รัฐตำรวจ: อำนาจทางกฎหมายของรัฐบาลไทยในการสอดส่องพลเมืองบนโลกไซเบอร์[1]

The Police State: The Legal Power of Thai Government to Surveil Citizens in Cyberspace

ทศพล ทรรศนกุลพันธ์
คณะนิติศาสตร์ มหาวิทยาลัยเชียงใหม่ 239 ถ.ห้วยแก้ว ต.สุเทพ อ.เมือง จ.เชียงใหม่ 50200

Tossapon Tassanakunlapan
Faculty of Law, Chiang Mai University 239 Huay Kaew Road, Muang District, Chiang Mai, Thailand, 50200

E-mail : tossapon.t@cmu.ac.th
Received: August 9, 2021; Revised: November 17, 2021; Accepted: November 24, 2021

บทคัดย่อ

การสถาปนารัฐที่ใช้กฎหมายเป็นเครื่องมือรับรองอำนาจในการสอดส่องควบคุมประชาชน และนำข้อมูลที่ได้จากการสอดส่องไปประกอบสำนวนฟ้องร้องดำเนินคดีต่อพลเมืองผู้ตื่นตัวทางการเมืองในลักษณะ “รัฐตำรวจ” แตกต่างจากการปกครองแบบ “นิติรัฐ” ที่รัฐจะใช้อำนาจปกครองภายใต้กรอบของกฎหมายเพื่อประกันสิทธิเสรีภาพตามกฎหมายของประชาชน บทความวิจัยนี้วิเคราะห์บทบาทของรัฐบาลไทยในการสอดส่องกิจกรรมของประชาชนโดยอาศัยการเพิ่มศักยภาพทางกฎหมายเพื่อเอื้อให้เกิดปฏิบัติการด้านข่าวกรองและสอดส่องได้ครอบคลุมขึ้นไปจนถึงการนำข้อมูลทำเป็นสำนวนฟ้องคดีในชั้นศาลในหลายกรณี แล้วจึงชี้ให้เห็นความกังวลที่เกิดจากแนวโน้มดังกล่าวเพื่อพยายามเสนอแนวทางในการป้องกันการสอดส่องตามอำเภอใจอันมี

[1] บทความนี้เป็นส่วนหนึ่งของโครงการวิจัย “การพัฒนามาตรการคุ้มครองพลเมืองจากการสอดส่องโดยรัฐ” โดยได้รับการสนับสนุนทุนพัฒนานักวิจัยรุ่นใหม่ มหาวิทยาลัยเชียงใหม่

ลักษณะการละเมิดสิทธิความเป็นส่วนตัว สิทธิในข้อมูลส่วนบุคคล เสรีภาพในการแสดงออก ชุมนุม และสมาคม ที่บั่นทอนความมั่นใจของประชาชนในการมีส่วนร่วมทางการเมือง

คำสำคัญ: การสอดส่อง, สิทธิมนุษยชน, ความเป็นส่วนตัว, อินเทอร์เน็ต

Abstract

The establishment of a state that uses the law as a means of ensuring its power to monitor and control the people and use the information obtained from surveillance to use in prosecution cases against politically active citizens in a "Police State" manner, which is different from the "Legal State" regime whereby the state uses its powers under the legal framework to guarantee rights and liberties according to the law of the people. This research paper analyzes the role of the Thai government in surveillance of people's activities, from enhancing its legal capacity to facilitate intelligence and surveillance operations, to the use of information in many court cases. Accordingly, article points out the concerns caused by the trend for proposing a way to prevent arbitrary surveillance that infringes on the right to privacy, right to personal information and freedom of expression, association and assembly which could lead to undermine people's confidence in political participation.

Keywords: Surveillance, Human Rights, Privacy, Internet

1. เปิดกำแพงบังตา

ข้อกล่าวอ้างสำคัญของรัฐบาลไทยในการเพิ่มศักยภาพในด้านข่าวกรองและออกกฎหมายที่ให้อำนาจสอดส่องการสื่อสารของประชาชน คือ “ถ้าประชาชนไม่ได้ทำผิดจะกลัวอะไร” โดยมิได้คำนึงหลักการพื้นฐานเบื้องต้นว่า แม้ประชาชนมิได้ทำผิดกฎหมายอันใดก็มีสิทธิความเป็นส่วนตัว ปลอดจากการแทรกแซงการสื่อสาร อันเป็นสิทธิพื้นฐานตามกฎหมายอันเป็นหลักประกันความมั่นคงปลอดภัยในชีวิตและทรัพย์สิน

ยิ่งไปกว่านั้นการตกอยู่ภายใต้ระบอบการปกครองเผด็จการมานานก็ทำให้ประชาชนรู้สึกชินชาต่อการสอดส่องโดยรัฐ และหลงลืมความเป็นส่วนตัวด้วยความคิดที่ว่า “รัฐมองเห็นการสื่อสารอยู่แล้ว” การพยายามสร้างมาตรการทางกฎหมายเพื่อป้องกันการสอดส่องหรือเอาผิดเจ้าพนักงานรัฐที่ละเมิดความเป็นส่วนตัวของประชาชนหาได้จำเป็นไม่ ก็เป็นอีกอุปสรรคหนึ่งต่อการผลักดันการสร้างหลักประกันสิทธิความเป็นส่วนตัว

แนวโน้มทั้งสองประการอาจนำไปสู่การสถาปนารัฐที่ใช้กฎหมายเป็นเครื่องมือรับรองอำนาจในการสอดส่องควบคุมประชาชน และนำข้อมูลที่ได้จากการสอดส่องไปประกอบสำนวนฟ้องร้องดำเนินคดีต่อพลเมืองผู้ตื่นตัวทางการเมือง แสดงออกในลักษณะวิพากษ์วิจารณ์และต่อต้านแนวนโยบายของรัฐบาล อันเป็นการบั่นทอนการมีส่วนร่วมของประชาชนในการกำหนดอนาคตตนเองและสังคม รัฐที่จำกัดสิทธิของประชาชนด้วยการสอดส่องนี้มีคำเรียกขานว่า “รัฐตำรวจ”

รัฐตำรวจ (Police State[2]) คือ รูปแบบทางการเมืองที่รัฐบาลใช้อำนาจควบคุมวิถีชีวิตทางการเมือง เศรษฐกิจ และสังคมของประชาชน โดยมีการใช้อำนาจขององค์กรในกระบวนการยุติธรรมหรือองค์กรทางปกครองด้านความมั่นคงปฏิบัติการที่มีลักษณะละเมิดสิทธิเสรีภาพของประชาชนตามกฎหมาย ในลักษณะที่แสดงต่อสาธารณชนว่าเป็นการรวบรวมข้อมูลข่าวกรองขึ้นเป็นพยานหลักฐานทำสำนวนดำเนินคดีฟ้องสู่ศาล ถ้อยคำนี้มีที่มาทางประวัติศาสตร์จากรัฐปรัสเซีย (ระบบกฎหมายเยอรมัน) เพื่อแสดงว่าในศตวรรษที่ 19 มีการสถาปนา “รัฐพลเรือน” ที่ใช้อำนาจในการปกครองประชากรโดยควบคุมกิจกรรมของพลเมืองอย่างเข้มงวดหรือมีลักษณะจำกัดสิทธิเสรีภาพตามรัฐธรรมนูญของประชาชน แตกต่างจากการปกครองแบบ “นิติรัฐ” ที่รัฐจะใช้อำนาจปกครองภายใต้กรอบของกฎหมายเพื่อประกันสิทธิเสรีภาพตามกฎหมายของประชาชน[3] และมีกลไกตรวจสอบถ่วงดุลอำนาจ

โดยบทความวิจัยนี้จะนำแนวคิดนี้มาใช้เป็นกรอบวิเคราะห์บทบาทของรัฐบาลไทยในการสอดส่องกิจกรรมของประชาชนโดยอาศัยการเพิ่มศักยภาพทางกฎหมายเพื่อเอื้อให้เกิดปฏิบัติการ

---

[2] s. v., “Police State,” *Merriam-Webster* (Merriam-Webster, n.d.), accessed July 25, 2021, https://www.merriamwebster.com/dictionary/police%20state.

[3] Brian Chapman, “‘The Police-State.’ Government and Opposition 3, No.4” (Cambridge University Press, 1968): 428-440, accessed July 25, 2021, https://www.jstor.org/stable/44481889.

ด้านข่าวกรองและสอดส่องได้ครอบคลุมขึ้นไปจนถึงการนำข้อมูลทำเป็นสำนวนฟ้องคดีในชั้นศาล ในหลายกรณี แล้วจึงชี้ให้เห็นความกังวลที่เกิดจากแนวโน้มดังกล่าวเพื่อพยายามเสนอแนวทางในการป้องกันการสอดส่องตามอำเภอใจอันมีลักษณะการละเมิดสิทธิความเป็นส่วนตัว สิทธิในข้อมูลส่วนบุคคล เสรีภาพในการแสดงออก ชุมนุมและสมาคม ที่สอดคล้องกับพันธกรณีสิทธิมนุษยชนระหว่างประเทศที่ไทยเป็นภาคี ฝ่าฝืนบทบัญญัติของรัฐธรรมนูญ และบั่นทอนความมั่นใจของประชาชนในการมีส่วนร่วมทางการเมือง

2. วงวิชาการมองการสอดส่องโดยรัฐไว้อย่างไร

กรอบทางทฤษฎีที่กล่าวถึงการสอดส่องประชาชนโดยรัฐปรากฏอยู่ในผลงานทางวิชาการที่ชี้ให้เห็นยุทธวิธีของรัฐสมัยใหม่ในการสร้างอำนาจปกครองประชากรในดินแดนของตนด้วยการสอดส่องพฤติกรรมทั้งหลายของประชาชนให้ประชาชนตระหนักรู้ด้วยตัวเองว่ามีเจ้าหน้าที่ของรัฐจับจ้องอยู่ หากกระทำการอันใดที่ขัดต่อแนวนโยบายของผู้มีอำนาจรัฐจะต้องโทษทัณฑ์ได้ เนื่องจากรัฐพร้อมที่จะเข้าจับกุมคุมขังและดำเนินคดีได้ทันทีเพราะได้มีการรวบรวมข่าวกรองเกี่ยวกับบุคคลเป้าหมายนั้นอยู่แล้ว

2.1. ยุทธศาสตร์ของรัฐในการมองเห็นประชาชนเพื่อเสริมอำนาจในการปกครอง

การพยายามสร้างกลไกการสอดส่องของผู้ปกครองหรือรัฐ เพื่อควบคุมพฤติกรรม ผู้อยู่ใต้ปกครองอยู่เสมอ กลไกการสอดส่องนับเป็นเครื่องมือที่สำคัญยิ่งในการรักษาระเบียบสาธารณะ (Public Order) ของรัฐ ตามประวัติศาสตร์แล้ว กลไกการควบคุมสอดส่องพฤติกรรมมนุษย์อาจถูกบังคับผ่านบรรทัดฐานบางอย่างที่เกี่ยวข้องกับเรื่องศาสนาและวัฒนธรรม[4] แต่เมื่อก้าวสู่ยุคที่รัฐสมัยใหม่ (Modern State) ถือกำเนิดขึ้น กลไกการสอดส่องก็เปลี่ยนมาอยู่ภายใต้กลไกการบังคับอย่างเป็นผ่านระบบงานราชการ (Bureaucracy) การจัดการ (Management) และการใช้อำนาจตามกฎหมายของเจ้าหน้าที่รัฐ (Policing) ซึ่งก่อนหน้านี้ การสอดส่องอาจอยู่ในรูปแบบการสอดส่องจากภายนอก (External surveillance) ที่ฝ่ายเจ้าหน้าที่รัฐต้องลงมือปฏิบัติโดยตรง เช่น การเดินตรวจตรา การยืนเฝ้าระวัง หรือวิธีการอย่างอื่นที่เจ้าหน้าที่ต้องลงแรงปฏิบัติงานเอง ต่อมานักปราชญ์ชาวฝรั่งเศสอย่าง มิเชล ฟูโกต์ ได้อธิบายการทำงานของสิ่งที่เรียกว่า ‘Panopticism’ ใน

[4] Stephen Graham and David Wood, “Digitizing Surveillance: Categorization, Space, Inequality,” *Critical Social Policy* 23, no. 2 (2003): 227-248.

Discipline and Punish: The Birth of the Prison[5] ซึ่งเผยแพร่ออกมาช่วงปี 1975 เพื่อนำเสนอว่า รูปแบบการสอดส่องซึ่งมีจุดประสงค์ในการรักษาระเบียบและควบคุมพฤติกรรมของผู้คนในสังคมใหม่ ที่ทรงประสิทธิภาพมากกว่าวิธีการในอดีต จะต้องเกิดจากการออกแบบทางสถาปัตยกรรมและการจัดสรรพื้นที่ให้ผลลัพธ์ที่ขึ้นจากการควบคุมสอดส่องเกิดขึ้นอยู่ตลอดเวลา แม้ว่าการปฏิบัติการสอดส่องจะไม่ได้เกิดขึ้นอย่างต่อเนื่องก็ตาม เช่น การสร้างหอคอยสังเกตการณ์ ณ จุดศูนย์กลางของพื้นที่ใดพื้นที่หนึ่ง ทั้งนี้ เป็นไปเพื่อให้มโนสำนึก (Consciousness) ของผู้ที่อยู่ในพื้นที่ต้องตกอยู่ในสภาวะที่เหมือนกับว่าตนกำลังถูกจ้องมองหรือสอดส่องอยู่ทุกขณะ จนนำไปสู่การกำกับควบคุมตนเอง โดยไม่จำเป็นต้องมีการกระทำใด ๆ ของผู้ปกครองหรือรัฐ

อย่างไรก็ตาม ความก้าวหน้าของเทคโนโลยีการตรวจจับและการบันทึกข้อมูลต่าง ๆ ได้ช่วยให้การสอดส่องทั้งแบบปัจเจกบุคคลและแบบกลุ่มนั้นทรงประสิทธิภาพขึ้นหลายเท่าตัว แม้ว่าจะไม่มีการเฝ้าสังเกตการณ์โดยตรงแบบต่อเนื่อง หรือการออกแบบทางสถาปัตยกรรมและการจัดสรรพื้นที่ก็ตาม ซึ่งทางด้านของ สตีเฟน เกรแฮม (Stephen Graham) และ เดวิด วูด (David Wood) ในบทความชื่อว่า *Digitizing surveillance categorization, space, inequality*[6] ได้ศึกษา ผลกระทบทางสังคมที่เกิดจากการสอดส่องดิจิทัล และการเปลี่ยนแปลงกลไกการสอดส่องจากรูปแบบที่อิงอยู่กับกลไกการทำงานของระบบรัฐราชการ (Bureaucratic System) และระบบอนาล็อค (Analog) สู่ระบบดิจิทัล (Digitization) ที่มีเทคโนโลยีเข้ามาช่วยให้การสอดส่องสามารถขยายขอบเขตกว้างขวางยิ่งขึ้นภายในระยะเวลาอันสั้น พร้อมทั้งยังเสริมพลังแก่ระบบการระบุตัวตนของบุคคล (Identification) การติดตามบุคคล พฤติกรรมและคุณลักษณะต่าง ๆ ของประชากร (Tracking) ให้สามารถดำเนินไปได้อย่างต่อเนื่องและแสดงผลได้แบบตามเวลาจริง (Real-Time) เช่น การติดกล้องวงจรปิดตามสถานที่ต่าง ๆ โดยกล้องมีคุณสมบัติพิเศษซึ่งสามารถการระบุตัวตนของบุคคลได้ เป็นต้น

[5] Michel Foucault, *Discipline and Punish: The Birth of the Prison*, translated from the French by Alan Sheridan, (New York: Vintage Books, 1995): 195-228.

