swift and user-friendly exchange of operational and strategic crime-related information among:

1.Europol's liaison officers, analysts and experts

2.Member States

บังคับใช้กฎหมายของประเทศสมาชิกสามารถแลกเปลี่ยนข้อมูลข่าวกรองแบบเข้ารหัสได้อย่างมีประสิทธิภาพและปลอดภัย และที่สำคัญ Europol ยังมีบทบาทในการจัดตั้ง Joint Investigative Teams (JITs) ซึ่งเป็นกลไกความร่วมมือในการสืบสวนคดีข้ามชาติ โดยเจ้าหน้าที่จากหลายประเทศสามารถทำงานร่วมกันภายใต้กรอบที่ตกลงร่วมกัน ซึ่งช่วยลดอุปสรรคทางกฎหมายระหว่างรัฐและทำให้การดำเนินการรวดเร็วขึ้น หากเปรียบเทียบกับอาเซียนแล้ว แม้ภูมิภาคนี้จะยังไม่มีองค์กรระดับภูมิภาคที่มีอำนาจและขีดความสามารถเช่น Europol แต่ก็สามารถพัฒนา *แนวทางกึ่งทางการ* ให้ใกล้เคียงกับกรณีของยุโรปได้ โดยเฉพาะการพัฒนากลไกในระดับปฏิบัติการผ่านบันทึกข้อตกลง (MoU) หรือแผนความร่วมมือเฉพาะทาง อาทิ การจัดตั้งศูนย์กลางการประสานข่าวกรองไซเบอร์อาเซียน ซึ่งอาจอยู่ภายใต้การบริหารของ ASEAN Secretariat หรือ AMMTC และเชื่อมโยงกับศูนย์ไซเบอร์ของแต่ละประเทศ โดยมุ่งเน้นการรวบรวม วิเคราะห์ และแบ่งปันข้อมูลภัยคุกคามข้ามชาติแบบเรียลไทม์ อีกประเด็นหนึ่งที่สามารถเรียนรู้จากสหภาพยุโรปได้ คือการพัฒนา แนวทางการฝึกอบรมร่วมและการยกระดับมาตรฐานการปฏิบัติ โดย Europol และ EC3 ได้จัดตั้งศูนย์ฝึกอบรมไซเบอร์ร่วมกับมหาวิทยาลัย สถาบันวิจัย และหน่วยงานภาคเอกชน ซึ่งช่วยให้เกิดฐานข้อมูลความรู้เทคโนโลยีที่ทันสมัย และความเข้าใจร่วมกันระหว่างเจ้าหน้าที่จากแต่ละประเทศ อาเซียนเองก็ควรจัดตั้งศูนย์ฝึกอบรมระดับภูมิภาคด้านอาชญากรรมไซเบอร์ ที่มีการรับรองหลักสูตรร่วมกัน เพื่อสร้างเครือข่ายความร่วมมือในระยะยาวและเสริมสร้างความไว้วางใจระหว่างประเทศสมาชิก อย่างไรก็ดี อาเซียนต้องพิจารณาความแตกต่างในโครงสร้างอำนาจอธิปไตยระหว่างประเทศสมาชิก ซึ่งอาจทำให้ไม่สามารถตั้งองค์กรแบบรวมศูนย์ได้เหมือนสหภาพดังนั้นการดำเนินการควรใช้แนวทางแบบ *bottom-up* โดยการสนับสนุนกลไกความร่วมมือระหว่างหน่วยงานเฉพาะของแต่ละประเทศให้เชื่อมโยงกันอย่างไม่เป็นทางการก่อน แล้วจึงค่อย ๆ ยกระดับความร่วมมือเหล่านี้ขึ้นมาอยู่ภายใต้การรับรองในระดับรัฐมนตรีหรือเลขาธิการอาเซียน

5.1.4 การสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยจากแก๊งคอลเซ็นเตอร์

การสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยจากแก๊งคอลเซ็นเตอร์ถือเป็นนโยบายสาธารณะ เนื่องจากเกี่ยวข้องกับความปลอดภัยของประชาชนและความมั่นคงทางเศรษฐกิจและสังคมของประเทศ แนวทางนี้สามารถกำหนดให้เป็นส่วนหนึ่งของมาตรการป้องกันอาชญากรรมทางไซเบอร์และการคุ้มครองผู้บริโภคในระดับประเทศและระดับภูมิภาคที่ต้องอาศัยความร่วมมือจากหลายฝ่าย ได้แก่ หน่วยงานรัฐบาล ภาคเอกชน องค์กรระหว่างประเทศ และประชาชนทั่วไป โดยการให้ความรู้เกี่ยวกับรูปแบบของการหลอกลวง วิธีการรับมือ และช่องทางการแจ้งเบาะแส เมื่อประชาชนมีความรู้และตระหนักถึงภัย โดยอาชญากรรมข้ามชาติมีลักษณะที่แตกต่างจากอาชญากรรมปกติที่ไม่สามารถ

---

3.Third Parties with which Europol has cooperation agreements / working arrangements.

อธิบายได้ด้วยแนวคิดอาชญาวิทยาแบบดั้งเดิมได้อย่างสมบูรณ์ หากแต่ต้องคำนึงถึงปัจจัยแวดล้อมทั้งทาง เศรษฐกิจ สังคม และการเมือง อันทำให้การจัดการกับปัญหาดังกล่าวจำเป็นต้องบูรณาการแนวคิดใน 3 ด้าน ประกอบด้วย รัฐศาสตร์ นิติศาสตร์ และอาชญาวิทยา เพื่อให้สามารถอธิบายการจัดการปัญหาอาชญากรรมข้ามชาติได้อย่างครอบคลุมโดยหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องของแต่ละประเทศ ต้องนำกลไกความร่วมมือที่มีอยู่ในระดับประเทศ ระดับภูมิภาค และระดับระหว่างประเทศที่มีอยู่ไปใช้ ทำงานร่วมกันให้เกิดประโยชน์สูงสุด เพื่อให้สามารถต่อต้านปัญหาอาชญากรรมข้ามชาติได้อย่างเป็นรูปธรรมและเกิดประสิทธิผลสูงสุด อย่างไรก็ตาม การออกแบบแนวทางการสร้างความตระหนักรู้ที่มีประสิทธิภาพต้องอาศัยความเข้าใจในพฤติกรรมของเหยื่อและกลไกของอาชญากรรม ซึ่งทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory) จะเกิดขึ้นเมื่อมี 3 องค์ประกอบหลักมารวมกัน ได้แก่ (1) ผู้กระทำผิดที่ได้รับแรงจูงใจ (Motivated Offender) (2) เป้าหมายที่เหมาะสม (Suitable Target) และ (3) การขาดผู้ป้องกันที่มีประสิทธิภาพ (Lack of Capable Guardianship)[278] ซึ่งหากสามารถลดโอกาสที่ปัจจัยทั้งสามจะมาบรรจบกันได้ ก็จะช่วยลดอาชญากรรมลงได้ โดยในกรณีของแก๊งคอลเซ็นเตอร์ แนวคิดนี้สามารถนำมาใช้วิเคราะห์แนวทางในการสร้างความตระหนักรู้ให้ประชาชนเพื่อลดโอกาสตกเป็นเหยื่อ สามารถอธิบายได้ ดังนี้

1. ลดโอกาสที่เป้าหมายจะเหมาะสมสำหรับอาชญากร จากมุมมองของทฤษฎีกิจวัตรประจำวัน เหยื่อของแก๊งคอลเซ็นเตอร์มักเป็นกลุ่มที่มีความเสี่ยงสูง ผู้สูงอายุ คนที่ไม่คุ้นเคยกับเทคโนโลยี หรือผู้ที่มีความเร่งรีบในการทำธุรกรรมทางการเงิน มักเป็นกลุ่มที่อาชญากรเลือกเป็นเป้าหมายเพราะพวกเขามีโอกาสตกหลุมพรางได้ง่าย ดังนั้น การสร้างความตระหนักรู้จึงเป็นแนวทางสำคัญในการลดความเหมาะสมของเป้าหมาย โดยสามารถดำเนินการได้ในหลายรูปแบบ เช่น การรณรงค์ผ่านสื่อสาธารณะ โดยใช้โทรทัศน์ วิทยุ โซเชียลมีเดีย และป้ายโฆษณา เพื่อเตือนประชาชนเกี่ยวกับวิธีการของแก๊งคอลเซ็นเตอร์ รวมถึงแนวทางป้องกัน การบรรจุหลักสูตรความรู้ด้านอาชญากรรมไซเบอร์ในระบบการศึกษา เพื่อให้เยาวชนเข้าใจภัยอาชญากรรมทางออนไลน์ตั้งแต่เนิ่น ๆ และสามารถให้คำแนะนำแก่ผู้สูงอายุหรือบุคคลในครอบครัวที่อาจตกเป็นเหยื่อได้ และการจัดอบรมให้กับผู้สูงอายุและกลุ่มเปราะบางโดยให้หน่วยงานที่เกี่ยวข้อง เช่น ธนาคารและบริษัทโทรคมนาคม จัดกิจกรรมให้ความรู้เกี่ยวกับภัยจากแก๊งคอลเซ็นเตอร์เพื่อช่วยลดความเสี่ยงในการถูกหลอกลวง

2. การเปลี่ยนแปลงพฤติกรรมของประชาชนเพื่อลดความเสี่ยง แม้ว่าการสร้างความตระหนักรู้จะมุ่งเน้นที่เหยื่อเป็นหลัก แต่ก็สามารถมีผลต่อแรงจูงใจของผู้กระทำผิดได้ด้วย หากการหลอกลวงได้ผลน้อยลง โอกาสที่แก๊งคอลเซ็นเตอร์จะเติบโตย่อมน้อยลงตามไปด้วย โดยแนวทางที่

---

[278] Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44*(4), 588-608.

สามารถลดแรงจูงใจของอาชญากร ได้แก่ การสร้างวัฒนธรรมการรายงาน โดยให้ประชาชนที่เคยตกเป็นเหยื่อหรือพบเห็นพฤติกรรมต้องสงสัยแจ้งเบาะแสต่อเจ้าหน้าที่ เพื่อให้ข้อมูลเหล่านี้ถูกนำไปใช้ในการปรับปรุงมาตรการป้องกันในอนาคต การเปิดเผยข้อมูลเกี่ยวกับกระบวนการของแก๊งคอลเซ็นเตอร์ เพื่อทำให้ประชาชนตื่นตัวและไม่หลงกลง่าย เช่น รายงานข่าวเชิงสืบสวนที่เปิดโปงเครือข่ายของกลุ่มอาชญากรรมเหล่านี้ การส่งเสริม แนวทาง “รู้เท่าทันอาชญากรรม” ในระดับชุมชน โดยให้ชุมชนช่วยกันเฝ้าระวังและรายงานข้อมูลที่น่าสงสัยไปยังหน่วยงานที่เกี่ยวข้อง การสร้างแรงกดดันทางสังคม โดยให้ความรู้กับประชาชนว่าการทำงานให้กับแก๊งคอลเซ็นเตอร์เป็นความผิดร้ายแรง เพื่อป้องกันไม่ให้บุคคลตกเป็นเครื่องมือขององค์กรอาชญากรรม

3. เพิ่มจำนวนและประสิทธิภาพของ “ผู้ป้องกัน” (Guardian) ทฤษฎีกิจวัตรประจำวันชี้ว่า หากมีผู้ป้องกันที่มีประสิทธิภาพเพิ่มขึ้นจะช่วยลดโอกาสที่อาชญากรรมจะเกิดขึ้น[279] ในกรณีของแก๊งคอลเซ็นเตอร์ ผู้ป้องกันสามารถอยู่ในหลายระดับ ตั้งแต่เจ้าหน้าที่รัฐไปจนถึงบุคคลทั่วไป โดยแนวทางที่ควรดำเนินการ การเพิ่มบทบาทของธนาคารและผู้ให้บริการโทรคมนาคมในการตรวจสอบธุรกรรมที่น่าสงสัยและระงับหมายเลขโทรศัพท์ที่ใช้ก่ออาชญากรรม การส่งเสริมให้เจ้าหน้าที่รัฐและองค์กรภาคประชาชนมีส่วนร่วมในการรณรงค์และแจ้งเตือนประชาชนอย่างต่อเนื่อง การสนับสนุนชุมชนออนไลน์และเครือข่ายอาสาสมัครให้ช่วยกันแจ้งเตือนภัยผ่านแพลตฟอร์มโซเชียลมีเดีย การเพิ่มบทบาทของธนาคารและผู้ให้บริการโทรคมนาคม ในการตรวจสอบธุรกรรมที่น่าสงสัยและระงับหมายเลขโทรศัพท์ที่ใช้ก่ออาชญากรรม

## 5.3 วิเคราะห์มาตรการที่เหมาะสมในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ กรณีแก๊งคอลเซ็นเตอร์

### 5.3.1 มาตรการที่เหมาะสมในรในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

เมื่อพิจารณาถึงโครงสร้างความร่วมมือของอาเซียน จะพบว่าแม้จะมีกรอบความร่วมมือด้านความมั่นคงและกฎหมายระหว่างประเทศในระดับอาเซียน แต่กรอบความร่วมมือเหล่านั้นยังมีข้อจำกัดสำคัญอยู่หลายประการ ทั้งในแง่ของความไม่ผูกพันทางกฎหมาย กลไกที่ไม่สามารถบังคับใช้ได้จริง และการประสานงานที่ไม่ทันต่อภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว ข้อจำกัดในเรื่องของ “หลักการไม่แทรกแซงกิจการภายใน” และ “หลักการเคารพเอกราช อธิปไตย ความเสมอภาค บูรณภาพแห่งดินแดนและอัตลักษณ์” ของรัฐสมาชิกอาเซียน *(ในหัวข้อที่ 4.3.1.1)* ซึ่งแม้จะเป็นหลักการ

---

[279] Felson, M., *Crime and Everyday Life* (Thousand Oaks, CA: Sage, 2002) 45–46.

สำคัญที่มีบทบาทในการธำรงเสถียรภาพของภูมิภาคอาเซียน แต่อาจกลับกลายเป็นอุปสรรคสำคัญต่อการดำเนินความร่วมมือเชิงลึกที่จำเป็นต่อการจัดการกับอาชญากรรมข้ามชาติที่มีลักษณะไร้พรมแดนและมีความเชื่อมโยงระหว่างประเทศอย่างใกล้ชิด ประเด็นปัญหาเหล่านี้ยิ่งทวีความรุนแรงมากขึ้นในกรณีของแก๊งคอลเซ็นเตอร์ ซึ่งอาศัยช่องโหว่ของระบบกฎหมายและช่องว่างในความร่วมมือระหว่างประเทศเป็นเครื่องมือสำคัญในการก่ออาชญากรรมข้ามพรมแดน ด้วยเหตุนี้ จึงเห็นว่ามีความจำเป็นอย่างยิ่งในการจัดทำข้อตกลงทางกฎหมายระดับภูมิภาคว่าด้วยการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ เพื่อสร้างความร่วมมือที่มีผลในทางปฏิบัติในทางระหว่างประเทศและมีพันธกรณีผูกพันที่รัฐสมาชิกต้องยึดถือและต้องปฏิบัติตามร่วมกันโดยสุจริต (Good faith) ตามหลักการแห่งกฎหมายสนธิสัญญาว่าด้วย “สัญญาต้องได้รับการปฏิบัติตาม” *(Pacta sunt servanda)*[280] ทั้งนี้ การดำเนินการในลักษณะดังกล่าว ไม่จำเป็นต้องขัดกับหลักอธิปไตยของรัฐ หากแต่สามารถออกแบบให้ยืดหยุ่นและเป็นไปในแนวทางของความร่วมมือโดยสมัครใจที่ยังคงเคารพอำนาจภายในของแต่ละประเทศ โดยอาศัยแนวทางตามหลักสากลในกฎหมายระหว่างประเทศซึ่งบัญญัติไว้อย่างชัดแจ้งว่า การดำเนินการใด ๆ ที่กระทบต่ออำนาจของรัฐต้องอยู่ภายใต้ความยินยอมของรัฐสมาชิกอย่างชัดแจ้ง ดังนั้น หากรัฐสมาชิกเห็นพ้องต้องกันในการจัดทำข้อตกลงก็ย่อมไม่ถือว่าเป็นการละเมิดอธิปไตย หากแต่เป็นการใช้อำนาจอธิปไตยของตน เพื่อเข้าสู่พันธกรณีด้วยเจตจำนงเสรี[281] เช่นเดียวกับที่รัฐต่าง ๆ เข้าร่วมเป็นภาคีในอนุสัญญาสหประชาชาติ หรือสนธิสัญญาระหว่างประเทศอื่น ๆ ที่มีผลผูกพัน เพื่อให้ข้อตกลงมีผลในทางปฏิบัติได้จริง อาเซียนควรกำหนดให้มีการจัดประชุมรัฐมนตรีด้านกฎหมายหรือความมั่นคงของภูมิภาคเพื่อให้สัตยาบันร่วมกัน และอาจจัดตั้งคณะทำงานถาวรด้านการต่อต้านอาชญากรรมไซเบอร์ภายใต้ประชาคมการเมืองและความมั่นคงของอาเซียน (ASEAN Political-Security Community) เพื่อทำหน้าที่ในการติดตาม ประเมินผล และเสนอมาตรการใหม่ให้ทันต่อสถานการณ์ที่เปลี่ยนแปลง ทั้งนี้ การออกแบบกลไกดังกล่าวควรตั้งอยู่บนหลักของความโปร่งใส ยืดหยุ่น และเคารพบริบททางการเมืองและกฎหมายของแต่ละประเทศ เพื่อให้

---

[280] Vienna Convention on the Law of Treaties

Article 26 [Pacta sunt servanda] Every treaty in force is binding upon the parties to it and must be performed by them in good faith.

