บทความวิชาการ

พลวัตของการสร้างความมั่นคงปลอดภัยไซเบอร์และการท้าทายเสรีภาพพลเมืองในยุคดิจิทัล

จิรวัฒน์ ศรีเรือง[a]

บทคัดย่อ

บทความวิชาการนี้มุ่งสำรวจความเป็นพลวัตในการสร้างความมั่นคงปลอดภัยทางไซเบอร์ของรัฐกับการคุ้มครองเสรีภาพของประชาชนในยุคดิจิทัลที่มีความสัมพันธ์ที่ซับซ้อนและท้าทาย โดยวิเคราะห์ว่าการตอบสนองต่อภัยคุกคามทางไซเบอร์ภายหลังเหตุการณ์ 9/11 และในภูมิทัศน์ปัจจุบันของประเทศต่างๆ ทั่วโลก รวมถึงประเทศไทย มีแนวโน้มที่จะมอบอำนาจที่กว้างขวางขึ้นแก่รัฐในการเฝ้าระวัง สอดส่อง และควบคุมกิจกรรมออนไลน์ผ่านกฎหมายและมาตรการควบคุมต่างๆ ซึ่งส่งผลกระทบโดยตรงต่อสิทธิในความเป็นส่วนตัว เสรีภาพในการแสดงความคิดเห็น และเสรีภาพในการเข้าถึงข้อมูล ทั้งนี้เน้นย้ำถึงความสำคัญอย่างยิ่งของการสร้างสมดุลที่เหมาะสมและยั่งยืนระหว่างความมั่นคงและเสรีภาพ โดยอาศัยหลักการของนิติรัฐ ความโปร่งใส ความจำเป็นและได้สัดส่วนของการจำกัดสิทธิ เพื่อป้องกันการใช้อำนาจรัฐที่อาจเกินขอบเขตและธำรงรักษาสังคมประชาธิปไตยที่เคารพสิทธิและเสรีภาพของพลเมือง การไม่สามารถรักษาสมดุลนี้อาจนำไปสู่การกัดกร่อนบรรยากาศแห่งความไว้วางใจและการลดทอนคุณค่าของเสรีภาพในโลกดิจิทัล

คำสำคัญ: ความมั่นคงไซเบอร์, ความเป็นส่วนตัว, การเมืองและการปกครองดิจิทัล

[a] อาจารย์ประจำหลักสูตรรัฐศาสตรบัณฑิต สาขาวิชารัฐศาสตร์ วิชาเอกการเมืองและการปกครองดิจิทัล วิทยาลัยการจัดการเพื่อการพัฒนา มหาวิทยาลัยทักษิณ, Email: jirawat.sr@tsu.ac.th

รับบทความ: 26 มิถุนายน 2568 แก้ไขบทความ: 30 ตุลาคม 2568 ตอบรับบทความ: 31 ตุลาคม 2568

Viewpoint

Dynamics of Cybersecurity and Challenges to Civil Liberties in the Digital Era

Jirawat Sriruang[a]

Abstract

This academic article explores the dynamic relationship between state-led cybersecurity measures and the protection of individual freedoms in the digital era a relationship that is inherently complex and challenging. It analyzes how global and national responses to cyber threats, particularly in the aftermath of the 9/11 attacks and within the current digital landscape, have increasingly granted governments broader powers to monitor, surveil, and regulate online activities through laws and control mechanisms. Such measures directly impact fundamental rights, including privacy, freedom of expression, and freedom of information. The article underscores the critical importance of maintaining a balanced and sustainable approach between security and liberty, grounded in the principles of the rule of law, transparency, necessity, and proportionality of rights restrictions. This balance is essential to prevent the abuse of state power and to preserve a democratic society that respects citizens' rights and freedoms. Failure to sustain this equilibrium risks eroding public trust and diminishing the value of freedom in the digital realm.