[6] Stephen Graham and David Wood, "Digitizing Surveillance: Categorization, Space, Inequality," *Critical Social Policy* 23, no. 2 (2003): 227-248.

กรณีเดียวกัน มีงานศึกษาอีกชิ้นหนึ่ง[7] ได้เสนอเพิ่มเติมอีกว่า ความก้าวหน้าของเทคโนโลยีที่ส่งเสริมให้กลไกการสอดส่องมีประสิทธิภาพมากขึ้น ได้ช่วยเปลี่ยนโฉมหน้าการบังคับใช้กฎหมาย และนำไปสู่การใช้เครื่องมือการตรวจตราทางดิจิทัล (Digital policing) และการตรวจตราเชิงป้องกัน (Preventive policing) ซึ่งทั้งสองสิ่งนี้ได้อำนวยประโยชน์แก่การคุ้มครองสิทธิส่วนบุคคลและกระบวนการพิจารณาความอาญาเป็นอย่างมาก ด้วยเหตุที่ได้เข้าไปมีส่วนช่วยลดทอนความสลับซับซ้อนของการบังคับใช้กฎหมาย เปิดโอกาสให้มีเปลี่ยนแปลงจุดสนใจจากที่เดิมทีจะเน้นไปที่การตรวจตราเชิงสืบสวนสอบสวน (Investigative policing) ไปเป็นการตรวจตราเชิงป้องกัน (Preventive policing) อย่างไรก็ตาม การตรวจตราทางดิจิทัล (Digital policing) และการตรวจตราเชิงป้องกัน (Preventive policing) อาจนำไปสู่ปัญหาการดำเนินคดีที่ล้นเกินแบบไร้ประสิทธิภาพ (Inefficient overdeterrence) งานศึกษาดังกล่าวจึงนำเสนอให้มีแก้ไขกฎหมายลดโทษทางอาญาให้เบาลง โดยเฉพาะกับบุคคลผู้กระทำความผิดครั้งแรก ถึงอย่างนั้น ปัญหาดังกล่าวในห้วงเวลานี้ กำลังกลายเป็นปัญหาที่แก้ไขยากยิ่งขึ้น ด้วยข้อเท็จจริงที่ว่า มีบุคคลหลายคนต้องถูกจับกุม และถูกตัดสินลงโทษอันเนื่องมาจากการทิ้งรอยเท้าดิจิทัล (Digital footprint) บนพื้นที่โลกออนไลน์ไว้เป็นจำนวนมาก จนกลายมาเป็นพยานหลักฐานย้อนกลับมาเอาผิดบุคคลเหล่านั้น[8]

2.2. การรักษาอำนาจรัฐด้วยการมองเห็นความลับของประชาชนและห้ามประชาชนตรวจตราข่าวกรองของรัฐ

เมื่อเครือข่ายอินเทอร์เน็ตมีอิทธิพลต่อชีวิตของมนุษย์มากขึ้นด้วยการสร้างพื้นที่เสมือนจริงอย่างพื้นที่ไซเบอร์ (Cyberspace) ซึ่งเป็นพื้นที่ที่มนุษย์หลายล้านคนกระโดดเข้ามาทำกิจกรรมแลกเปลี่ยนข้อมูลข่าวสารกันอย่างหนาแน่นผ่านเครือข่ายสังคมออนไลน์ทั้งหลาย เช่น เฟซบุ๊ก (Facebook) ทวิตเตอร์ (Twitter) ไลน์ (Line) ฯลฯ ขณะที่รัฐหลายรัฐก็ได้พัฒนาศักยภาพการสอดส่องของตนให้ไปไกลเกินกว่าการจัดสรรพื้นที่เพื่อให้ผู้อยู่ใต้การปกครองมีสำนึกว่าตนเองกำลังถูกควบคุมสอดส่อง หรือการอาศัยความก้าวหน้าของเทคโนโลยีการตรวจจับและบันทึกภาพ โดยเยฟเกนี่ โมโรซอฟ (Evgeny Morozov) ซึ่งเป็นบุคคลสำคัญในแวดวงงานศึกษาเกี่ยวกับผลกระทบ

---

[7] Manuel A. Utset, “Digital Surveillance and Preventive Policing,”. *Connecticut Law Review*, 49(5) (2017): 1453-1494.

[8] Ibid.,

ของเทคโนโลยีที่มีต่อการเมืองและสังคม ในงานชื่อว่า The Net delusion The Dark Side of Internet Freedom โมโรซอฟ ได้มีข้อเสนอที่สั่นคลอนความเชื่อของผู้คนที่เชื่อว่าอินเทอร์เน็ตสร้างพื้นที่แห่งเสรีภาพ โดยเสนอว่า แท้จริงแล้ว อินเทอร์เน็ตต่างหากที่เป็นตัวจำกัดและบั่นทอนเสรีภาพของผู้คน ความเชื่อที่เชื่อว่าอินเทอร์เน็ตจะช่วยให้มนุษย์สามารถปลดปล่อยทางการเมือง (Political emancipation) จากผู้มีอำนาจได้ เป็นเพียงความเชื่อของชาวไซเบอร์ที่ลุ่มหลงถึงโลกในอุดมคติ หรือไซเบอร์ยูโทเปียน (cyberutopians) เท่านั้น ปัจจัยสำคัญ คือ พลานุภาพของอินเทอร์เน็ตมักถูกรัฐบาลอำนาจนิยมใช้เพื่อตอบสนองผลประโยชน์ในทางการเมืองของตนเองได้อย่างดี หนึ่งในนั้นคือการบังคับใช้กลไกการสอดส่อง เพื่อติดตามสิ่งต่าง ๆ ที่ถูกเผยแพร่ลงในเครือข่ายสังคมออนไลน์ รวมถึงการจัดประเภท (Categorization) ผู้คน เช่น การจัดให้คนกลุ่มหนึ่งเป็นพวกผู้ก่อการร้าย และการพยายามใช้ปฏิบัติการเพื่อให้ได้มาซึ่งข้อมูลระบุตัวบุคคล (Identify) ของผู้ใช้อินเทอร์เน็ต อีกทั้ง อินเทอร์เน็ตยังถูกใช้เพื่อเป็นพื้นที่การเผยแพร่เนื้อหาโฆษณาชวนเชื่อของฝ่ายรัฐบาลอำนาจนิยมอีกด้วย ดังนั้น จากสิ่งที่โมโรซอฟได้นำเสนอ จะเห็นว่าการที่ผู้คนส่วนใหญ่เข้าใจกันว่าอินเทอร์เน็ตจะช่วยให้มนุษย์พบกับอิสระและมีเสรีภาพมากขึ้นเป็นความคิดที่อาจถูกเพียงครึ่งเดียว เพราะอีกด้านหนึ่ง อินเทอร์เน็ตก็ให้อำนาจแก่ฝ่ายรัฐนำไปใช้ปกป้องตนเองได้ไม่น้อยไปกว่ากัน

งานศึกษาของ ไฮดิ โบโกเซียน (Heidi Boghosian) เรื่อง *Spying on Democracy Government Surveillance, Corporate Power, and Public Resistance*[9] ได้นำเสนอแง่มุมที่องค์กรเอกชน หรือบรรษัทและหน่วยงานความมั่นคงสามารถร่วมกันใช้อำนาจการสอดส่องในลักษณะที่เป็นการช่วยเหลือส่งเสริมการละเมิดสิทธิส่วนบุคคลของพลเมืองเน็ตได้อย่างแนบเนียน เริ่มจากการกำหนดจัดประเภทคนบางกลุ่ม โดยเฉพาะนักเคลื่อนไหวสิทธิมนุษยชนที่มักถูกรัฐมองว่าเป็นผู้ก่อความวุ่นวาย และมีพฤติกรรมอันเป็นภัยคุกคามต่อความปลอดภัยหรือความมั่นคงของรัฐ เมื่อรัฐต้องการข้อมูลใด ๆ ก็ตามของประชาชนและนักเคลื่อนไหว รัฐก็อาจขอข้อมูลส่วนบุคคลต่าง ๆ ของผู้ใช้บริการที่มีอยู่ในฐานข้อมูลเอกชน หรือบรรษัท ที่ไม่จำกัดอยู่เฉพาะแต่ผู้ให้บริการสื่อสังคมออนไลน์เท่านั้น แต่ยังหมายความถึง ผู้ให้บริการโทรคมนาคม (telecommunications companies) นักเก็บรวบรวมข้อมูล (data aggregators) และสำนักข่าวกรองเอกชน (private

[9] Heidi Boghosian, *Spying on Democracy: Government Surveillance, Corporate Power, and Public Resistance* (San Francisco: City Lights Publishers, 2013).

intelligence firms) ด้วย และสถานการณ์เช่นนี้ก็ได้ส่งผลให้เกิดกระบวนการสอดส่อง ที่ไม่หยุดยั้ง (Relentless Surveillance) ขึ้นในพื้นที่สื่อสังคมออนไลน์ และบนโลกดิจิทัล

การบังคับใช้กลไกการสอดส่องทางปฏิบัตินั้น ขณะที่รัฐพยายามพัฒนาศักยภาพตนเองเพื่อทำให้การควบคุมพฤติกรรม และสอดส่องความเคลื่อนไหวต่าง ๆ ที่เกิดขึ้นในสังคมทั้งบนพื้นที่ทางกายภาพ และพื้นที่ออนไลน์ เป็นไปโดยมีประสิทธิภาพมากที่สุด แต่การสอดส่องที่ต้องรักษาสมดุลระหว่างประโยชน์สาธารณะและการคุ้มครองสิทธิเสรีภาพของปัจเจกบุคคลเป็นเรื่องที่เกิดขึ้นได้ยากมาก เนื่องจากมันต้องเผชิญหน้ากับความก้าวหน้าของเทคโนโลยีที่ไปไกลจนส่งผลให้การแทรกแซงและการรุกล้ำความเป็นส่วนตัวเกิดขึ้นได้ง่ายกว่าอดีตอย่างมาก อีกทั้ง ระบบกฎหมายที่เป็นอยู่กลับไม่สามารถจัดการกับปัญหาเหล่านั้นได้ด้วย และหลายรัฐยังคงขาดระบบการตรวจสอบที่มีประสิทธิภาพพอที่จะจำกัดการใช้อำนาจของเจ้าหน้าที่ฝ่ายความมั่นคงให้เป็นไปตามหลักความจำเป็นและหลักความได้สัดส่วน เพื่อป้องกันการละเมิดสิทธิส่วนบุคคลและสิทธิมนุษยชนขั้นพื้นฐานที่เกิดจากกลไกการสอดส่องของรัฐและบรรษัทที่ดำเนินธุรกิจเกี่ยวกับเทคโนโลยีและระบบสารสนเทศ เช่นเดียวกับบทบัญญัติกฎหมายทั้งในระดับกฎหมายภายในของรัฐ และกฎหมายระหว่างประเทศ ยังมีความคลุมเครือ รวมถึงกลไกการบังคับให้การใช้อำนาจของรัฐต้องเป็นไปตามกฎหมายบัญญัติ หรือ “Legal Mechanism” ยังคงไร้ประสิทธิภาพเช่นกัน[10]

3. ประวัติศาสตร์การเสริมศักยภาพในการมองเห็นประชาชนของรัฐบาลไทย

แม้รัฐธรรมนูญแห่งราชอาณาจักรไทยจะได้รับรองสิทธิในความเป็นส่วนตัวและข้อมูลส่วนบุคคลไว้ในมาตรา 32 เช่นเดียวกับสนธิสัญญาระหว่างประเทศด้านสิทธิมนุษยชนที่รัฐไทยอนุวัติการแล้วอย่างกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights (ICCPR)) ก็ได้กำหนดให้ การบังคับใช้กลไกการสอดส่องในทางปฏิบัติ โดยคำนึงถึงการรักษาสมดุลระหว่างการปกป้องคุ้มครองสิทธิเสรีภาพของปัจเจกบุคคลที่จะไม่ถูกแทรกแซงความเป็นส่วนตัว และการป้องกันรักษาผลประโยชน์ของคนส่วนใหญ่ เป็นหน้าที่พื้นฐานของรัฐทุกรัฐที่จะต้องปฏิบัติตาม แต่ในอีกด้าน งานศึกษา

[10] **Marco Milanovic**, “Human rights treaties and foreign surveillance: Privacy in the digital age,”. *Harvard International Law Journal*, 56(1) (2015): 81-146.

ต่างประเทศชิ้นหนึ่งที่เกี่ยวกับประเด็นนี้ เสนอว่า[11] ยิ่งเทคโนโลยีและระบบการสื่อสารถูกพัฒนาให้ก้าวหน้ามากเท่าใด โอกาสที่รัฐจะสอดส่องและแทรกแซงความเป็นส่วนตัวของผู้คนก็ยิ่งมีเพิ่มมากขึ้นเท่านั้น ซึ่งอาจอยู่ในรูปแบบของการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อจัดทำฐานข้อมูลต่าง ๆ ที่เป็นประโยชน์แก่งานบริหาร รวมถึงการจัดทำประวัติส่วนตัว หรือรายละเอียดของบุคคลที่เป็นเป้าหมายของรัฐ โดยทั้งหมดอาจส่งผลกระทบต่อสิทธิส่วนบุคคลของผู้คนจำนวนมาก อีกทั้งแม้เรื่องสิทธิส่วนบุคคลจะเป็นเรื่องที่ได้รับการรับรองว่าเป็นสิทธิมนุษยชนขั้นพื้นฐาน ซึ่งอาจไม่ได้เป็นสิทธิโดยสมบูรณ์ (absolute right) แต่ในระดับกฎหมายระหว่างประเทศ ก็กำหนดว่าการจำกัดหรือรุกล้ำสิทธิส่วนบุคคลจะกระทำได้แต่เฉพาะกรณีที่มีความจำเป็น มีเหตุผลอันชอบธรรม และได้สัดส่วนเท่านั้น แต่หากขยับลงมาระดับกลไกภายในของรัฐ พบว่า กฎหมายที่ควบคุมหรือให้อำนาจแก่เจ้าหน้าที่รัฐในการสอดส่องแทรกแซงความเป็นส่วนตัวประชาชนของตน ยังมีข้อบกพร่องเกี่ยวกับการไม่สามารถรักษาสมดุลระหว่างสิทธิของปัจเจกบุคคลกับประโยชน์สาธารณะได้ และหลายประเทศยังไม่มีกฎหมายที่ควบคุมก็ใช้อำนาจของเจ้าหน้าที่รัฐเสียด้วยซ้ำ จึงเป็นเหตุให้หลายคนต้องถูกละเมิดความเป็นส่วนตัวจากการใช้อำนาจสอดส่องโดยไม่ชอบด้วยกฎหมายและมีลักษณะตามอำเภอใจของเจ้าหน้าที่ฝ่ายความมั่นคงอยู่จำนวนมากในหลายประเทศ[12]

โดยในหัวข้อนี้จะทำการสำรวจประวัติศาสตร์การพัฒนาศักยภาพด้านการข่าวกรองของรัฐไทยที่เพิ่มอำนาจในการสอดส่องประชาชนผ่านมาตรการทางกฎหมายและกลไกต่าง ๆ ที่ให้อำนาจแก่รัฐบาลในการสอดส่องการสื่อสารและกิจกรรมของประชาชนผ่านเครื่องมือต่าง ๆ ตั้งแต่หลังสงครามโลกครั้งที่ 2 มาจนถึงยุคหลังการรัฐประหาร พ.ศ.2557 ที่มีการสถาปนา “รัฐตำรวจ” ขึ้นอย่างเข้มแข็ง

---

[11] Badala Tachilisa Balule and Bojosi Otlhogile, “Balancing the Right to Privacy and the Public Interest: Surveillance by the State of Private Communications for Law Enforcement in Botswana,” *Statute Law Review* 37, no. 1 (July 24, 2015): 1-14.

