

บทบาทของเจ้าหน้าที่ตำรวจในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ  
ภายใต้พระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรม  
ทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568

The Role of the Police in Preventing and Suppressing Transnational Crime  
under the Royal Decree on the Prevention and Suppression  
of Technological Crime (No. 2), B.E. 2568 (2025)

อิสเรศวร์ ลักขมีพิเชษฐ์<sup>1</sup>

คณะตำรวจศาสตร์ โรงเรียนนายร้อยตำรวจ

90 หมู่ที่ 7 ตำบลสามพราน อำเภอสามพราน จังหวัดนครปฐม 73110, ประเทศไทย

อีเมลติดต่อ: issares\_63@hotmail.com

Issares Luxmeepichet<sup>2</sup>

Faculty of Police Science, Royal Thai Police Cadet Academy

90, Moo 7, Sam Phran, Sam Phran District, Nakhon Pathom 73110, Thailand

Email: issares\_63@hotmail.com

Received: April 7, 2025 Revised: July 20, 2025 Accepted: July 23, 2025

### บทคัดย่อ

บทความนี้มีวัตถุประสงค์เพื่อศึกษาบทบาทของเจ้าหน้าที่ตำรวจในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ ภายใต้พระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 และเพื่อเสนอแนวทางในการพัฒนาบทบาทและศักยภาพของเจ้าหน้าที่ตำรวจให้สอดคล้องกับการเผชิญภัยคุกคามจากอาชญากรรมข้ามชาติในยุคดิจิทัล ผู้ศึกษาเลือกใช้ระเบียบวิธีวิจัยเชิงคุณภาพ โดยเน้นการศึกษาเชิงเอกสารเป็นหลัก

จากการศึกษาพบว่า บทบาทของเจ้าหน้าที่ตำรวจในการป้องกันและปราบปรามอาชญากรรมข้ามชาติภายใต้พระราชกำหนดฉบับนี้มิได้จำกัดอยู่เพียงการจับกุมผู้กระทำความผิดตามประมวลกฎหมายอาญา แต่ได้ขยายขอบเขตไปสู่การมีส่วนร่วมในกระบวนการจัดการเชิงโครงสร้างของสังคม จากบทบาทด้านต่าง ๆ ได้แก่

<sup>1</sup> อาจารย์.

<sup>2</sup> Lecturer.

ด้านการบังคับใช้กฎหมาย ด้านการป้องกันล่วงหน้าและการเฝ้าระวังเชิงเทคโนโลยี ด้านการวิเคราะห์และรวบรวมข่าวกรองทางไซเบอร์ ด้านความร่วมมือระหว่างหน่วยงาน ด้านการพัฒนาองค์ความรู้และสมรรถนะขององค์กร และในเชิงนโยบายและกลไกโครงสร้างและเจ้าหน้าที่ตำรวจต้องพัฒนาศักยภาพด้านเทคโนโลยี กฎหมาย และจริยธรรม ตลอดจนเสนอแนวทางปรับปรุงกฎหมายให้ทันสมัย บูรณาการข้อมูลข่าวกรองและสร้างความร่วมมือระหว่างประเทศอย่างเป็นระบบ พัฒนาเครือข่ายฐานข้อมูลภายในประเทศให้เชื่อมโยงอย่างมีประสิทธิภาพและส่งเสริมการมีส่วนร่วมของประชาชนกับภาคเอกชนในฐานะหุ้นส่วนความมั่นคงเพื่อสร้างระบบความปลอดภัยเชิงรุกจากฐานรากของสังคม

**คำสำคัญ:** เจ้าหน้าที่ตำรวจ; อาชญากรรมข้ามชาติ; อาชญากรรมทางเทคโนโลยี; พระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568

### Abstract

This research article aims to examine the role of police officers in preventing and suppressing transnational crime under the Royal Decree on the Prevention and Suppression of Technology Crime (No. 2), B.E. 2568 (2025). It also proposes approaches to enhance their roles and capabilities in confronting digital-age transnational crime threats. The researcher employed qualitative research methodology, primarily focusing on documentary research.

The study has shown that police officers' roles under this Royal Decree extend beyond merely arresting offenders under the Criminal Code. They now include active participation in the structural management of society across various dimensions, including law enforcement roles, preventive and surveillance roles, cyber intelligence roles, cooperation roles, organizational knowledge and capacity-building roles, and governance and policy roles. Police officers must strengthen their technological, legal, and ethical competencies, advocate for legal modernization, integrate intelligence systems, and build systematic international cooperation. Additionally, the development of interconnected domestic data networks and the promotion of public-private partnerships are essential to creating proactive and grassroots-driven security systems.

**Keywords:** Police Officers; Transnational Crime; Cybercrime; Royal Decree on the Prevention and Suppression of Technology Crime (No. 2), B.E. 2568 (2025)