Keywords: Cybersecurity, Privacy, Digital Politics and Governance

---

[a] Lecturer, Bachelor of Political Science Program, Major in Political Science, Major in Digital Politics and Governance, College of Management for Development, Thaksin University. Email: jirawat.sr@tsu.ac.th

Received: 26 June 2025 ***Revised: 30 October 2025*** ***Accepted: 31 October 2025***

บทนำ

ในยุคแห่งการปฏิวัติทางดิจิทัลที่ข้อมูลข่าวสารและการเชื่อมต่อออนไลน์ได้กลายเป็นปัจจัยสำคัญในการขับเคลื่อนสังคม เศรษฐกิจ และการเมือง ความมั่นคงปลอดภัยทางไซเบอร์จึงได้ผงาดขึ้นเป็นวาระแห่งชาติที่รัฐบาลทั่วโลกมิอาจละเลย การแสวงหาความมั่นคงในโลกเสมือนจริงนี้ นำมาซึ่งความพยายามในการกำหนดนโยบาย ออกกฎหมาย และใช้มาตรการควบคุมต่างๆ เพื่อป้องกันภัยคุกคามนานัปการ ตั้งแต่การโจมตีโครงสร้างพื้นฐานสำคัญ การจารกรรมข้อมูล ไปจนถึงการบิดเบือนข้อมูลข่าวสารและการแทรกแซงทางการเมือง อย่างไรก็ตาม ภายใต้ร่มเงาของการสร้างเกราะกำบังทางไซเบอร์นี้ ได้ปรากฏพลวัตเชิงอำนาจที่ซับซ้อนและท้าทาย โดยเฉพาะอย่างยิ่งในความสัมพันธ์ระหว่างรัฐกับพลเมือง

บทความวิชาการนี้มุ่งที่จะสำรวจพลวัตของความสัมพันธ์เชิงอำนาจอันละเอียดอ่อนระหว่างการสร้างความมั่นคงปลอดภัยทางไซเบอร์ของรัฐกับการคุ้มครองเสรีภาพของประชาชนในบริบทของโลกดิจิทัลที่เปลี่ยนแปลงไปอย่างรวดเร็ว โดยจะฉายภาพให้เห็นถึงการตอบสนองของรัฐชาติต่อภัยคุกคามทางไซเบอร์ภายหลังเหตุการณ์สำคัญอย่าง 911 ที่นำไปสู่การปรับเปลี่ยนนโยบายและกฎหมายที่ส่งผลกระทบต่อขอบเขตของเสรีภาพพลเมือง

จากข้อมูลขององค์กรภาคประชาสังคม เช่น Freedom House (2023) ชี้ให้เห็นว่า ในขณะที่บางประเทศ เช่น ไอซ์แลนด์ ยังคงรักษาระดับเสรีภาพทางอินเทอร์เน็ตไว้สูง แต่หลายประเทศทั่วโลกกลับมีแนวโน้มที่รัฐบาลจะเพิ่มการควบคุมและจำกัดการเข้าถึงข้อมูลออนไลน์มากขึ้น โดยภาพรวมทั่วโลกเสรีภาพทางอินเทอร์เน็ตถดถอยลงติดต่อกันเป็นปีที่ 13 รายงานของ Pew Research Center (2019) ซึ่งเป็นองค์กรวิจัยของภาคประชาสังคมในสหรัฐอเมริกา ใน "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information" ปี 2019 พบว่าประชาชนมีความกังวลอย่างมีนัยสำคัญเกี่ยวกับความเป็นส่วนตัวและการสอดส่องของรัฐบาล โดยมีถึง 64% ของชาวอเมริกันที่แสดงความกังวลเกี่ยวกับวิธีการที่รัฐบาลใช้ข้อมูลส่วนตัวที่ถูกเก็บรวบรวมไป กระทั่งในปี 2025 ความกังวลนี้ไม่ได้อยู่แค่เรื่องการเฝ้ามองจากรัฐบาลเท่านั้น แต่รวมถึงบริษัทเทคโนโลยีที่มีข้อมูลการใช้งานข้อมูลส่วนบุคคล และบทบาทในการเข้าถึง แม้จะมีความกังวลสูง แต่ผู้คนจำนวนมากไม่รู้สึกว่าตนเองมีอำนาจ ในยุคดิจิทัลที่มีการใช้เทคโนโลยีมากขึ้น เช่น โทรศัพท์มือถือ แอปพลิเคชัน IoT ความรู้เกี่ยวกับวิธีป้องกัน/ควบคุมข้อมูลส่วนตัวจึงยังมีจำกัด ในทางเดียวกัน จีนเป็นตัวอย่างที่โดดเด่นของประเทศที่ใช้เทคโนโลยีเพื่อสร้างระบบควบคุมและเฝ้าระวังอินเทอร์เน็ตที่ซับซ้อนที่สุดในโลก หรือที่รู้จักกันในชื่อ Great Firewall โดย รายงานของ GreatFire.org ที่ก่อตั้งโดยกลุ่มชาวจีน ซึ่งเป็นกลุ่มต่อต้านการเซ็นเซอร์ ระบุว่ามีเว็บไซต์มากกว่า 100,000 เว็บไซต์ ที่ถูกบล็อกในจีน ณ เดือนกุมภาพันธ์