[12] Badala Tachilisa Balule and Bojosi Otlhogile, “Balancing the Right to Privacy and the Public Interest: Surveillance by the State of Private Communications for Law Enforcement in Botswana,” *Statute Law Review* 37, no. 1 (July 24, 2015): 14.

3.1. การพัฒนาศักยภาพในการมองของรัฐบาลไทยหลังสงครามโลกครั้งที่ 2 ตลอดช่วงสงครามเย็น

ก่อนมีบทบัญญัติกฎหมายที่ให้อำนาจการสอดส่องบนโลกไซเบอร์แก่เจ้าหน้าที่รัฐโดยตรง ไม่ได้หมายความว่า รัฐไทยจะไม่มีกลไกการสอดส่องประชาชน เพราะกลไกดังกล่าวถือเป็นเครื่องมือทางอำนาจที่รัฐไทย รวมถึงรัฐในอีกหลายประเทศขาดไม่ได้ การพัฒนาศักยภาพการสอดส่อง ช่วงแรกจะอยู่ในรูปแบบการจัดเตรียม วางแผนปรับปรุงหน่วยงาน หรือองค์กรที่มีอำนาจหน้าที่เกี่ยวกับการป้องกันภัยความมั่นคงและการก่ออาชญากรรม เพื่อส่งเสริมประสิทธิภาพให้สามารถรับมือกับความเคลื่อนไหวต่างๆ ในพื้นที่โลกออนไลน์ ซึ่งอาจส่งผลกระทบต่อความมั่นคงของรัฐ และความปลอดภัยสาธารณะ

ผลผลิตในการพัฒนาศักยภาพการสอดส่องของยุคสมัยสงครามเย็นนั้น ได้แก่ หน่วยงานความมั่นคงของรัฐไทยที่มีอำนาจหน้าที่อย่างเข้มข้นในการเฝ้าระวัง สอดส่อง ควบคุมการสื่อสารและการกระทำต่าง ๆ ของประชาชนที่ผู้มีอำนาจเห็นว่าเป็นภัยต่อความมั่นคง และส่งผลเสียต่อการยืนหยัดสู้เพื่ออุดมการณ์ทางการเมืองช่วงนั้น อาทิ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร สำนักงานข่าวกรองแห่งชาติ สำนักงานสภาความมั่นคงแห่งชาติ ฯลฯ

หน่วยงานที่มีหน้าที่รับผิดชอบ และปฏิบัติงานเกี่ยวกับด้านความมั่นคงมามากกว่าหนึ่งร้อยปี หรือนับตั้งแต่สมัยรัชกาลที่ 6 อย่างสำนักงานสภาความมั่นคงแห่งชาติ (สมช.) นับเป็นหน่วยงานสำคัญที่มีอำนาจหน้าที่ในการสอดส่อง เฝ้าระวัง และติดตามความเคลื่อนไหวต่าง ๆ ที่อาจส่งผลกระทบต่อความมั่นคงในประเทศ

หน่วยงานสำคัญที่ทำหน้าที่สอดส่อง เป็นหูเป็นตาให้แก่รัฐ อีกหน่วยงานหนึ่ง ได้แก่ สำนักงานข่าวกรองแห่งชาติ (สขช.) ซึ่งเป็นหน่วยข่าวระดับชาติหน่วยเดียวของรัฐไทยที่เป็นหน่วยราชการพลเรือน และมีหัวหน้าส่วนราชการเป็นข้าราชการพลเรือนสามัญ โดยมีอำนาจหน้าที่ตามพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2528

ในช่วงสงครามเย็นเป็นช่วงที่ต้องมีการเฝ้าระวัง สอดส่อง ป้องกันประเทศจากอุดมการณ์คอมมิวนิสต์ที่รัฐไทยมองว่าเป็น “ภัยคุกคามความมั่นคงของชาติ” และมาพร้อมกับการแลกเปลี่ยนเผยแพร่ข้อมูลข่าวสาร และสื่อสิ่งพิมพ์ต่าง ๆ รัฐไทยจึงทำการจัดตั้ง “กองอำนวยการป้องกันและปราบปรามคอมมิวนิสต์” ก่อนถูกเปลี่ยนให้มาใช้ชื่อ “กองอำนวยการรักษาความมั่นคงภายใน

ราชอาณาจักร" (กอ.รมน.) ในปี 2516[13] โดยอดีตที่ผ่านมาถือเป็นหน่วยงานหลักที่มีความรับผิดชอบในภารกิจป้องกันและปราบปรามคอมมิวนิสต์ ทบทวนวิเคราะห์เพื่อพัฒนานโยบายตลอดจนยุทธศาสตร์และยุทธวิธี เพื่อให้สามารถยุติสถานการณ์ก่อการร้ายให้สำเร็จลงโดยเร็ว[14]

3.2. การปรับทิศทางรัฐจากสงครามต้านคอมมิวนิสต์สู่สงครามต้านภัยคุกคามจากอาชญากรรมร้ายแรง

เมื่อสิ้นสุดสถานการณ์สงครามเย็นลง รัฐไทยจึงปรับโครงสร้าง กอ.รมน. ไปในหลากหลายรูปแบบ เช่น ในปี 2525 มีหน้าที่รับผิดชอบดำเนินปฏิบัติภารกิจทางด้านการป้องกันและปราบปรามยาเสพติดการจัดระเบียบและเสริมความมั่นคงชายแดนการพัฒนาเพื่อความมั่นคงเฉพาะพื้นที่ การแก้ปัญหาชนกลุ่มน้อยและผู้หลบหนีเข้าเมือง การแก้ปัญหาความขัดแย้งโดยสันติวิธี (หน่วยสันตินิมิต) การปฏิบัติงานด้านการข่าวและปฏิบัติการจิตวิทยา (ปจว.)[15] หรือในปี 2543 กับการเป็นหน่วยงานหลักในการแก้ไขปัญหาจังหวัดชายแดนภาคใต้ หลังจากมีมติ คณะรัฐมนตรีให้ยกเลิกพระราชบัญญัติป้องกันการกระทำอันเป็นคอมมิวนิสต์ พ.ศ.2495 ต่อมาหน้าที่และงานรับผิดชอบของ กอ. รมน. กลายเป็นการถูกปรับโครงสร้างให้เน้นไปที่การแก้ไขปัญหาสามจังหวัดชายแดนภาคใต้เป็นส่วนใหญ่ ทั้งภายใต้คำสั่งนายกรัฐมนตรีที่ 158/2545[16] และการรื้อโครงสร้างอีกครั้งตามคำสั่งนายกรัฐมนตรีที่ 205/2549 โดยส่วนหลังนี้เป็นการจัดตั้งให้มี ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.)[17] และกองบัญชาการผสมพลเรือน ตำรวจ ทหารที่ 43 (พตท.43)[18]

บทบาทของสำนักงานสภาความมั่นคงแห่งชาติ (สมช.) ระหว่างปี 2540-2550 ไม่ต่างจากงานของกอ.รมน. มากนัก เพราะต้องร่วมกันปฏิบัติหน้าที่ในพื้นที่สามจังหวัดภาคใต้ การต่อต้าน

---

[13] กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร, "ประวัติความเป็นมา., *ISOC*., สืบค้นเมื่อ 28 เมษายน 2564, https://www.isoc.go.th/about.php.

[14] เรื่องเดียวกัน.

[15] กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร, "ประวัติความเป็นมา., *ISOC*., สืบค้นเมื่อ 28 เมษายน 2564, https://www.isoc.go.th/about.php.

[16] มติชน, 3 กรกฎาคม 2545, หน้า 45

[17] ประชาชาติธุรกิจ, 9 ตุลาคม 2549, หน้า 43.

[18] มติชนสุดสัปดาห์, 27 ตุลาคม 2549, หน้า 25 – 26.

“ก่อการร้าย” และร่วมจัดการปัญหายาเสพติดกับเจ้าหน้าที่ป้องกันและปราบปรามยาเสพติด[19] เป็นหลัก

แม้พระราชบัญญัติข่าวกรองแห่งชาติฉบับแรกได้ประกาศใช้ก่อนที่จะมีความก้าวหน้าทางเทคโนโลยีและระบบการสื่อสาร แต่ พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2528 ยังนับว่าเป็นกฎหมายที่กำหนดอำนาจหน้าที่ของสำนักงานข่าวกรองแห่งชาติไว้กว้างขวางพอที่จะใช้ได้กับบริบททางการเมืองช่วงทศวรรษที่ 2540 และเป็นฐานอำนาจให้แก่เจ้าหน้าที่รัฐในการดำเนินกลไกการสอดส่องประชาชน และความเคลื่อนไหวในโลกออนไลน์ที่เพิ่งถูกพัฒนาในระยะแรกเริ่มได้[20] ตัวอย่างเช่น ติดตามสถานการณ์ภายในประเทศและต่างประเทศที่มีผลกระทบต่อความมั่นคงแห่งชาติ และรายงานต่อนายกรัฐมนตรีและสภาความมั่นคงแห่งชาติ ศึกษา วิจัยและพัฒนาเกี่ยวกับกิจการ การข่าวกรอง การต่อต้านข่าวกรอง และการรักษาความปลอดภัยฝ่ายพลเรือนเพื่อเพิ่มประสิทธิภาพในการปฏิบัติงาน กระจายข่าวกรองที่มีผลกระทบต่อความมั่นคงแห่งชาติให้หน่วยงานของรัฐหรือรัฐวิสาหกิจที่เกี่ยวข้องใช้ประโยชน์ตามความเหมาะสมเป็นศูนย์กลางประสานกิจการการข่าวกรอง การต่อต้านข่าวกรอง และการรักษาความปลอดภัยฝ่ายพลเรือนกับหน่วยข่าว

[19] มติชน, 20 ตุลาคม 2544, หน้า 24

[20] พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2528 มาตรา 4 (20 สิงหาคม 2528): 2.

กรองอื่นภายในประเทศ รวมไปถึงอำนาจหน้าที่ในการปฏิบัติงานเกี่ยวกับกิจการการข่าวกรอง[21] การต่อต้านข่าวกรอง[22] การข่าวกรองทางการสื่อสาร[23] และการรักษาความปลอดภัยฝ่ายพลเรือน[24]

ในเดือนตุลาคมปี 2545 รัฐบาลทักษิณ ชินวัตร จัดตั้ง กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร หรือ “ไอซีที” โดยมีการกล่าวถึงขนาดว่าเป็นการปฏิรูประบบราชการไทย เป็นครั้งที่ 3 ในประวัติศาสตร์ สำนักงานข้าราชการพลเรือน (ก.พ.) ระบุประโยชน์ของกระทรวงดังกล่าวว่า “จะทำให้ประเทศไทยมีองค์กรรับผิดชอบจัดการด้านเทคโนโลยีและการสื่อสารที่ชัดเจน เพราะในอนาคต คอมพิวเตอร์ โทรคมนาคม และสารสนเทศ จะต้องนำมาประยุกต์ใช้ร่วมกันเพื่อเป็นเครื่องมือทางการค้า การลงทุน อุตสาหกรรม การศึกษาและบันเทิง”[25] บทบาทหน้าที่ส่วนหนึ่งของกระทรวงไอซีทีจะเน้นไปที่การตรวจสอบ เฝ้าระวัง สอดส่องความเคลื่อนไหวต่าง ๆ บนพื้นที่ออนไลน์ ที่รัฐมองว่ามีผลกระทบต่อ “ความมั่นคง ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชน” ซึ่งอาจจะยังมีจำนวนข้อมูลข่าวสารที่ถูกแลกเปลี่ยนกันไม่มากนัก[26]

ส่วนประเด็นปัญหาความมั่นคงและการก่อความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้ ไอซีทีเคยร่วมประสานกับผู้ให้บริการโทรศัพท์เคลื่อนที่ 3 บริษัท ควบคุมจัดการจดทะเบียนซิมการ์ดโดยให้ประชาชนในพื้นที่จังหวัดภาคใต้ที่มักเกิดเหตุการณ์ความรุนแรง ไปแสดงตนต่อผู้

---

[21] พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2528 มาตรา 3 “การข่าวกรอง” หมายความว่า การดำเนินการเพื่อให้ทราบถึงความมุ่งหมายกำลังความสามารถ และความเคลื่อนไหว รวมทั้งวิถีทางของต่างชาติหรือองค์การก่อการร้ายที่อาจกระทำการอันเป็นการกระทบกระเทือนต่อความมั่นคงแห่งชาติ ทั้งนี้ เพื่อให้รัฐบาลนำมาประกอบการพิจารณาในการกำหนดนโยบายแห่งชาติ

[22] “การต่อต้านข่าวกรอง” หมายความว่า การดำเนินการเพื่อต่อต้านการกระทำของต่างชาติหรือองค์การก่อการร้ายที่มุ่งหมายจะให้ได้ไปซึ่งความลับของชาติ หรือทำลายความมั่นคงแห่งชาติโดยการจารกรรม การบ่อนทำลาย การก่อวินาศกรรม และการก่อการร้าย

[23] “การข่าวกรองทางการสื่อสาร” หมายความว่า การใช้เทคนิคและการดำเนินกรรมวิธีทางเครื่องมือสื่อสารด้วยการดักรับการติดต่อสื่อสารทางสัญญาณวิทยุ เพื่อให้ได้มาซึ่งข่าวเกี่ยวกับความเคลื่อนไหวของต่างชาติหรือองค์การก่อการร้ายอันอาจจะมีผลกระทบกระเทือนต่อความมั่นคงแห่งชาติ

[24] “การรักษาความปลอดภัยฝ่ายพลเรือน” หมายความว่า การให้คำแนะนำ ช่วยเหลือและกำกับดูแลส่วนราชการฝ่ายพลเรือน ราชการส่วนท้องถิ่นและรัฐวิสาหกิจ ในการดำเนินการเพื่อรักษาความปลอดภัยแก่เจ้าหน้าที่ สถานที่ เอกสารและสิ่งของอื่น ๆ ของทางราชการให้พ้นจากการจารกรรม การบ่อนทำลาย การก่อวินาศกรรม และการก่อการร้าย

[25] มติชน, 24 กันยายน 2545, หน้า 13

[26] มติชน, 22 ธันวาคม 2549, หน้า 16.