## 1. บทนำ

### 1.1 ความเป็นมาและความสำคัญของปัญหา

ในยุคแห่งโลกาภิวัตน์ที่เทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทเป็นโครงสร้างพื้นฐานสำคัญของการดำเนินชีวิตประจำวัน การเปลี่ยนผ่านเข้าสู่สังคมดิจิทัลอย่างเต็มรูปแบบได้ส่งผลให้เกิดการขยายตัวทางเศรษฐกิจ การเข้าถึงองค์ความรู้ และการนำนวัตกรรมมาใช้ในระดับที่ไม่เคยมีมาก่อน ทำให้พื้นที่ดิจิทัลซึ่งเปิดกว้างอย่างไร้ขอบเขตดังกล่าวกลับกลายเป็นช่องทางที่อาชญากรสามารถใช้ในการกระทำความผิดรูปแบบใหม่ได้อย่างสะดวกและยากต่อการติดตามอาชญากรรมข้ามชาติจึงมิได้มีลักษณะจำกัดอยู่ในรูปแบบการกระทำทางกายภาพที่ข้ามพรมแดนเช่นในอดีตอีกต่อไป หากแต่ได้วิวัฒน์ไปสู่การใช้เทคโนโลยีเป็นเครื่องมือหลักในการกระทำความผิด โดยอาชญากรรมเหล่านี้มีความซับซ้อนสูง สามารถซ่อนตัวอยู่ในเครือข่ายอินเทอร์เน็ตและโลกเสมือนจริง และสามารถก่อผลกระทบเป็นวงกว้างภายในเวลาอันรวดเร็วตัวอย่างที่เห็นได้ชัด ภัยคุกคามของอาชญากรรมรูปแบบใหม่จึงเป็นความท้าทายสำคัญต่อกลไกการบังคับใช้กฎหมายของรัฐซึ่งยังคงอิงกับขอบเขตอำนาจภายในประเทศ ขณะเดียวกันอาชญากรรมข้ามชาติกลับไม่จำกัดด้วยพรมแดนทางภูมิศาสตร์ และสามารถดำเนินการจากจุดใดในโลกก็ได้โดยไม่ต้องปรากฏตัวทางกายภาพ ส่งผลให้ประเทศไทยต้องเร่งปรับตัวทั้งในด้านกฎหมายและกลไกการบังคับใช้ เพื่อให้สามารถตอบโต้และควบคุมภัยคุกคามจากอาชญากรรมข้ามชาติที่ใช้เทคโนโลยีเป็นเครื่องมือได้อย่างมีประสิทธิภาพหนึ่งในกลไกทางกฎหมายที่มีบทบาทสำคัญในการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยีในประเทศไทย คือ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ซึ่งเป็นกฎหมายที่ถูกจัดทำขึ้นเพื่อตอบสนองต่อความจำเป็นเร่งด่วนในการปรับปรุงและเสริมสร้างประสิทธิภาพของกรอบกฎหมายที่เกี่ยวข้องกับการควบคุมอาชญากรรมในยุคดิจิทัล เนื่องจากการพัฒนาอย่างรวดเร็วของเทคโนโลยีสารสนเทศและการสื่อสารได้ส่งผลให้รูปแบบของอาชญากรรมมีความซับซ้อนและเปลี่ยนแปลงอย่างต่อเนื่อง การกระทำผิดที่เกี่ยวข้องกับเทคโนโลยี แม้ว่าพระราชกำหนดดังกล่าวจะมีผลบังคับใช้มาไม่นาน และได้รับการออกแบบให้ทันสมัยมากขึ้นเพื่อรองรับความท้าทายใหม่ ๆ แต่ก็ยังไม่สามารถตอบโจทย์พัฒนาการของอาชญากรรมข้ามชาติในรูปแบบทางเทคโนโลยีได้อย่างเต็มที่ อาจกล่าวได้ว่าอาชญากรรมได้พัฒนารูปแบบได้เร็วกว่าการพัฒนากฎหมาย ด้วยเหตุนี้ การปรับปรุงกฎหมายให้สอดคล้องกับความเปลี่ยนแปลงในเทคโนโลยีและพฤติกรรมของผู้กระทำความผิดจึงยังคงเป็นความจำเป็นเร่งด่วน นอกจากนี้ ยังต้องมีการประสานงานและความร่วมมือระหว่างหน่วยงานภาครัฐ ภาคเอกชน และองค์กรระหว่างประเทศ เพื่อให้สามารถแลกเปลี่ยนข้อมูลและดำเนินมาตรการป้องกันอย่างมีประสิทธิภาพต่อภัยคุกคามที่ไม่หยุดนิ่งนี้ได้ อย่างทัน่วงทีและครอบคลุมมากยิ่งขึ้น อย่างไรก็ตาม จากการบังคับใช้กฎหมายดังกล่าวพบข้อจำกัดหลายประการ ปรากฏว่าผู้กระทำความผิดอาชญากรรมทางเทคโนโลยีมีการโอนเงินที่ได้จากการกระทำความผิดผ่านช่องทาง การซื้อขายสินทรัพย์ดิจิทัล ที่ไม่ได้รับอนุญาตตามกฎหมายว่าด้วยการประกอบธุรกิจสินทรัพย์ดิจิทัล ส่งผลให้เกิดอุปสรรคในการตรวจสอบธุรกรรมและติดตามนำเงินคืนแก่ผู้เสียหาย นอกจากนี้ ยังไม่มีมาตรการในการระงับการใช้เลขหมายโทรศัพท์เคลื่อนที่ซึ่งเป็นเครื่องมือสำคัญที่ถูกใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี รวมถึงอาชญากรรมฟอกเงินตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน อีกทั้งกระบวนการในการคืนเงินแก่ผู้เสียหายยังล่าช้า ทำให้ผู้เสียหายไม่ได้รับการเยียวยาอย่างทัน่วงที ปัญหายังรวมถึงการกระทำความผิดเกี่ยวกับการพนันออนไลน์ การละเมิดข้อมูลส่วนบุคคล และการแสวงหา

ผลประโยชน์จากความผิดพลาดนี้ ซึ่งล้วนเป็นพฤติกรรมที่สามารถนำไปสู่อาชญากรรมทางเทคโนโลยีในรูปแบบที่ซับซ้อนมากยิ่งขึ้น ขณะเดียวกันยังพบว่า บางสถาบันการเงินและผู้ประกอบธุรกิจขาดมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างเพียงพอ ทำให้เกิดช่องว่างให้ผู้กระทำความผิดอาศัยจุดอ่อนของระบบการเงินก่ออาชญากรรม สร้างความเสียหายแก่ประชาชนและประเทศชาติในวงกว้าง<sup>3</sup>

จากสถิติระหว่างเดือนตุลาคม 2566 ถึงพฤศจิกายน 2567 พบว่า มีคดีอาชญากรรมทางเทคโนโลยีเกิดขึ้นมากถึง 402,542 คดี คิดเป็นมูลค่าความเสียหายรวมกว่า 42,662 ล้านบาท ซึ่งสะท้อนให้เห็นถึงความไม่เพียงพอของมาตรการตามพระราชกำหนดฯ ดังกล่าว ด้วยเหตุนี้ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจึงเห็นถึงความจำเป็นเร่งด่วนในการแก้ไขเพิ่มเติมพระราชกำหนดฯ พ.ศ. 2566 เพื่อเพิ่มมาตรการที่มีประสิทธิภาพยิ่งขึ้นในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีและกลุ่มมิจฉาชีพในโลกออนไลน์<sup>4</sup>

พระราชกำหนดฯ ด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 จึงได้ถูกตราขึ้นมาเพื่อเป็นเครื่องมือทางกฎหมายที่มีความทันสมัย ครอบคลุม และสามารถใช้ตอบสนองต่อภัยคุกคามในโลกไซเบอร์ได้อย่างมีประสิทธิภาพ โดยเฉพาะในประเด็นที่เกี่ยวข้องกับการกระทำผิดของขบวนการอาชญากรรมข้ามชาติ ซึ่งมักมีความซับซ้อนทั้งในเชิงโครงสร้างวิธีการ และการข้ามเขตอำนาจศาล จึงจำเป็นต้องมีการพัฒนากฎหมายที่สามารถตอบโจทย์ปัญหาได้ในระดับสากล

เจ้าหน้าที่ตำรวจ โดยเฉพาะเจ้าหน้าที่ตำรวจที่ปฏิบัติหน้าที่ด้านเทคโนโลยีและอาชญากรรมข้ามชาติ จึงมีบทบาทสำคัญในฐานะกลไกหลักของรัฐที่ต้องปฏิบัติการในเชิงรุกและป้องกันควบคู่ไปกับการบังคับใช้กฎหมาย บทบาทของเจ้าหน้าที่ตำรวจในกระบวนการนี้จึงไม่ได้มีเพียงแค่การจับกุมผู้กระทำความผิดเท่านั้น แต่ยังรวมถึงการรวบรวมพยานหลักฐาน การวิเคราะห์ข้อมูลข่าวกรองการปฏิบัติการร่วมกับหน่วยงานในประเทศและต่างประเทศ ตลอดจนการป้องกันภัยล่วงหน้าผ่านการเฝ้าระวังเชิงเทคโนโลยี ด้วยการประยุกต์ใช้เทคโนโลยีและนวัตกรรมสารสนเทศอย่างมีประสิทธิภาพ ประสานงานและปฏิบัติการร่วมกับหน่วยงานที่เกี่ยวข้องทั้งในระดับประเทศและระดับนานาชาติ ซึ่งเป็นสิ่งจำเป็นอย่างยิ่งในยุคที่อาชญากรรมข้ามชาติขยายตัวและซับซ้อนมากขึ้น บทบาทเชิงรุกนี้สะท้อนให้เห็นถึงความจำเป็นในการพัฒนาศักยภาพและความเชี่ยวชาญของเจ้าหน้าที่ตำรวจอย่างต่อเนื่อง เพื่อให้สามารถรับมือกับภัยคุกคามในยุคดิจิทัลได้อย่างมีประสิทธิภาพและยั่งยืน การศึกษาและวิเคราะห์บทบาทของเจ้าหน้าที่ตำรวจภายใต้กรอบกฎหมายใหม่อย่างพระราชกำหนดฉบับนี้จึงมีความจำเป็นอย่างยิ่ง สอดคล้องกับเป้าหมายของนโยบายความมั่นคงของรัฐที่มุ่งเน้นการเสริมสร้างกลไกความมั่นคงในโลกไซเบอร์ โดยเฉพาะการใช้กฎหมายเป็นเครื่องมือควบคุมพฤติกรรมที่เป็นภัยคุกคามผ่านระบบดิจิทัล การศึกษาบทบาทของตำรวจภายใต้กฎหมายฉบับใหม่นี้จึงสามารถเสนอแนะเชิงนโยบายและแนวทางการพัฒนาที่นำไปสู่การเพิ่มประสิทธิภาพของกระบวนการบังคับใช้กฎหมายในภาพรวมได้อย่างชัดเจน