2024 (Freedom House, 2024) และแพลตฟอร์มต่างประเทศยอดนิยมส่วนใหญ่ เช่น Google, Wikipedia, Facebook, Instagram และ YouTube ยังไม่สามารถเข้าถึงได้

บทความนี้ ส่วนที่ 1 จะวิเคราะห์เปรียบเทียบแนวทางการดำเนินงานของรัฐบาลในระบอบการเมืองที่แตกต่างกัน ไม่ว่าจะเป็นรัฐเสรีนิยมประชาธิปไตย หรือรัฐที่เน้นความมั่นคงแห่งชาติเป็นลำดับแรก ในการจัดการกับความท้าทายดังกล่าว โดยจะพิจารณาถึงผลกระทบของมาตรการควบคุมทางไซเบอร์ต่อสิทธิขั้นพื้นฐานของประชาชน อาทิ สิทธิในความเป็นส่วนตัว ส่วนที่ 2 ผลกระทบเชิงนโยบายในบริบทของประเทศไทยในแง่ของการใช้กฎหมายความมั่นคงไซเบอร์และกฎหมายที่เกี่ยวข้องซึ่งส่งผลกระทบต่อภาคประชาสังคม สื่อ และสิทธิดิจิทัลของประชาชน โดยเฉพาะอย่างยิ่งกฎหมายหลักอย่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม พ.ศ. 2560 และ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่ถูกวิพากษ์วิจารณ์ว่ามีบทบัญญัติที่คลุมเครือและเปิดกว้างต่อการตีความ ซึ่งให้อำนาจแก่เจ้าหน้าที่รัฐในการเฝ้าระวังและควบคุมเนื้อหาออนไลน์อย่างกว้างขวางเกินกว่าเหตุนั้น มีผลกระทบอย่างไร และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่บังคับใช้นั้นมีข้อจำกัดอย่างไร ส่วนที่ 3 จะนำเสนอแนวคิดในการสร้างความสมดุลระหว่างการสร้างความมั่นคงปลอดภัยไซเบอร์ของรัฐ กับการรักษาความเป็นส่วนตัวของพลเมืองว่าควรมีแนวทางอย่างไร และการคาดการณ์ถึงฉากทัศน์ที่จะเป็นอีกขดหนึ่งของพลวัตที่จะเกิดขึ้นต่อในการสร้างความสมดุลความมั่นคงปลอดภัยทางไซเบอร์นี้ และในส่วนที่ 4 ของบทความนี้จะวิเคราะห์ว่าการแสวงหาความมั่นคงปลอดภัยทางไซเบอร์ของรัฐนั้น มีปฏิสัมพันธ์อย่างไรกับแนวคิดเรื่องอำนาจอธิปไตย ความมั่นคงแห่งรัฐ สัญญาประชาคม และสิทธิพลเมือง และจะมุ่งเน้นไปที่การพิจารณาถึงบทบาทของรัฐและภาคประชาสังคมในการกำหนดภูมิทัศน์ทางไซเบอร์และสมดุลแห่งอำนาจดังกล่าว คำถามสำคัญที่บทความนี้มุ่งตอบคือ รัฐชาติสามารถสร้างความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างไร โดยไม่ลดทอนเสรีภาพของประชาชนจนเกินขอบเขตที่ยอมรับได้ และกลไกใดที่จะสามารถประกันความสมดุลที่ยั่งยืนระหว่างความมั่นคงกับเสรีภาพในโลกดิจิทัลที่ยังคงมีการเปลี่ยนแปลงอยู่ตลอดเวลา การวิเคราะห์นี้จะนำไปสู่การพิจารณาถึงความท้าทายในอนาคตและข้อเสนอแนะเชิงนโยบายเพื่อนำไปสู่การสร้างสภาพแวดล้อมทางไซเบอร์ที่ทั้งปลอดภัยและเคารพสิทธิเสรีภาพของประชาชน