ให้บริการภายในเวลาที่กำหนด และตั้งเงื่อนไขว่า หากไม่ไปรายงานจะไม่สามารถใช้งานโทรศัพท์เคลื่อนที่ติดต่อสื่อสารได้ อีกทั้ง กระทรวงไอซีทียังทำงานร่วมกับ คณะกรรมการกิจการโทรคมนาคมแห่งชาติ หรือ กทช. (ปัจจุบันมีชื่อว่า คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือ กสทช.) ในปฏิบัติการควบคุมการใช้คลื่นความถี่จากต่างประเทศ เพื่อป้องกันการใช้คลื่นความถี่สูงจุดชนวนระเบิด[27]

ปรากฏการณ์ที่ชี้ให้เห็นถึงการพัฒนาศักยภาพกลไกการสอดส่องอย่างชัดเจนคือกรณีการตราพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 และ การแก้ไขเพิ่มเติมกฎหมายป้องกันและปราบปรามยาเสพติดเมื่อปี 2545 เพื่อกำหนดมาตรการพิเศษให้เจ้าพนักงานสามารถได้มาซึ่งข้อมูลข่าวสารในสิ่งสื่อสารที่ถูกใช้เพื่อ ประโยชน์ในการกระทำความผิดเกี่ยวกับการฟอกเงินและยาเสพติดได้ บทบัญญัติทั้งสองนับเป็นต้นแบบของการให้อำนาจหน้าที่แก่เจ้าพนักงานในการดำเนินกลไกการเฝ้าระวัง ติดตาม และสอดส่องความเคลื่อนไหวที่อาจนำไปสู่การก่ออาชญากรรมอย่างใดอย่างหนึ่งเป็นการเฉพาะ ก่อนจะเป็นบทบัญญัติสำคัญที่ถูกใส่ไว้ในกลุ่มกฎหมายป้องกันและปราบปรามอาชญากรรมอีกหลายฉบับ เช่น พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556

3.3. การหวนคืนสู่สังเวียนของหน่วยงานความมั่นคงไทยท่ามกลางความขัดแย้งทางการเมือง

ภายหลังการรัฐประหารเมื่อวันที่ 19 กันยายน พ.ศ. 2549 รัฐบาลที่มาจากการรัฐประหารมีคำสั่งนายกรัฐมนตรีที่ 205/2549 ผลักดันการตราพระราชบัญญัติการรักษาความมั่นคงในราชอาณาจักร โดยแฝงนัยของการสร้าง “รัฐตำรวจ” ด้วยการขยับขยายขอบเขตอำนาจแก่เจ้าหน้าที่ กอ. รมน. อย่างล้นเกิน[28] และสร้างสภาวะยกเว้นให้กลายเป็นภาวะปกติที่มอบอำนาจพิเศษแก่เจ้าหน้าที่ความมั่นคงในลักษณะถาวร ซึ่งก่อนหน้านี้ กฎหมายดังกล่าวถูกรัฐสภาตีตกไปหลายต่อหลายครั้ง ตั้งแต่สมัยรัฐบาลชวน หลีกภัย จนถึงรัฐบาลทักษิณ ชินวัตร เนื่องจากสมาชิกสภาที่มาจากการเลือกตั้งส่วนใหญ่เห็นตรงกันว่าเนื้อหาของพระราชบัญญัติฉบับนี้ทำลายสิทธิ

[27] ประชาชาติธุรกิจ, 20 ตุลาคม 2548, หน้า 17.

[28] มติชน, 15 พฤศจิกายน 2550, หน้า 6.

เสรีภาพขั้นพื้นฐานของประชาชนอย่างร้ายแรง แต่ทันทีที่มีการรัฐประหารขึ้นเมื่อ 19 กันยายน พ.ศ. 2549 มีการฉีกรัฐธรรมนูญ รวบอำนาจ ล้มรัฐบาล ล้มรัฐสภาลง และจัดตั้งสภานิติบัญญัติแห่งชาติขึ้นมาเป็นฝ่ายนิติบัญญัติแทนรัฐสภา พระราชบัญญัติการรักษาความมั่นคง ในราชอาณาจักรจึงถูกตราออกมาอย่างรวดเร็วใน พ.ศ. 2550

กอ. รมน. เล็งเห็นว่า[29] ภัยคุกคามในช่วงทศวรรษที่ 2550 เริ่มแปรเปลี่ยนเป็นภัยคุกคามในรูปแบบใหม่ และจำเป็นต้องเร่งดำเนินการ ซึ่งหมายความว่า จะต้องมีกลไกที่มีประสิทธิภาพรู้เท่าทันภัยคุกคาม ทั้งปัญหายาเสพติด การหลบหนีเข้าเมือง การก่อการร้าย อาชญากรรมข้ามชาติที่อาศัยความก้าวหน้าของเทคโนโลยีการสื่อสาร เพื่อหลบหลีกการตรวจสอบ และเฝ้าระวังของเจ้าหน้าที่ฝ่ายความมั่นคง จากกรณีแฮกเกอร์เจาะข้อมูลของกระทรวงไอซีที กอ. รมน. จึงได้กำชับหน่วยกำลังหลักทั้งหมดและประสานงานร่วมกันกับตำรวจนครบาลใน กทม. และ กอ. รมน. ระดับภาค โดยเฉพาะข้อมูลที่เป็นความลับ กอ. รมน. ต้องคุมเข้ม เพราะกลัวโดนเจาะข้อมูลเหมือนกันกับกรณีของกระทรวง ไอซีที ทั้งนี้ โฆษก กอ. รมน. ยังเน้นย้ำถึงความสำคัญของพระราชบัญญัติการรักษาความมั่นคงในราชอาณาจักรด้วยว่า กฎหมายดังกล่าวจะช่วยให้ “สามารถเข้าไปตรวจสอบในชั้นต้นว่าการใช้สัญญาณเกี่ยวพันอะไรกับความมั่นคงแค่ไหน”[30]

ด้วยเหตุที่มีพระราชบัญญัติการรักษาความมั่นคงในราชอาณาจักร ให้อำนาจแก่เจ้าหน้าที่ฝ่ายความมั่นคง ในการดำเนินกิจการที่เกี่ยวกับการรักษาความมั่นคงอย่างกว้างขวาง[31] กินความไปถึงอำนาจเกี่ยวกับการสอดส่อง “ติดตาม ตรวจสอบ และประเมินแนวโน้มของสถานการณ์ที่อาจก่อให้เกิดภัยคุกคามด้านความมั่นคงภายในราชอาณาจักร”[32] และเพื่อให้ปฏิบัติการ “เสริมสร้างให้ประชาชนตระหนักในหน้าที่ที่ต้องพิทักษ์รักษาไว้ซึ่งชาติ ศาสนา และพระมหากษัตริย์ สร้างความรักความสามัคคีของคนในชาติ รวมทั้งส่งเสริมให้ประชาชนเข้ามามีส่วนร่วมในการป้องกัน และแก้ไขปัญหาต่างๆ ที่กระทบต่อความมั่นคงภายในราชอาณาจักรและ

[29] ข่าวสด, 20 มิถุนายน 2551, หน้า 6.

[30] มติชน, 18 มกราคม 2551, หน้า 11.

[31] มติชน, 18 ตุลาคม 2550, หน้า 2.

[32] พระราชบัญญัติการรักษาความมั่นคงในราชอาณาจักร พ.ศ. 2551 มาตรา 7(1), *ราชกิจจานุเบกษา ฉบับกฤษฎีกา* เล่มที่ 125 ตอนที่ 39 ก (27 กุมภาพันธ์ 2551): 35.

ความสงบเรียบร้อยของสังคม”[33] จึงมีความกังวลว่าถ้อยคำและเงื่อนไขในการใช้อำนาจที่คลุมเครือ จะนำไปสู่การตีความของเจ้าพนักงานของรัฐในลักษณะเปิดช่องให้ตนเองใช้อำนาจสอดส่องกิจกรรมต่าง ๆ ของประชาชนว่า “อะไร” เป็นภัยต่อความมั่นคงชาติ หรือแท้ที่จริงแล้วเป็นการสอดส่องเพื่อความมั่นคงของ “รัฐบาล” หรือ “หน่วยงานความมั่นคง” เองเสียมากกว่า

อย่างไรก็ดี จุดเปลี่ยนทางประวัติศาสตร์ที่ทำให้เห็นว่า รัฐไทยได้พัฒนากลไกการสอดส่องเพื่อรับมือกับปัญหาอาชญากรรมและภัยคุกคามที่มาพร้อมกับความก้าวหน้าทางเทคโนโลยีสารสนเทศ ก็คือ การประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550

3.4. การสถาปนาอำนาจรัฐรวมศูนย์การสอดส่องประชาชนเพื่อความมั่นคงของชาติในสมรภูมิดิจิทัล

รัฐไทยเริ่มตระหนักถึงความเปลี่ยนแปลง คือ การตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งมีบทบัญญัติให้อำนาจแก่เจ้าหน้าที่รัฐในการดำเนินกลไกการสอดส่องผู้คนโลกออนไลน์อย่างชัดแจ้งเป็นครั้งแรก จากนั้นมีการปรับปรุงแก้ไขหนึ่งครั้งโดยการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 โดยหนึ่งในเหตุผลหลักคือ เนื่องมาจาก “...รูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้นตามพัฒนาการทางเทคโนโลยีซึ่งเปลี่ยนแปลงอย่างรวดเร็ว...” ซึ่งฉบับหลังนี้ มีการปรับปรุงแก้ไขเพิ่มเติมอำนาจหน้าที่ของเจ้าหน้าที่รัฐเกี่ยวกับการสอดส่องด้วยเช่นกัน

รัฐไทยจึงได้ทำการแก้ไขเพิ่มกฎหมายเกี่ยวกับการปราบปรามอาชญากรรมทางคอมพิวเตอร์ และขยายอำนาจรัฐในการกำกับควบคุมความเคลื่อนไหวของข้อมูลข่าวสารบนโลกออนไลน์ รวมถึงการแสดงความคิดเห็นต่าง ๆ ในพื้นที่สื่อสังคมออนไลน์มากขึ้น ด้วยการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 พร้อมทั้งยังปรับปรุงโครงสร้างการทำงานหน่วยงานที่เกี่ยวข้อง และมอบภารกิจให้แก่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) หลายประการ เช่น

[33] พระราชบัญญัติการรักษาความมั่นคงในราชอาณาจักร พ.ศ. 2551 มาตรา 7(4), *ราชกิจจานุเบกษา ฉบับกฤษฎีกา* เล่มที่ 125 ตอนที่ 39 ก (27 กุมภาพันธ์ 2551): 36.

งานสอดส่องเฝ้าระวังงานตรวจพิสูจน์หลักฐาน การตรวจยึดและอายัด และงานด้านประสานความร่วมมือผู้ให้บริการอินเทอร์เน็ตและให้บริการสื่อออนไลน์ในการกำกับควบคุม[34]

ยิ่งไปกว่านั้นยังมีการตรา พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จึงเป็นเสาหลักทางประวัติศาสตร์ในการสถาปนาอำนาจในการสอดส่องของรัฐขึ้นโดยอาศัยเงื่อนไขความวิกฤติ

แม้มีพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 แต่กลับถูกชะลอ การบังคับใช้เพื่อคุ้มครองประชาชน และแม้จะบังคับใช้เต็มรูปแบบก็ยังมีมาตรา 4 (2) ที่ยกเว้นการคุ้มครองสิทธิในข้อมูลส่วนบุคคล หากเป็นการใช้อำนาจของรัฐในการป้องกันและปราบปรามอาชญากรรม ก่อการร้าย และรักษาความมั่นคง ที่เป็นการใช้อำนาจตามกฎหมายอื่น ๆ อันหมายถึงกฎหมายที่ให้อำนาจสอดส่องทั้งหลายที่ได้กล่าวถึงไปแล้วและจะกล่าวถึงในหัวข้อถัดไป

เมื่อพิจารณาถึงการจัดโครงสร้างองค์กรและให้อำนาจในการสอดส่อง การปรับโครงสร้างกองอำนวยการรักษาความมั่นคงภายในตามคำสั่งสำนักนายกรัฐมนตรี ที่ 312 /2562 เรื่อง “การจัดโครงสร้าง การแบ่งส่วนงาน หน้าที่และอำนาจของส่วนงาน และอัตรากำลังของกองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร” เพื่อ “ปรับโครงสร้าง กอ.รมน. ใหม่เพิ่ม 4 ส่วนงานรองรับปัญหาสิทธิมนุษยชน ภัยไซเบอร์” หนึ่งในนั้น คือ “ศูนย์ดิจิทัลเพื่อความมั่นคง” ซึ่งมีหน้าที่และอำนาจ เช่น กำหนดนโยบาย วางแผน อำนวยการ ประสานงาน กำกับดูแล และดำเนินการเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสาร และการปฏิบัติการด้านไซเบอร์ของ กอ.รมน. เป็นต้น [35]

สอดรับกับการเสริมศักยภาพการสอดส่องเพื่อให้ได้มาซึ่งพยานหลักฐานในการดำเนินคดีทางกฎหมาย ในเดือนกันยายน ปี 2563 ก็มีการตราพระราชกฤษฎีกาตั้งตำรวจสืบสวนสอบสวนคดี

---

[34] การตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560, *ราชกิจจานุเบกษา ฉบับ กฤษฎีกา* เล่มที่ 134 ตอนที่ 10 ก (24 มกราคม 2560).

[35] ข่าวเนชั่นสุดสัปดาห์, “จัดโครงสร้าง กอ.รมน. รับมือภัยความมั่นคงยุคใหม่,” 2 ธันวาคม 2562, *เนชั่นสุดสัปดาห์*, (สืบค้นเมื่อ 29 เมษายน 2564), https://www.nationweekend.com/content/government_inside/3599.

ทางเทคโนโลยีระดับกองบัญชาการเพิ่ม[36] เหตุผลในการประกาศใช้พระราชกฤษฎีกา กล่าวว่า[37] “ในปัจจุบันโครงสร้างของสำนักงานตำรวจแห่งชาติในปัจจุบันไม่สามารถรองรับปัญหาที่มีความซับซ้อนจากการใช้เทคโนโลยีในการกระทำความผิดในลักษณะต่าง ๆ และมีการนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์โดยมิชอบ หรือเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นความผิดตามกฎหมาย กระทบสิทธิของผู้อื่น หรือ ความมั่นคงของประเทศ” และ อำนาจหน้าที่หลัก ๆ ของกองบัญชาการดังกล่าวประกอบไปด้วย การดำเนินการเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ทั่วราชอาณาจักร การปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา กฎหมายว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่น อันเป็นความผิดทางอาญาเกี่ยวกับอาชญากรรมทางเทคโนโลยีและความผิดอื่นที่เกี่ยวเนื่อง ดำเนินการเกี่ยวกับการรวบรวมข้อมูล ตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี ตลอดจนดำเนินการเกี่ยวกับการพิสูจน์หลักฐานดิจิทัล การตรวจสถานที่เกิดเหตุ และเก็บรวบรวมพยานหลักฐานดิจิทัลเพื่อสนับสนุนการปฏิบัติงานสืบสวนสอบสวนของหน่วยงานต่าง ๆ [38]

หลักฐานทางประวัติศาสตร์กฎหมายเหล่านี้ล้วนเป็นการสะท้อนให้เห็นถึงการสถาปนา “รัฐตำรวจ” ที่รวมศูนย์การใช้อำนาจสอดส่องประชาชนของรัฐบาลไทยที่ได้มีความพยายามผลักดันกฎหมายและสร้างกลไกบังคับตามอย่างชัดแจ้ง

---

[36] พระราชกฤษฎีกา แบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ (ฉบับที่ 5) พ.ศ.2563, *ราชกิจจานุเบกษา ฉบับกฤษฎีกา* เล่มที่ 137 ตอนที่ 71 ก (8 กันยายน 2563).

[37] หมายเหตุท้าย พระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ (ฉบับที่ 5) พ.ศ.2563, *ราชกิจจานุเบกษา ฉบับ กฤษฎีกา* เล่มที่ 137 ตอนที่ 71 ก (8 กันยายน 2563).

[38] ประชาไท, “พระราชกฤษฎีกาตั้งตำรวจสืบสวนสอบสวนคดีทางเทคโนโลยีระดับกองบัญชาการเพิ่ม,” *ประชาไท*, แก้ไขล่าสุด 8 กันยายน 2563, สืบค้นเมื่อ 29 เมษายน 2564, https://prachatai.com/journal/2020/09/89430.