<sup>3</sup> สำนักงานเลขาธิการคณะรัฐมนตรี, “ร่างพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ ...) พ.ศ. ...,” แก้ไขครั้งล่าสุด 2568, สืบค้นเมื่อ 2 กุมภาพันธ์ 2568, [https://www.resolution.soc.go.th/?prep\\_id=412882/](https://www.resolution.soc.go.th/?prep_id=412882/)

<sup>4</sup> สำนักเลขาธิการนายกรัฐมนตรี, “สรุปข่าวการประชุม ครม.,” แก้ไขครั้งล่าสุด 2568, สืบค้นเมื่อ 2 กุมภาพันธ์ 2568, [https://www.thaigov.go.th/news/contents/ministry\\_details/92827/](https://www.thaigov.go.th/news/contents/ministry_details/92827/)

การศึกษาบทบาทของตำรวจในมิตินี้จึงไม่ได้เป็นเพียงการพิจารณาภารกิจเชิงปฏิบัติเท่านั้น แต่ยังรวมถึงการวิเคราะห์ความสามารถในการตอบสนองเชิงนโยบาย การบูรณาการข้อมูลข่าวกรอง และการดำเนินการเชิงยุทธศาสตร์ที่มีประสิทธิภาพ งานวิจัยนี้ยังมีความมุ่งหมายที่จะเสนอแนวทางสนับสนุนเชิงวิชาการต่อการออกแบบนโยบาย การปรับปรุงกลไกความร่วมมือระหว่างประเทศ ตลอดจนการยกระดับขีดความสามารถของเจ้าหน้าที่ตำรวจให้สอดคล้องกับบริบทของความมั่นคงสมัยใหม่ ซึ่งต้องอาศัยทั้งเครื่องมือทางเทคโนโลยี ความรู้ด้านกฎหมายระหว่างประเทศและความเข้าใจเชิงลึกเกี่ยวกับธรรมชาติของเครือข่ายอาชญากรรมข้ามชาติ และผลการศึกษายังสามารถเป็นพื้นฐานในการกำหนดแนวทางการฝึกอบรมเจ้าหน้าที่ การจัดสรรทรัพยากร และการสร้างกลไกสนับสนุนจากภาคีที่เกี่ยวข้อง อันจะช่วยยกระดับการบังคับใช้กฎหมายของไทยให้สามารถเผชิญหน้ากับภัยคุกคามระดับโลกได้อย่างมีประสิทธิภาพและยั่งยืน

## 1.2 วัตถุประสงค์

1.2.1 เพื่อศึกษาบทบาทของเจ้าหน้าที่ตำรวจในการป้องกันและปราบปรามอาชญากรรมข้ามชาติภายใต้พระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568

1.2.2 เพื่อเสนอแนวทางในการพัฒนาบทบาทและศักยภาพของเจ้าหน้าที่ตำรวจให้สอดคล้องกับการเผชิญภัยคุกคามจากอาชญากรรมข้ามชาติในยุคดิจิทัล

## 1.3 ขอบเขตการวิจัย

การศึกษานี้ มุ่งศึกษาเชิงเนื้อหาในการศึกษาบทบาทของเจ้าหน้าที่ตำรวจภายใต้พระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 โดยมีขอบเขตผู้ให้ข้อมูลสำคัญ ได้แก่ เจ้าหน้าที่ตำรวจที่มีหน้าที่เกี่ยวข้องโดยตรงกับการป้องกันและปราบปรามอาชญากรรมข้ามชาติในมิติทางเทคโนโลยี เจ้าหน้าที่ระดับนโยบายหรือผู้กำกับดูแลด้านกฎหมายไซเบอร์ ผู้เชี่ยวชาญด้านกฎหมายอาญา เทคโนโลยี และความมั่นคงไซเบอร์ ตัวแทนจากหน่วยงานร่วมปฏิบัติ โดยการคัดเลือกผู้ให้ข้อมูลจะยึดหลักเจตจำนงในการให้ข้อมูลอย่างตรงไปตรงมา มีความเกี่ยวข้องกับภารกิจตามวัตถุประสงค์ของการวิจัยและมีประสบการณ์เชิงปฏิบัติจริง

## 1.4 ระเบียบวิธีวิจัย

การดำเนินการวิจัยในครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยใช้วิธีการศึกษาค้นคว้าจากเอกสาร (Documentary Study) เพื่อวิเคราะห์และสังเคราะห์องค์ความรู้พื้นฐานเกี่ยวกับกฎหมายกลไกการบังคับใช้ บริบทของอาชญากรรมข้ามชาติในยุคดิจิทัล และกฎหมายที่ใช้ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และจะสัมภาษณ์ผู้ให้ข้อมูลสำคัญที่มีบทบาทในการปฏิบัติงานจริง โดยใช้การสัมภาษณ์แบบมีโครงสร้าง (Structured Interview) ควบคู่กับการสื่อสารแบบสองทาง (Two-way Communication) เพื่อให้ได้ข้อมูลที่ลึกซึ้ง ชัดเจนและสะท้อนมุมมองจากภาคปฏิบัติที่เกี่ยวข้องกับบทบาทของเจ้าหน้าที่ตำรวจภายใต้พระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 อย่างรอบด้าน

## 1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ทราบบทบาทของเจ้าหน้าที่ตำรวจในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ ภายใต้พระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568

1.5.2 เสนอแนวทางในการพัฒนาบทบาทและศักยภาพของเจ้าหน้าที่ตำรวจให้สอดคล้องกับการเผชิญภัยคุกคามจากอาชญากรรมข้ามชาติในยุคดิจิทัล

## 2. ผลการศึกษาวิจัย

จากการศึกษาเรื่องบทบาทของเจ้าหน้าที่ตำรวจในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ ภายใต้พระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 พบว่า พระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 กำหนดให้เจ้าหน้าที่ตำรวจมีอำนาจหน้าที่ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีอย่างครอบคลุม ซึ่งถือเป็นการเปลี่ยนแปลงจากการปฏิบัติแบบเดิมที่เน้นการปราบปรามหลังเกิดเหตุ แนวทางใหม่นี้ จึงมีความทันสมัยและสอดคล้องกับลักษณะของอาชญากรรมข้ามชาติที่มีการวางแผนและดำเนินการอย่างซับซ้อน ดังต่อไปนี้

### 2.1 การควบคุมการเปิดบัญชี ระวังการให้บริการหรือการทำธุรกรรม หรือปิดบัญชี กับบุคคลที่เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยี

บทบาทของเจ้าหน้าที่ตำรวจในฐานะส่วนหนึ่งของโครงสร้างของศูนย์ป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี หรือ ศปอท. มีได้จำกัดอยู่เพียงการสืบสวนสอบสวนในเชิงรับ แต่กลับมีลักษณะ “การควบคุมเชิงระบบ” ตำรวจไม่เพียงมีหน้าที่รวบรวมพยานหลักฐานหรือติดตามตัวผู้กระทำความผิดเท่านั้น แต่ยังเป็นกลไกที่เชื่อมโยงกับโครงสร้างของระบบการเงินดิจิทัลในการ สกัดกั้น และป้องกันความเสียหายทางเศรษฐกิจ และยังสร้าง “พันธมิตรร่วม” ระหว่างตำรวจกับภาคการเงิน เจ้าหน้าที่ตำรวจไม่ได้เป็นเพียงผู้ใช้กฎหมาย แต่เป็นผู้ควบคุมจุดตัดสำคัญในโครงสร้างทางเศรษฐกิจ อันมีความเสี่ยงต่อการถูกแสวงหาประโยชน์ในทางมิชอบ หากปราศจากกลไกนี้ กระบวนการฟอกเงินดิจิทัลผ่านระบบธนาคารหรือแพลตฟอร์มคริปโตอาจไม่สามารถหยุดยั้งได้ทันเวลา