[281] Vienna Convention on the Law of Treaties

Article 6 “Every State possesses capacity to conclude treaties”

Article 11: “The consent of a State to be bound by a treaty may beexpressed by signature, exchange of instruments constituting a treaty, ratification, acceptance, approval or accession, or by any other means if so agreed”.

เกิดการยอมรับร่วมกัน และสามารถบังคับใช้ได้จริงในทางปฏิบัติ ซึ่งจากการศึกษาสามารถวิเคราะห์มาตรการที่เหมาะสมในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ ดังนี้

1. องค์การอาเซียนสมควรมีคำนิยามของคำว่า “แก๊งคอลเซ็นเตอร์” โดยคำนึงถึงรูปแบบที่ในสภาวะปัจจุบันมีการกระทำของอาชญากรแก๊งคอลเซ็นเตอร์ที่ซับซ้อนและมีกลยุทธ์เพิ่มขึ้น ภายในนิยามควรระบุให้ชัดเจนว่าอาชญากรรมดังกล่าวคือ “การกระทำความผิดโดยกลุ่มบุคคลที่มีการจัดตั้ง มีการแบ่งหน้าที่ และมีเป้าหมายในการหลอกลวงหรือข่มขู่ผู้อื่นผ่านระบบโทรคมนาคมหรือเทคโนโลยีดิจิทัล เพื่อแสวงหาผลประโยชน์โดยมิชอบด้วยกฎหมาย และการกระทำนั้นมีผลกระทบหรือมีการเชื่อมโยงระหว่างรัฐสมาชิกมากกว่าหนึ่งประเทศขึ้นไป” องค์ประกอบที่สำคัญอีกประการหนึ่งคือการใช้เทคโนโลยีเป็นเครื่องมือในการกระทำผิด ไม่ว่าจะเป็นการโทรผ่านระบบ VoIP การใช้บอทหรือระบบอัตโนมัติในการส่งข้อความหลอกลวง การปลอมตัวเป็นเจ้าหน้าที่รัฐ หรือการอำพรางเส้นทางการเงินผ่านคริปโตเคอร์เรนซีและบัญชีม้า อีกประเด็นหนึ่งที่สมควรพิจารณาในกระบวนการกำหนดนิยาม คือ เรื่องของ “เหยื่อ” เพราะการหลอกลวงโดยแก๊งคอลเซ็นเตอร์ในปัจจุบันไม่ได้จำกัดอยู่เฉพาะกลุ่มประชากรใดกลุ่มหนึ่งเท่านั้น แต่ขยายตัวไปยังผู้สูงอายุ คนทำงานทั่วไป และแม้แต่เด็กและเยาวชน การมีนิยามที่ครอบคลุมถึงผู้ได้รับความเสียหายทางเศรษฐกิจ สังคม หรือจิตใจจากการกระทำขององค์กรอาชญากรรมจะทำให้สามารถจัดวางมาตรการคุ้มครองและเยียวยาได้ตรงจุดยิ่งขึ้น เช่นเดียวกับการที่ต้องให้ความสำคัญกับผู้ที่อาจถูกหลอกให้เข้าไปเป็นส่วนหนึ่งของเครือข่ายโดยไม่รู้ตัว เช่น ผู้ที่ถูกหลอกให้เปิดบัญชีให้ผู้อื่นใช้ หรือผู้ที่ถูกจ้างให้โทรหลอกลวงโดยอ้างว่าเป็นงานออนไลน์ ท้ายที่สุด การกำหนดนิยามของอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์จึงไม่ใช่เพียงแค่การให้คำนิยามทางกฎหมาย หากแต่เป็นการสร้างเครื่องมือทางความเข้าใจร่วมในระดับภูมิภาค ที่จะเป็นรากฐานของความร่วมมือในการบังคับใช้กฎหมาย การสืบสวนสอบสวนข้ามพรมแดน และการคุ้มครองเหยื่อที่เหมาะสม

2. มาตรการด้านการติดตามและยึดทรัพย์สินที่เกี่ยวข้องกับอาชญากรรม ถือเป็นมาตรการสำคัญที่ไม่เพียงส่งผลต่อการปราบปราม แต่ยังส่งผลโดยตรงต่อการลดแรงจูงใจในการก่ออาชญากรรมข้ามชาติกรณีของแก๊งคอลเซ็นเตอร์ซึ่งมีวัตถุประสงค์หลักอยู่ที่ผลประโยชน์ทางเศรษฐกิจเป็นหลัก ในกรอบของสหภาพยุโรป มีเครื่องมือทางกฎหมายที่เรียกว่า Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime[282] ซึ่งกำหนดให้

[282] Directive 2014/42/EU เรื่องการอายัดและริบทรัพย์สินที่เกี่ยวข้องกับอาชญากรรม มีบทบัญญัติหลายข้อที่เกี่ยวข้องกับการริบทรัพย์สินที่ได้จากการกระทำความผิด เพื่อช่วยให้การปราบปรามอาชญากรรมข้ามชาติ รวมถึงอาชญากรรมที่เกิดจากแก๊งคอลเซ็นเตอร์มีประสิทธิภาพมากขึ้น โดยมีเนื้อหาหลัก ๆ ดังนี้:

รัฐสมาชิกมีหน้าที่ระบุ ยึด และริบทรัพย์สินที่เกี่ยวข้องกับการกระทำความผิดทางอาญาอย่างครอบคลุม ไม่ว่าจะเป็นทรัพย์สินที่ได้มาจากการกระทำความผิดโดยตรง หรือทรัพย์สินที่แปลงสภาพแล้ว โดยอนุญาตให้มีการริบทรัพย์แม้ไม่มีคำพิพากษาลงโทษจำเลยในบางกรณี ทั้งนี้ เพื่อป้องกันไม่ให้เครือข่ายอาชญากรรมสามารถหลบเลี่ยงกระบวนการยุติธรรมผ่านช่องโหว่ทางกฎหมายได้ เมื่อพิจารณาในบริบทของอาเซียนยังไม่มีกรอบทางกฎหมายที่เฉพาะเจาะจงในระดับภูมิภาคเกี่ยวกับการอายัดและริบทรัพย์สินอาชญากรรมข้ามชาติที่มีผลผูกพันทางกฎหมายต่อรัฐสมาชิกโดยตรง สนธิสัญญาความช่วยเหลือทางอาญา (ASEAN MLAT) แม้จะเปิดทางให้รัฐสมาชิกสามารถร้องขอการดำเนินมาตรการทางกฎหมายระหว่างกันได้ เช่น การสอบสวน พยานหลักฐาน หรือการติดตามทรัพย์สิน แต่ก็ยังอาศัยกลไกแบบทวิภาคีที่ต้องดำเนินการผ่านช่องทางทางการทูต เช่น การส่งหนังสือคำร้องผ่านกระทรวงการต่างประเทศ หรือสถานเอกอัครราชทูตของแต่ละประเทศ[283] ซึ่งเป็นกระบวนการที่ล่าช้าและไม่ตอบสนองต่อความเร่งด่วนของการติดตามทรัพย์สินที่อาจถูกโยกย้ายหรือแปลงสภาพได้อย่างรวดเร็วในโลกดิจิทัลปัจจุบัน ซึ่งหากนำมาตรการด้านการติดตามและยึดทรัพย์สินที่เกี่ยวข้องกับอาชญากรรมข้ามชาติมาปรับใช้ในบริบทของอาเซียนจะต้องอาศัยความร่วมมือระหว่างประเทศอย่างใกล้ชิด ทั้งในแง่การแลกเปลี่ยนข้อมูลทรัพย์สิน การติดตามเส้นทางเงินและการออกคำสั่งอายัดข้ามพรมแดน จึงควรมีการบัญญัติมาตรฐานขั้นต่ำในอนุสัญญาระดับอาเซียนว่าด้วยอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ ซึ่งควรครอบคลุมประเด็นสำคัญโดยให้รัฐสมาชิกต้องจัดตั้งกฎหมายว่าด้วย การริบทรัพย์สินโดยไม่ต้องมีคำพิพากษาอย่างชัดเจน ให้เป็นแนวทางปฏิบัติที่รัฐสมาชิกต้องตราเป็นกฎหมายภายในประเทศเพื่อรองรับกรณีที่ไม่สามารถนำตัวจำเลยเข้าสู่

---

1. การอายัดทรัพย์สิน (Asset Freezing) กำหนดให้ประเทศสมาชิกต้องสามารถอายัดทรัพย์สินที่เกี่ยวข้องกับการกระทำความผิดได้ทันทีหลังจากที่มีการเปิดการสอบสวน โดยไม่ต้องรอคำตัดสินจากศาล ซึ่งจะช่วยป้องกันไม่ให้ทรัพย์สินที่ได้จากการกระทำความผิดถูกย้ายหรือใช้ไปในทางที่ผิดก่อนที่จะมีการตัดสินคดี

2. การริบทรัพย์สิน (Asset Confiscation) การริบทรัพย์สินที่เกี่ยวข้องกับการกระทำความผิดเป็นมาตรการที่สำคัญในการปราบปรามอาชญากรรม โดยให้สามารถริบทรัพย์สินที่ได้จากการกระทำความผิด ซึ่งไม่จำเป็นต้องเชื่อมโยงกับอาชญากรรมโดยตรง เพียงแค่สามารถแสดงให้เห็นว่าเป็นทรัพย์สินที่ได้จากการกระทำผิดได้

3. การแลกเปลี่ยนข้อมูลและความร่วมมือระหว่างประเทศ โดยเน้นให้การแลกเปลี่ยนข้อมูลระหว่างประเทศสมาชิกเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ โดยการแลกเปลี่ยนข้อมูลเกี่ยวกับทรัพย์สินที่ได้จากการกระทำความผิด รวมถึงความร่วมมือในการดำเนินการยึดและริบทรัพย์สินข้ามพรมแดน; โปรดดู: ‘Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union’ (European Union) https://eur-lex.europa.eu/eli/dir/2014/42/oj/eng accessed 19 March 2025.

[283] United Nations Office on Drugs and Crime (UNODC), Manual on Mutual Legal Assistance and Extradition (2012).

กระบวนการยุติธรรมได้ อีกทั้งออกแบบกลไกการออกคำสั่งอายัดหรือริบทรัพย์สินข้ามประเทศโดยไม่ต้องผ่านกระบวนการทางการทูต กล่าวคือ คำสั่งศาล หรือคำสั่งของพนักงานสอบสวนหรืออัยการจากรัฐสมาชิกหนึ่ง ควรสามารถส่งตรงไปยังหน่วยงานที่มีอำนาจของอีกรัฐสมาชิกหนึ่งได้โดยไม่ต้องผ่านการส่งคำร้องผ่านกระทรวงการต่างประเทศ หรือการรับรองผ่านสถานเอกอัครราชทูตอีกต่อไป และต้องมีการกำหนดรูปแบบและเนื้อหาของคำร้องให้เป็นมาตรฐานกลาง และมีข้อกำหนดด้านเวลาในการดำเนินการที่ชัดเจน พร้อมกลไกคุ้มครองสิทธิผู้ถือทรัพย์ที่สุจริตเพื่อไม่ให้กลายเป็นการละเมิดสิทธิ์โดยไม่ตั้งใจเพื่อให้มาตรการเหล่านี้ไม่เป็นการละเมิดสิทธิขั้นพื้นฐาน โดยอาจกำหนดให้มีขั้นตอนการอุทธรณ์ หรือการพิสูจน์สถานะผู้ถือทรัพย์อย่างเหมาะสมการยกระดับกลไกทางกฎหมายในประเด็นการติดตามและยึดทรัพย์เช่นนี้ ไม่เพียงช่วยลดแรงจูงใจในการกระทำความผิดของเครือข่ายอาชญากรรมข้ามชาติ แต่ยังช่วยให้กระบวนการยุติธรรมในภูมิภาคมีความทันสมัยและมีมาตรฐานร่วมกันที่สามารถตอบสนองต่อภัยคุกคามรูปแบบใหม่ได้อย่างแท้จริง

3. มาตรการด้านพยานหลักฐานในกระบวนการสอบสวนและดำเนินคดีอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ ซึ่งถือเป็นองค์ประกอบสำคัญในการดำเนินคดีอาญา โดยเฉพาะในกรณีของอาชญากรรมข้ามชาติอย่างแก๊งคอลเซ็นเตอร์ ซึ่งมีความซับซ้อนในเชิงโครงสร้างองค์กร การกระทำผิดข้ามเขตแดน และใช้เทคโนโลยีเป็นเครื่องมือในการกระทำความผิด ความท้าทายที่สำคัญในเรื่องนี้คือ ความล่าช้าในการจัดเก็บพยานหลักฐานที่เกี่ยวข้องกับการกระทำผิดซึ่งมักกระจายอยู่ในหลายประเทศ ปัญหาเกี่ยวกับความไม่ชัดเจนของอำนาจในการเข้าถึงข้อมูลในระบบเทคโนโลยีสารสนเทศ การไม่มีกลไกกลางที่สามารถรวบรวม วิเคราะห์ หรือประมวลผลข้อมูลอย่างมีมาตรฐานเดียวกันและการขาดข้อตกลงที่มีผลผูกพันในการรับรองความถูกต้องของพยานหลักฐานที่ได้มาจากต่างประเทศ ในกรณีแก๊งคอลเซ็นเตอร์การกระทำผิดมักเริ่มต้นจากการหลอกลวงผ่านโทรศัพท์หรือระบบออนไลน์ ซึ่งหลักฐานสำคัญมักอยู่ในรูปแบบดิจิทัล เช่น ข้อมูลการโทร ข้อมูล IP address บัญชีธนาคารที่ใช้รับโอนเงิน บันทึกการสื่อสาร และโปรแกรมที่ใช้ในการแฝงตัวหรือปลอมแปลงตัวตนทางออนไลน์ หลักฐานเหล่านี้มักถูกลบหรือทำลายอย่างรวดเร็ว ทำให้การสืบสวนที่ล่าช้าอาจไม่สามารถเก็บรวบรวมข้อมูลที่สำคัญได้ทันเวลา ยิ่งไปกว่านั้นหลักฐานทางดิจิทัลเหล่านี้มักอยู่ภายใต้การควบคุมของผู้ให้บริการที่ตั้งอยู่ในประเทศที่สาม ซึ่งไม่ได้มีข้อตกลงด้านการให้ความช่วยเหลือทางกฎหมายกับประเทศที่กำลังสืบสวน ทำให้เกิดช่องว่างในการเข้าถึงข้อมูล จากสถานการณ์ดังกล่าวจึงมีความจำเป็นอย่างยิ่งที่อาเซียนควรกำหนดมาตรการด้านพยานหลักฐานในกรอบข้อตกลงระดับภูมิภาคอย่างชัดเจน โดยเฉพาะอย่างยิ่งการรับรองให้พยานหลักฐานดิจิทัลที่ได้จากประเทศสมาชิกอาเซียนอื่นสามารถนำไปใช้ในกระบวนการยุติธรรมของแต่ละรัฐได้โดยไม่ต้องมีการรับรองซ้ำซ้อนตามกระบวนการทางการทูต กล่าวคือ พยานหลักฐานที่ได้จากประเทศสมาชิกหนึ่งไม่ควรต้องผ่านการส่งคำร้องผ่านกระทรวงการต่างประเทศ หรือการรับรองผ่านสถานเอกอัครราชทูตเพื่อให้มีผลใช้ได้ใน