4. กฎหมายที่ให้อำนาจพิเศษแก่รัฐบาลในการสอดส่องประชาชนทำกิจกรรมในโลกไซเบอร์

หากมองปรากฏการณ์ระดับโลกจะพบงานชื่อว่า *The right to privacy and the future of mass surveillance*[39] ซึ่งได้อ้างถึงบทบัญญัติมาตรา 7 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง และบทบัญญัติมาตรา 8 ของอนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (European Convention on Human Rights - ECHR) ที่ได้ระบุถึงสิทธิในการได้รับความเคารพชีวิตส่วนตัวและครอบครัว งานศึกษาได้ชี้ให้เห็นปัญหาที่บทบัญญัติกฎหมายระหว่างประเทศทั้งสองไม่สามารถนำมาบังคับใช้เพื่อควบคุมการใช้อำนาจสอดส่องของประเทศมหาอำนาจอย่างสหรัฐอเมริกา และสหราชอาณาจักรที่ได้รับการรับรองให้อำนาจในการใช้กลไกการสอดส่องมากกว่าประเทศอื่นในยุโรปด้วยกัน เนื่องจากเป็นประเทศที่ตกเป็นเป้าหมายแรก ๆ ในการใช้ความรุนแรงของผู้ก่อการร้าย แต่ด้วยเหตุที่กรอบทางกฎหมายที่ไม่มีขอบเขตที่ชัดเจน ได้นำไปสู่ปัญหาการบังคับใช้กลไกการสอดส่องที่ไม่ได้สัดส่วน และยังมีลักษณะเป็นการสอดส่องโดยไร้เป้าหมาย (Untargeted Cyber Surveillance) แต่เหวี่ยงแหครอบคลุมทั้งคนในประเทศและต่างประเทศ

เมื่อสำรวจย้อนมาที่รัฐไทยก็จะพบมาตรการทางกฎหมายที่เอื้อให้เกิดการสอดส่องกิจกรรมของประชาชนโดยรัฐบาลขึ้นในรูปแบบของกฎหมายความมั่นคงที่อ้างความจำเป็นในการป้องกันภัยคุกคามหรือการแทรกซึมดังปรากฏในกฎหมายดังต่อไปนี้

4.1. กฎหมายเกี่ยวข้องกับกิจกรรมในโลกไซเบอร์

กลางปี 2562 รัฐไทย ประกาศใช้กฎหมายที่ยึดโยงกับโลกยุคดิจิทัลพร้อมกันถึง 2 ฉบับ ได้แก่ 1) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ 2) พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นับว่าเป็นก้าวสำคัญอีกก้าวหนึ่งของรัฐไทยที่เริ่มตระหนักถึงปัญหาความมั่นคงทางไซเบอร์ และการปกป้องคุ้มครองข้อมูลส่วนบุคคลของประชาชน

[39] Kinfe Micheal Yilma, "The United Nations Data Privacy System and Its Limits," *International Review of Law, Computers & Technology* 33, no. 2 (2018): 224-248.

สาระสำคัญของ พ.ร.บ.การรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ชี้ให้เห็นถึง การอุดช่องว่างบางอย่างที่กฎหมายเดิมมีอยู่ คือ การตั้ง “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” (กมช.) National Cyber Security Committee : NCSC) ประกอบด้วย (1) นายกรัฐมนตรี เป็นประธานกรรมการ (2) กรรมการโดยตำแหน่ง ได้แก่ รัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอีเอส) ปลัดกระทรวงการคลัง ปลัดกระทรวงยุติธรรม ผู้บัญชาการตำรวจแห่งชาติแห่งชาติ และเลขาธิการสภาความมั่นคงแห่งชาติ (3) กรรมการผู้ทรงคุณวุฒิ ไม่เกิน 7 คน เป็นผู้กำหนดนโยบายและแผนงาน พร้อมทั้งให้มี คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) ซึ่งมีรัฐมนตรีกระทรวงดิจิทัลฯ เป็นประธาน โดย กกม. จะกำหนดรายชื่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 8 ด้าน ได้แก่ ความมั่นคงของรัฐ บริการภาครัฐที่สำคัญ การเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม การขนส่งและโลจิสติกส์ พลังงานและสาธารณูปโภค สาธารณสุข และด้านอื่น ๆ ตามที่มีการกำหนดเพิ่มเติม ซึ่งมีหน้าที่ต้องปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยที่กำหนด[40] ในแง่นี้ มีโอกาสที่บรรษัทเจ้าของเทคโนโลยีจะเข้ามามีส่วนร่วมในกลไกการเฝ้าระวังสอดส่องกับเจ้าหน้าที่ความมั่นคงได้อย่างเปิดเผยมากขึ้น

กฎหมายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กำหนดให้ผู้มีอำนาจหน้าที่ที่เกี่ยวข้องจะต้องติดตาม ตรวจสอบและเฝ้าระวังภัยต่าง ๆ เพื่อประเมินสถานการณ์ที่เกิดขึ้นอยู่ตลอดเวลา ทั้งยังได้แบ่งประเภทภัยคุกคามทางไซเบอร์ออกเป็น 3 ระดับ[41] คือ

หนึ่ง ภัย “ไม่ร้ายแรง” หมายถึง ภัยคุกคามที่มีความเสี่ยงทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือบริการของรัฐด้อยประสิทธิภาพลง

สอง ภัย “ร้ายแรง” หมายถึง การโจมตีระบบ มุ่งเป้าที่ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทำให้บริการภาครัฐ ความมั่นคงของรัฐ การป้องกันประเทศ เศรษฐกิจ สาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหายจนไม่สามารถทำงานหรือใช้บริการได้ และ

---

[40] ICT-Prachachat, “ประกาศแล้ว! 2 กฎหมายฮอต' ไซเบอร์ซิเคียวริตี้-คุ้มครองข้อมูลส่วนบุคคล',” *ประชาชาติธุรกิจ*, แก้ไขล่าสุด 27 พฤษภาคม 2562, สืบค้นเมื่อ 29 เมษายน 2564, https://www.prachachat.net/ict/news-331574.

[41] เรื่องเดียวกัน.

สาม “วิกฤต” คือกรณีที่มีการโจมตีที่ส่งผลกระทบรุนแรงในวงกว้าง ทำให้ระบบล้มเหลวจนรัฐไม่สามารถควบคุมได้ มีความเสี่ยงที่จะลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ หรือเป็นภัยที่กระทบต่อความสงบเรียบร้อยของประชาชนหรือความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งตกอยู่ในภาวะคับขัน ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญ[42]

เมื่อพิจารณาถึงคำนิยามส่วนหนึ่งของภัยคุกคามไซเบอร์ในระดับ “ร้ายแรง” และ “วิกฤต” ข้างต้น จะพบว่า “ตัวบทบัญญัติ” นั้นเปิดโอกาสให้รัฐและผู้บังคับใช้กฎหมายสามารถตีความได้อย่างกว้าง อาทิ “ภัยที่กระทบต่อความสงบเรียบร้อยของประชาชน “ความมั่นคงของรัฐ” หรือ “มาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญ” กลายเป็นช่องที่สร้างความชอบธรรมให้แก่เจ้าหน้าที่ฝ่ายความมั่นคงใช้อำนาจในการสอดส่องความเคลื่อนไหวต่าง ๆ ในโลกออนไลน์ได้ตลอดเวลา นอกจากนี้ ในกรณี “ร้ายแรง” หรือ “วิกฤต” เพื่อประโยชน์ในการป้องกัน ประเมินผล รับมือปราบปราม ระงับ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เจ้าหน้าที่รัฐตามกฎหมายนี้มีอำนาจขอข้อมูลที่เป็นปัจจุบันและต่อเนื่องจากผู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์จากบรรษัทผู้ให้บริการ ซึ่งบรรษัทนั้นต้องให้ความร่วมมือและให้ความสะดวกแก่ กกม. โดยเร็ว

4.2. ความกังวลต่อแนวโน้มการสร้างกฎหมายที่ให้อำนาจรัฐบาลในการสอดส่องกิจกรรมของประชาชน

แนวโน้มในการสอดส่องกิจกรรมทั้งหลายที่รัฐบาลเห็นว่าเป็นภัยคุกคามต่อความมั่นคงได้แสดงออกมาอย่างต่อเนื่องผ่านการผลักดันกฎหมายที่มีลักษณะติดตามสอดส่อง เก็บข้อมูล เพื่อสืบย้อนหลัง แล้วแสวงหาพยานหลักฐานมาดำเนินคดีทางอาญาต่อเป้าหมายการสอดส่อง เช่น การผลักดัน ร่างกฎหมายว่าด้วยการดำเนินงานขององค์กรที่ไม่แสวงหารายได้หรือผลกำไรมาแบ่งปันกัน และร่างพระราชบัญญัติส่งเสริมและพัฒนาองค์กรภาคประชาสังคม

ตามที่ คณะรัฐมนตรี (ครม.) มีมติเมื่อวันที่ 23 กุมภาพันธ์ 2564 อนุมัติหลักการร่างกฎหมายว่าด้วยการดำเนินงานขององค์กรที่ไม่แสวงหารายได้หรือผลกำไรมาแบ่งปันกัน และร่าง

[42] ICT-Prachachat, “ประกาศแล้ว! 2 กฎหมายฮอต' ไซเบอร์ซิเคียวริตี้-คุ้มครองข้อมูลส่วนบุคคล',” *ประชาชาติธุรกิจ*, แก้ไขล่าสุด 27 พฤษภาคม 2562, สืบค้นเมื่อ 29 เมษายน 2564, https://www.prachachat.net/ict/news-331574.

พระราชบัญญัติส่งเสริมและพัฒนาองค์กรภาคประชาสังคม พ.ศ. .... โดยให้สำนักงานคณะกรรมการกฤษฎีกา (สคก.) นำไปประกอบการพิจารณายกร่างกฎหมาย และเปิดรับความคิดเห็นจากผู้มีส่วนเกี่ยวข้อง ก่อนเสนอ ครม. พิจารณาอีกครั้ง ซึ่ง ครม. มีมติเห็นชอบเพิ่มเติมหลักการร่างกฎหมายดังกล่าว เพื่อให้สอดคล้องกับข้อกำหนดตามมาตรฐานสากลด้านการป้องกันและปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง (Anti-Money Laundering and Combating the Financing of Terrorism: AML/CFT) เมื่อ สคก. ได้ดำเนินการปรับปรุงเพิ่มเติมร่างกฎหมายดังกล่าวแล้ว จะมีการเปิดให้ประชาชนทั่วไปได้ร่วมแสดงความคิดเห็นอีกครั้ง[43]

ข้อสังเกตที่สำคัญ คือ มาตรา 6 ของร่างพระราชบัญญัติฉบับนี้ให้อำนาจหน่วยงานภาครัฐในการเข้าไปในสำนักงานขององค์กรไม่แสวงหากำไรเพื่อตรวจสอบและยึดข้อมูลการสื่อสารทางอิเล็กทรอนิกส์ขององค์กรเป้าหมาย อันมีลักษณะฝ่าฝืนต่อกระบวนการนิติธรรม (Due Process) ซึ่งอาจถูกใช้เพื่อการข่มขู่ได้ ทั้งยังเป็นการละเมิดการคุ้มครองความเป็นส่วนตัวของกลุ่มเสี่ยงที่องค์กรดูแลไปจนถึงเกิดภัยคุกคามต่อครอบครัวของพวกเขา เนื่องจากข้อมูลอ่อนไหวจะถูกเก็บเป็นความลับขององค์กรที่ให้ความช่วยเหลือเหยื่อผู้เสียหาย นอกจากนี้ เจ้าหน้าที่ขององค์กรยังอาจได้รับความเสี่ยงภัยโดยเฉพาะอย่างยิ่งหากพวกเขาทำงานในกรณีตรวจสอบการใช้อำนาจโดยมิชอบและการทุจริตของเจ้าหน้าที่รัฐ

การอ้างว่าการผลักดันกฎหมายดังกล่าวเป็นการทำตามพันธกรณีระหว่างประเทศด้านการต่อต้านอาชญากรรมระหว่างประเทศโดยเฉพาะการฟอกเงินขององค์กรอาชญากรรมข้ามชาติและการก่อการร้ายนั้น เป็นการสร้างตราบาปต่อองค์กรพัฒนาเอกชน (Non-Governmental Organization – NGOs) โดยตรงเป็นการปฏิบัติในฐานะผู้ต้องสงสัยว่าจะเป็นอาชญากรตั้งแต่ยังไม่มีคำพิพากษาของศาล การกำหนดภาระหน้าที่ในการต้องจดทะเบียน รายงานที่มารายได้ การใช้งบประมาณ และเก็บข้อมูลไว้ให้ตรวจสอบ หาไม่แล้วจะต้องโทษทางอาญา ล้วนเป็นการบังคับให้องค์กรพัฒนาเอกชน “เปิดเผย” ข้อมูลเพื่อให้รัฐ “สอดส่อง” การทำงานตั้งแต่ต้น และสามารถ

---

[43] กองบรรณาธิการ The Standard, “ครม. ไฟเขียว เพิ่มหลักการร่างกฎหมาย NGO รวม 8 ประเด็น ต้องเปิดเผยข้อมูลองค์กร-งบการเงิน,” *THE STANDARD*, แก้ไขล่าสุด 29 มิถุนายน 2564, เข้าถึงเมื่อ 30 มิถุนายน 2564, https://thestandard.co/cabinet-increases-the-principle-of-drafting-ngo-law.โดยดูข้อมูลต้นทางมติคณะรัฐมนตรีได้ที่เว็บไซต์ทางการของรัฐบาลไทย https://www.thaigov.go.th/news/contents/details/39334

“มองย้อนกลับ” ไปเพื่อแสวงหาพยานหลักฐานมาดำเนินคดีต่อองค์กรพัฒนาเอกชนได้ ตั้งแต่ยังไม่มีการนำเสนอพยานหลักฐานต่อองค์กรตุลาการให้เห็นมูลเหตุที่เป็นการกระทำความผิดกฎหมายเพื่อขอหมายศาลในการตรวจค้นและเก็บพยานหลักฐานภายใต้ระบบควบคุมการใช้อำนาจมิให้ละเมิดสิทธิมนุษยชน

5. สถานะทางกฎหมายพยานของข่าวกรองที่ได้จากการสอดส่องประชาชน

งานศึกษาด้านอาชญาวิทยาและกระบวนการยุติธรรมทางอาญาในยุคดิจิทัล[44] ได้นำเสนอว่าการสร้างระบบฐานข้อมูลจะช่วยพัฒนาศักยภาพแก่รัฐในการบังคับใช้กฎหมายเพื่อตรวจจับและสืบสวนสอบสวนการก่ออาชญากรรม รวมถึงการก่อการร้าย เนื่องจากจะเป็นแหล่งรวมข้อมูลจำนวนมหาศาลให้รัฐสามารถหยิบใช้เพื่อการดังกล่าวได้อย่างสะดวก อย่างไรก็ตาม รัฐก็ไม่ควรใช้อำนาจเก็บรวบรวม สำรวจ หรือใช้ข้อมูลในฐานข้อมูลตามอำเภอใจ แต่จะต้องคำนึงถึงการเคารพสิทธิส่วนบุคคลและความเป็นส่วนตัวของประชาชนด้วย ตัวอย่างเช่น การจัดเก็บข้อมูลอัตลักษณ์ของบุคคลที่ไม่ได้ปรากฏให้เห็นแก่สาธารณชน ควรจะต้องมีพฤติการณ์ที่เพียงพอหรือควรเชื่อได้ว่าบุคคลนั้นเป็นผู้กระทำความผิด และอาจต้องได้รับมอบอำนาจจากหมายศาลด้วย หรือ กรณีที่หากเจ้าหน้าที่เห็นว่าจะใช้วิธีการรวบรวมข้อมูลเพื่อจัดทำประวัติของผู้ต้องสงสัยแทนการบังคับใช้กฎหมายตามปกติ การปฏิบัติหน้าที่ควรคำนึงหลักความจำเป็นและได้สัดส่วน เพื่อหลีกเลี่ยงการเลือกประติบัติโดยไม่ชอบด้วยกฎหมาย ขณะเดียวกัน ศาลก็ควรประเมินให้แน่ใจด้วยว่าประวัติส่วนตัวของบุคคลที่ถูกจัดทำขึ้นมีกระบวนการตรวจสอบความถูกต้อง หรือมีปัจจัยเสี่ยงที่ทำให้เกิดอคติระหว่างการจัดทำหรือไม่ด้วย รวมทั้ง การดำเนินการใด ๆ เกี่ยวกับการเก็บรวบรวมข้อมูลบุคคลก็ควรต้องอยู่ภายใต้กรอบของกฎหมายอย่างที่สังคมสามารถตรวจสอบได้ และเป็นไปตามวิถีทางของประชาธิปไตย เป็นต้น[45]

แม้อำนาจในการรวบรวมพยานหลักฐานดิจิทัลจะมีความสำคัญต่อกระบวนการยุติธรรมในโลกไซเบอร์ แต่กลับมีความพยายามตั้งคำถามต่อข้อเสนอหรือความเชื่อเช่นว่านั้นอยู่ไม่น้อย เช่น บทความสั้นเรื่อง *Computer forensics: Characteristics and preservation of digital*

[44] Christopher Slobogin, Policing, databases, and surveillance. Criminology, Criminal Justice, *Law & Society*, 18(3) (2017): 70-84.