### 2.2 แนวคิดทฤษฎีและความเป็นมาของมาตรการการลงโทษในคดีค้ำมนุษย์ของประเทศไทย

บทบัญญัติดังกล่าวมุ่งเน้นให้เจ้าหน้าที่ตำรวจ โดยเฉพาะสำนักงานตำรวจแห่งชาติมีบทบาทสำคัญในการตรวจสอบและจัดการกับการใช้บริการโทรคมนาคมที่เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยี โดยเฉพาะในกรณีที่ปรากฏพยานหลักฐานอันควรเชื่อได้ว่า เบอร์โทรศัพท์ บริการเครือข่าย หรือแพลตฟอร์มการสื่อสาร ถูกใช้เป็นเครื่องมือในการกระทำความผิด บทบาทแรกของเจ้าหน้าที่ตำรวจในกรณีนี้คือ การตรวจสอบและประเมินพยานหลักฐาน ซึ่งอาจมาจากการสืบสวนสอบสวนโดยตรง หรือการประมวลข้อมูลที่ได้จากหน่วยงานอื่น เช่น ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.) หรือ กรมสอบสวนคดีพิเศษ (Department of Special Investigation: DSI) การมีอำนาจในการประเมินความน่าเชื่อถือของพยานหลักฐาน ทำให้สำนักงานตำรวจแห่งชาติสามารถมีบทบาทเป็น “ผู้เริ่มต้นกระบวนการควบคุมความเสี่ยง” ในเชิงนโยบายและเทคโนโลยี

บทบาทต่อมาคือ การแจ้งให้สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ดำเนินการสั่งการต่อผู้ให้บริการเครือข่าย ซึ่งเป็นขั้นตอนสำคัญในการแปลงอำนาจการสืบสวนของตำรวจให้กลายเป็นกลไกที่สามารถปิดกั้นพฤติกรรมอาชญากรรมได้ทันที ตำรวจจึงไม่ได้เพียงแค่สืบสวนหรือจับกุม แต่เป็น “ตัวกลาง” ที่มีหน้าที่ประสานการสั่งระงับบริการโทรคมนาคมซึ่งเป็นโครงสร้างพื้นฐานที่อาชญากรใช้ในการกระทำผิด

ภายใต้กลไกดังกล่าว การสั่งระงับการให้บริการโทรคมนาคมต้องอาศัยความร่วมมือข้ามหน่วยงาน โดยสำนักงานตำรวจแห่งชาติเป็นหนึ่งในผู้ที่มีสิทธิร่วมตัดสินใจ ร่วมกับกรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน หรือ ป.ป.ง. และ กิจการโทรคมนาคมแห่งชาติ ทั้งในส่วนของ การระงับบริการและการ “ยกเลิกการระงับบริการ” เมื่อไม่ปรากฏพฤติการณ์หรือพยานหลักฐานเพิ่มเติม การมีบทบาทร่วมกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขเช่นนี้ ทำให้สำนักงานตำรวจแห่งชาติต้องปฏิบัติหน้าที่ด้วยความรอบคอบ มีข้อมูลสนับสนุนที่ชัดเจน และสามารถรับผิดชอบต่อผลกระทบที่เกิดขึ้นต่อผู้ใช้งานโทรคมนาคม เพื่อให้หน่วยงานที่มีอำนาจควบคุมการสื่อสารดำเนินการในรูปแบบที่ถูกต้องตามกฎหมายและไม่ละเมิดสิทธิขั้นพื้นฐานของประชาชนโดยไม่จำเป็น

### 2.3 การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์หรือนำข้อมูลคอมพิวเตอร์ที่ผิดกฎหมาย ออกจากระบบคอมพิวเตอร์ในกรณีที่มีการประกอบธุรกิจสินทรัพย์ดิจิทัลโดยไม่ได้รับอนุญาต

บทบาทของเจ้าหน้าที่ตำรวจในมาตรานี้จึงมีลักษณะเชิงตอบสนองฉับพลันต่อภัยคุกคามทางเศรษฐกิจและเทคโนโลยี ที่เกิดขึ้นผ่านเครือข่ายอินเทอร์เน็ต ซึ่งอาจมีลักษณะเร่งด่วน การที่เจ้าหน้าที่ตำรวจสามารถสั่งระงับการแพร่กระจายของข้อมูลเหล่านี้ได้ “โดยพลัน” แสดงถึงอำนาจเฉพาะตัวในระดับปฏิบัติการ ซึ่งต้องอาศัยดุลยพินิจที่เฉียบคมและทันต่อสถานการณ์ ในทางปฏิบัติเจ้าหน้าที่ตำรวจจึงมีหน้าที่ทั้งในเชิงการสืบสวนสอบสวน และการบริหารจัดการภัยไซเบอร์ ผ่านการควบคุมเนื้อหาในระบบดิจิทัล ต้องมีเครื่องมือเทคโนโลยี และกำลังเจ้าหน้าที่ที่มีความเชี่ยวชาญด้านไซเบอร์อย่างเพียงพอ ตลอดจนต้องมีระบบเฝ้าระวังและรายงาน (Cyber Threat Intelligence) ที่สามารถระบุภัยคุกคามในลักษณะเรียลไทม์ (Real-Time) ซึ่งสิ่งเหล่านี้จำเป็นต้องมีการลงทุนและพัฒนาศักยภาพอย่างต่อเนื่องภายในสำนักงานตำรวจแห่งชาติ

### 2.4 การคืนเงินแก่ผู้เสียหายจากอาชญากรรมทางเทคโนโลยี

เจ้าหน้าที่ตำรวจมีบทบาทสำคัญในฐานะ หน่วยเก็บ รวบรวม และประมวลผลข้อมูลทางการเงินเชิงพฤติกรรมที่เกี่ยวข้องกับการกระทำผิด ตำรวจต้องมีความสามารถในการวิเคราะห์ธุรกรรมและสื่อสารกับสถาบันการเงินเพื่อให้ได้มาซึ่งข้อมูลที่เชื่อมโยงกับขบวนการอาชญากรรมในลักษณะเครือข่าย การที่ตำรวจต้องส่งรายงานไปยังสำนักงานป้องกันและปราบปรามการฟอกเงินยังแสดงถึงบทบาทในการสนับสนุน กระบวนการป้องกันการฟอกเงินโดยตรง ซึ่งเป็นแนวทางใหม่ของการบังคับใช้กฎหมายในเชิงรุก ที่มุ่งเน้นไม่เพียงแต่การจับกุมผู้กระทำผิดเท่านั้น แต่ยังรวมถึงการติดตามทรัพย์สินที่ได้มาจากอาชญากรรม และการช่วยเหลือผู้เสียหายให้ได้รับเงินคืนอย่างเป็นธรรม ซึ่งเจ้าหน้าที่ตำรวจจะมีบทบาทเกี่ยวข้องกับการยืนยันข้อเท็จจริงทางคดี การประสานข้อมูลและสนับสนุนการสอบสวนเสริม หากสำนักงานป้องกันและปราบปรามการฟอกเงินการดูแลความสงบเรียบร้อยกรณีมีข้อขัดแย้งหากมีข้อพิพาทหรือการคัดค้านผลการคืน