กระบวนการพิจารณาคดีของอีกรัฐหนึ่ง ซึ่งเป็นขั้นตอนแบบดั้งเดิมภายใต้ระบบการขอความช่วยเหลือทางกฎหมายทวิภาคี (Mutual Legal Assistance Treaty – MLAT) ที่มีข้อจำกัดด้านความล่าช้าและขั้นตอนทางราชการจำนวนมาก ขั้นตอนดังกล่าวมักต้องเริ่มจากการยื่นคำร้องโดยหน่วยงานผู้ร้อง เช่น อัยการ หรือกระทรวงยุติธรรม ไปยังหน่วยงานกลางของประเทศตนเอง จากนั้นต้องส่งผ่านกระทรวงการต่างประเทศเพื่อออกหนังสือทางการทูตถึงประเทศคู่สัญญา และเมื่อถึงปลายทาง คำร้องจะต้องผ่านกระบวนการตรวจสอบซ้ำโดยหน่วยงานของรัฐนั้น เช่น กระทรวงการต่างประเทศ อัยการสูงสุด หรือหน่วยงานยุติธรรม ก่อนที่จะนำเสนอให้ศาลรับรองหรืออนุญาตให้ดำเนินการสอบสวนหรือรับพยานหลักฐานนั้นได้ กระบวนการเหล่านี้อาจใช้เวลาหลายเดือน และไม่เหมาะกับลักษณะของอาชญากรรมสมัยใหม่ที่พยานหลักฐานมักอยู่ในรูปแบบดิจิทัลซึ่งสามารถถูกลบหรือทำลายได้อย่างรวดเร็ว ด้วยเหตุนี้ อาเซียนควรออกแบบกลไกที่ใช้หลักการยอมรับพยานหลักฐานโดยอัตโนมัติ หรือการยอมรับโดยตรง ซึ่งเปิดทางให้ศาลหรือพนักงานสอบสวนของรัฐหนึ่งสามารถยอมรับพยานหลักฐานที่ได้จากหน่วยงานของรัฐสมาชิกอื่นได้ทันทีภายใต้กรอบของข้อตกลงร่วมที่มีผลผูกพันทางกฎหมาย โดยไม่จำเป็นต้องผ่านกระบวนการรับรองซ้ำ หรือผ่านกระบวนการทูตดังที่ใช้ใน MLAT อีกต่อไป ทั้งนี้ หลักการดังกล่าวต้องตั้งอยู่บนพื้นฐานของความไว้เนื้อเชื่อใจในกระบวนการยุติธรรมของกันและกัน และการกำหนดมาตรฐานขั้นต่ำร่วมกันในเรื่องกระบวนการจัดเก็บ การรักษาความครบถ้วนของข้อมูล , การตรวจสอบความถูกต้องและการจัดทำเอกสารประกอบที่สามารถตรวจสอบย้อนกลับได้ เพื่อให้พยานหลักฐานที่ส่งข้ามพรมแดนมีความน่าเชื่อถือเพียงพอต่อการนำไปใช้ในศาลหรือการสอบสวนของรัฐอื่น เช่นเดียวกับแนวทางในสหภาพยุโรปที่มีการพัฒนา European Investigation Order[284] (EIO) ภายใต้ Directive 2014/41/EU ซึ่งกำหนดให้ประเทศสมาชิกสามารถร้องขอและส่งมอบพยานหลักฐานในคดีอาญาได้โดยตรงระหว่างหน่วยงานที่มีอำนาจ เช่น ศาล อัยการ หรือพนักงานสอบสวน โดยไม่ต้องผ่านกระทรวงการต่างประเทศหรือหน่วยงานทางการทูต

---

[284] Article 1: The European Investigation Order and obligation to execute it

1. A European Investigation Order (EIO) is a judicial decision issued or validated by a judicial authority of a Member State (“the issuing State”) to have one or several specific investigative measure(s) carried out in another Member State (“the executing State”) with a view to gathering evidence within the framework of criminal proceedings, including proceedings brought by administrative authorities in respect of acts which are punishable under the national law of the issuing State by virtue of being infringements of the rules of law and where the decision may give rise to proceedings before a court having jurisdiction in particular in criminal matters.

2. Member States shall execute an EIO on the basis of the principle of mutual recognition and in accordance with this Directive.

3. The execution of an EIO may be refused only on the grounds specified in this Directive.

EIO ยังมีแบบฟอร์มมาตรฐานกลางที่ช่วยลดความคลาดเคลื่อนและเร่งความเร็วของกระบวนการ อีกทั้งยังกำหนดให้รัฐสมาชิกมีหน้าที่ตอบสนองต่อคำร้องภายในระยะเวลาที่กำหนดเว้นแต่จะมีเหตุผลทางกฎหมายชัดเจนที่ไม่สามารถดำเนินการได้ ดังนั้น มาตรการด้านพยานหลักฐานจึงควรได้รับการยกระดับจากระดับทวิภาคีสู่ระดับพหุภาคีในกรอบของอาเซียน เพื่อให้สามารถตอบสนองต่ออาชญากรรมข้ามชาติในรูปแบบใหม่อย่างแก๊งคอลเซ็นเตอร์ได้อย่างทันท่วงที สอดคล้องกับหลักการของ *UN Convention against Transnational Organized Crime (UNTOC)* ที่ให้ความสำคัญกับการสร้างกลไกความร่วมมือด้านกระบวนการยุติธรรมทางอาญาในระดับระหว่างประเทศอย่างมีประสิทธิภาพและครอบคลุมทุกด้านของการดำเนินคดี

4. มาตรการด้านการคุ้มครองพยานและผู้เสียหาย ควรได้รับการพิจารณาในฐานะหลักประกันพื้นฐานแห่งความยุติธรรม การดำเนินคดีอาญาที่มีมิติระหว่างประเทศย่อมต้องพึ่งพาคำให้การของพยานและความร่วมมือจากผู้เสียหายเป็นอย่างมาก อย่างไรก็ตามในความเป็นจริงพยานและผู้เสียหายมักเผชิญกับแรงกดดันจากทั้งความกลัวต่อการถูกตอบโต้จากเครือข่ายอาชญากรและความไม่มั่นใจในระบบยุติธรรมของรัฐ เมื่อไม่มีกลไกรองรับทางกฎหมายที่จะให้ความคุ้มครองได้อย่างเพียงพอ ปัญหาที่เกิดขึ้นอย่างแพร่หลายในประเทศสมาชิกอาเซียน คือ การขาดกรอบกฎหมายที่ให้ความคุ้มครองอย่างชัดเจนต่อพยานและผู้เสียหายในลักษณะข้ามพรมแดน แม้ในบางประเทศอาจมีกฎหมายภายในที่ให้การคุ้มครองอยู่บ้าง แต่กลับไม่สามารถใช้ได้จริงในคดีที่เกี่ยวข้องกับอาชญากรรมข้ามชาติเพราะไม่มีความเชื่อมโยงระหว่างกฎหมายภายในกับพันธกรณีระหว่างประเทศหรือความร่วมมือเชิงกลไกกับประเทศอื่นในภูมิภาค ในกรอบของภูมิภาคอาเซียนจึงมีความจำเป็นอย่างยิ่งที่จะต้องกำหนดมาตรการคุ้มครองพยานและผู้เสียหายไว้ในระดับภูมิภาค โดยต้องมีหลักการที่ยึดโยงกับสิทธิมนุษยชนขั้นพื้นฐาน ไม่ว่าจะเป็นสิทธิในการได้รับการคุ้มครองจากอันตราย สิทธิในการไม่ถูกเลือกปฏิบัติ และสิทธิในการเข้าถึงกระบวนการยุติธรรมอย่างเท่าเทียม การให้คำจำกัดความที่ครอบคลุมว่า “ผู้เสียหาย” คือผู้ที่ได้รับผลกระทบทั้งโดยตรงและโดยอ้อมจากการกระทำผิดทางอาญา รวมถึงการยอมรับว่า “พยาน” ในคดีอาชญากรรมข้ามชาตินั้นอาจเป็นพลเมืองของประเทศอื่นและอยู่ในเขตอำนาจศาลที่แตกต่างกัน ก็เป็นสิ่งที่ต้องบัญญัติไว้อย่างชัดเจนในกรอบความร่วมมือทางกฎหมาย อีกทั้งการคุ้มครองพยานและผู้เสียหายไม่อาจพิจารณาในมิติกายภาพเพียงอย่างเดียว แต่ต้องรวมถึงการคุ้มครองข้อมูลส่วนบุคคล การปกป้องความลับของพยาน การห้ามติดต่อหรือข่มขู่ผู้เสียหายในระหว่างพิจารณาคดีและการรับรองว่าผู้เสียหายมีสิทธิในการมีส่วนร่วมในกระบวนการยุติธรรม ตลอดจนได้รับข้อมูลเกี่ยวกับความคืบหน้าของคดีของตนอย่างต่อเนื่อง

5. มาตรการคุ้มครองข้อมูลส่วนบุคคลเพื่อป้องกันอาชญากรรมข้ามชาติในอาเซียน ในบริบทของอาชญากรรมข้ามชาติยุคดิจิทัลซึ่งใช้ข้อมูลส่วนบุคคลของเหยื่อเป็นเครื่องมือหลักในการหลอกลวง ไม่ว่าจะเป็นชื่อ-นามสกุล หมายเลขบัตรประชาชน บัญชีธนาคาร หรือข้อมูลธุรกรรม

การเงิน การเข้าถึงหรือรั่วไหลของข้อมูลเหล่านี้กลายเป็นทรัพยากรเชิงอาชญากรรมที่สำคัญที่สุดในการดำเนินการขององค์กรอาชญากรรมไซเบอร์ ด้วยเหตุนี้ มาตรการคุ้มครองข้อมูลส่วนบุคคลจึงไม่ควรถูกมองเพียงในแง่ของการคุ้มครองสิทธิพลเมือง หากแต่เป็น เครื่องมือเชิงป้องกันเชิงโครงสร้าง ที่สามารถตัดวงจรการกระทำผิดตั้งแต่ต้นทางได้ โดยจากการศึกษาพบว่าสหภาพยุโรปมีระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ General Data Protection Regulation (GDPR) ถือเป็นแบบอย่างของการกำหนดมาตรฐานสูงสุดในการปกป้องข้อมูล โดยกำหนดให้ทั้งภาครัฐและเอกชนต้องรับผิดชอบต่อการเก็บ ใช้ และจัดเก็บข้อมูลส่วนบุคคลอย่างรัดกุม โปร่งใส และปลอดภัย หากเกิดการรั่วไหล ต้องแจ้งเหตุแก่หน่วยงานกำกับภายใน 72 ชั่วโมง และหากมีผลกระทบร้ายแรงต้องแจ้งผู้เสียหายโดยตรง[285] นอกจากนี้ ยังมีบทบัญญัติเกี่ยวกับการประเมินความเสี่ยงล่วงหน้า (Data Protection Impact Assessment: DPIA) ในกรณีที่มีการประมวลผลข้อมูลขนาดใหญ่หรือใช้เทคโนโลยีใหม่ที่อาจกระทบสิทธิของบุคคล ทำให้เกิดกลไกการป้องกันเชิงคาดการณ์ที่สำคัญต่อการลดความเสี่ยงของข้อมูลรั่วไหล ซึ่งจากหลักการของ GDPR จึงชัดเจนว่าการคุ้มครองข้อมูลส่วนบุคคลไม่ใช่เพียงมาตรการคุ้มครองสิทธิเท่านั้นแต่เป็นกลไกสกัดกั้นไม่ให้ข้อมูลตกไปอยู่ในมือของเครือข่ายอาชญากรรม สำหรับภูมิภาคอาเซียนแม้จะยังไม่มีกฎหมายกลางที่มีผลผูกพันในระดับภูมิภาคเช่น GDPR แต่ก็ได้ริเริ่มจัดทำกรอบความร่วมมือ ได้แก่ ASEAN Framework on Personal Data Protection (2016) และ ASEAN Data Management Framework (2021) ที่เป็นเพียงกรอบเชิงนโยบาย ด้วยเหตุนี้ การจัดทำมาตรการคุ้มครองข้อมูลส่วนบุคคลในระดับภูมิภาค จึงควรถูกผลักดันให้เป็นมาตรการเชิงป้องกันภายใต้กลไกความร่วมมือด้านความมั่นคงไซเบอร์ของอาเซียนด้วยเหตุนี้ การจัดทำมาตรการคุ้มครองข้อมูลส่วนบุคคลในระดับภูมิภาค จึงควรถูกผลักดันให้เป็น มาตรการเชิงป้องกัน ภายใต้กลไกความร่วมมือด้านความมั่นคงไซเบอร์ของอาเซียน

6. มาตรการด้านการส่งผู้ร้ายข้ามแดน การส่งผู้ร้ายข้ามแดนเป็นกลไกสำคัญในการบังคับใช้กฎหมายอาญาระหว่างประเทศ โดยเฉพาะในบริบทของอาชญากรรมข้ามชาติรูปแบบใหม่ เช่น แก๊งคอลเซ็นเตอร์ ซึ่งผู้กระทำผิดมักเคลื่อนย้ายข้ามพรมแดนหรืออาศัยประเทศที่ไม่มีความตกลงส่งผู้ร้ายข้ามแดนเพื่อหลบหนีการจับกุม อย่างไรก็ตาม ในบริบทของอาเซียน ปรากฏว่าจนถึงปัจจุบัน ยังไม่มีอนุสัญญาพหุภาคีว่าด้วยการส่งผู้ร้ายข้ามแดนที่ใช้ร่วมกันระหว่างสมาชิกทั้ง 10 ประเทศ ส่งผลให้การดำเนินความร่วมมือในเรื่องนี้ต้องอาศัยความตกลงทวิภาคีเป็นหลัก ซึ่งกระจัดกระจาย ไม่ครอบคลุม และมีลักษณะเฉพาะที่แตกต่างกันในแต่ละคู่ภาคี แม้ว่าความตกลงทวิภาคีจะสามารถตอบสนองต่อบริบทความสัมพันธ์ของรัฐคู่ภาคีได้อย่างยืดหยุ่น แต่ข้อจำกัดสำคัญคือการที่รัฐสมาชิกจำนวนหนึ่งของอาเซียนยังไม่มีความตกลงซึ่งกันและกัน ทำให้เกิดช่องว่างทางกฎหมาย และเปิด

[285] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR).

โอกาสให้ผู้กระทำความผิดสามารถเคลื่อนไหวในภูมิภาคโดยไม่ถูกส่งตัวกลับมาดำเนินคดี[2] ในกรณีของแก๊งคอลเซ็นเตอร์ ช่องว่างดังกล่าวยิ่งส่งผลรุนแรง เนื่องจากเครือข่ายอาชญากรรมประเภทนี้มีลักษณะเคลื่อนที่เร็ว ใช้ประเทศเป็นฐานปฏิบัติการชั่วคราว และอาศัยช่องว่างของระบบกฎหมายเพื่อหลีกเลี่ยงการรับโทษ อีกทั้งในการนี้ หลักการในมาตรา 16 แห่งอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมข้ามชาติ ปี ค.ศ. 2000[286] (United Nations Convention against

---

[286] United Nations Convention against Transnational Organized Crime 2000 (UNTOC)
Article 16 – Extradition

1. This article shall apply to the offences covered by this Convention or the Protocols thereto where the person who is the subject of the request for extradition is located in the territory of the requested State Party, provided that the offence for which extradition is sought is punishable under the domestic law of both the requesting State Party and the requested State Party.

2. If the request for extradition includes several separate offences, at least one of which is extraditable under this article and some of which are not extraditable by reason of their period of imprisonment but are related to the extraditable offence, the requested State Party may apply this article also in respect of those offences.

3. Each of the offences to which this article applies shall be deemed to be included as an extraditable offence in any extradition treaty existing between States Parties. States Parties undertake to include such offences as extraditable offences in every extradition treaty to be concluded between them.

4. If a State Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another State Party with which it has no extradition treaty, it may consider this Convention the legal basis for extradition in respect of any offence to which this article applies.

5. States Parties that make extradition conditional on the existence of a treaty shall:

(a) At the time of deposit of their instrument of ratification, acceptance or approval of or accession to this Convention, inform the Secretary-General of the United Nations whether they will take this Convention as the legal basis for cooperation on extradition with other States Parties to this Convention; and

(b) If they do not take this Convention as the legal basis for cooperation on extradition, seek, where appropriate, to conclude treaties on extradition with other States Parties to this Convention in order to implement this article.

6. States Parties which do not make extradition conditional on the existence of a treaty shall recognize offences to which this article applies as extraditable offences between themselves.