[45] Christopher Slobogin, Policing, databases, and surveillance. Criminology, Criminal Justice, *Law & Society*, 18(3) (2017): 79-80.

evidence[46] ได้เสนอว่า หลักฐานดิจิทัลที่เกี่ยวข้องกับการกระทำความผิดทางอาญา จำเป็นต้องมีการเก็บรักษา (Preservation) การตรวจสอบ (examination) และการวิเคราะห์ (analysis) โดยใช้กระบวนการทางนิติวิทยาศาสตร์ที่สมเหตุสมผล ไม่ว่าจะเป็นไปเพื่อแสดงความบริสุทธิ์หรือพิสูจน์ความผิดของผู้ต้องสงสัยก็ตาม ทั้งนี้ ผู้ปฏิบัติงานที่เกี่ยวข้องจะต้องปฏิบัติหน้าที่ตามมาตรฐานทางวิทยาศาสตร์ ซึ่งรวมถึง “Chain of Custody” อันหมายถึง ขบวนการในการปฏิบัติงานกับพยานหลักฐานดิจิทัล เริ่มตั้งแต่ขั้นตอนการเก็บหลักฐาน การควบคุมการเข้าถึง การส่งต่อ-รับมอบ ในกรณีที่มีการปฏิบัติงานร่วมกับหน่วยงานอื่น ไปจนถึงการทำลายพยานหลักฐาน โดยในทุกขั้นตอนต้องมีการบันทึกการดำเนินงานอย่างละเอียด และมีการลงชื่อผู้รับผิดชอบเพื่อเป็นหลักฐาน

บทบาทขององค์กรตุลาการในการตรวจสอบสถานะของพยานหลักฐานที่ได้จากการสอดส่องเก็บข้อมูลด้วยชุดกฎหมายความมั่นคงและปราบปรามอาชญากรรมหลายฉบับจึงมีความสำคัญมากต่อการประกันสิทธิเสรีภาพของประชาชนทั้งในมิติของสิทธิในกระบวนการยุติธรรมที่จะสามารถต่อสู้คดีที่ถูกหน่วยงานของรัฐกล่าวหาปรักปรำด้วยพยานที่รวบรวมขึ้นด้วยกระบวนการของฝ่ายความมั่นคงที่ขาดการตรวจสอบตั้งแต่ต้น และยังส่งผลต่อความมั่นใจของปัจเจกชนและกลุ่มที่จะใช้เสรีภาพในการแสดงออก ชุมนุมและสมาคมกันโดยไม่ตกอยู่ในสภาวะหวาดกลัวว่าจะถูกจับตาการเคลื่อนไหว

6. หลักฐานการสอดส่องของรัฐบาลในสมรภูมิราชอาณาจักรไทย

สถานการณ์ในรัฐไทยนั้นปรากฏการแทรกซึมแฝงฝังลัทธิอำนาจนิยมของฝ่ายความมั่นคงเข้าขับเคลื่อนขบวนการเคลื่อนไหวทางสังคมดังที่ พวงทอง ภวัครพันธุ์ ได้นำเสนอไว้ใน Infiltrating Society: The Thai Military's Internal Security Affairs[47] ที่แสดงให้เห็นความพยายามของฝ่ายความมั่นคงในการใช้กลยุทธ์แทรกซึมเข้าไปฝังอุดมการณ์รัฐที่กองทัพประสงค์ให้ฝังอยู่ในสำนึกของพลเรือนผ่านกระบวนการเคลื่อนไหวทางสังคมของหลายองค์กรภาคประชาสังคม โดยเฉพาะเมื่อต้องเผชิญกับความท้าทายจากอุดมการณ์ทางการเมืองที่สั่นคลอนสถานะของฝ่ายความมั่นคงหรือ

[46] Loren D. Mercer, “Computer Forensics: Characteristics and Preservation of Digital Evidence,” *FBI Law Enforcement Bulletin* 73, no. 3 (2004): 28-32.

[47] Puangthong Pawakapan, “Infiltrating Society: The Thai Military’s Internal Security Affairs,” *ISEAS – Yusof Ishak Institute*, (2021).

กองทัพ สอดคล้องกับงานศึกษาของ ปิ่นแก้ว เหลืองอร่ามศรี[48] ที่ฉายภาพให้เห็นความเป็น “Cyber Dystopia” และการทำให้พื้นที่ทางไซเบอร์เป็นเรื่องเกี่ยวกับทางการทหาร (Militarization of cyberspace) ด้วยการทำให้เกิดสภาวะยกเว้น (state of exception) ที่เจ้าหน้าที่ฝ่ายความมั่นคงมีอำนาจรุกล้ำความเป็นส่วนตัวของประชาชนบนโลกออนไลน์ได้อยู่เสมอ โดยสภาวะยกเว้นดังกล่าวที่เกิดขึ้นเนื่องจากการยกระดับการใช้มาตรการการแทรกแซงสอดส่องและการสร้างบรรยากาศความเงียบบนพื้นที่ไซเบอร์ของสังคมไทยยุคหลังรัฐประหาร พ.ศ.2557 เป็นต้นมา โดย ปิ่นแก้ว ได้ชี้ให้เห็นว่า การกระทำเช่นนั้นของรัฐบาลทหารแสดงให้เห็นถึงกระบวนการบางอย่างที่รัฐไทยได้ก่อสงครามไซเบอร์ด้วยการรวมเอาการใช้กองกำลังทางการทหารและการสนับสนุนจากมวลชนกลุ่มหนึ่งเข้ามาเป็นหนึ่งในยุทธวิธีเพื่อควบคุมสอดส่องความเคลื่อนไหวที่เกิดขึ้นบนสื่อสังคมออนไลน์ โดยเฉพาะกับนักกิจกรรมและนักสิทธิมนุษยชนไทยทั้งหลาย ทั้งนี้ กระบวนการของรัฐบาลทหารเกิดขึ้นอย่างมีประสิทธิภาพผ่านสามกลไกสำคัญ คือ (1) การสอดส่องมวลชน (mass surveillance) เช่น การปิดกั้นเนื้อหาหรือการเซนเซอร์ (censorship) การสร้างข่าวปลอมหรือการสกัดกั้นเนื้อหาต่าง ๆ (Deception/Interception)[49] (2) การสอดส่องโดยมวลชน (surveillance by the masses) ผ่านการรับอาสาสมัครในโครงการลูกเสือไซเบอร์ที่ภาครัฐจัดตั้งขึ้นเพื่อนำมาช่วยเสริมศักยภาพในการสอดส่อง รวมถึงการปล่อยให้เกิดกรณีการล่าแม่มดขึ้น (Witch Hunts) หรือการไล่ล่าทำร้าย การละเมิดบุคคลอื่นๆ ที่มีพฤติกรรมเป็นปฏิปักษ์ต่อรัฐบาล[50] และ (3) การทำให้การสอดส่องดูเหมือนเป็นเรื่องปกติ (normalization of surveillance) ในสังคมไทย กลไกทั้งสามได้ทำให้สื่อสังคมออนไลน์ในไทยกลายเป็นสิ่งที่เรียกว่า “digital panopticon” อย่างสมบูรณ์แบบด้วยการสร้างบรรยากาศแห่งความเงียบงันอันเนื่องมาจากที่ประชาชนและพลเมืองเน็ต โดยความรู้สึกว่าที่ตนเองกำลังถูกรัฐสอดส่องครอบงำสมองและจิตใจอยู่ตลอดเวลาได้ในท้ายที่สุด[51] ยังส่งผลให้การประชันขันแข่งทาง

[48] Pinkaew Laungaramsri, “Mass surveillance and the militarization of cyberspace in post-coup Thailand,” *ASEAS – Austrian Journal of South-East Asian Studies*, *9*(2) (2016): 195-214.

[49] Pinkaew Laungaramsri. “Mass surveillance and the militarization of cyberspace in post-coup Thailand,” *ASEAS – Austrian Journal of South-East Asian Studies*, *9*(2) (2016): 202

[50] Ibid, 204-205.

[51] Ibid, 209-210.

อุดมการณ์ของฝ่ายความมั่นคงนั้นได้เปรียบกว่าฝ่ายสนับสนุนเสรีนิยมประชาธิปไตยและสิทธิมนุษยชนที่ถูกจับจ้องสอดส่องโดยรัฐ

6.1. การบังคับลงทะเบียนซิมมือถือแบบเติมเงิน และโครงการซิงเกิลเกตเวย์

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ขานรับนโยบายด้านความมั่นคง เร่งเดินหน้าให้มีการลงทะเบียนผู้ใช้โทรศัพท์เคลื่อนที่แบบเติมเงินทั่วประเทศในปี 2557 ช่วงหลังการรัฐประหารไม่กี่เดือน พร้อมทั้งยังกำหนดเงื่อนไขว่า หากประชาชนผู้ใช้โทรศัพท์คนใดไม่ดำเนินการลงทะเบียนภายในกรอบระยะเวลา (30 กรกฎาคม 2558) ก็จะต้องถูกระงับหมายเลขโทรศัพท์และทำให้ไม่สามารถใช้งานหมายเลขดังกล่าวได้ สถานการณ์ก่อนหน้านี้ที่ยังไม่ได้เปิดให้มีการลงทะเบียน “ทำให้กรณีเมื่อมีการกระทำที่ผิดกฎหมายเกิดขึ้นโดยอาศัยช่องทางผ่านโทรศัพท์เคลื่อนที่ ส่งผลให้เจ้าหน้าที่ผู้รักษากฎหมายใช้เวลาค่อนข้างมากในการสืบหาตัวผู้กระทำผิด”[52]

เว็บไซต์ของ กสทช. ระบุเหตุผลของการลงทะเบียนดังกล่าวว่า[53] “ประเทศไทยมีการใช้โทรศัพท์มือถือมากถึง 100 ล้านเลขหมาย โดยเป็นการใช้ซิมแบบเติมเงิน (prepaid) 90 ล้านเลขหมาย และส่วนใหญ่ไม่ลงทะเบียนซิม ทำให้เกิดช่องทางในการนำเอาซิมไปใช้ในทางที่ผิดและเป็นอันตรายต่อสังคมไทย ไม่ว่าจะเป็นการใช้โทรศัพท์ในการข่มขู่ หลอกลวง ซื้อขายยาเสพติด จุดระเบิด จนนำไปสู่ความเสียหายต่อชีวิตและทรัพย์สินของประชาชน และความมั่นคงของประเทศ และไม่สามารถหาผู้กระทำความผิดมาลงโทษได้ และในแง่มุมของการใช้บริการ การไม่ลงทะเบียนซิม ทำให้ผู้ใช้บริการเกิดความยุ่งยากในการเรียกร้องสิทธิต่าง ๆ เช่น การเรียกคืนเงินเมื่อเลิกใช้บริการ และการป้องกันปัญหาผู้แอบอ้างนำหมายเลขของเราไปใช้บริการ เป็นต้น”

อีกหนึ่งการพัฒนาศักยภาพการสอดส่องที่เกี่ยวข้องกับการป้องกันภัยความมั่นคง ซึ่งสอดคล้องกับแผนงานนโยบายด้านความมั่นคง และชี้ให้เห็นว่ารัฐไทย ต้องแสวงหากลไกบางอย่างเพื่อมาคัดง้าง ต้านทานกระแสความเปลี่ยนแปลงของระบบข้อมูลข่าวสาร ที่ผู้มีอำนาจมองว่าอาจ

---

[52] เรื่องเดียวกัน.

[53] สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ, “ทำไมต้องลงทะเบียนซิมโทรศัพท์เคลื่อนที่ระบบเติมเงิน,” (2558), *กสทช*, สืบค้นเมื่อ 29 เมษายน 2564, http://sim.nbtc.go.th/why.php

ส่งผลกระทบต่อความมั่นคง คือ ความพยายามในการสร้างระบบ “Single gateway” ขึ้นมาตามมติคณะรัฐมนตรี 30 มิถุนายน 2558[54] เพื่อให้เจ้าหน้าที่ฝ่ายความมั่นคงสามารถดำเนินการสอดส่อง คัดกรองเนื้อหาที่เผยแพร่มาจากต่างประเทศ ผ่านช่องทางโครงข่ายที่รัฐเป็นผู้ควบคุมอยู่ฝ่ายเดียว และในวันที่ 25 สิงหาคม 2558 นายกรัฐมนตรีได้เน้นย้ำให้กระทรวงไอซีทีเร่งรัดจัดซิงเกิลเกตเวย์อีกครั้ง และให้รายงานความคืบหน้าในเดือนกันยายน[55] แต่โครงการดังกล่าวถูกกระแสสังคมต่อต้านอย่างรุนแรง จนรัฐบาล ต้องพับโครงการเก็บไป[56]

6.2. เสริมพลัง สภาความมั่นคงแห่งชาติ (สมช.) และ กองอำนวยการรักษาความมั่นคงภายใน (กอ.รมน.)