## 2.5 การจัดตั้งศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

บทบาทของตำรวจในศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ไม่ได้จำกัดเพียงแค่การปฏิบัติงานทางเทคนิคหรือการสืบสวนสอบสวนเท่านั้น แต่ยังรวมถึงการทำหน้าที่เป็น ตัวกลางสำคัญในการสื่อสารนโยบายของสำนักงานตำรวจแห่งชาติ ไปยังหน่วยงานและผู้มีส่วนได้ส่วนเสียอื่น ๆ เพื่อให้แน่ใจว่าการปฏิบัติหน้าที่สอดคล้องกับกรอบกฎหมายและนโยบายที่เกี่ยวข้อง ทั้งนี้ยังต้องเสนอแนวทาง และมาตรการบังคับใช้กฎหมายที่เหมาะสมและยืดหยุ่น เพื่อตอบสนองต่อสถานการณ์ของอาชญากรรมทาง เทคโนโลยีที่มีความเปลี่ยนแปลงอย่างรวดเร็วและความหลากหลาย ทั้งในแง่ของวิธีการ กระบวนการ และ เทคโนโลยีที่ถูกใช้โดยผู้กระทำความผิด การมีตำรวจที่ได้รับการแต่งตั้งใน ศปอท. จึงเป็นกุญแจสำคัญที่จะช่วย สร้างความต่อเนื่องในกระบวนการบังคับใช้กฎหมาย รวมถึงเพิ่มประสิทธิภาพในการประสานงานเชิงกลยุทธ์และ การวางแผนป้องกันปราบปราม

### 2.6 ความรับผิดชอบทางแพ่งของสถาบันการเงินหรือผู้ประกอบการธุรกิจ ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น ผู้ให้บริการอื่นที่เกี่ยวข้อง หรือผู้ให้บริการสื่อสังคมออนไลน์ ในความเสียหายที่เกิดจากอาชญากรรมทางเทคโนโลยี

บทบาทสำคัญของตำรวจภายใต้มาตรานี้คือการรวบรวม หลักฐานเชิงระบบ เพื่อใช้ประกอบการ ชี้ให้เห็นว่า ผู้ให้บริการรายใด ละเลย มาตรการป้องกันที่ควรมีและปล่อยให้เกิดช่องว่างที่อาชญากรใช้แทรกซึม หากเจ้าหน้าที่ตำรวจสามารถพิสูจน์ได้ว่าสถาบันใดบกพร่องในหน้าที่ ก็จะทำให้ผู้เสียหายสามารถเรียกร้องความ รับผิดชอบหรือค่าชดเชยได้ตามกฎหมาย โดยตำรวจมีหน้าที่จัดทำสำนวน ประกอบพยานหลักฐาน และให้ข้อมูลต่อ หน่วยงานที่มีอำนาจตัดสินใจพิพาทหรือดำเนินการลงโทษเพิ่มเติม

## 2.7 เพิ่มบทกำหนดโทษอาญา

การเพิ่มบทลงโทษทางแพ่งและอาญาสำหรับความผิดทางเทคโนโลยี เจ้าหน้าที่ตำรวจมีบทบาท สำคัญในการสอบสวนและดำเนินคดี โดยเฉพาะในกรณีที่นิติบุคคลหรือผู้ให้บริการไม่ปฏิบัติตามคำสั่งของศูนย์ ปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.) หรือละเลยคำสั่งโดยจงใจ ตำรวจต้องตรวจสอบเส้นทางบัญชี ที่เกี่ยวข้อง การแจ้งเตือน และการสั่งการภายใน หากพบความบกพร่องโดยรู้เห็นเป็นใจ สามารถดำเนินคดีอาญา ต่อกรรมการหรือผู้จัดการได้ นอกจากนี้ ตำรวจยังต้องรับผิดชอบในการรวบรวมหลักฐานและดำเนินคดีกับผู้ ที่ฝ่าฝืนคำสั่ง เช่น เจ้าของเว็บไซต์/เพจที่ไม่ลบข้อมูลสินทรัพย์ดิจิทัลผิดกฎหมาย หรือผู้ให้บริการโฮสติ้งที่เพิกเฉย โดยต้องทำงานร่วมกับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมในการสืบสวนและออกหมายจับ อีกบทบาทสำคัญ คือการตรวจสอบซิมการ์ดที่เชื่อมโยงกับบัญชีม้าหรือกระเป๋าสินทรัพย์ดิจิทัลที่ใช้ในการหลอกลวง หากพบการ ลงทะเบียนปลอม สามารถตรวจสอบย้อนหลังถึงผู้ขายและดำเนินคดี รวมถึงสืบหาเครือข่ายอาชญากรรมข้ามชาติ ที่เกี่ยวข้องกับการจำหน่ายซิมการ์ดผิดกฎหมายได้ด้วย

โดยสรุปแล้วมาตรา 5 และมาตรา 7/1 ได้วางบทบาทของเจ้าหน้าที่ตำรวจไว้อย่างชัดเจนในฐานะ ผู้มีอำนาจในการสั่งระงับบริการทางโทรคมนาคมหรือข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิด ซึ่งแสดงให้เห็นถึงอำนาจเชิงบริหารของตำรวจในฐานะผู้ควบคุมช่องทางของความเสียหาย มิใช่เพียงรอให้มีการ กระทำความผิดเกิดขึ้นแล้วจึงเข้าไปจับกุม แต่สามารถแทรกแซงก่อนที่ความเสียหายจะเกิดขึ้นจริงในระดับวงกว้าง

และแสดงถึงการจัดการกับโครงสร้างสถานการณ์ที่อาจนำไปสู่ความเสียหายทางอาชญากรรมล่วงหน้าอย่างมีประสิทธิภาพ ไม่ใช่รอเพียงการจับกุมผู้กระทำผิดเท่านั้น แต่เป็นการลดแรงจูงใจและโอกาสในการก่ออาชญากรรมที่สอดคล้องกับแนวคิดว่าการออกแบบหรือปรับเปลี่ยนสภาพแวดล้อมในเชิงระบบสามารถทำให้อาชญากรรมมือได้ยากและเสี่ยงมากขึ้น

ในขณะที่มาตรา 8/1 และมาตรา 8/2 ได้แสดงให้เห็นถึงบทบาทของตำรวจในกระบวนการวิเคราะห์และคืนเงินให้แก่ผู้เสียหาย โดยการรายงานข้อมูลธุรกรรมและการมีส่วนร่วมกับสำนักงานป้องกันและปราบปรามการฟอกเงินในการตรวจสอบและประกาศบัญชีต้องสงสัย การดำเนินการเหล่านี้ต้องอาศัยความร่วมมือระหว่างหน่วยงานและการตัดสินใจบนฐานข้อมูลที่ซับซ้อน ตำรวจจึงต้องมีทั้งความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความเข้าใจในกฎหมายฟอกเงินควบคู่กันไป และยังคงสะท้อนถึงการใช้อ้างอิงข้อมูลและการประสานงานข้ามหน่วยงานเพื่อบริหารความเสี่ยงอย่างเป็นระบบตามหลักการของทฤษฎีรูปแบบกิจกรรมตามกิจวัตรประจำวัน (Routine Activity Theory)<sup>5</sup> ที่ชี้ให้เห็นว่า อาชญากรรมเกิดขึ้นเมื่อมีผู้กระทำผิดที่มีแรงจูงใจ พบกับเหยื่อที่เหมาะสมในสภาพแวดล้อมที่ขาดการป้องกันที่มีประสิทธิภาพ การมีตำรวจทำหน้าที่ประสานงานตรวจสอบข้อมูลธุรกรรมและเฝ้าระวังบัญชีที่เกี่ยวข้อง จึงเป็นการเพิ่ม “ผู้ป้องกันที่มีประสิทธิภาพ” เพื่อป้องกันไม่ให้อาชญากรรมเกิดขึ้นได้ง่าย