Transnational Organized Crime: UNTOC) ได้เสนอแนวทางสำคัญที่สามารถนำมาปรับใช้ได้ โดยบัญญัติว่า หากรัฐภาคีไม่มีสนธิสัญญาการส่งผู้ร้ายข้ามแดนระหว่างกันให้สามารถใช้อนุสัญญานี้เป็นพื้นฐานทางกฎหมายในการร้องขอและดำเนินกระบวนการส่งผู้ร้ายข้ามแดนได้ หลักการดังกล่าวเปิดโอกาสให้ประเทศสมาชิกอาเซียนสามารถใช้ UNTOC เป็นกลไกเสริมในกรณีที่ยังไม่มีข้อตกลงทวิภาคี และสะท้อนเจตนารมณ์ร่วมของประชาคมระหว่างประเทศในการขจัดข้อจำกัดเชิงโครงสร้างด้านเขตอำนาจศาล แต่ทว่ามาตราดังกล่าวมิได้กำหนดขั้นตอนหรือกระบวนการปฏิบัติไว้โดยละเอียด ทั้งในแง่ของแบบฟอร์มคำร้อง เอกสารประกอบ หรือกรอบเวลาการพิจารณาคำขอ ทำให้การดำเนินการในระดับปฏิบัติอาจแตกต่างกันในแต่ละประเทศและเป็นฐานในการร้องขอส่งผู้ร้ายข้ามแดนยังไม่ก่อให้เกิดพันธะเชิงบังคับที่เข้มงวดต่อรัฐภาคี กล่าวคือ รัฐยังมีดุลพินิจว่าจะให้ความร่วมมือหรือไม่โดยไม่ต้องมีบทลงโทษหากปฏิเสธคำขอ อีกทั้งยังเปิดช่องให้รัฐภาคีสามารถอ้างข้อยกเว้นได้ในหลายกรณี เช่น หากเห็นว่าการส่งผู้ร้ายข้ามแดนกระทบต่อ “อธิปไตย ความมั่นคง หรือผลประโยชน์แห่งชาติ” ซึ่งเป็นข้อยกเว้นที่ตีความได้กว้างและเปิดโอกาสให้รัฐใช้เป็นเหตุผลในการปฏิเสธความร่วมมือ โดยเฉพาะในกรณีที่เกี่ยวข้องกับอาชญากรรมที่มีลักษณะอ่อนไหวหรือแทรกซ้อนกับประเด็นทางการเมืองหรือความมั่นคงภายใน ดังนั้นอาเซียนควรมีมาตรการด้านการส่งผู้ร้ายข้ามแดนและควรบัญญัติให้ชัดเจนถึงหลักเกณฑ์และขั้นตอนการส่งผู้ร้ายข้ามแดน โดยเฉพาะในกรณีที่เกี่ยวข้องกับความผิดฐานอาชญากรรมข้ามชาติที่มีผลกระทบในหลายประเทศ สำหรับกรณีที่ผู้ต้องหายินยอม หรือในกรณีที่หลักฐานชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็ว มีประสิทธิภาพ และลดภาระของหน่วยงานบังคับใช้กฎหมายและฝ่ายตุลาการของแต่ละประเทศ การจัดทำอนุสัญญาในลักษณะนี้จะเป็นก้าวสำคัญของอาเซียนในการพัฒนา “ประชาคมยุติธรรมทางอาญาระหว่างประเทศ” ภายในภูมิภาค และเป็นสัญญาณถึงเจตจำนงร่วมในการต่อสู้กับอาชญากรรมข้ามชาติอย่างเป็นระบบและ

---

7.Extradition shall be subject to the conditions provided for by the domestic law of the requested State Party or by applicable extradition treaties, including, inter alia, conditions in relation to the minimum penalty requirement for extradition and the grounds upon which the requested State Party may refuse extradition.

8. States Parties shall, subject to their domestic law, endeavour to expedite extradition procedures and to simplify evidentiary requirements relating thereto in respect of any offence to which this article applies.

9. Subject to the provisions of its domestic law and its extradition treaties, the requested State Party may, upon being satisfied that the circumstances so warrant and are urgent and at the request of the requesting State Party, take a person whose extradition is sought and who is present in its territory into custody or take other appropriate measures to ensure his or her presence at extradition proceedings.

จริงจัง โดยไม่ปล่อยให้ปัญหาเขตอำนาจศาลหรือความแตกต่างทางระบบกฎหมายเป็นอุปสรรคต่อความยุติธรรม

**5.3.2 มาตรการในระดับประเทศสมาชิกอาเซียนที่เหมาะสมในการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์**

ประเทศสมาชิกอาเซียนในปัจจุบันยังคงเผชิญข้อจำกัดหลายประการในการจัดการกับอาชญากรรมข้ามชาติกรณีของแก๊งคอลเซ็นเตอร์ ซึ่งมีลักษณะการดำเนินการที่ซับซ้อนและใช้ประโยชน์จากช่องว่างทางกฎหมายระหว่างประเทศ อีกทั้งยังอาศัยเทคโนโลยีเป็นเครื่องมือในการอำพรางตัวตน การหลอกลวงข้ามพรมแดน และการเคลื่อนย้ายเงินอย่างรวดเร็ว การแก้ไขปัญหาเหล่านี้ในระดับประเทศจึงต้องอาศัยการพัฒนากฎหมายภายในให้สามารถตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพและทันต่อสถานการณ์ ทั้งนี้ อาเซียนในฐานะองค์กรความร่วมมือระดับภูมิภาคสามารถมีบทบาทเชิงแนะนำแก่ประเทศสมาชิกในการส่งเสริมให้ศึกษารูปแบบมาตรการทางกฎหมายที่มีประสิทธิภาพจากประเทศที่ประสบความสำเร็จในการควบคุมอาชญากรรมไซเบอร์ โดยจากการศึกษาถึงประเทศออสเตรีเลียและประเทศสหาราชอาณาจักร *(โปรดดูในหัวข้อที่ 3.2.3)* พบว่าได้มีแนวทางการดำเนินนโยบายและการตรากฎหมายที่ครอบคลุม ตั้งแต่การควบคุมต้นทางของอาชญากรรมการจัดการบัญชีธนาคารต้องสงสัย ไปจนถึงการคุ้มครองสิทธิผู้เสียหาย ผู้วิจัยเห็นว่าสามารถนำมาปรับใช้เป็นแนวทางในการพัฒนากฎหมายภายในของประเทศสมาชิกได้อย่างเหมาะสม โดยมีมาตรการที่สำคัญ ดังนี้

1. การกำหนดหน้าที่ของผู้ให้บริการโทรคมนาคมและแพลตฟอร์มดิจิทัลให้ต้องให้ความร่วมมือกับเจ้าหน้าที่ของรัฐในกระบวนการสืบสวนและระงับอาชญากรรม โดยออสเตรเลียได้ตรา Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 หรือ TOLA Act[287] ซึ่งให้อำนาจเจ้าหน้าที่ร้องขอข้อมูลทางเทคนิคจากผู้ให้บริการ ไม่ว่าจะเป็นรหัสผ่าน ข้อมูล metadata หรือการเข้าถึงระบบ backdoor ได้โดยชอบด้วยกฎหมาย[1] กฎหมายลักษณะนี้ช่วยให้เจ้าหน้าที่สามารถวิเคราะห์พฤติกรรมของผู้ต้องสงสัยได้อย่างรวดเร็ว และสกัดกั้นการกระทำความผิดได้ตั้งแต่ในระยะเริ่มต้น ประเทศสมาชิกอาเซียนสามารถนำแนวคิดนี้ไปประยุกต์ใช้โดยการบัญญัติหน้าที่ทางกฎหมายแก่ผู้ให้บริการในประเทศ เช่น การปรับปรุงกฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์ หรือกฎหมายโทรคมนาคม ให้มีความชัดเจนในเรื่องภาระหน้าที่ของเอกชนในการให้ข้อมูลต่อรัฐภายใต้หลักการคุ้มครองสิทธิส่วนบุคคล

---

[287] ‘Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)’ (Government of Australia) <https://www.legislation.gov.au/Details/C2018A00148> accessed 30 June 2025.

2. การให้อำนาจหน่วยงานของรัฐในการอายัดบัญชีหรือทรัพย์สินต้องสงสัยโดยไม่จำเป็นต้องรอคำพิพากษาในคดีอาญา ซึ่งเป็นหลักการสำคัญใน *Proceeds of Crime Act 2002*[288] ของสหราชอาณาจักร[2] กฎหมายดังกล่าวเปิดช่องให้รัฐสามารถอายัดบัญชีที่มีเหตุอันควรเชื่อว่าเกี่ยวข้องกับอาชญากรรม แม้ยังไม่มีการพิสูจน์ความผิดในกระบวนการศาล ทั้งยังเปิดทางให้สถาบันการเงินสามารถยื่นรายงานธุรกรรมต้องสงสัย (Suspicious Activity Report: SAR) ได้อย่างรวดเร็ว แนวทางนี้สามารถนำไปปรับใช้ในกฎหมายว่าด้วยการฟอกเงินของประเทศสมาชิกอาเซียน เช่น การเพิ่มเติมบทบัญญัติที่ให้อำนาจแก่หน่วยงานสืบสวน เช่น สำนักงานป้องกันและปราบปรามการฟอกเงิน ให้สามารถออกคำสั่งอายัดชั่วคราวในกรณีเร่งด่วน เพื่อหยุดยั้งความเสียหายที่อาจขยายวงกว้าง

3. การเข้าถึงข้อมูลดิจิทัลของผู้ใช้โดยรัฐภายใต้การควบคุมที่สมดุลตามหลักนิติธรรม ตัวอย่างเช่น *Investigatory Powers Act 2016* ของสหราชอาณาจักร ซึ่งกำหนดให้การเข้าถึงข้อมูลของเจ้าหน้าที่ต้องผ่านกระบวนการอนุมัติจากผู้พิพากษาหรือองค์กรกำกับดูแลอิสระ[289] การควบคุมลักษณะนี้ช่วยลดการใช้อำนาจรัฐโดยพลการและรักษาสิทธิของประชาชน ประเทศสมาชิกอาเซียนควรจัดให้มีกลไกถ่วงดุลในลักษณะเดียวกัน โดยอาจจัดตั้งคณะกรรมการกลางในการอนุญาตเข้าถึงข้อมูล หรือกำหนดให้การออกคำสั่งต้องมีการบันทึกและตรวจสอบจากองค์กรที่เป็นอิสระ

4. มาตรการคุ้มครองผู้เสียหายซึ่งในออสเตรเลียมีการตรา ePayments Code ที่กำหนดให้ธนาคารต้องแจ้งเตือนลูกค้าเมื่อพบธุรกรรมที่มีลักษณะผิดปกติ และต้องคืนเงินให้ผู้เสียหายภายในระยะเวลาที่กำหนด หากสามารถพิสูจน์ได้ว่าไม่ได้มีส่วนรู้เห็นกับการกระทำความผิด มาตรการลักษณะนี้สามารถนำไปพัฒนาต่อในระบบกฎหมายของประเทศสมาชิกอาเซียน โดยการออกแนวปฏิบัติที่มีผลผูกพัน หรือบัญญัติไว้ในกฎหมายว่าด้วยการคุ้มครองผู้บริโภคทางการเงิน เพื่อสร้างมาตรฐานขั้นต่ำให้ธนาคารต้องรับผิดชอบในการช่วยเหลือเหยื่อคดีแก๊งคอลเซ็นเตอร์

จากบทวิเคราะห์ข้างต้นจะเห็นได้ว่าแม้มาตรการเหล่านี้จะเป็นกฎหมายภายในของประเทศต้นทาง แต่อาเซียนสามารถส่งเสริมให้ประเทศสมาชิกนำมาใช้เป็นต้นแบบในการพัฒนากฎหมายของตน โดยพิจารณาปรับให้เหมาะสมกับบริบททางสังคม ระบบกฎหมาย และโครงสร้างอำนาจรัฐของแต่ละประเทศ อันจะช่วยยกระดับประสิทธิภาพของกฎหมายภายในประเทศสมาชิกให้สามารถรับมือกับลักษณะอาชญากรรมข้ามชาติที่เปลี่ยนแปลงอย่างรวดเร็วในยุคดิจิทัลได้อย่างมีประสิทธิภาพและสอดคล้องกับมาตรฐานสากล

---

[288] 'Proceeds of Crime Act 2002 (UK), Part 5 – Civil recovery' (UK Government) <https://www.legislation.gov.uk/ukpga/2002/29/contents> accessed 30 June 2025.

[289] 'Proceeds of Crime Act 2002 (UK), Part 5 – Civil recovery' (UK Government) <https://www.legislation.gov.uk/ukpga/2002/29/contents> accessed 30 June 2025.

ดังนั้น การรับมือกับปัญหาแก๊งคอลเซ็นเตอร์ซึ่งเป็นรูปแบบหนึ่งของอาชญากรรมข้ามชาติที่ส่งผลกระทบอย่างรุนแรงต่อประชาชนในภูมิภาคอาเซียน การปรับปรุงกฎหมายและการบังคับใช้กฎหมายให้เท่าทันกับลักษณะอาชญากรรมที่เปลี่ยนแปลงอย่างรวดเร็วเป็นสิ่งจำเป็นอย่างยิ่ง สมัชชารัฐสภาอาเซียนในฐานะกลไกด้านนิติบัญญัติของภูมิภาค ควรมีบทบาทเชิงรุกในการผลักดันให้เกิดการพัฒนาและกลไกการประสานความร่วมมือทางกฎหมายในการต่อต้านอาชญากรรมข้ามชาติ โดยเฉพาะในประเด็นการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์ ผ่านกระบวนการออกแบบกฎหมายที่หลากหลายรูปแบบเพื่อกำหนดกรอบแนวทางร่วมกันในการรับมือกับภัยคุกคามรูปแบบนี้ นอกจากนี้ ควรส่งเสริมการแลกเปลี่ยนองค์ความรู้และแนวปฏิบัติที่ดีระหว่างรัฐสภาของแต่ละประเทศสมาชิก รวมทั้งสนับสนุนการพัฒนาระบบทางการเงินและการค้าด้วยนวัตกรรมที่ปลอดภัย เพื่อเสริมสร้างโครงสร้างธุรกรรมที่มีความน่าเชื่อถือและสามารถป้องกันการถูกแทรกแซงจากขบวนการหลอกลวงที่แฝงตัวอยู่ในระบบเศรษฐกิจดิจิทัลของภูมิภาคได้อย่างมีประสิทธิภาพ

**ตารางที่ 5.1** แนวทางและมาตรการของอาเซียนในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์

| การป้องกันและปราบปรามอาชญากรรมข้ามชาติ โดยเฉพาะกรณีแก๊งคอลเซ็นเตอร์ | | |
|---|---|---|
| แนวทางในการป้องกันและปราบปราม | แนวทางที่ 1 การบูรณาการแผนยุทธศาสตร์ความร่วมมือด้านความมั่นคงทางอาชญากรรมไซเบอร์ | อาเซียนควรยกระดับแผนยุทธศาสตร์จากเอกสารนโยบายทั่วไปไปสู่รูปแบบที่มีผลผูกพันมากขึ้น เช่น ปฏิญญาร่วมรัฐมนตรี หรือ MoU ที่มีกรอบโครงสร้าง ภารกิจ และแผนปฏิบัติการที่ชัดเจน ควรดำเนินการผ่าน APSC Council และ ASEAN Secretariat พร้อมวางระบบติดตามผล และประสานข้อมูลแบบ Multi-layered ระหว่างระดับภูมิภาคและระดับชาติ เพื่อยกระดับแผนสู่กลไกปฏิบัติการร่วมที่มีประสิทธิภาพและยั่งยืน |
| | แนวทางที่ 2 การพัฒนากลไกการแบ่งปันข้อมูลข่าวกรอง | ควรปรับให้เน้นถึงการพัฒนาแพลตฟอร์มกลางสำหรับแบ่งปันข้อมูลทางไซเบอร์ โดยแพลตฟอร์มนี้ควรมีระบบรักษาความปลอดภัยที่แข็งแกร่ง เพื่อให้ประเทศสมาชิกมั่นใจในการแลกเปลี่ยนข้อมูล การแลกเปลี่ยนข้อมูลแบบเรียลไทม์ระหว่างหน่วยงานของประเทศสมาชิกถือเป็นปัจจัยพื้นฐานในการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์อย่างมีประสิทธิภาพ โดยเฉพาะในกรณีที่อาชญากรมีการเคลื่อนไหวอย่างรวดเร็วและซับซ้อน การแบ่งปันข้อมูลข่าวกรอง ไม่ว่าจะเป็นตำแหน่งที่ตั้งของแก๊งคอลเซ็นเตอร์ รายละเอียดของการทำธุรกรรมที่ต้องสงสัย และวิธีการที่แก๊งเหล่านี้เป็นตัวช่วยสำคัญในการติดตามและยับยั้งกิจกรรมผิดกฎหมายได้ทันท่วงที อีกทั้งการจัดตั้งระบบแลกเปลี่ยนข้อมูลกลางที่ปลอดภัยและเชื่อถือได้ |