เอกสารยุทธศาสตร์ กอ.รมน. พ.ศ. 2560-2564 ในส่วนของสถานการณ์ความมั่นคง ได้ระบุหัวข้อ “ภัยความมั่นคง” หลักที่ต้องเตรียมพร้อมรับมือถึง 10 หัวข้อซึ่งสะท้อนความกว้างขวางของงาน กอ.รมน. และการจัดลำดับความสำคัญภัยความมั่นคงที่รัฐต้องเฝ้าระวัง แน่นอนว่าต้องกินความไปถึงปฏิบัติการสอดส่อง อันประกอบด้วย การปราบปรามการกระทำอันเป็นการล่วงละเมิดสถาบันพระมหากษัตริย์ การขจัดความเห็นต่างและความขัดแย้งทางความคิดของคนภายในชาติ ซึ่งไม่สอดคล้องกับธรรมชาติความแตกต่างหลากหลายของมนุษย์อย่างสิ้นเชิง การแก้ไขสถานการณ์ในจังหวัดชายแดนภาคใต้ การเฝ้าระวังติดตามภัยคุกคามไซเบอร์ การรับมือกับภัยพิบัติทางธรรมชาติ การจัดการปัญหาแรงงานต่างด้าวและผู้หลบหนีเข้าเมือง การป้องกันการก่อการร้ายและอาชญากรรมข้ามชาติ การแก้ไขปัญหายาเสพติด รับมือกับปัญหาทรัพยากรธรรมชาติ

---

[54] Thai PBS News, “ประมวลเหตุการณ์ผู้ใช้อินเทอร์เน็ตประท้วง ‘ซิงเกิล เกตเวย์,’” *Thai PBS* (Thai PBS, October 1, 2015), แก้ไขล่าสุด 1 ตุลาคม 2558, สืบค้นเมื่อ 29 เมษายน 2564, https://news.thaipbs.or.th/content/5617.

[55] Thai PBS News, “ประมวลเหตุการณ์ผู้ใช้อินเทอร์เน็ตประท้วง ‘ซิงเกิล เกตเวย์,’” *Thai PBS* (Thai PBS, October 1, 2015), แก้ไขล่าสุด 1 ตุลาคม 2558, สืบค้นเมื่อ 29 เมษายน 2564, https://news.thaipbs.or.th/content/5617.

[56] Warong ThaiPublica, “ซี้ยังไม่ดำเนินการ ‘ซิงเกิล เกตเวย์,’” *ThaiPublica*, แก้ไขล่าสุด 6 พฤศจิกายน 2558, สืบค้นเมื่อ 29 เมษายน 2564 https://thaipublica.org/jabted_issue/ซี้ยังไม่ดำเนินการ-ซิง/

และสิ่งแวดล้อมที่กำลังเกิดขึ้น รวมถึง ศึกษา ประเมิน และติดตามผลกระทบที่เกิดจากข้อตกลงและพันธกรณีระหว่างประเทศต่อความมั่นคงภายใน[57]

กอ.รมน. ยุคใหม่ที่ “ใหญ่กว่าเดิม” เสมือนเป็น “หูตา-แขนขากองทัพ แทรกซึม ทุกสมัย กระจายทุกพื้นที่” รวมไปถึงเป็นการส่งไม้ต่ออำนาจของคณะรักษาความสงบแห่งชาติ (คสช.) ที่กำลังหมดวาระลง ไปยัง กอ.รมน. เพื่อให้คนกลุ่มหนึ่งยังคงสามารถ เพื่อให้ปฏิบัติการกำกับควบคุมสังคมแบบเบ็ดเสร็จอยู่คงดำเนินต่อไป[58] รักษาภาวะของการใช้การทหารนำการเมือง และรวมถึงปฏิบัติการนอกเหนือกระบวนการยุติธรรม ให้มีลักษณะเป็นปกติธรรมชาติมากที่สุด[59]

สภาความมั่นคงแห่งชาติ (สมช.) นับเป็นอีกหนึ่งหน่วยงานความมั่นคงที่ไม่ได้นิ่งนอนใจต่อการเตรียมพร้อมรับมือภัยคุกคามรูปแบบใหม่ที่เกิดขึ้น ด้วยการประกาศแผนงานและการเตรียมพร้อมตามนโยบายความมั่นคงแห่งชาติช่วงระหว่างปี 2555-2559 ซึ่งได้ให้ความสำคัญกับประเด็นการเสริมสร้างและพัฒนาศักยภาพการป้องกันประเทศ รวมถึงการมีแนวนโยบายทั้งเสริมศักยภาพกองทัพ การผนึกกำลังจากทุกภาคส่วนในการป้องกันประเทศและให้มีส่วนร่วมในการสนับสนุนการดำเนินงานของกองทัพตั้งแต่ในสภาวะปกติ การส่งเสริมและพัฒนาวิทยาศาสตร์และเทคโนโลยีการป้องกันประเทศและความมั่นคง ตลอดจนถึงการนำศักยภาพของกองทัพมาสนับสนุนภารกิจนอกเหนือจากสงคราม ในเรื่องการพัฒนาศักยภาพกลไกการสอดส่อง สมช. เน้นย้ำให้มีระบบการเฝ้าระวังภัยอย่างต่อเนื่อง เพื่อตรวจสอบภัยคุกคามต่อความมั่นคงและความปลอดภัยสาธารณะเป็นสำคัญ ไม่ว่าจะเป็นการก่อการร้าย ภยันตรายที่เกิดจากทั้งฝีมือของมนุษย์และธรรมชาติ โดยนำความก้าวหน้าทางวิทยาศาสตร์และเทคโนโลยีมาสนับสนุน[60]

---

[57] กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร, “ส่วนที่ 3 สถานการณ์ด้านความมั่นคง, ยุทธศาสตร์กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. 2560 – 2564,” (กรุงเทพฯ: กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร, 2560) หน้า 25 – 28.

[58] นัชชา ตันติวิทยาพิทักษ์ และมุทิตา เชื้อชั่ง, “กอ.รมน. ยุคใหม่ใหญ่กว่าเดิม: หูตา-แขนขากองทัพ แทรกซึมทุกสมัย กระจายทุกพื้นที่,” *ประชาไท*, แก้ไขล่าสุด 19 กันยายน 2562, สืบค้นเมื่อ 29 เมษายน 2564, https://prachatai.com/journal/2019/09/84410.

[59] เรื่องเดียวกัน.

[60] สภาความมั่นคงแห่งชาติ, “สถานการณ์และความเปลี่ยนแปลงของบริบทความมั่นคงในระยะ 7 ปี,” *นโยบายความมั่นคงแห่งชาติ พ.ศ. 2558 -2564*, หน้า 3 – 8.

6.3. การกำหนดภารกิจและบทบาทของกองบัญชาการป้องกันและปราบปรามคดีอาชญากรรมทางคอมพิวเตอร์ (ปอท.) และ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

เดิมการทำงานของ ปอท. จะอยู่ภายใต้การสนับสนุนของกระทรวงไอซีที โดยเป็นผู้สนับสนุนงบประมาณเพื่อใช้ในการปฏิบัติการตามภารกิจต่าง ๆ ที่ได้รับมอบหมาย ส่วนบทบาทหน้าที่ของกระทรวงไอซีที เริ่มมีเพิ่มมากขึ้นจากอดีตที่ผ่านมา โดยเฉพาะอย่างยิ่งในภารกิจเกี่ยวกับการแก้ไขปัญหาด้านความผิดทางเทคโนโลยีและการสื่อสาร ได้แก่ การทำหน้าที่เกี่ยวกับงานป้องกัน ปราบปราม สืบสวนและสอบสวน ดำเนินงานในส่วนการขอคำสั่งศาลให้ระงับการเผยแพร่เนื้อหาที่ไม่เหมาะสม และการรวบรวมพยานหลักฐานการกระทำความผิดในขั้นต้น[61] ทั้งนี้ ตอนหลังในเดือนกันยายนปี 2559 กระทรวงไอซีที ได้เปลี่ยนชื่อเป็น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม หรือ กระทรวงดีอีเอส ซึ่งการปรับโครงสร้างการทำงานและให้มีขอบเขตอำนาจหน้าที่มากขึ้น เพราะเห็นว่า สังคมกำลังถูกขับเคลื่อนโดยเทคโนโลยีดิจิทัลเป็นหลัก[62] โดยมีหน้าที่สนับสนุนในเชิงเทคนิคและบุคลากรผู้เชี่ยวชาญ

การตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 พร้อมทั้งยังปรับปรุงโครงสร้างการทำงานหน่วยงานที่เกี่ยวข้อง และขยายอำนาจหน้าที่ให้แก่ ปอท. หลายประการ เช่น งานสอดส่องเฝ้าระวัง งานตรวจพิสูจน์หลักฐาน การตรวจยึดและอายัด และงานด้านประสานความร่วมมือผู้ให้บริการอินเทอร์เน็ตและให้บริการสื่อออนไลน์ในการกำกับควบคุม[63]

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฉบับหลังนี้เป็นเสมือนหมุดหมายครั้งสำคัญที่สะท้อนถึงการเสริมศักยภาพและขยายอำนาจในการสอดส่องชีวิตผู้คนในสังคมออนไลน์ของรัฐไทย ตัวอย่างเช่น ในเรื่องการกำหนดภาระหน้าที่แก่ผู้ให้บริการที่จะต้องระงับหรือลบข้อมูลที่กระทบกระเทือนต่อความมั่นคงโดยให้เวลาเพียง 24 ชั่วโมง หลังจากได้รับแจ้ง

---

[61] สภาความมั่นคงแห่งชาติ, “สถานการณ์และความเปลี่ยนแปลงของบริบทความมั่นคงในระยะ 7 ปี,” *นโยบายความมั่นคงแห่งชาติ พ.ศ. 2558 -2564*, หน้า 2.

[62] พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ 17) พ.ศ. 2559 มาตรา 5, *ราชกิจจานุเบกษา ฉบับกฤษฎีกา* เล่มที่ 133 ตอนที่ 80 ก (15 กันยายน 2559): 1.

[63] การตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560, *ราชกิจจานุเบกษา ฉบับ กฤษฎีกา* เล่มที่ 134 ตอนที่ 10 ก (24 มกราคม 2560).

มิเช่นนั้นจะต้องรับโทษเท่ากับผู้โพสต์ หรือ การบัญญัติกฎหมายไว้อย่างกว้างในมาตรา 14 (2) และมาตรา 14 (3) เป็นเหตุให้กฎหมายถูกนำมาบังคับใช้เพื่อ “ตบปาก” ผู้ใช้สื่อสังคมออนไลน์ที่แสดงความเห็นวิพากษ์วิจารณ์ผู้มีอำนาจ ตลอดจนถึงเนื้อหาในเว็บไซต์ที่แม้ไม่ผิดกฎหมายแต่หากเจ้าหน้าที่รัฐเห็นว่าเนื้อหาเหล่านั้น “ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน” ก็อาจถูกปิดกั้นการเข้าถึงได้[64] เป็นต้น

เพื่อเสริมศักยภาพการสอดส่องให้ได้มากที่สุด ในเดือนกันยายน ปี 2563 ก็มีการตราพระราชกฤษฎีกาตั้งตำรวจสืบสวนสอบสวนคดีทางเทคโนโลยีระดับกองบัญชาการเพิ่ม[65] เหตุผลในการประกาศใช้พระราชกฤษฎีกา กล่าวว่า[66] “ในปัจจุบันโครงสร้างของสำนักงานตำรวจแห่งชาติในปัจจุบันไม่สามารถรองรับปัญหาที่มีความซับซ้อนจากการใช้เทคโนโลยีในการกระทำความผิดในลักษณะต่าง ๆ และมีการนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์โดยมิชอบ หรือเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นความผิดตามกฎหมาย กระทบสิทธิของผู้อื่น หรือความมั่นคงของประเทศ” และ อำนาจหน้าที่หลัก ๆ ของกองบัญชาการดังกล่าวประกอบไปด้วย การดำเนินการเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ทั่วราชอาณาจักร การปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา กฎหมายว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่น อันเป็นความผิดทางอาญาเกี่ยวกับอาชญากรรมทางเทคโนโลยีและความผิดอื่นที่เกี่ยวเนื่อง ดำเนินการเกี่ยวกับการรวบรวมข้อมูล ตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี ตลอดจนดำเนินการเกี่ยวกับการพิสูจน์หลักฐานดิจิทัล การตรวจสถานที่เกิดเหตุ และเก็บรวบรวมพยานหลักฐานดิจิทัลเพื่อสนับสนุนการปฏิบัติงานสืบสวนสอบสวนของหน่วยงานต่าง ๆ เป็นต้น[67]

---

[64] โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน, “กระทรวงดีอีออกประกาศชัด ผู้ให้บริการต้องลบข้อมูลเกี่ยวกับความมั่นคงภายใน 24 ชั่วโมง,” *ilaw*, แก้ไขล่าสุด 25 กรกฎาคม 2560, สืบค้นเมื่อ 29 เมษายน 2564, https://ilaw.or.th/node/4575.

[65] พระราชกฤษฎีกา แบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ (ฉบับที่ 5) พ.ศ.2563, *ราชกิจจานุเบกษา ฉบับกฤษฎีกา* เล่มที่ 137 ตอนที่ 71 ก (8 กันยายน 2563).

[66] หมายเหตุท้าย พระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ (ฉบับที่ 5) พ.ศ.2563

[67] ประชาไท, “พระราชกฤษฎีกาตั้งตำรวจสืบสวนสอบสวนคดีทางเทคโนโลยีระดับกองบัญชาการเพิ่ม,” *ประชาไท*, แก้ไขล่าสุด 8 กันยายน 2563, สืบค้นเมื่อ 29 เมษายน 2564, https://prachatai.com/journal/2020/09/89430.

6.4. การใช้ข้อมูลจากการสอดส่องเพื่อดำเนินคดีความมั่นคงต่อนักกิจกรรม ทางการเมือง

"ศูนย์ทนายความเพื่อสิทธิมนุษยชน" ซึ่งได้รับการร้องเรียนจากผู้ใช้ทวิตเตอร์ในบัญชีชื่อ "นิรนาม_" (@ssj_2475) (ไม่ประสงค์จะเปิดเผยชื่อสกุล) เมื่อวันที่ 20 กุมภาพันธ์ 2563 อาศัยอยู่ในจังหวัดชลบุรีว่าได้ถูกเจ้าหน้าที่ตำรวจเข้าตรวจค้นห้องพัก และพาตัวไปยังสถานีตำรวจภูธรเมืองพัทยา โดยไม่มีหมายจับ ก่อนถูกแจ้งข้อกล่าวหาตามมาตรา 14 (3) พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เนื่องจากได้ทำการทวิตภาพและข้อความที่เกี่ยวกับพระเจ้าอยู่หัวรัชกาลที่ 10 ทั้งนี้ คำร้องขอฝากขังระบุด้วยว่าก่อนเกิดเหตุเจ้าหน้าที่ตำรวจชุดจับกุมตรวจสอบความเคลื่อนไหวกลุ่มที่มีแนวคิดต่อต้านสถาบันพระมหากษัตริย์ และได้พบบัญชีทวิตเตอร์ "นิรนาม_" เปิดใช้งานเมื่อเดือนตุลาคม 2561 จากการดำเนินการทางอิเล็กทรอนิกส์ โดยแหล่งข่าว พบว่า "บัญชีดังกล่าว มีการเชื่อมต่ออินเทอร์เน็ตของบริษัททรูจำนวน 2 ครั้ง ในช่วงเดือนมกราคมปี 2563 โดยมีการระบุถึงหมายเลขไอพีแอดเดรสในการเชื่อมต่อทั้งสองครั้ง และจากการตรวจสอบกับบริษัททรู มูฟ เอช ยูนิเวอร์แซล คอมมิวนิเคชั่น จำกัด หมายเลขไอพีดังกล่าวเป็นของหมายเลขโทรศัพท์ซึ่งผู้ต้องหาลงทะเบียนเปิดใช้"[68]

การจับกุม ผู้ใช้บัญชีทวิตเตอร์ "นิรนาม_" ได้ยืนยันถึงการประสานงานร่วมกันระหว่างรัฐและบรรษัทผู้ให้บริการอินเทอร์เน็ตที่ชัดเจนที่สุดกรณีหนึ่ง อีกทั้ง หากกล่าวเฉพาะคดีความ "นิรนาม_" ยังแสดงให้เห็นถึง การพัฒนากลไกการสอดส่องอันสืบเนื่องมาตั้งแต่การบังคับประชาชนลงทะเบียนหมายเลขโทรศัพท์ ที่ส่งผลให้รัฐสามารถเข้าถึงข้อมูลส่วนตัวของผู้ใช้ได้ง่ายขึ้นตั้งแต่ปี 2557-2558

7. แนวทางในการกำกับดูแลปฏิบัติการสอดส่องและสร้างความโปร่งใสในระบบข่าวกรอง

รายงานของสำนักงานข้าหลวงใหญ่เพื่อสิทธิมนุษยชนแห่งองค์กรสหประชาชาติ (Report of the Office of the United Nations High Commissioner for Human Rights) ก็ได้นำเสนอ

---

[68] ประชาไท, "'นิรนาม_' ถูกจับคดี พ.ร.บ.คอมฯ เหตุทวิตเกี่ยวกับ ร.10 ศาลไม่ให้ประกัน อ้างเป็นเรื่องร้ายแรง," *ประชาไท*, แก้ไขล่าสุด 20 กุมภาพันธ์ 2563, สืบค้นเมื่อ 29 เมษายน 2564, https://prachatai.com/journal/2020/02/86426 ().