มาตรา 8/5 ถึง มาตรา 8/6 ได้จัดตั้ง “ศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี” หรือ ศปอท. ซึ่งสำนักงานตำรวจแห่งชาติเป็นหนึ่งในหน่วยงานหลักที่ส่งเจ้าหน้าที่เข้าร่วมปฏิบัติงานภายในศูนย์ฯ บทบาทของตำรวจภายใน ศปอท. ไม่ได้จำกัดแค่การปราบปรามอาชญากรรมแต่รวมถึงการบริหารข้อมูล การติดตามตรวจสอบบัญชีต้องสงสัย การแลกเปลี่ยนข้อมูลข้ามหน่วยงาน และการเผยแพร่ข้อมูลเพื่อประโยชน์สาธารณะ ทั้งหมดนี้แสดงให้เห็นถึงภาพของ “ตำรวจในฐานะกลไกปกครอง” (Governance Actor) ที่ไม่ได้จำกัดอยู่กับหน้าที่ปฏิบัติการภาคสนามเท่านั้นแสดงให้เห็นถึงการสร้าง “กลไกการป้องกันเชิงสถานการณ์” ที่รวมหน่วยงานต่าง ๆ ไว้ด้วยกัน ตำรวจที่เข้าร่วมปฏิบัติงานใน ศปอท. จึงมีบทบาทสำคัญในการแลกเปลี่ยนข้อมูล การติดตามตรวจสอบและการส่งระงับธุรกรรมที่อาจเป็นช่องทางของอาชญากรรม ซึ่งเป็นการใช้การบริหารจัดการสถานการณ์ในระดับโครงสร้างโดยตรง

มาตรา 8/10 ถึง มาตรา 8/12 ได้เน้นย้ำให้เห็นว่าในการควบคุมอาชญากรรมเทคโนโลยี ตำรวจไม่สามารถทำงานเพียงลำพัง แต่ต้องอาศัยการบังคับใช้กฎหมายร่วมกับภาคเอกชนและกำกับให้ผู้ให้บริการเครือข่ายโทรคมนาคม หรือสถาบันการเงิน ต้องรับผิดชอบร่วมกันในความเสียหายที่เกิดขึ้น หากละเลยไม่ปฏิบัติตามมาตรการป้องกันที่กำหนดไว้โดยหน่วยงานกำกับดูแล บทบัญญัติเหล่านี้มอบอำนาจให้ตำรวจเป็นกลไกในการคานอำนาจตลาด และรักษาสมดุลของผลประโยชน์สาธารณะ สอดคล้องกับแนวคิดการป้องกันอาชญากรรมเชิงสถานการณ์ที่เน้นการปรับระบบหรือสภาพแวดล้อมให้ไม่เหมาะสมต่อการกระทำผิด เช่น การกำหนดมาตรฐานและมาตรการป้องกันในเครือข่ายโทรคมนาคมและการเงินที่ช่วยลดโอกาสการเกิดอาชญากรรมโดยรวม

<sup>5</sup> Cohen and M. Felson, “Social Change and Crime Rate Trends: A Routine Activity Approach,” *American Sociological Review* 44, no. 4 (August 1979): 588–608.

มาตรา 11/1 และมาตรา 11/2 สะท้อนบทบาทของตำรวจในเชิงจริยธรรมและความมั่นคงของข้อมูลส่วนบุคคล ตำรวจมีหน้าที่ในการติดตาม ตรวจสอบ และนำผู้กระทำความผิดเกี่ยวกับการใช้ข้อมูลบัตรประชาชน หรือข้อมูลของผู้เสียชีวิตไปดำเนินคดีตามกฎหมาย มาตรา 11/1 เน้นให้เห็นว่าอาชญากรรมในโลกยุคดิจิทัลไม่ได้เกี่ยวข้องกับเฉพาะการหลอกลวงทางการเงิน แต่รวมถึงการละเมิดข้อมูลส่วนบุคคล ซึ่งเป็นรากฐานของความมั่นคงในยุคข้อมูลข่าวสาร การกระจายอำนาจให้แก่ตำรวจในหลายมาตราเป็นภาพสะท้อนของการยกระดับภารกิจของตำรวจให้สอดคล้องกับอาชญากรรมในบริบทใหม่ ภายใต้หลักการของ “การบริหารจัดการความเสี่ยง” มากกว่าการบังคับใช้กฎหมายแบบเน้นเฉพาะการจับกุม โดยตำรวจจำเป็นต้องมีความสามารถในการวิเคราะห์สถานการณ์เชิงระบบ ประเมินความเชื่อมโยงของข้อมูล และใช้ดุลยพินิจในการเลือกวิธีตอบสนองที่เหมาะสมกับสถานการณ์ การเปลี่ยนผ่านบทบาทของตำรวจนี้สอดคล้องกับแนวคิดเชิงทฤษฎีสมัยใหม่ เช่น แนวคิดของมิลเลอร์ (Miller) ที่มองว่าตำรวจ คือ ผู้มีบทบาทในการกำกับดูแล (Governance Actor)<sup>6</sup> และแนวคิดของโจบาร์ด (Jobard) ที่เสนอว่าตำรวจคือผู้ปฏิบัติงานที่ต้องทำหน้าที่ทั้งการคุ้มครองสาธารณะ การจัดการชุมชน และการเป็นกลไกทางการเมือง โดยทั้งหมดนี้ไม่อาจแยกขาดจากกัน เพราะตำรวจในยุคเทคโนโลยีมีได้ทำหน้าที่เพียง “จับฟ้อง จำคุก” หากแต่เป็นกลไกสำคัญของรัฐในการรักษาความมั่นคง ความสงบและความยุติธรรมในชีวิตประจำวันของประชาชน และแสดงให้เห็นถึงการยกระดับบทบาทของตำรวจในฐานะ “ผู้บริหารจัดการสถานการณ์” ที่ใช้มาตรการป้องกันเชิงสถานการณ์อย่างครบวงจร ตั้งแต่การสั่งระงับบริการที่เสี่ยง การประสานงานและเฝ้าระวังข้อมูลธุรกรรม จนถึงการร่วมมือกับภาคเอกชนและหน่วยงานต่าง ๆ เพื่อสร้างระบบป้องกันที่เข้มแข็งและมีประสิทธิภาพ ซึ่งสอดคล้องกับแนวคิดทฤษฎีสมัยใหม่ทั้งในมิติการบริหารจัดการความเสี่ยงและการป้องกันโอกาสในการก่ออาชญากรรมอย่างเป็นระบบและยั่งยืน<sup>7</sup> ซึ่งพระราชกำหนดฉบับนี้ได้สะท้อนให้เห็นถึงความเข้าใจที่ลึกซึ้งเกี่ยวกับบริบทของอาชญากรรมทางเทคโนโลยี และได้ออกแบบบทบาทของตำรวจให้สอดคล้องกับโลกที่เปลี่ยนแปลงไป โดยตำรวจต้องทำหน้าที่มากกว่าการบังคับใช้กฎหมายอย่างแยกส่วน หากแต่ต้องมีบทบาทในฐานะผู้บริหารจัดการสถานการณ์และความเสี่ยงในเชิงโครงสร้าง ภายใต้กรอบกฎหมายที่สร้างความชอบธรรม ความชัดเจน และความไว้วางใจจากสังคม

### 3. สรุปผล และข้อเสนอแนะ

จากการศึกษาเรื่องบทบาทของเจ้าหน้าที่ตำรวจในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ ภายใต้พระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 ผู้เขียนสามารถสรุปผลและเสนอแนะดังต่อไปนี้

#### 3.1 สรุปผล

ในยุคที่อาชญากรรมทางเทคโนโลยีมีความซับซ้อนและแพร่หลายอย่างรวดเร็ว พระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 ได้ถูกตราขึ้นเพื่อวางกลไกการบังคับใช้กฎหมายให้สามารถรับมือกับภัยคุกคามยุคดิจิทัลอย่างมีประสิทธิภาพ โดยเฉพาะการวางโครงสร้าง

<sup>6</sup> E. J. Miller, “The Concept of the Police,” *Criminal Law and Philosophy* 17, no. 3 (September 2023): 573–595.