**ตารางที่ 5.1** (ต่อ)

| การป้องกันและปราบปรามอาชญากรรมข้ามชาติ โดยเฉพาะกรณีแก๊งคอลเซ็นเตอร์ | | |
|---|---|---|
| | แนวทางที่ 3 การพัฒนากลไกความร่วมมือระหว่างประเทศในระดับปฏิบัติการ | อาเซียนจึงควรมีการพัฒนากลไกระดับภูมิภาคที่เน้นการประสานงานข้ามพรมแดน รวมถึงการสนับสนุนให้ ASEANAPOL (องค์กรตำรวจอาเซียน) มีบทบาทสำคัญในการรวบรวมและแชร์ข้อมูลข่าวกรอง จะช่วยลดอุปสรรคทางกฎหมายที่อาจเกิดขึ้นระหว่างประเทศ |
| | แนวทางที่ 4 การสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยจากแก๊งคอลเซ็นเตอร์ | การส่งเสริม แนวทางรู้เท่าทันอาชญากรรมในระดับชุมชนโดยให้ชุมชนช่วยกันเฝ้าระวังและรายงานข้อมูลที่น่าสงสัยไปยังหน่วยงานที่เกี่ยวข้อง การสร้างแรงกดดันทางสังคม โดยให้ความรู้กับประชาชนว่าการทำงานให้กับแก๊งคอลเซ็นเตอร์เป็นความผิดร้ายแรง เพื่อป้องกันไม่ให้บุคคลตกเป็นเครื่องมือขององค์กรอาชญากรรม |
| มาตรการในการป้องกันและปราบปราม | มาตรการที่ 1 การกำหนดคำนิยามของคำว่าแก๊งคอลเซ็นเตอร์ | อาเซียนควรกำหนดนิยามแก๊งคอลเซ็นเตอร์ให้ชัดเจน โดยเน้นลักษณะการกระทำที่เป็นระบบ ใช้เทคโนโลยีหลอกลวงหรือข่มขู่ข้ามพรมแดน มีเป้าหมายแสวงหาผลประโยชน์โดยมิชอบ และควรครอบคลุมทั้งผู้เสียหายและผู้ที่ถูกหลอกให้มีส่วนร่วมในอาชญากรรม เพื่อเป็นพื้นฐานสำหรับความร่วมมือระดับภูมิภาคในการปราบปรามและคุ้มครองเหยื่อ |

**ตารางที่ 5.1** (ต่อ)

| การป้องกันและปราบปรามอาชญากรรมข้ามชาติ โดยเฉพาะกรณีแก๊งคอลเซ็นเตอร์ | |
|---|---|
| มาตรการที่ 3 มาตรการด้านพยานหลักฐานในกระบวนการสอบสวนและดำเนินคดีอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ | อาเซียนควรกำหนดมาตรการร่วมด้านพยานหลักฐานในคดีอาชญากรรมข้ามชาติโดยเฉพาะพยานหลักฐานดิจิทัล ให้สามารถใช้ร่วมกันได้โดยไม่ต้องรับรองซ้ำผ่านกระบวนการทางการทูต เพื่อเพิ่มประสิทธิภาพในการสืบสวนและดำเนินคดีแก๊งคอลเซ็นเตอร์อย่างทันท่วงที ตามแนวทางของสหภาพยุโรปและหลักการของ UNTOC |
| มาตรการที่ 4 มาตรการด้านการคุ้มครองพยานและผู้เสียหาย | อาเซียนควรจัดให้มีมาตรการคุ้มครองพยานและผู้เสียหายจากอาชญากรรมข้ามชาติในระดับภูมิภาค โดยยึดหลักสิทธิมนุษยชนครอบคลุมทั้งการคุ้มครองทางกายภาพ การปกป้องข้อมูลส่วนบุคคลและสิทธิในการมีส่วนร่วมในกระบวนการยุติธรรม |
| มาตรการที่ 5 มาตรการคุ้มครองข้อมูลส่วนบุคคลเพื่อป้องกันอาชญากรรมข้ามชาติในอาเซียน | ควรพัฒนามาตรการคุ้มครองข้อมูลส่วนบุคคลในระดับภูมิภาคโดยอ้างอิงแนวทาง GDPR ของสหภาพยุโรปที่เน้นความรับผิดชอบของภาครัฐและเอกชนในการจัดการข้อมูลส่วนบุคคลอย่างเข้มงวด |
| มาตรการที่ 6 มาตรการด้านการส่งผู้ร้ายข้ามแดน | อาเซียนควรเร่งจัดทำอนุสัญญาระดับภูมิภาคว่าด้วยการส่งผู้ร้ายข้ามแดน เพื่อให้เกิดกลไกความร่วมมือทางอาญาที่มีผลผูกพันทางกฎหมาย รองรับการติดตาม ควบคุม และส่งตัวผู้กระทำความผิดในคดีอาชญากรรมข้ามชาติ และสอดคล้องกับบริบทของอาชญากรรมไร้พรมแดน |

**ที่มา** สรุปโดยผู้วิจัย

# บทที่ 6

# บทสรุปและข้อเสนอแนะ

## 6.1 ข้อสรุป

การศึกษาเรื่องมาตรการทางกฎหมายของอาเซียนในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ ผู้วิจัยมีวัตถุประสงค์ เพื่อศึกษาถึงสภาพปัญหาของแก๊งคอลเซ็นเตอร์ภายในภูมิภาคอาเซียนและมาตรการทางกฎหมายของอาเซียนและกลุ่มประเทศสมาชิกอาเซียนในการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์โดยศึกษาเปรียบเทียบกับมาตรการระหว่างประเทศที่เกี่ยวข้องในการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์

อาชญากรรมข้ามชาติในรูปแบบของแก๊งคอลเซ็นเตอร์ถือเป็นวิวัฒนาการของพฤติกรรมอาชญากรรมในศตวรรษที่ 21 อาชญากรรมประเภทนี้มิได้เกิดขึ้นโดยฉับพลันหากแต่เป็นผลสะสมจากปัจจัยหลายประการที่เกิดขึ้นท่ามกลางการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศ ระบบเศรษฐกิจโลก และโครงสร้างความมั่นคงของชาติ การกระทำความผิดของแก๊งคอลเซ็นเตอร์มีลักษณะเฉพาะที่แตกต่างจากอาชญากรรมไซเบอร์ทั่วไป กล่าวคือ มิได้เป็นการกระทำของบุคคลหรือกลุ่มย่อยแบบเฉพาะกิจ หากแต่เป็นการกระทำโดยเครือข่ายที่มีลักษณะขององค์กรอาชญากรรมข้ามชาติ ซึ่งมีการวางโครงสร้าง ควบคุมและกระจายการกระทำความผิดในระดับภูมิภาคอย่างมีแบบแผน โดยแก๊งคอลเซ็นเตอร์เป็นการละเมิดสิทธิมนุษยชนที่ร้ายแรงและเป็นปัญหาที่บั่นทอนความมั่นคงของมนุษย์ที่มีความเชื่อมโยงกับปัญหาระดับโลกอื่น ๆ ซึ่งเทคโนโลยีสารสนเทศและการติดต่อสื่อสารที่ก้าวหน้าอย่างรวดเร็วได้เปิดโอกาสให้อาชญากรสามารถขยายขอบเขตการกระทำผิดของตนได้โดยไม่ถูกจำกัดด้วยพรมแดนทางภูมิศาสตร์ ภูมิภาคเอเชียตะวันออกเฉียงใต้ ซึ่งเป็นศูนย์กลางเศรษฐกิจที่มีอัตราการเติบโตสูงและเป็นจุดเชื่อมโยงสำคัญของระบบการค้าระหว่างประเทศได้กลายเป็นพื้นที่ที่เครือข่ายอาชญากรรมข้ามชาติแฝงตัวเข้ามาดำเนินกิจกรรมผิดกฎหมายเพิ่มขึ้นอย่างต่อเนื่อง ซึ่งปัญหาที่เกิดขึ้นส่งผลกระทบอย่างกว้างขวางทั้งในระดับภูมิภาคและระหว่างประเทศจำเป็นอย่างยิ่งที่ทุกประเทศต้องช่วยกันแก้ไขปัญหาสถานการณ์ ซึ่งจากการศึกษาถึงแนวคิดและทฤษฎีที่เกี่ยวข้องพบว่าการปราบปรามแก๊งคอลเซ็นเตอร์ในระดับภูมิภาคและระหว่างประเทศไม่สามารถพึ่งพากลไกของชาติแต่เพียงลำพัง จำเป็นต้องอาศัยกรอบความร่วมมือระหว่างประเทศ *(International Co-operation)* ที่ตั้งอยู่บนแนวคิดของสำนักเสรีนิยมสมัยใหม่ (Neo-Liberalism) ที่ยอมรับว่าการอยู่ร่วมกันอย่างสงบสุขของรัฐต่าง ๆ ต้องอาศัยการประสานผลประโยชน์ ความเชื่อมั่นระหว่างกันและกลไกความร่วมมือ

ทั้งในระดับรัฐบาลและระดับปฏิบัติการ นอกจากนี้ แนวคิดว่าด้วยการให้ความช่วยเหลือซึ่งกันและกันทางอาญา (International Mutual Assistance in Criminal Matters) ยังได้เสนอกรอบการให้ความร่วมมือที่ครอบคลุมทั้งในระดับไม่เป็นทางการ กึ่งทางการ และอย่างเป็นทางการ โดยเฉพาะอย่างยิ่งในรูปแบบของการแลกเปลี่ยนข้อมูล การสืบสวนร่วม และการดำเนินการขอส่งผู้ร้ายข้ามแดนซึ่งเป็นกระบวนการสำคัญในการจัดการกับเครือข่ายอาชญากรรมที่ดำเนินกิจการแบบไร้พรมแดน ในขณะเดียวกัน แนวคิดเครือข่ายเชิงนโยบายด้านกระบวนการยุติธรรมทางอาญา (Criminal Justice Policy Network) ได้เน้นย้ำถึงความสำคัญของการสร้างระบบเครือข่ายที่ผนึกกำลังระหว่างหน่วยงานตำรวจ อัยการ ศาล และหน่วยงานที่เกี่ยวข้องในหลายประเทศ ซึ่งจะช่วยให้การดำเนินคดีมีความสอดคล้องมีข้อมูลร่วมที่ทันสมัยและสามารถตอบสนองต่อภัยคุกคามในลักษณะที่ซับซ้อนและเปลี่ยนแปลงได้อย่างรวดเร็ว แม้แนวคิดดังกล่าวจะชี้ให้เห็นความสำคัญของความร่วมมือในการจัดการอาชญากรรมข้ามชาติประเภทแก๊งคอลเซ็นเตอร์แต่อุปสรรคเชิงโครงสร้างและข้อจำกัดด้านกลไกความร่วมมือยังคงเป็นปัจจัยที่ขัดขวางการบังคับใช้มาตรการอย่างมีประสิทธิภาพในอภูมิภาคอาเซียน ดังนั้นการวิเคราะห์สภาพปัญหาและการประเมินกลไกความร่วมมือระหว่างประเทศจึงเป็นสิ่งจำเป็นเพื่อเสนอแนวทางการพัฒนากฎหมายและการบูรณาการความร่วมมือที่ตอบสนองต่อภัยคุกคามรูปแบบใหม่นี้อย่างเหมาะสมและยั่งยืน โดยผู้เขียนได้นำเสนอรายละเอียดดังต่อไปนี้

**6.1.1 สภาพปัญหาในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์**

อาเซียนเป็นภูมิภาคที่มีความแตกต่างทั้งทางด้านเชื้อชาติ วัฒนธรรม ศาสนา และภาษา โดยในภูมิภาคเอเชียตะวันออกเฉียงใต้รวมทั้งประเทศไทยล้วนตะหนักว่า อาชญากรรมข้ามชาติในรูปแบบแก๊งคอลเซ็นเตอร์ถือเป็นภัยคุกคามยุคใหม่ที่มีความซับซ้อนและเชื่อมโยงกับอาชญากรรมรูปแบบอื่น ได้แก่ การค้ามนุษย์ การฟอกเงิน และอาชญากรรมไซเบอร์ ทำให้ส่งผลกระทบต่อประชาชน เศรษฐกิจและยังส่งผลอย่างกว้างขวางทางด้านสังคม วัฒนธรรม ความมั่นคง ทั้งในระดับภูมิภาคและระหว่างประเทศ จากการศึกษาพบสภาพปัญหาที่สำคัญ คือ ข้อจำกัดในการบังคับใช้กฎหมายในประเทศที่มีพื้นที่ชายแดนที่ควบคุมได้ยาก หรือมีความไม่มั่นคงทางการเมือง อาทิ พื้นที่ชายแดนไทย-เมียนมาร์ ลาว หรือบางส่วนของกัมพูชา ซึ่งมักถูกใช้เป็นฐานปฏิบัติการของแก๊งคอลเซ็นเตอร์ที่จับเหยื่อมาจากหลายประเทศในภูมิภาคและกระทำการหลอกลวงผ่านอินเทอร์เน็ตโดยยากต่อการตรวจจับ ในบางกรณียังมีข้อสงสัยว่ามีเจ้าหน้าที่รัฐในบางประเทศมีส่วนเกี่ยวข้องหรือเพิกเฉยต่อพฤติกรรมเหล่านี้ อีกทั้งปัญหาในการแลกเปลี่ยนข้อมูลข่าวกรองและการประสานงานระหว่างประเทศที่ยังไม่เป็นระบบและมีประสิทธิภาพต่ำ โดยขาดศูนย์กลางการที่เชื่อมต่อกันได้แบบเรียลไทม์ ส่งผลให้การติดตามเส้นทางการเงิน การระบุผู้กระทำผิด และการจับกุมตัวผู้ต้องหาเป็นไปอย่างล่าช้าไม่ทันต่อการเคลื่อนย้ายของเครือข่ายอาชญากร สุดท้ายนี้เป็นปัญหาในเรื่องของข้อจำกัดด้าน

ทรัพยากร ทั้งบุคลากร งบประมาณและเทคโนโลยี โดยเฉพาะในประเทศที่ยังมีระดับการพัฒนาทางเศรษฐกิจต่ำ เจ้าหน้าที่บังคับใช้กฎหมายจำนวนมากยังขาดความรู้ด้านอาชญากรรมไซเบอร์และไม่มีเครื่องมือทางเทคโนโลยีที่ทันสมัยเพียงพอในการตรวจสอบ ติดตาม และวิเคราะห์ข้อมูลดิจิทัลที่ใช้ในการกระทำความผิด ซึ่งทำให้ปัญหาแก๊งคอลเซ็นเตอร์ไม่ได้รับการจัดการอย่างตรงจุด

**6.1.2 ความร่วมมือในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ของภูมิภาคอาเซียน**

ในด้านของแนวทางในการป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์ในกลุ่มประเทศสมาชิกอาเซียน ปัจจุบันได้มีการดำเนินการในหลายด้านเพื่อต่อต้านอาชญากรเหล่านี้ โดยจากการศึกษาพบว่า อาเซียนได้พยายามพัฒนากรอบความร่วมมือด้านการปราบปรามอาชญากรรมข้ามชาติผ่านข้อตกลงและแผนปฏิบัติการต่าง ๆ ปฏิญญาอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Declaration on Transnational Crime) และกลไกความร่วมมือภายใต้กรอบ ASEAN Ministerial Meeting on Transnational Crime (AMMTC) ซึ่งมีเป้าหมายในการประสานความร่วมมือระหว่างประเทศสมาชิกในด้านการแลกเปลี่ยนข้อมูล การพัฒนากฎหมายร่วมกัน และการเสริมสร้างขีดความสามารถของหน่วยงานบังคับใช้กฎหมาย นอกจากนี้อาเซียนยังมี ASEANAPOL (ASEAN Chiefs of National Police) ซึ่งเป็นเครือข่ายความร่วมมือของหน่วยงานตำรวจระดับภูมิภาคที่ช่วยในการแบ่งปันข้อมูลด้านอาชญากรรม รูปแบบการกระทำความผิด และเทคนิคการสืบสวน โดยเฉพาะในกรณีที่เครือข่ายอาชญากรมีการเคลื่อนย้ายจากประเทศหนึ่งไปยังอีกประเทศหนึ่งผ่านช่องออนไลน์หรือผ่านด่านชายแดนที่ไม่มีระบบควบคุมที่เข้มงวด ซึ่งจะพบว่าความร่วมมือเหล่านี้ยังไม่มีความครอบคลุมทั้ง 10 ประเทศ แม้ในกฎบัตรอาเซียนเองก็ได้ตระหนักถึงปัญหาสำคัญที่เกี่ยวกับคุมครองสิทธิมนุษยชนที่สำคัญ ด้วยเหตุนี้ อาเซียนในฐานะองค์กรความร่วมมือระดับภูมิภาคจึงต้องเร่งดำเนินมาตรการที่มีประสิทธิภาพเพื่อป้องกันและปราบปรามแก๊งคอลเซ็นเตอร์ผ่านกลไกความร่วมมือทั้งในระดับภูมิภาคและระดับนานาชาติ การจัดการกับปัญหานี้ไม่เพียงแต่เป็นความจำเป็นเพื่อรักษาความมั่นคงของประเทศสมาชิกเท่านั้น แต่ยังมีความสำคัญต่อเสถียรภาพทางเศรษฐกิจและความเชื่อมั่นของประชาชนในระบบการเงินและกระบวนการยุติธรรมของภูมิภาค

จากการศึกษากฎหมายระหว่างประเทศที่สำคัญเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมข้ามชาติ พบว่า ในกรณีของสหภาพยุโรป (EU) ได้มีการพัฒนากรอบกฎหมายและกลไกที่เข้มแข็งในการรับมือกับอาชญากรรมที่มีลักษณะซับซ้อน เช่น การหลอกลวงผ่านเทคโนโลยีและอาชญากรรมไซเบอร์ โดยเฉพาะใน Directive 2013/40/EU ว่าด้วยการโจมตีต่อระบบสารสนเทศ และ European Investigation Order (EIO) ภายใต้ Directive 2014/41/EU ซึ่งช่วยให้ประเทศสมาชิกสามารถร่วมมือในการสืบสวนสอบสวนและส่งต่อพยานหลักฐานได้อย่างรวดเร็วและมีประสิทธิภาพ สหภาพยุโรปยังได้จัดตั้งหน่วยงานกลาง ได้แก่ Europol และ European Cybercrime