อย่างไรก็ตาม งานวิชาการและนโยบายในปัจจุบันมักจะพิจารณาการสร้างความมั่นคงปลอดภัยทางไซเบอร์และการคุ้มครองเสรีภาพพลเมืองแยกส่วนกัน หรือมุ่งเน้นที่การวิเคราะห์กฎหมายแต่ละฉบับอย่างโดดเดี่ยว ช่องว่างที่สำคัญ คือการขาดซึ่งกรอบการวิเคราะห์เชิงบูรณาการที่จะประเมินผล กระทบรวมของชุดมาตรการความมั่นคงไซเบอร์

วิธีการศึกษา

บทความนี้ใช้วิธีการวิเคราะห์เอกสาร (Document Analysis) ได้แก่ กฎหมาย นโยบายความมั่นคงไซเบอร์ รายงานของรัฐบาล รายงานขององค์กรระหว่างประเทศ เช่น องค์กรภาคประชาสังคม อาทิ Freedom House และ Human Rights Watch รวมถึงบทความทางวิชาการและงานวิจัยที่เกี่ยวข้อง

นอกจากนี้ ยังใช้วิธี การวิเคราะห์เปรียบเทียบ (Comparative Analysis) เพื่อศึกษาแนวทางการจัดการความมั่นคงไซเบอร์และเสรีภาพพลเมืองในระดับสากล โดยแบ่งการเปรียบเทียบออกเป็นสองกลุ่มหลักเพื่อแสดงให้เห็นถึงความแตกต่างของแนวคิดและนโยบายได้แก่ กลุ่มประเทศประชาธิปไตยแบบเสรีนิยม เช่น สหรัฐอเมริกาและสหภาพยุโรป ซึ่งมีแนวโน้มในการให้ความสำคัญกับหลักนิติรัฐและสิทธิพลเมืองเป็นหลัก และกลุ่มประเทศที่มีแนวโน้มอำนาจนิยม เช่น จีน รัสเซีย อินเดีย และอียิปต์ ซึ่งให้ความสำคัญกับความมั่นคงแห่งรัฐเหนือสิทธิพลเมือง โดยใช้เกณฑ์ในการเลือกกรณีศึกษาของแต่ละกลุ่ม คือ การมีบริบททางการเมืองที่แตกต่างกันอย่างชัดเจนและมีมาตรการด้านความมั่นคงไซเบอร์ที่โดดเด่นและเป็นตัวแทนของแนวทางนั้นๆ

ทั้งนี้ได้วิเคราะห์กฎหมายที่เกี่ยวข้องของไทย 3 ฉบับ ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (และที่แก้ไข พ.ศ.2560), พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) เปรียบเทียบเพื่อหาแนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์ให้เกิดความสมดุลกับเสรีภาพพลเมือ