<sup>7</sup> F. Jobard, *Conceptualizing of Police* (New York: Springer, 2014), 65.

ให้เจ้าหน้าที่ของรัฐ โดยเฉพาะเจ้าหน้าที่ตำรวจมีบทบาทเชิงรุกทั้งในระดับการเฝ้าระวัง การระงับเหตุ การสืบสวน สอบสวน และการเยียวยาความเสียหายให้แก่ประชาชนผู้เสียหายจากอาชญากรรมประเภทนี้ บทบาทของเจ้าหน้าที่ตำรวจในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ ภายใต้พระราชกำหนดฉบับนี้มีได้จำกัดอยู่เพียงการจับกุมผู้กระทำความผิดตามประมวลกฎหมายอาญา แต่ได้ขยายขอบเขตไปสู่การมีส่วนร่วมในกระบวนการจัดการเชิงโครงสร้างของสังคม เช่น การแจ้งเตือน การสั่งระงับธุรกรรม การร้องขอข้อมูล และการประสานงานกับหน่วยงานกำกับดูแลหลายฝ่าย ซึ่งอาจกล่าวได้ว่าสะท้อนถึงการเปลี่ยนผ่านจากบทบาทตำรวจในฐานะ “ผู้บังคับใช้กฎหมาย” ไปสู่บทบาทใหม่ในฐานะ “ผู้บริหารจัดการสถานะความเสี่ยงของสังคม” จากบทบาทด้านต่าง ๆ ดังนี้

ประการแรก คือ บทบาทด้านการบังคับใช้กฎหมาย (Law Enforcement Role) ซึ่งยังคงเป็นรากฐานหลักของการปฏิบัติหน้าที่ของตำรวจ แต่ภายใต้บริบทของพระราชกำหนดฉบับใหม่นี้ บทบาทดังกล่าวได้ถูกขยายขอบเขตไปสู่การปฏิบัติที่อิงกับเทคโนโลยี โดยเฉพาะในกรณีของอาชญากรรมไซเบอร์ที่มีลักษณะซับซ้อนและใช้เครื่องมือดิจิทัลในการซ่อนตัว ตำรวจต้องสามารถใช้เครื่องมือทางกฎหมายในการเข้าถึงข้อมูลดิจิทัล สืบค้นแหล่งที่มาของการกระทำความผิด และพิสูจน์ทรัพย์สินที่เกี่ยวข้อง เพื่อให้สามารถดำเนินคดีได้ตามกระบวนการยุติธรรมอย่างมีประสิทธิภาพ

ประการที่สอง คือ บทบาทด้านการป้องกันล่วงหน้าและการเฝ้าระวังเชิงเทคโนโลยี (Preventive and Surveillance Role) โดยเฉพาะในยุคที่การก่ออาชญากรรมสามารถเกิดขึ้นผ่านระบบอินเทอร์เน็ตโดยไม่มีการปรากฏตัวทางกายภาพ เจ้าหน้าที่ตำรวจต้องพัฒนาแนวทางในการคาดการณ์ภัยล่วงหน้า เช่น การเฝ้าระวังเว็บไซต์ต้องสงสัย การตรวจสอบบัญชีต้องห้าม หรือการวิเคราะห์ข้อมูลโซเชียลมีเดีย เพื่อป้องกันมิให้เกิดความเสียหายขึ้นก่อนที่จะมีผู้เสียหายจริง แนวทางดังกล่าวสะท้อนให้เห็นถึงการเปลี่ยนผ่านของตำรวจจาก “เครื่องมือแห่งการปราบปราม” ไปสู่ “กลไกแห่งการป้องกัน”

ประการที่สาม คือ บทบาทด้านการวิเคราะห์และรวบรวมข่าวกรองทางไซเบอร์ (Cyber Intelligence Role) ซึ่งเป็นองค์ประกอบที่สำคัญในการต่อสู้กับอาชญากรรมข้ามชาติในยุคดิจิทัล เนื่องจากการกระทำความผิดในลักษณะนี้มีกอสัยโครงข่ายซับซ้อนและข้ามพรมแดน เจ้าหน้าที่ตำรวจต้องมีความเชี่ยวชาญในการวิเคราะห์ข้อมูลที่มีความหนาแน่นสูง ใช้เครื่องมือด้านข้อมูลขนาดใหญ่ (Big Data) และปัญญาประดิษฐ์ ในการจำแนกพฤติกรรมผิดปกติ ตลอดจนเชื่อมโยงข้อมูลเพื่อหาตัวผู้กระทำความผิดอย่างแม่นยำและทันต่อเหตุการณ์

ประการที่สี่ คือ บทบาทด้านความร่วมมือระหว่างหน่วยงาน (Cooperation Role) ทั้งในระดับภายในประเทศและระหว่างประเทศ ตำรวจต้องมีความสามารถในการประสานงานกับหน่วยงานต่างประเทศ องค์การบังคับใช้กฎหมายระหว่างประเทศ รวมถึงหน่วยงานของรัฐภายในประเทศที่เกี่ยวข้อง อาทิ สำนักงานป้องกันและปราบปรามการฟอกเงิน กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสำนักงานอัยการสูงสุด เพื่อให้สามารถแลกเปลี่ยนข้อมูล สืบสวนร่วม และติดตามจับกุมผู้กระทำความผิดข้ามชาติได้อย่างมีประสิทธิภาพ

ประการที่ห้า คือ บทบาทด้านการพัฒนาองค์ความรู้และสมรรถนะขององค์กร (Capacity Building Role) ซึ่งมีความสำคัญในการรับมือกับภัยคุกคามที่เปลี่ยนแปลงอยู่ตลอดเวลา เจ้าหน้าที่ตำรวจในยุคใหม่ต้องมีความรู้ด้านกฎหมายไซเบอร์ การวิเคราะห์ดิจิทัลฟอเรนสิกส์ ความเข้าใจเกี่ยวกับการเงินดิจิทัล และเทคโนโลยีใหม่ ๆ

เช่น บล็อกเชน (Blockchain) หรือคริปโตเคอร์เรนซี การพัฒนาหลักสูตรฝึกอบรม การใช้แพลตฟอร์มการเรียนรู้ผ่านระบบออนไลน์ ตลอดจนการจัดตั้งหน่วยงานเฉพาะทางจึงเป็นสิ่งจำเป็นเพื่อสร้างกำลังคนที่มีความพร้อมต่อสู้กับอาชญากรรมข้ามชาติอย่างยั่งยืน

ประการสุดท้าย คือ บทบาทในเชิงนโยบายและกลไกโครงสร้าง (Governance and Policy Role) ตำรวจไม่ควรถูกมองว่าเป็นเพียงผู้รับนโยบาย แต่ควรเป็นผู้เสนอแนวทางการปรับปรุงกฎหมายที่ล่าช้าให้ทันต่อภัยคุกคามสมัยใหม่ รวมถึงเป็นผู้ให้ข้อมูลเชิงประจักษ์แก่รัฐในการกำหนดนโยบายความมั่นคงไซเบอร์ที่มีประสิทธิภาพ ตำรวจจึงควรได้รับการยกระดับให้เป็นกลไกสำคัญในการกำหนดทิศทางของนโยบายด้านอาชญากรรมดิจิทัล ทั้งในระดับชาติและระดับภูมิภาค