Centre (EC3) เพื่อรับผิดชอบด้านการสืบสวนอาชญากรรมไซเบอร์โดยตรง ส่งผลให้สามารถติดตามกลุ่มอาชญากรที่มีโครงข่ายข้ามพรมแดนได้อย่างมีระบบและต่อเนื่อง ในทางตรงกันข้ามทำให้เห็นว่าภูมิภาคอาเซียนยังขาดกรอบอนุสัญญาระดับภูมิภาคที่มีผลบังคับใช้เฉพาะเจาะจงเกี่ยวกับอาชญากรรมข้ามชาติในลักษณะของแก๊งคอลเซ็นเตอร์ ซึ่งมีพฤติกรรมการหลอกลวงผ่านโทรคมนาคมและระบบออนไลน์อย่างเป็นระบบและเคลื่อนไหวข้ามเขตแดน การขาดกลไกทางกฎหมายที่มีมาตรฐานเดียวกันระหว่างประเทศสมาชิก ทำให้การติดตามและดำเนินคดีกับกลุ่มอาชญากรดังกล่าวเป็นไปอย่างล่าช้าและไม่สอดคล้องกันในทางปฏิบัติ

ดังนั้น เมื่ออาเซียนก้าวเข้าสู่การเป็นประชาคมอย่างสมบูรณ์ ภูมิภาคอาเซียนสมควรอย่างยิ่งที่จะมีกฎหมายกลางในรูปแบบอนุสัญญาการในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ ซึ่งเปรียบเสมือนเป็นธรรมนูญกฎหมายแม่บทที่ใช้ระดับมาตรฐานทางกฎหมายเกี่ยวกับเรื่องแก๊งคอลเซ็นเตอร์ในระดับเดียวกันทั้ง 10 ประเทศในภูมิภาคเพื่อกำหนดกรอบความร่วมมืออย่างเป็นทางการในการป้องกัน ปราบปราม และดำเนินคดีกับแก๊งคอลเซ็นเตอร์ที่กระทำผิดในลักษณะข้ามชาติและสร้างมาตรฐานร่วมในทางกฎหมายที่อาเซียนสามารถใช้ได้โดยไม่ขัดต่อหลักอธิปไตยของแต่ละประเทศ รวมถึงการให้สัตยาบัน หรือภาคยานุวัติเพื่อให้อนุสัญญานั้นมีผลบังคับใช้ได้จริงโดยผ่านความเห็นชอบจากรัฐสภาทั้งนี้เพื่อให้ทันต่อสภาวการณ์ที่ในปัจจุบันทวีความรุนแรงมากขึ้นในภูมิภาคอาเซียน อีกทั้ง ในภูมิภาคอาเซียนที่ประกอบด้วยสิบประเทศสมาชิก มีความจำเป็นอย่างยิ่งที่จะต้องจัดทำอนุสัญญาพหุภาคีว่าด้วยการส่งผู้ร้ายข้ามแดนที่ใช้ร่วมกันในระดับภูมิภาค เพื่อสร้างหลักประกันด้านกฎหมายในการให้ความร่วมมือทางอาญาระหว่างรัฐสมาชิกอย่างเป็นระบบและต่อเนื่อง การที่ประเทศสมาชิกลงนามและให้สัตยาบันในอนุสัญญาดังกล่าวจะช่วยลดข้อจำกัดของการใช้ความตกลงทวิภาคีแบบกระจัดกระจายซึ่งเป็นอยู่ในปัจจุบัน และส่งเสริมให้การติดตาม ควบคุม และส่งตัวผู้ต้องหาในคดีอาชญากรรมข้ามชาติเป็นไปอย่างรวดเร็ว มีประสิทธิภาพ และไม่ติดขัดด้วยข้อจำกัดทางเขตอำนาจศาลหรือกระบวนการทางการทูต นอกจากนี้ อาเซียนยังควรจัดตั้งองค์กรตรวจสอบในระดับภูมิภาคที่มีลักษณะเป็นองค์กรกลาง ซึ่งมีสถานะเป็นกลางไม่อยู่ภายใต้อิทธิพลของประเทศใดประเทศหนึ่ง เพื่อทำหน้าที่เป็นหน่วยงานกลางในการตรวจสอบ ติดตาม และประสานงานด้านการส่งผู้ร้ายข้ามแดน รวมถึงความร่วมมือทางกฎหมายในคดีอาชญากรรมข้ามชาติ

## 6.2 ข้อเสนอแนะ

การศึกษาครั้งนี้มีวัตถุประสงค์เพื่อวิเคราะห์มาตรการของอาเซียนในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ โดยเน้นกรณีแก๊งคอลเซ็นเตอร์ซึ่งเป็นหนึ่งในรูปแบบของอาชญากรรมไซเบอร์ที่กำลังเป็นภัยคุกคามต่อความมั่นคงทางเศรษฐกิจและสังคมในภูมิภาคอาเซียน

อย่างรุนแรง ซึ่งจากการศึกษาพบว่า แม้ว่าอาเซียนจะมีความพยายามในการดำเนินมาตรการต่าง ๆ เพื่อรับมือกับอาชญากรรมข้ามชาติ โดยมีความร่วมมือในรูปแบบต่าง ๆ รวมถึงการส่งเสริมการประสานงานผ่านศูนย์อาชญากรรมไซเบอร์อาเซียน แต่ยังคงประสบปัญหาในหลายด้าน ไม่ว่าจะเป็นความไม่เท่าเทียมกันของกฎหมายในแต่ละประเทศ ช่องว่างของระบบกฎหมายที่เอื้อให้ประเทศหนึ่งกลายเป็นฐานปฏิบัติการของแก๊งคอลเซ็นเตอร์ ความล่าช้าในการแลกเปลี่ยนข้อมูลระหว่างประเทศสมาชิกและการขาดกลไกในการพิจารณาคดีอาญาข้ามพรมแดนที่มีประสิทธิภาพ โดยผู้เขียนมีเสนอแนะดังนี้

**6.2.1 ข้อเสนอแนะด้านแนวนโยบาย**

1. อาเซียนควรยกระดับแผนยุทธศาสตร์ความร่วมมือด้านความมั่นคงทางอาชญากรรมไซเบอร์จากเอกสารเชิงนโยบายไปสู่กลไกปฏิบัติการร่วมอย่างเป็นรูปธรรม โดยจัดทำปฏิญญารัฐมนตรี หรือ MoU ระหว่างประเทศสมาชิก เพื่อกำหนดกรอบความร่วมมือที่ชัดเจน ทั้งในระดับโครงสร้าง ภารกิจ และระยะเวลา พร้อมให้คณะมนตรี APSC และ ASEAN Secretariat รับผิดชอบในการประสาน ติดตาม และขับเคลื่อนผ่านแผนระดับภูมิภาคเชื่อมโยงกับแผนระดับชาติ โดยใช้แนวทางการประสานงานแบบหลายชั้น (multi-layered coordination) เพื่อให้สามารถตอบสนองต่อภัยไซเบอร์ข้ามชาติอย่างมีประสิทธิภาพ

2. พัฒนาแผนปฏิบัติการอาเซียนว่าด้วยการปราบปรามอาชญากรรมข้ามชาติ (ASEAN Plan of Action in Combating Transnational Crime) ให้ครอบคลุมประเด็นของแก๊งคอลเซ็นเตอร์โดยตรงและกำหนดเป้าหมายเฉพาะด้าน เช่น การแลกเปลี่ยนข่าวกรองไซเบอร์ การพัฒนาศักยภาพเจ้าหน้าที่ และการสร้างระบบข้อมูลกลางในระดับภูมิภาค

3. เสริมสร้างความร่วมมือด้านการแลกเปลี่ยนข้อมูลข่าวกรอง เพื่อยกระดับความร่วมมือในส่วนนี้ รวมถึงสนับสนุนหน่วยงานในประเทศสมาชิกในการเชื่อมโยงข้อมูลเชิงลึก นอกจากนี้ ควรมีกลไกสนับสนุนด้านกฎหมายและความไว้วางใจระหว่างรัฐ โดยอาเซียนอาจจัดทำข้อตกลงร่วมว่าด้วยการคุ้มครองและใช้ประโยชน์จากข่าวกรองอาชญากรรมไซเบอร์เพื่อกำหนดขอบเขตการใช้ การเปิดเผย และการรักษาความลับของข้อมูลข่าวกรองที่ได้รับจากประเทศสมาชิกอื่น ๆ อันจะช่วยลดความกังวลของบางประเทศที่ไม่พร้อมเปิดเผยข้อมูลอ่อนไหว และช่วยสร้างความมั่นใจในการร่วมมือระยะยาว

4. การเผยแพร่ความรู้และสร้างภูมิคุ้มกันแก่ประชาชนในภูมิภาคหนึ่งในแนวทางสำคัญในการป้องกันและลดผลกระทบจากอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ คือการยกระดับความรู้ ความเข้าใจและภูมิคุ้มกันทางดิจิทัลของประชาชนในภูมิภาคอาเซียน โดยเฉพาะในยุคที่เทคโนโลยีสารสนเทศได้กลายเป็นส่วนหนึ่งของชีวิตประจำวัน การหลอกลวงผ่านโทรศัพท์ การส่งลิงก์ปลอม การอ้างตนเป็นเจ้าหน้าที่รัฐ หรือการใช้แพลตฟอร์มโซเชียลมีเดียในการลวงเหยื่อ ล้วนเป็น

เทคนิคที่อาชญากรไซเบอร์ปรับเปลี่ยนได้อย่างรวดเร็วและซับซ้อนมากขึ้นเรื่อย ๆ เพื่อลดช่องว่างนี้ อาเซียนควรกำหนดให้การเผยแพร่ความรู้และสร้าง “ภูมิคุ้มกันทางไซเบอร์” เป็นหนึ่งในเป้าหมายหลักของแผนความร่วมมือด้านความมั่นคงทางไซเบอร์ ในอีกด้านหนึ่งภาคเอกชน เช่น ธนาคาร บริษัทเทคโนโลยี ผู้ให้บริการโทรศัพท์และหน่วยงานโลจิสติกส์ควรมีบทบาทร่วมในฐานะ “แนวหน้า” ในการตรวจจับพฤติกรรมต้องสงสัยพร้อมให้ข้อมูลแก่ผู้บริโภคโดยการจัดทำแคมเปญระดับภูมิภาค เพื่อเผยแพร่ความรู้เกี่ยวกับภัยคุกคามจากแก๊งคอลเซ็นเตอร์ และวิธีการป้องกันตนเอง

**6.2.2 ข้อเสนอแนะด้านมาตรการทางกฎหมาย**

1. อาเซียนควรกำหนดมาตรการในการติดตาม อายัด และริบทรัพย์สินที่เกี่ยวข้องกับอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ พร้อมทั้งจัดตั้งกลไกความร่วมมือด้านการแลกเปลี่ยนข้อมูลทางการเงินและคำสั่งอายัดข้ามพรมแดน ทั้งนี้ควรกำหนดบทบัญญัติคุ้มครองสิทธิของผู้ถือทรัพย์สินโดยสุจริตอย่างรัดกุม เพื่อป้องกันการละเมิดสิทธิขั้นพื้นฐานโดยไม่ตั้งใจ

2. อาเซียนควรกำหนดกรอบความร่วมมือด้านพยานหลักฐานระดับภูมิภาคที่มีผลผูกพันทางกฎหมาย โดยเฉพาะในส่วนของพยานหลักฐานทางดิจิทัล เพื่อให้สามารถนำมาใช้ในกระบวนการยุติธรรมของแต่ละประเทศได้โดยไม่ต้องผ่านการรับรองซ้ำซ้อน พร้อมจัดตั้งกลไกกลางในการรวบรวม วิเคราะห์ และแลกเปลี่ยนพยานหลักฐานระหว่างประเทศสมาชิก

3. อาเซียนควรจัดให้มีมาตรการด้านการคุ้มครองพยานและผู้เสียหายในระดับภูมิภาคอย่างจริงจัง โดยยกระดับความร่วมมือระหว่างประเทศสมาชิกเพื่อให้เกิดระบบการคุ้มครองที่มีประสิทธิภาพ ครอบคลุมทั้งมาตรการด้านกายภาพ การดูแลความปลอดภัยส่วนบุคคล และการรักษาข้อมูลส่วนบุคคลของพยานและผู้เสียหายซึ่งผู้เสียหายมักต้องเผชิญกับความกลัวในการถูกข่มขู่หรือคุกคาม ควรส่งเสริมให้มีระบบแจ้งเตือน ความช่วยเหลือด้านจิตสังคม และสิทธิในการติดตามความคืบหน้าของคดี นอกจากนี้ ประเทศสมาชิกควรมีแนวทางร่วมกันในการรับรองความปลอดภัยและความมั่นใจของพยาน เพื่อสร้างแรงจูงใจในการให้ความร่วมมือกับกระบวนการยุติธรรมระหว่างประเทศได้อย่างมีประสิทธิภาพ

4. อาเซียนควรพัฒนามาตรการคุ้มครองข้อมูลส่วนบุคคลในระดับภูมิภาค โดยอ้างอิงแนวทาง GDPR ของสหภาพยุโรปที่กำหนดความรับผิดชอบและมาตรฐานการจัดการข้อมูลอย่างเข้มงวด พร้อมระบบแจ้งเหตุและการประเมินความเสี่ยงล่วงหน้า ซึ่งจะช่วยป้องกันข้อมูลรั่วไหลและลดความเสี่ยงการถูกนำไปใช้ในการกระทำผิด อาเซียนควรผลักดัน ASEAN Framework on Personal Data Protection และ ASEAN Data Management Framework ให้กลายเป็นมาตรการบังคับใช้เชิงปฏิบัติ เพื่อยกระดับการป้องกันอาชญากรรมไซเบอร์ในภูมิภาคอย่างมีประสิทธิภาพ

5. มาตรการด้านการส่งผู้ร้ายข้ามแดนควรได้รับการผลักดันให้มีการจัดทำอนุสัญญาพหุภาคีว่าด้วยการส่งผู้ร้ายข้ามแดนในระดับภูมิภาคอาเซียนอย่างเร่งด่วนเพื่อทดแทนระบบความตกลง

ทวิภาคีที่ล่าช้าและกระจัดกระจาย ซึ่งไม่ทันต่อรูปแบบของอาชญากรรมข้ามชาติอย่างแก๊งคอลเซ็นเตอร์ที่เคลื่อนไหวรวดเร็วและอาศัยช่องโหว่ทางกฎหมาย การมีอนุสัญญาแบบรวมศูนย์จะช่วยเสริมสร้างกลไกทางกฎหมายที่มีผลผูกพันในการติดตาม ควบคุม และส่งตัวผู้ต้องหาได้อย่างมีประสิทธิภาพ รวมถึงลดอุปสรรคในเรื่องเขตอำนาจศาล และแสดงให้เห็นถึงความมุ่งมั่นร่วมกันของอาเซียนในการสร้างประชาคมยุติธรรมทางอาญาในภูมิภาค

**6.2.3 ข้อเสนอแนะด้านปฏิบัติ**

1. เห็นควรที่องค์การอาเซียนจะเข้ามามีส่วนร่วมอย่างแข็งขันจริงจังในการปรับปรุงการทำงานของตำรวจอาเซียน (ASEANAPOL) เพื่อให้เป็นกลไกระดับปฏิบัติหลักในการป้องกันและปราบปรามอาชญากรรมข้ามชาติกรณีแก๊งคอลเซ็นเตอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้ และให้ตำรวจอาเซียนมุ่งประสานงานระหว่างประเทศสมาชิกและส่งเสริมการแลกเปลี่ยนข้อมูลระหว่างประเทศสมาชิกเกี่ยวกับแก๊งคอลเซ็นเตอร์อย่างทันท่วงทีเพื่อให้สามารถติดตามและจัดการป้องกันและปราบปรามได้อย่างมีประสิทธิภาพและมีประสิทธิผล