สถานการณ์ของสิทธิส่วนบุคคลในโลกยุคดิจิทัล (The right to privacy in the digital age)[69] ว่า แม้หลักกฎหมายระหว่างประเทศที่ว่าด้วยสิทธิมนุษยชนจะได้กำหนดกรอบทางกฎหมายให้รัฐมีหน้าที่อันเกี่ยวกับการสนับสนุนและการปกป้องคุ้มครองสิทธิส่วนบุคคลของปัจเจกบุคคลไว้อย่างเป็นสากล (Universal) แต่ก็ยังปรากฏให้เห็นถึงกรณีที่มีการกระทำอันเป็นละเมิดสิทธิมนุษยชนให้เห็นอยู่ดาษดื่น เนื่องจากในทางปฏิบัติแล้ว หลายรัฐยังคงขาดบทบัญญัติ และ/หรือ การบังคับกฎหมายเพื่อควบคุมการทำงานของเจ้าหน้าที่รัฐที่เพียงพอ และอาจมีกระบวนการป้องกันหรือเฝ้าระวังที่อ่อนแอและไร้ประสิทธิภาพ รวมถึงบางรัฐก็ไม่อาจหยิบยื่นความรับผิดให้แก่เจ้าหน้าที่รัฐที่ปฏิบัติหน้าที่เกี่ยวกับการสอดส่องในลักษณะที่เป็นการละเมิดสิทธิส่วนบุคคล อันเนื่องมาจากการใช้อำนาจตามอำเภอใจหรือไม่ชอบด้วยกฎหมายได้

การสลับสับเปลี่ยนสถานะของ “ความเป็นส่วนตัวของประชาชน” ที่พึงได้รับการคุ้มครองปกป้องไม่ให้มีการแทรกแซงสอดส่องการสื่อสารและดักเก็บข้อมูลส่วนบุคคลนั้นเกิดจากความพยายามของรัฐในการสร้างฐานข้อมูลข่าวกรองโดยอ้างเรื่อง “ความมั่นคงของชาติ” ที่ปราศจากการตระหนักถึง “ความมั่นคงของมนุษย์” ในการสื่อสารภายใต้บริบทของโลกยุคดิจิทัล เนื่องจากรัฐมุ่งแสวงหาข้อมูลที่เป็น “ความลับของประชาชน” มาบนพื้นฐานของการกล่าวอ้างว่าหากประชาชนไม่ได้มีการกระทำความผิดและบริสุทธิ์ใจก็ควรเปิดให้รัฐมองเห็นกิจกรรมในชีวิตส่วนตัวได้โดยไม่มีการปิดกั้นแบบ “รัฐตำรวจ” เพื่อเสริมศักยภาพในการมองเห็นของรัฐป้องปรามการเคลื่อนไหวของประชาชนเพราะทำให้รู้สึกว่าถูกจับจ้องตลอดเวลา

ในทางกลับกัน “ความโปร่งใสของรัฐ” อันเป็นรากฐานสำคัญของธรรมาภิบาลในการปกครองประเทศในระบอบประชาธิปไตยและเป็นการยืนยันความรับผิดชอบของรัฐต่อการใช้อำนาจปกครองโดยเคารพสิทธิมนุษยชนของประชาชน กลับถูกปรับเปลี่ยนไปเป็น “ความลับสูงสุดของชาติ” ที่ผู้นำรัฐและองคาพยพด้านความมั่นคงสงวนไว้มิให้ประชาชนมองเห็น เสมือนว่าเป็น “เรื่องส่วนตัวของชาติ” ที่ผู้ทรงอำนาจจะพึงเก็บงำรักษาไว้ไม่ให้ใครเข้าถึง เพื่อคงไว้ซึ่งอำนาจในการปกครองของตนจากหลังม่าน

---

[69] The United Nations High Commissioner for Human Rights. *Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age*. (New York: United Nations, 2014), https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc

ดังนั้นการเปลี่ยนกระบวนทัศน์จึงเป็นการทลายกำแพงด่านแรกเพื่อเปิดให้เห็นการทำงานและผลงานที่แท้จริงของรัฐเพื่อธำรงไว้ซึ่ง “ความมั่นคงของมนุษย์ในรัฐชาติไทย” และคุ้มครอง “สิทธิความเป็นส่วนตัวของประชาชน” อันเป็นรากฐานสำคัญของการปกครองในระบอบประชาธิปไตยที่ต้องคุ้มครองสิทธิเสรีภาพของประชาชนไว้เพื่อให้พลเมืองทั้งหลายกล้าที่จะแสดงออกและมีส่วนร่วมในการกำหนดอนาคตของประเทศได้อย่างปลอดภัยตามครรลองการปกครองในระบอบประชาธิปไตยที่มีการคุ้มครองสิทธิมนุษยชนของประชาชนภายใต้หลักการ “นิติรัฐ” ที่มีการตรวจสอบถ่วงดุลการใช้อำนาจของรัฐบาล

References

ICT-Prachachat. “ประกาศแล้ว! 2กฎหมายฮอตไซเบอร์ซิเคียวริตี้-คุ้มครองข้อมูลส่วนบุคคล'.” *ประชาชาติธุรกิจ*. แก้ไขล่าสุด 27 พฤษภาคม 2562, สืบค้นเมื่อ 29 เมษายน 2564, https://www.prachachat.net/ict/news-331574.

Thai PBS News. “ประมวลเหตุการณ์ผู้ใช้อินเทอร์เน็ตประท้วง ‘ซิงเกิล เกตเวย์.’” *Thai PBS* (Thai PBS, October 1, 2015)” แก้ไขล่าสุด 1 ตุลาคม 2558” สืบค้นเมื่อ 29 เมษายน 2564, https://news.thaipbs.or.th/content/5617.

Warong ThaiPublica. “ชี้ยังไม่ดำเนินการ ‘ซิงเกิล เกตเวย์.’” *ThaiPublica*” แก้ไขล่าสุด 6 พฤศจิกายน 2558. สืบค้นเมื่อ 29 เมษายน 2564 https://thaipublica.org/jabted_issue/ชี้ยังไม่ดำเนินการ-ซิง/

โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน. “กระทรวงดีอีออกประกาศชัด ผู้ให้บริการต้องลบข้อมูลเกี่ยวกับความมั่นคงภายใน 24 ชั่วโมง.” *Ilaw*. แก้ไขล่าสุด 25 กรกฎาคม 2560. สืบค้นเมื่อ 29 เมษายน 2564, https://ilaw.or.th/node/4575.

กองบรรณาธิการ The Standard. “ครม. ไฟเขียว เพิ่มหลักการร่างกฎหมาย NGO รวม 8 ประเด็น ต้องเปิดเผยข้อมูลองค์กร-งบการเงิน.” *THE STANDARD*. แก้ไขล่าสุด 29 มิถุนายน 2564. เข้าถึงเมื่อ 30 มิถุนายน 2564. https://thestandard.co/cabinet-increases-the-principle-of-drafting-ngo-law.โดยดูข้อมูลต้นทางมติคณะรัฐมนตรีได้ที่เว็บไซต์ทางการของรัฐบาลไทย https://www.thaigov.go.th/news/contents/details/39334

กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร. “ประวัติความเป็นมา. *ISOC*. สืบค้นเมื่อ 28 เมษายน 2564. https://www.isoc.go.th/about.php.

กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักรใ “ส่วนที่ 3 สถานการณ์ด้านความมั่นคง, ยุทธศาสตร์กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. 2560 – 2564.” (กรุงเทพฯ: กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร, 2560) หน้า 25 – 28.

การตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560. *ราชกิจจานุเบกษา ฉบับ กฤษฎีกา* เล่มที่ 134 ตอนที่ 10 ก (24 มกราคม 2560).

การตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560. *ราชกิจจานุเบกษา ฉบับ กฤษฎีกา* เล่มที่ 134 ตอนที่ 10 ก (24 มกราคม 2560).

ข่าวเนชั่นสุดสัปดาห์. “จัดโครงสร้าง กอ.รมน. รับมือภัยความมั่นคงยุคใหม่.” 2 ธันวาคม 2562. *เนชั่นสุดสัปดาห์*. (สืบค้นเมื่อ 29 เมษายน 2564). https://www.nationweekend.com/content/government_inside/3599.

ข่าวสด, 20 มิถุนายน 2551, หน้า 6.

นัชชา ตันติวิทยาพิทักษ์ และมุทิตา เชื้อชั่ง. “กอ.รมน. ยุคใหม่ใหญ่กว่าเดิม: หูตา-แขนขากองทัพ แทรกซึมทุกสมัย กระจายทุกพื้นที่.” *ประชาไท*. แก้ไขล่าสุด 19 กันยายน 2562. สืบค้นเมื่อ 29 เมษายน 2564. https://prachatai.com/journal/2019/09/84410.

ประชาไท. “'นิรนาม_' ถูกจับคดี พ.ร.บ.คอมฯ เหตุทวิตเกี่ยวกับ ร.10 ศาลไม่ให้ประกัน อ้างเป็นเรื่องร้ายแรง.” *ประชาไท*. แก้ไขล่าสุด 20 กุมภาพันธ์ 2563. สืบค้นเมื่อ 29 เมษายน 2564, https://prachatai.com/journal/2020/02/86426 ().

ประชาไท. “พระราชกฤษฎีกาตั้งตำรวจสืบสวนสอบสวนคดีทางเทคโนโลยีระดับกองบัญชาการเพิ่ม.” *ประชาไท*. แก้ไขล่าสุด 8 กันยายน 2563, สืบค้นเมื่อ 29 เมษายน 2564. https://prachatai.com/journal/2020/09/89430.

ประชาชาติธุรกิจ, 20 ตุลาคม 2548, หน้า 17.

ประชาชาติธุรกิจ, 9 ตุลาคม 2549, หน้า 43.

พระราชกฤษฎีกา แบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ (ฉบับที่ 5) พ.ศ.2563. *ราชกิจจานุเบกษา ฉบับ กฤษฎีกา* เล่มที่ 137 ตอนที่ 71 ก (8 กันยายน 2563).

พระราชบัญญัติการรักษาความมั่นคงในราชอาณาจักร พ.ศ. 2551 มาตรา 7(1). *ราชกิจจานุเบกษา ฉบับกฤษฎีกา* เล่มที่ 125 ตอนที่ 39 ก (27 กุมภาพันธ์ 2551): 35.

พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2528 มาตรา 4 (20 สิงหาคม 2528): 2.

พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ 17) พ.ศ. 2559 มาตรา 5. *ราชกิจจานุเบกษา ฉบับ กฤษฎีกา* เล่มที่ 133 ตอนที่ 80 ก (15 กันยายน 2559): 1.

มติชน, 15 พฤศจิกายน 2550, หน้า 6.

มติชน, 18 ตุลาคม 2550, หน้า 2.

มติชน, 18 มกราคม 2551, หน้า 11.

มติชน, 20 ตุลาคม 2544, หน้า 24

มติชน, 22 ธันวาคม 2549, หน้า 16.

มติชน, 24 กันยายน 2545, หน้า 13

มติชน, 3 กรกฎาคม 2545, หน้า 45

มติชนสุดสัปดาห์, 27 ตุลาคม 2549, หน้า 25 – 26.

สภาความมั่นคงแห่งชาติ. “สถานการณ์และความเปลี่ยนแปลงของบริบทความมั่นคงในระยะ 7 ปี.” *นโยบายความมั่นคงแห่งชาติ พ.ศ. 2558 -2564*, หน้า 3 – 8.

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ, “ทำไมต้องลงทะเบียนซิมโทรศัพท์เคลื่อนที่ระบบเติมเงิน.” (2558). *กสทช*. สืบค้นเมื่อ 29 เมษายน 2564. http://sim.nbtc.go.th/why.php

Balule, Badala Tachilisa, and Bojosi Otlhogile. “Balancing the Right to Privacy and the Public Interest: Surveillance by the State of Private Communications for Law Enforcement in Botswana.” *Statute Law Review* 37, no. 1 (July 24, 2015): 1–14.

Boghosian, Heidi. *Spying on Democracy: Government Surveillance, Corporate Power, and Public Resistance*. San Francisco: City Lights Publishers, 2013.

Chapman, Brian. “‘The Police-State.’ Government and Opposition 3, No. 4 .” Cambridge University Press, 1968. Last modified 1968. Accessed July 25, 2021. https://www.jstor.org/stable/44481889.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books, 1995.

Graham, Stephen, and David Wood. “Digitizing Surveillance: Categorization, Space, Inequality.” *Critical Social Policy* 23, no. 2 (2003): 227–248.

Greenwald. G., “The Harm of Surveillance, *No place to hide :Edward Snowden, the NSA and the Surveillance State*,” (New York: Metropolitan Books, 2014), 170-209

Losey, J., “Surveillance of Communications: A Legitimization Crisis and the Need for Transparency.” *International Journal of Communication, 9*(10) (2015): 3450–3459.

Mercer, Loren D. “Computer Forensics: Characteristics and Preservation of Digital Evidence.” *FBI Law Enforcement Bulletin* 73, no. 3 (2004): 28–32.

Milanovic, M., “Human rights treaties and foreign surveillance: Privacy in the digital age.” *Harvard International Law Journal*, 56(1) (2015): 81-146.

Pinkaew Laungaramsri. "Mass surveillance and the militarization of cyberspace in post-coup Thailand." *ASEAS – Austrian Journal of South-East Asian Studies*, *9*(2) (2016): 195-214.

Puangthong Pawakapan. "*Infiltrating Society: The Thai Military's Internal Security Affairs*," ISEAS – Yusof Ishak Institute, 2021.

Slobogin, C., "Policing, databases, and surveillance. Criminology." Criminal Justice, *Law & Society*, 18(3) (2017): 70-84.

The United Nations High Commissioner for Human Rights. *Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age*. (New York: United Nations, 2014), https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc

Utset, M. A., "Digital Surveillance and Preventive Policing." *Connecticut Law Review*, 49(5) (2017): 1453-1494.

v., s. "Police State." *Merriam-Webster*. Merriam-Webster, n.d. Accessed July 25, 2021. https://www.merriam-webster.com/dictionary/police%20state.

Yilma, K. M., "The United Nations Data Privacy System and Its Limits." *International Review of Law. Computers & Technology* 33. no. 2 (2018): 224-248.