บทบาทของเจ้าหน้าที่ตำรวจในยุคดิจิทัลไม่ได้จำกัดเพียงการบังคับใช้กฎหมายเท่านั้น แต่ต้องครอบคลุมตั้งแต่การเฝ้าระวัง การวิเคราะห์ข่าวกรอง การปฏิบัติการร่วม การพัฒนาศักยภาพ และการเสนอเชิงนโยบายในลักษณะองค์รวม ตำรวจในฐานะ “governance actor” ถือเป็นหน้าที่เปลี่ยนผ่านจากตำรวจในโลกกายภาพสู่ตำรวจในโลกดิจิทัลไม่ใช่แค่การเปลี่ยนเครื่องมือ แต่คือการปรับเปลี่ยนวิธีคิด บทบาทและสถานะของตำรวจในฐานะกลไกหลักของรัฐที่ต้องเผชิญหน้ากับอาชญากรรมข้ามชาติในรูปแบบต่าง ๆ และการเป็นผู้ขับเคลื่อนนโยบายด้านความมั่นคงทางไซเบอร์ในเชิงรุก (Policy Advocacy Role) ด้วยเช่นกัน

### 3.2 ข้อเสนอแนะ

จากการศึกษาเรื่องบทบาทของเจ้าหน้าที่ตำรวจในการป้องกันและปราบปรามอาชญากรรมข้ามชาติ ภายใต้พระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568 ผู้เขียนมีข้อเสนอแนะดังนี้

3.2.1 เห็นควรให้เจ้าหน้าที่ตำรวจต้องรับผิดชอบต่อการพัฒนาศักยภาพขององค์กรและบุคลากรภายในให้มีความพร้อมในการเผชิญกับภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว ทั้งในด้านเทคนิค กฎหมาย และจริยธรรมวิชาชีพ ซึ่งรวมถึงการจัดอบรมด้าน (Cybersecurity), การสืบสวนดิจิทัล (Digital Forensics), การใช้เครื่องมือตรวจสอบบนคลาวด์ (Cloud-based Investigation Tools) และการปฏิบัติตามหลักสิทธิมนุษยชน (Human Rights Compliance) ควบคู่ไปกับการรักษาความมั่นคงของชาติ

3.2.2 เห็นควรให้เจ้าหน้าที่ตำรวจต้องสามารถวิเคราะห์สภาพแวดล้อมทางเทคโนโลยีและภัยคุกคามที่เกิดขึ้น พร้อมเสนอแนวทางการพัฒนากฎหมายให้ทันสมัยและตอบสนองต่อสภาพการณ์ที่เปลี่ยนแปลงได้อย่างมีประสิทธิภาพ ซึ่งรวมถึงการเสนอปรับปรุงโครงสร้างหน่วยงาน กลไกบูรณาการข้อมูลระหว่างภาครัฐ เอกชน และประชาชน ตลอดจนการวางยุทธศาสตร์ระดับชาติเพื่อป้องกันและปราบปรามอาชญากรรมในโลกดิจิทัลอย่างยั่งยืน

3.2.3 เห็นควรให้เจ้าหน้าที่ตำรวจควรได้รับการสนับสนุนให้พัฒนาเครือข่ายความร่วมมือระหว่างประเทศอย่างเป็นระบบเนื่องจากอาชญากรรมข้ามชาติมักดำเนินการโดยกลุ่มที่มีเครือข่ายข้ามพรมแดนการทำงานเชิงเดี่ยวหรืออยู่ภายใต้ระบบราชการที่แยกส่วนจึงไม่สามารถตอบสนองต่อภัยคุกคามรูปแบบนี้ได้อย่างทันเวลา ดังนั้น จึงควรมีการพัฒนาความร่วมมือในระดับภูมิภาคและระดับโลกอย่างเข้มแข็ง ผ่านข้อตกลงด้าน

กฎหมายระหว่างประเทศ เช่น อนุสัญญาปาแลร์โม (Palermo Convention) ความตกลงด้านการแลกเปลี่ยนข้อมูลข่าวกรอง (Intelligence Sharing Agreements) และการจัดตั้งกลไกการสืบสวนร่วม (Joint Task Force) ตลอดจนการใช้ระบบติดตามผู้กระทำความผิดระหว่างประเทศ เช่น ระบบ I-24/7 เพื่อให้สามารถติดตาม ตรวจสอบ และดำเนินคดีกับเครือข่ายอาชญากรรมข้ามชาติได้อย่างมีประสิทธิภาพ

3.2.4 เห็นควรให้ส่งเสริมการบูรณาการฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้เชื่อมโยงกันระหว่างหน่วยงานภายในประเทศระบบฐานข้อมูลที่กระจัดกระจายเป็นอุปสรรคสำคัญต่อการสืบสวนสอบสวนที่มีความซับซ้อนในยุคดิจิทัล ดังนั้น หน่วยงานตำรวจควรพัฒนาระบบฐานข้อมูลที่สามารถเชื่อมโยงข้อมูลระหว่างสำนักงานตำรวจแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานป้องกันและปราบปรามการฟอกเงิน และหน่วยงานด้านความมั่นคงอื่น ๆ โดยใช้เทคโนโลยีสารสนเทศที่ปลอดภัย เช่น ระบบบล็อกเชน (Blockchain) สำหรับการตรวจสอบย้อนกลับ หรือการใช้ระบบฐานข้อมูลกลาง (Centralized Intelligence Database) เพื่อเพิ่มประสิทธิภาพในการติดตามพฤติกรรมต้องสงสัย วิเคราะห์รูปแบบอาชญากรรม และประเมินความเสี่ยงในเชิงลึกอย่างแม่นยำและรวดเร็ว

3.2.5 เห็นควรให้ส่งเสริมการมีส่วนร่วมของประชาชนและภาคเอกชนในฐานะ “หุ้นส่วนความมั่นคง” ในยุคดิจิทัลที่ภัยคุกคามสามารถแฝงตัวอยู่ในชีวิตประจำวันของประชาชน ตำรวจไม่สามารถปฏิบัติภารกิจได้โดยลำพัง การมีภาคประชาสังคมและภาคเอกชนเข้ามามีบทบาทในการเฝ้าระวัง แจ้งเบาะแส และร่วมรณรงค์ให้ความรู้จึงเป็นสิ่งสำคัญ โดยเฉพาะการสร้างเครือข่ายพลเมืองตื่นรู้ด้านดิจิทัล (Digital Citizenship) การจัดตั้งศูนย์รับแจ้งเหตุออนไลน์ที่เข้าถึงง่าย การสร้างระบบการรายงานอาชญากรรมแบบ Real-Time ผ่านแอปพลิเคชัน และการส่งเสริมกลไก “ตำรวจชุมชนไซเบอร์” (Cyber Community Policing) เพื่อสร้างความไว้วางใจระหว่างประชาชนกับตำรวจ รวมถึงเสริมความยั่งยืนของการบังคับใช้กฎหมายด้วยพลังจากฐานรากของสังคม

## References

- Cohen and M. Felson. “Social Change and Crime Rate Trends: A Routine Activity Approach.” *American Sociological Review* 44, no. 4 (August 1979): 588–608.
- E. J. Miller. “The Concept of the Police.” *Criminal Law and Philosophy* 17, no. 3 (September 2023): 573–595.
- F. Jobard. *Conceptualizing of Police*. New York: Springer, 2014.
- Office of the Prime Minister. “Summary of Cabinet Meeting News” Last modified January 28, 2025. Accessed February 2, 2025. [https://www.thaigov.go.th/news/contents/ministry\\_details/92827/](https://www.thaigov.go.th/news/contents/ministry_details/92827/) [In Thai]
- Office of the Secretariat to the Cabinet. “Draft Royal Decree on Measures for the Prevention and Compliance of Technology B.E. ... .” Last modified January 28, 2025. Accessed February 2, 2025. [https://www.resolution.soc.go.th/?prep\\_id=412882/](https://www.resolution.soc.go.th/?prep_id=412882/) [In Thai]