2. ภูมิภาคอาเซียนควรมีการจัดตั้งองค์กรกลางด้านการสืบสวนสอบสวนในระดับภูมิภาคที่มีสถานะเป็นองค์การถาวรของอาเซียน เพื่อใช้เป็นกลไกหลักในการประสานงาน การกำหนดมาตรฐาน และดำเนินการสืบสวนในคดีอาชญากรรมข้ามชาติในกรณีของแก๊งคอลเซ็นเตอร์ซึ่งมีลักษณะการกระทำผิดที่ซับซ้อนและแผ่ขยายข้ามพรมแดน การมีองค์กรระดับภูมิภาคที่สามารถกำหนดแนวทางการสอบสวนที่เป็นมาตรฐานเดียวกันให้แก่ทั้ง 10 ประเทศสมาชิกจะช่วยลดความเหลื่อมล้ำในการปฏิบัติ ป้องกันความล่าช้าในการติดตามผู้กระทำผิด และส่งเสริมความยุติธรรมให้กับเหยื่ออย่างเท่าเทียม โดยองค์กรดังกล่าวอาจพัฒนาโครงสร้างและภารกิจให้มีลักษณะคล้ายกับหน่วยงานเฉพาะทาง และสามารถประสานงานเชิงลึกกับหน่วยงานภายในประเทศสมาชิก รวมทั้งจัดตั้งทีมเฉพาะกิจ ข้ามชาติได้อย่างรวดเร็วและมีประสิทธิภาพ ในทางหลักการ องค์กรกลางนี้ควรมีบทบาทหลักในสามมิติ ได้แก่

1) การประสานงานและอำนวยความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายของแต่ละประเทศ

2) การกำหนดมาตรฐานและแนวทางการสอบสวนที่เป็นหนึ่งเดียวในระดับภูมิภาค และ

3) การปฏิบัติภารกิจร่วมในการสืบสวนคดีที่มีลักษณะข้ามพรมแดน

โดยมีฐานข้อมูลกลางและศูนย์วิเคราะห์ข่าวกรองที่สามารถสนับสนุนการสืบสวนได้แบบเรียลไทม์ ทั้งนี้ เพื่อให้กลไกนี้สามารถขับเคลื่อนได้จริง องค์กรควรมีสถานะเป็น “องค์กรถาวร” ภายใต้กรอบของอาเซียนและได้รับการรับรองในระดับรัฐมนตรีด้านความมั่นคงหรือความยุติธรรม ซึ่งมีการจัดตั้งหน่วยงานเฉพาะเพื่อสืบสวนคดีเกี่ยวกับอาชญากรรมข้ามชาติและอาชญากรรมทาง

เทคโนโลยีโดยตรง การมีองค์กรกลางเช่นนี้จะเป็นก้าวสำคัญในการรวบรวมและตรวจสอบพยานหลักฐานที่สำคัญและทำให้การนำตัวผู้กระทำผิดมาลงโทษสามารถดำเนินการได้อย่างเป็นระบบและมีประสิทธิภาพในระดับภูมิภาค อย่างไรก็ตาม มีข้อสังเกตว่าการจัดตั้งองค์กรถาวรต้องอาศัยความร่วมมือทางการเมืองระดับสูงและงบประมาณจากสมาชิกทั้งหมด

# รายการอ้างอิง


**หนังสือ**

**ภาษาไทย**

ชาญชัย แสวงศักดิ์, *กฎหมายอาชญากรรมทางเทคโนโลยี*, (กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์ 2564), 132–135.

วัชรพล ประสารราชกจ, *ปัญหาอาชญากรรมข้ามชาติและนโยบายความมั่นคงมุมมองไทยยุโรปและนานาชาติ* (กรุงเทพฯ: จุฬาลงกรณ์มหาวิทยาลัย 2544) 59-60.

วันชัย รุจนวงศ์, *ผ่าองค์กรอาชญากรรม: มะเร็งร้ายของสังคม* (กรุงเทพฯ: สำนักพิมพ์มติชน ส.ค. 2548) 24–26.

สมศักดิ์ โกศัยสุข, *อาชญากรรมข้ามชาติ: กฎหมายและกลไกการบังคับใช้*, (กรุงเทพฯ: วิญญูชน 2563), 87–89.

สมศักดิ์ โกศัยสุข, *กฎหมายอาญาภาคความผิด ลักษณะความผิดเกี่ยวกับทรัพย์*, (กรุงเทพฯ: วิญญูชน 2562) 72–74.

อัณณพ ชูบำรุง, *ทฤษฎีอาชญาวิทยา* (กรุงเทพฯ: สำนักพิมพ์โอเดียนสโตร์, 2527).

**ภาษาต่างประเทศ**

Edwin H. Sutherland, *White Collar Crime* (New York: Dryden Press 1949).

Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy* (New Jersey: Princeton University Press, 2005) 103–104.

Felson Marcus, *Crime and Everyday Life*. 3rd ed. (Thousand Oaks, CA: Sage Publications 2002) 45–46.

**บทความ**

**ภาษาไทย**

คณาธิป ทองรวีวงศ์, ‘การคุ้มครองสิทธิมนุษยชนจากมาตรการความร่วมมือระหว่างประเทศในกรอบของสหประชาชาติว่าด้วยการเข้าถึงข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์ เพื่อการป้องกันและปราบปรามอาชญากรรมไซเบอร์’ (วารสารมหาวิทยาลัยหาดใหญ่, 1265).

จักรพงษ์ กังวานโสภณ, ‘ความผิดฐานฉ้อโกง: ศึกษากรณีการหลอกลวงทางโทรศัพท์ (แก๊งคอลเซ็นเตอร์)’ (2565) 14(2) วารสารวิจัยและพัฒนา มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา <https://so06.tci-thaijo.org/index.php/rdibsru/article/view/255877> สืบค้นเมื่อ 18 พฤษภาคม 2568.

ชิตพล กาญจนกิจ, ‘ความท้าทายของรัฐอาเซียนในการต่อต้านอาชญากรรมข้ามชาติ’ (2560) 46(1) วารสารสังคมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย 51–78.

ชิตพล กาญจนกิจ, ‘ความร่วมมือระหว่างประเทศว่าด้วยกระบวนการยุติธรรมทางอาญาอาเซียน: ข้อเสนอเชิงยุทธศาสตร์เพื่อการเตรียมความพร้อมเข้าสู่ประชาคมอาเซียน,’ NIDA Development Journal ปีที่ 56, ฉบับที่ 3 (2559) 1–32.

ชิตพล กาญจนกิจ, ‘สหวิทยาการในการจัดการปัญหาอาชญากรรมข้ามชาติ (Interdisciplinary Approach to Fighting Transnational Crime)’ (ฝ่ายสนธิสัญญาและกฎหมาย กองการต่างประเทศ, 2556) 10.

นวภัทร สมกำเนิด และธรรมวิทย์ เทอดอุดมธรรม.“อาชญากรรมข้ามชาติ: การใช้บัตรเครดิตปลอมของอาชญากรข้ามรัสเซียและกลุ่มประเทศยุโรปตะวันออก.” วารสารวิชาอาชญาวิทยาและนิติวิทยาศาสตร์โรงเรียนนายร้อยตำรวจ, 17(2), 137–152.

วีระพงษ์ บุญโญภาส, ‘ยุโรปกับนโยบายความมั่นคง : อาชญากรรมข้ามชาติทางเศรษฐกิจ’ (2543) 8(1) วารสารยุโรปศึกษา ศูนย์ยุโรปศึกษา จุฬาลงกรณ์มหาวิทยาลัย 57–58.

สักกรินทร์ นิยมศิลป์, วิจารณ์เรื่อง อาชญากรรมข้ามชาติ ภัยคุกคามไทยและอาเซียน, ใน เอกสารการประชุมวิชาการสถาบันวิจัยประชากรและสังคม มหาวิทยาลัยมหิดล (2565), <https://ipsr.mahidol.ac.th/wp-content/uploads/2022/03/447-IPSR-Conference-A15-fulltext.pdf> สืบค้นเมื่อ 16 พฤศจิกายน 2566.

สักกรินทร์ นิยมศิลป์, ‘อาชญากรรมข้ามชาติ ภัยคุกคามไทยและอาเซียน’ (2565) วารสารนิติศาสตร์ 238 <https://ipsr.mahidol.ac.th/wp-content/uploads/2022/03/447-IPSR-Conference-A15-fulltext.pdf> สืบค้นเมื่อวันที่ 27 มกราคม 2567.

อรพรรณ บัวทอง, “การบูรณาการการใช้กฎหมายอาญากับกฎหมายเฉพาะในการปราบปรามอาชญากรรมไซเบอร์,” *วารสารนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย*, ปีที่ 47, ฉบับพิเศษ (2564) 89–91.

**ภาษาต่างประเทศ**

Lawrence E. Cohen และ Marcus Felson, “Social Change and Crime Rate Trends: A Routine Activity Approach” (1979) 44(4) *American Sociological Review* 588–608.

Gary S. Becker, ‘Crime and Punishment: An Economic Approach’ (1968) Journal of Political Economy 76(2): 169–217.

Gilbert Geis, “White-Collar and Corporate Crime,” in The Oxford Handbook of Criminology, 3rd ed., ed. by Mike Maguire et al. (Oxford: Oxford University Press, 2002) 981–1010.

Patricia L. Brantingham and Paul J. Brantingham, “Nodes, Paths and Edges: Considerations on the Complexity of Crime and the Physical Environment,” Journal of Environmental Psychology 13, no. 1 (1993).

**วิทยานิพนธ์ การค้นคว้าอิสระ รายงานส่วนบุคคล**

ขวัญชนก ศรีภมร, ‘แนวทางการป้องกันอาชญากรรมที่เกิดจากแก๊งคอลเซ็นเตอร์ออนไลน์โดยมาตรการกำกับดูแลของอุตสาหกรรมโทรคมนาคม’ (วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต, คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย2565)

เขตต์เทพหัสดิน ณ อยุธยา, ‘การจัดตั้งองค์การตำรวจอาเซียน: ศึกษาเปรียบเทียบองค์การตำรวจสากล และสำนักงานตำรวจยุโรป’ (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยแม่ฟ้าหลวง, 2561)

แคทราย จันทรากา, ‘มาตรการทางกฎหมายของอาเซียนในการป้องกันและปราบปรามการค้ามนุษย์’ (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยแม่ฟ้าหลวง 2558).

จิตสุภา ฤทธิผลิน, ‘ทิศทางและนโยบายการกำกับดูแลกิจการกระจายเสียง และกิจการโทรทัศน์ในยุคของการหลอมรวมสื่อ: กรณีศึกษาเปรียบเทียบยุทธศาสตร์ของ FCC และ OFCOM’ (วิทยานิพนธ์, สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ, 2560).

นันทวดี คาดคะเน, ‘ปัญหาในการปราบปรามอาชญากรรมไซเบอร์ภายใต้กฎหมายระหว่างประเทศ’ (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์, 2561

พัลลภ หริ่งรอด, ‘มาตรการตามกฎหมายในการปราบปรามองค์กรอาชญากรรมข้ามชาติ ศึกษาเฉพาะกลุ่มคอลเซ็นเตอร์’ (วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต สาขากฎหมายอาญาและอาชญาวิทยา คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา, 2562).

**รายงานผลการวิจัย**

**ภาษาไทย**

สุมนทิพย์ จิตสว่าง ปิยะพร ตันณีกุล และ นัทธี จิตสว่าง, 'อาชญากรรมข้ามชาติ: ภัยคุกคามประเทศไทยเกี่ยวกับแก๊งคอลเซ็นเตอร์' (รายงานวิจัย, 2563).

**ภาษาต่างประเทศ**

UNODC, Transnational Organized Crime in Southeast Asia: Evolution, Growth and Impact (2019) 27–29.

**บล็อกและเว็บไซต์**

**ภาษาไทย**

กรมสอบสวนคดีพิเศษ, ‘รายงานสถานการณ์อาชญากรรมข้ามชาติ ประเภทแก๊งคอลเซ็นเตอร์’(2565) <https://www.dsi.go.th> สืบค้นเมื่อ 18 พฤษภาคม 2568.

กองอาเซียน กรมอาเซียน, ‘การประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมือง และความมั่นคงในภูมิภาคเอเชีย - แปซิฟิก (ASEAN Regional Forum – ARF)’ <http://www.led.go.th/asean/pdf/4/4-3.pdf> สืบค้นเมื่อ 12 เมษายน 2567.

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี, ‘หน้าที่และภารกิจ,’ <https://www.tcybercrime.police.go.th> สืบค้นเมื่อ 28 มิถุนายน 2568.

กองบัญชาการสอบสวนกลาง, ‘กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี,’ <https://www.cib.go.th/organization/technologycrime> สืบค้นเมื่อ 28 มิถุนายน 2568.

ข่าวเศรษฐกิจ, กสทช., ‘ค่ายมือถือ’ วันละล้านไร้น้ำยาปราบคอลเซ็นเตอร์’ <https://www.bangkokbiznews.com/business/1014117> สืบค้นเมื่อ 3 พฤษภาคม 2567.

‘คนไทยถูกหลอกลวงทางออนไลน์ 36 ล้านคน ความเสียหายเกือบ 50,000 ล้านบาท’ (สำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ (สสส.) และคณะเศรษฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย) <https://www.the101.world/tossapon-tassanapan-interview/> สืบค้น 9 กุมภาพันธ์ 2567.

จิราภพ ทวีสูงส่ง, ‘เรื่องใกล้ตัวกว่าที่คิด! “อาชญากรรมทางไซเบอร์” รู้จักไว้ป้องกันภัยไม่ตกเป็นเหยื่อ’ (Thai PBS, 23 กุมภาพันธ์ 2566) <https://www.thaipbs.or.th/now/content/68> สืบค้นเมื่อ 8 กรกฎาคม 2567.

ทศพล ทรรศนพรรณ, ‘วิกฤต “มิจฉาชีพออนไลน์” รัฐไทยทำอะไรได้ไหม (2566)<https://www.the101.world/tossapon-tassanapan-interview/> สืบค้น 9 กุมภาพันธ์ 2567.

ธนาคารแห่งประเทศไทย, ‘กลโกงบัตรต่าง ๆ’ <https://www.bot.or.th/th/satang-story/fraud/card-fraud.html> สืบค้นเมื่อ 27 มกราคม 2567.

ธิติรัตน์ สมบูรณ์, ‘รู้ เข้าใจและตระหนัก “อาชญากรรมทางไซเบอร์” (Cybercrime) ป้องกันภัยคุกคามใกล้ตัว’ (Chulalongkorn University, 25 ตุลาคม 2566) <https://www.chula.ac.th/news/138291/> สืบค้นเมื่อ 8 กรกฎาคม 2567.

บุญวัฒน์ สว่างวงศ์, ‘ทฤษฎีที่เกี่ยวข้องกับการก่ออาชญากรรมและการวัดสถิติอาชญากรรม’ (ระบบการเรียนรู้อิเล็กทรอนิกส์ E-Learning มหาวิทยาลัยราชภัฏสวนสุนันทา), <https://elcpg.ssru.ac.th/boonwat_sa/pluginfile.php/44/block_html/content/อาชญาวิทยา%20บทที่%204.pdf> , สืบค้นเมื่อ 23 กุมภาพันธ์ 2567.

ปฐมพงศ์ ศรีแสงจันทร์, ‘คณะทำงานพหุภาคีแก้ไขปัญหาคอลเซ็นเตอร์เสนอบอร์ด กสทช. ขีดเส้นตายให้โอเปอร์เรเตอร์ทุกรายสร้างระบบให้ประชาชนเลือกสมัครบริการปฏิเสธไม่รับสายที่โทรมาจากต่างประเทศ เพื่อลดความเดือดร้อนจากปัญหาดังกล่าวโดยเร็วที่สุด’ <https://www.nbtc.go.th/News/Press-Center/55326.aspx?lang=th-th> สืบค้นเมื่อ 3 พฤษภาคม 2567.

ผู้จัดการออนไลน์, ‘เปิดขั้นตอนแจ้งความออนไลน์ thaipoliceonline.com รับเฉพาะคดีอาชญากรรมทาเทคโนโลยี’<https://mgronline.com/onlinesection/detail/9650000021035> สืบค้นเมื่อ 24 เมษายน 2567.

ผลกระทบของแก๊งคอลเซ็นเตอร์ต่อเศรษฐกิจไทย’ (ธนาคารแห่งประเทศไทย, 2566) <https://sustainability.ais.co.th/th/update/aunjai-cyber/789/gang-call-center-scam> สืบค้น 9 กุมภาพันธ์ 2567.

พรพล น้อยธรรมราช, ‘ประชาคมการเมืองและความมั่นคงอาเซียน 2015 กับทฤษฎีการรวมตัวเชิงภูมิภาค : กรณีศึกษา เรื่องอาชญากรรมข้ามชาติในอาเซียน’ <http://dtad.dti.or.th/index.php?option=com_content&view=article&id=244:asean2015&catid=6:analysis&Itemid=11> สืบค้นเมื่อ 28 มีนาคม 2567.

พิมพ์ธัญญา ฆ้องเสนาะ, ‘บัญชีม้า’ <https://library.parliament.go.th/th/radioscript/rr2565-may6> สืบค้นเมื่อ 24 เมษายน 2567.

‘ภัยอาชญากรรมแก๊งคอลเซ็นเตอร์’ (สำนักหอสมุดแห่งชาติ) <https://dl.parliament.go.th/handle/lirt/600738> สืบค้น 19 มกราคม 2568.

ยุวมิตร, ‘Phishing คืออะไร ป้องกันอย่างไร’ (ThaiCERT, 15 สิงหาคม 2566) <https://www.thaicert.or.th/phishing-awareness.html> สืบค้นเมื่อ 8 กรกฎาคม 2567.

‘ลาวเร่งปราบปรามขบวนการแก๊งคอลเซ็นเตอร์ ยึดทรัพย์สินและควบคุมตัวชาวต่างชาติหลายพันคน’ (Intsharing, 14 สิงหาคม 2567) <https://intsharing.co/2024/08/14/ลาวเร่งปราบปราม ขบวนการ/> สืบค้นเมื่อ 4 มกราคม 2568.

วรรณวิภา เมืองถ้ำ, ‘แนวคิด หลักทฤษฎี นิยามกฎหมายอาชญากรรมข้ามชาติ ชุดวิชา 41719 กฎหมายกระบวนการยุติธรรมเกี่ยวกับการควบคุมและปราบปรามอาชญากรรมในประเทศและข้ามชาติที่สำคัญ’ (มหาวิทยาลัยสุโขทัยธรรมาธิราช) <https://www.stou.ac.th/schoolsweb/law/UploadedFile/หน่วยที่ 1.pdf> สืบค้นเมื่อ 20 กุมภาพันธ์ 2567.

วิกิพีเดีย, ‘โลกาภิวัตน์’ (วิกิพีเดีย, 22 พฤศจิกายน 2567) <https://th.wikipedia.org/wiki/โลกาภิวัตน์> สืบค้นเมื่อ 18 พฤษภาคม 2567.

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักข่าวกรองแห่งชาติ, ‘ออสเตรเลียเริ่มปิดกั้นข้อความหลอกลวงที่อ้างว่ามาจากหน่วยงานของรัฐบาล’ <https://www.nia.go.th/cyber/cyberpage/588/> สืบค้นเมื่อ 10 มีนาคม 2568.

สภ.โพธิ์กลาง อ.เมือง จว. นครราชสีมา, ‘การป้องกันอาชญากรรมเชิงรุก โดย ทฤษฎีสามเหลี่ยมอาชญากรรม’ (Phoklang Police Blogspot, 10 ตุลาคม 2016) <https://phoklangpolice.blogspot.com/2016/10/blog-post.html> สืบค้นเมื่อ 10 กุมภาพันธ์ 2024.

สำนักงานตำรวจแห่งชาติ, ‘คำสั่งสำนักงานตำรวจแห่งชาติ ที่ 46/2564 เรื่อง “การจัดตั้งกองบัญชาการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี”’ (2564) <https://www.royalthaipolice.go.th> สืบค้นเมื่อ 22 มิถุนายน 2568.

สำนักงานตำรวจแห่งชาติ, ‘คู่มือป้องกันภัยจากอาชญากรรมข้ามชาติ’ (สำนักงานตำรวจแห่งชาติ, 20 ธันวาคม 2565) <https://talatphlu.metro.police.go.th/wp-content/uploads/2022/12/คู่มือป้องกันภัยจากอาชญากรรมข้ามชาติ.pdf>สืบค้น เมื่อ 14 พฤศจิกายน 2566.

สำนักงานประชาสัมพันธ์จังหวัดสระแก้ว, ‘มาตรการ 3 ตัด: รัฐบาลเดินหน้ายุทธศาสตร์สกัดแก๊งคอลเซ็นเตอร์แนวชายแดน’ (เว็บไซต์กรมประชาสัมพันธ์) <https://www.prd.go.th/th/content/category/detail/id/39/iid/366469> สืบค้นเมื่อ 22 มิถุนายน 2568.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA), รายงานภัยคุกคามทางไซเบอร์ประจำปี 2566 (2566) <https://www.etda.or.th> สืบค้นเมื่อ 14 ธันวาคม 2567.

สุภาพิชญ์ ถิระวัฒน์, ‘กองบัญชาการตำรวจไซเบอร์’ < https://library.parliament.go.th/th/radioscript-rr2564-nov1> สืบค้นเมื่อ 24 เมษายน 2567.

‘อาชญากรรมแก๊งคอลเซ็นเตอร์’ (Research Cafe) <https://researchcafe.tsri.or.th/call-center-crime/> สืบค้นเมื่อ 1 กุมภาพันธ์ 2567.

‘องค์การตำรวจสากล’ (LIRT คลังสารสนเทศ สำนักงานเลขาธิการสภาผู้แทนราษฎร) <https://dl.parliament.go.th/handle/20.500.13072/617970> สืบค้นเมื่อ 7 มีนาคม 2567.

ไทยรัฐออนไลน์, ‘หวัง PDPA ลดแก๊งคอลเซ็นเตอร์’ <https://www.thairath.co.th/business/economics/2429726> สืบค้นเมื่อ 24 เมษายน 2567.

AIS Aunjai Cyber, “รวม 22 กลโกงมิจฉาชีพ ที่ใช้หลอกลวงเหยื่อบนโลกออนไลน์ พร้อมวิธีรับมือ,” AIS Sustainability, <https://sustainability.ais.co.th/th/update/aunjai-cyber/795> สืบค้นเมื่อ 18 มกราคม 2567.

Justice Channel, “Call Center Gang: เปิดโปงขบวนการหลอกเงินคนไทย สูญหลายพันล้าน,” Justice Channel, <https://justicechannel.org/listen/cybercrime/callcentergang> สืบค้นเมื่อ 18 มกราคม 2567.

Law for ASEAN, ‘ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ และบทวิเคราะห์กฎหมายไทยที่เกี่ยวข้อง’ (Law for ASEAN Journal, 2566) <https://lawforasean.krisdika.go.th/Content/View?Id=349&Type=1> สืบค้นเมื่อ 14 พฤศจิกายน 2566.

Law for ASEAN, ‘อาเซียนกับการจัดการปัญหาอาชญากรรมไซเบอร์’ (Law for ASEAN, 2 ธันวาคม 2565) <https://lawforasean.krisdika.go.th/File/files/cybersecurity_dec2.pdf> สืบค้นเมื่อ 14 พฤศจิกายน 2566.

Mobile Octa Admin, ‘Gogolook ปั้น Whoscall แพลตฟอร์มต่อต้านการฉ้อโกงแห่งแรกในประเทศไทย ปกป้องคนไทยไม่ให้ตกเป็นเหยื่อการใช้โทรศัพท์และข้อความหลอกลวง’ (2565) <https://www.mobileocta.com/gogolook-creates-whoscall-the-first-anti-fraud-platform-in-thailand/> สืบค้นเมื่อ 5 กรกฎาคม 2568.

Prachatai, 'เขตเศรษฐกิจพิเศษสามเหลี่ยมทองคำ: อุตสาหกรรมหลอกลวงในลาว' (ธันวาคม 2567) <https://prachatai.com/journal/2024/12/111689> สืบค้นเมื่อ 4 มกราคม 2568.

Thailand Institute of Justice, ‘องค์กรอาชญากรรมข้ามชาติ’ (TIJ, 29 มกราคม 2566) <https://www.tijthailand.org/area_of_work/detail/2> สืบค้นเมื่อ 2 กุมภาพันธ์ 2566.

**ภาษาต่างประเทศ**

AFP, ‘Hundreds Rescued from Philippines Scam Center—Police’ <https://manilastandard.net/news/314426243/hundreds-rescued-from-philippines-scam-center-police.html> accessed 15 March 2024.

‘Annual Report on Cybercrime’ (Cambodian National Police) <https://cnp.gov.kh> accessed 15 December 2024.

'Annual Crime Report 2024' (Royal Brunei Police Force) <https://bn.usembassy.gov/2024-trafficking-in-persons-report-brunei/> accessed 4 January 2025.

Bank Islam Brunei Darussalam, 'Public Advisory on Scam Calls' (Xinhua News Agency) <https://english.news.cn/20241219/3e4b4af6da724a63a497cdbeebb474ad/c.html> accessed 4 January 2025.

BBC News, ‘Hundreds rescued from love scam centre in the Philippines’ (4 April 2024) <https://www.bbc.com/news/world-asia-68562643> accessed 5 December 2024.

Beh, M. T., Combating Scam Syndicates in Malaysia and Southeast Asia (Penang Institute, 2025) <https://penanginstitute.org/publications/issues/combating-scam-syndicates-in-malaysia-and-southeast-asia/> accessed 5 July 2025.

Cyber Security Brunei, ‘Brunei Blocks Over 80 Fake Websites and 500 Suspicious Phone Numbers’ The Cyber Express <https://thecyberexpress.com/brunei-strengthens-cybersecurity/amp> accessed 15 December 2024.

Council of Europe Committee of Ministers, ‘Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime,’ <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f1094> accessed May 22 2024.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Official Journal of the European Union, L 218, 14 August 2013, 8–14, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040> accessed July 6 2025.

ENISA, ‘ENISA Mandate and Mission’ (2020), <https://www.enisa.europa.eu/about-enisa> accessed 16 May 2025.

European Commission, 'Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace' <https://bit.ly/2YrH1kl> accessed 24 April 2024.

European Commission, ‘EU Strategy to Tackle Organised Crime 2021–2025’ (Brussels: European Commission, 2021), available at: <https://ec.europa.eu/home-affairs/eu-strategy-tackle-organised-crime-2021-2025_en> accessed 16 May 2025.

European Commission, 'The EU’s Cybersecurity Strategy for the Digital Decade' (JOIN(2020) 18 final, 16 December 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN> accessed 27 June 2024.

Europol, 'European Cybercrime Centre - EC3' <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> accessed 27 June 2024.

European Arrest Warrant: Facilitating Judicial Cooperation in Criminal Matters’ (European Commission) <https://commission.europa.eu/law/european-arrest-warrant_en> accessed 16 May 2025.

Fam, C., ‘Report: Scam Calls in Malaysia Skyrocketed by 82.81% in 2024’ (The Star, 3 March 2025) https://www.thestar.com.my/tech/tech-news/2025/03/03/report-scam-calls-in-malaysia-skyrocketed-by-8281-in-2024 accessed 5 December 2025.

Global Anti-Scam Alliance (GASA), (Research) <https://www.gasa.org/research> accessed 15 December 2024.

‘History’ (INTERPOL) <http://www.interpol.int/en/About-INTERPOL/History> accessed 7 March 2024.

INTERPOL, ‘About INTERPOL: Overview’ <http://www.interpol.int/About-INTERPOL/Overview> accessed 18 May 2024.

INTERPOL, ‘INTERPOL Notices’, <http://www.interpol.int/INTERPOL-expertise/Notices> accessed 18 May 2024.

'Indonesia Rescues Citizens from Scam Centers in Myanmar' (AP News, 21 February 2025) <https://apnews.com/article/57d644b606335eecbd5d3a27a1053e3b> accessed 24 March 2025.

‘Lao Police Bust Nine Fraud Rings, Seize Thousands of Devices in 2024’ 2 January 2025) <https://laotiantimes.com/2025/01/02/lao-police-bust-nine-fraud-rings-seize-thousands-of-devices-in-2024/> accessed 4 January 2025.

'Laos Orders ‘Scam Centers’ in Golden Triangle SEZ to Be Completely Shut Down' (Business & Human Rights Resource Centre, 12 August 2024) https://www.business-humanrights.org/en/latest-news/laos-orders-scam-centres-in-golden-triangle-sez-to-be-completely-shut-down/ accessed 8 January 2025.

Marcin Rozmus, Ilona Topa, and Marika Walczak, ‘Harmonisation of Criminal Law in the EU Legislation - The Current Status and the Impact of the Treaty of Lisbon,’<http://www.ejtn.eu/Documents/Themis/THEMIS%20written%20paper%20-%20Poland%201.pdf>

Netizens Urged to Save Gov’t Anti-Scam Response Hotline 1326’ <https://www.pna.gov.ph/articles/1207775> accessed June 7 2024.

Ofcom, ‘Tackling Nuisance Calls and Messages,’ <https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/tackling-nuisance-calls-messages> accessed July 6 2025.

‘Online Scam Centres and Trafficking in Persons in Southeast Asia’ (UNODC, 2023) <https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf> accessed 6 July 2025.

‘Philippine National Police Anti-Cybercrime Group’ (PNP-ACG) <https://www.cybersecurityintelligence.com/philippine-national-police-anti-cybercrime-group-pnp-acg-4731.html> accessed May 27 2024.

‘Reuters, ‘Scam Hubs on Thai-Myanmar Border Still Have Up to 100,000 People’ (Thai Police Says 2025) <https://www.reuters.com/world/asia-pacific/scam-hubs- thai-myanmar-border-still-have-up-100000-people-thai-police-says-2025-03-18/> accessed 8 January 2025.

‘Scam Shield, ‘2024 Annual Scams and Cybercrime Brief’ (Singapore: National Crime Prevention Council, 2024) <https://www.scamshield.gov.sg/files/Scams%20and

%20Cybercrime%20Briefs/2024_annual_scams_and_cybercrime_brief.pdf> accessed 15 December 2024.

'Scam watch, 'Wangari Scam – Missed Call Scams' <https://www.scamwatch.gov.au> accessed May 19 2025.

Shahrizal, 'Malaysia Loses RM54.02 Billion To Scams, Report Reveals Alarming Rise' (Business Today, 4 October 2024) <https://www.businesstoday.com.my/...> accessed 5 December 2024.

Stock Titan, 'FICO Survey: 1 in 4 Indonesian Consumers Report Losing Money to Scams' (23 April 2024) <https://www.stocktitan.net/news/FICO/fico-survey-1-in-4-indonesian-consumers-report-losing-money-to-scams-fnj6ol7wggfn.html> accessed 4 January 2025.

The Star, 'Rich Facade of Scam Call Centres: How Syndicates Exploit High-End Properties in KL' <https://www.thestar.com.my/news/nation/2024/08/21/rich-facade-of-scam-call-centres> accessed 15 December 2024.

'Trafficked for Scams: Abuse in Southeast Asian Scam Center' (Human Rights Watch) <https://bangkok.ohchr.org/news/2022/online-scam-operations-and-trafficking-forced-criminality-southeast-asia> accessed 15 December 2024.

United Nations Office on Drugs and Crime (UNODC), Transnational Organized Crime in Southeast Asia: Evolution, Growth and Impact (2019) <https://www.unodc.org/> accessed 25 December 2024.

United Nations Office on Drugs and Crime (UNODC), United Nations Convention against Transnational Organized Crime and the Protocols Thereto, Articles 5–8 (2004), <https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html> accessed July 6 2025.

UNODC, Transnational Organized Crime in Southeast Asia: Evolution, Growth and Impact (2019), available at: <https://www.unodc.org/> accessed 5 July 2024.

'Vietnamese Lose $744mn to Online Scams in 2024: Report' (Tuoi Tre News, 17 December 2024) <https://tuoitrenews.vn/news/society/20241217/vietnamese-lose-744mn-to-online-scams-in-2024-report/83436.html> accessed 24 March 2025.

What is phishing | Attack techniques & scam examples | Imperva' (Imperva) <https://www.imperva.com/learn/application-security/phishing-attack-scam/> accessed 17 February 2024.

'Who does the data protection law apply to?' (European Commission) <https://ec.europa.eu/info/law/law-topic/dataprotection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en> accessed 11 October 2020.

**เอกสารอื่น ๆ**

**ภาษาไทย**

รังสรรค์ โรจน์ชีวิน และคณะ, 'กฎหมายคุ้มครองผู้บริโภค และการดำเนินคดีคุ้มครองผู้บริโภคประเทศออสเตรเลีย: ศึกษากรณีการหลอกลวงผู้บริโภคทางการค้าและการบังคับใช้โดย ACCC' (เอกสารประกอบการฝึกอบรมหลักสูตร "กฎหมายเกี่ยวกับวิธีพิจารณาความแพ่งชั้นสูง", มหาวิทยาลัยนิวเซาท์เวลส์ ประเทศออสเตรเลีย: สำนักการต่างประเทศ).

โชคสุข กรกิตติชัย, 'สหราชอาณาจักรบริเตนใหญ่และไอร์แลนด์เหนือ กับการป้องกันและปราบปรามการทุจริต' เอกสารวิชาการ อิเล็กทรอนิกส์ สำนักวิชาการ สำนักงานเลขาธิการสภาผู้แทนราษฎร (สิงหาคม 2565) 13.

**ภาษาต่างประเทศ**

Zainul, E., 'Malaysians lost US$12.8b to scams over the past year, survey reveals' (The Edge Malaysia, 3 October 2024).

Peter Andreas and Ethan Nadelmann, Policing the Globe: Criminalization and Crime Control in International Relations (New York: Oxford University Press, 2006) 5–6.

United Nations Development Programme, Human Development Report 1994: New Dimensions of Human Security (New York: Oxford University Press, 1994) 23–25

# ประวัติผู้ประพันธ์

**ชื่อ** สุพิชญา ศิรินภาดล

**ประวัติการศึกษา**

2566 ปริญญาตรี นิติศาสตรบัณฑิต
มหาวิทยาลัยแม่ฟ้าหลวง