911 หน่ออ่อนสู่ภูมิทัศน์ความมั่งปลอดภัยไซเบอร์ปัจจุบัน

“911” เหตุการณ์การโจมตีในประเทศสหรัฐอเมริกาเมื่อวันที่ 11 กันยายน 2001 ถือเป็นจุดเปลี่ยนสำคัญที่ไม่เพียงแต่ส่งผลกระทบต่อความมั่นคงในโลกกายภาพเท่านั้น แต่ยังส่งผลสะท้อนอย่างลึกซึ้งต่อแนวทางการสร้างความมั่นคงในโลกไซเบอร์ด้วย ความตระหนักถึงภัยคุกคามที่ไม่สมมาตรและการใช้ช่องทางที่คาดไม่ถึงในการโจมตี ทำให้รัฐบาลทั่วโลกหันมาให้ความสำคัญกับการเสริมสร้างความสามารถในการเฝ้าระวัง ป้องกัน และตอบโต้ภัยคุกคามในทุกมิติ รวมถึงโลกออนไลน์ โดยหลังเหตุการณ์ 911 รัฐบาลหลายประเทศได้ดำเนินมาตรการต่างๆ เพื่อเสริมสร้างความมั่นคง เช่น

สหรัฐอเมริกาออกกฎหมาย Patriot Act ทันทีในปี 2001 เพื่อขยายขอบเขตอำนาจของรัฐบาลในการสอดส่องการสื่อสารและข้อมูลส่วนบุคคล โดยอ้างเหตุผลด้านการป้องกันการก่อการร้าย (Lyon, 2003) กฎหมายนี้อนุญาตให้มีการดักฟังโทรศัพท์ การตรวจสอบอีเมล และการเข้าถึงบันทึกข้อมูลต่างๆ ได้ง่ายขึ้น มีการบังคับให้ผู้ให้บริการเก็บรักษาข้อมูล ในขณะที่อีกหลายประเทศได้ออกกฎหมายบังคับให้ผู้ให้บริการโทรคมนาคมและอินเทอร์เน็ตเก็บรักษาข้อมูลการสื่อสารของผู้ใช้งานเช่นกัน เพื่อให้หน่วยงานความมั่นคงสามารถเข้าถึงข้อมูลเหล่านี้ได้ในภายหลังเพื่อการสืบสวน (Bennett & Raab, 2006)

การขยายอำนาจการเฝ้าระวังของสหรัฐอเมริกาภายใต้ Patriot Act ไม่ได้จำกัดอยู่เพียงภายในประเทศเท่านั้น ผลกระทบของมันได้ขยายไปยังการควบคุมในประเทศอื่นๆ ทั่วโลก หลายรัฐบาลได้อ้างเหตุผลด้านความมั่นคงแห่งชาติและการต่อต้านการก่อการร้ายเพื่อออกกฎหมายและใช้มาตรการที่คล้ายคลึงกัน ซึ่งอนุญาตให้มีการสอดส่องพลเมืองและข้อมูลออนไลน์มากขึ้น (Freedom House, 2023) แรงจูงใจในการควบคุมในระดับที่สูงเช่นนี้มีรากฐานมาจากความเชื่อที่ว่า การเฝ้าระวังอย่างกว้างขวางเป็นเครื่องมือสำคัญในการป้องกันภัยคุกคามที่มองไม่เห็นและอาจเกิดขึ้นได้ทุกเมื่อ โดยเฉพาะอย่างยิ่งในยุคที่ผู้ก่อการร้ายและอาชญากรสามารถใช้เทคโนโลยีในการวางแผนและดำเนินการได้อย่างง่ายดาย

ข่าวการแอบดักฟัง ที่โด่งดังและสะท้อนถึงขอบเขตของการเฝ้าระวังระดับโลกคือ กรณีของเอ็ดเวิร์ด สโนว์เดน อดีตผู้รับเหมาของสำนักงานความมั่นคงแห่งชาติ (NSA) ซึ่งในปี 2013 ได้เปิดเผยเอกสารลับจำนวนมากที่แสดงให้เห็นถึงโครงการเฝ้าระวังลับของ NSA ที่มีขอบเขตกว้างขวางอย่างน่าตกใจ ข้อมูลที่สโนว์เดนเปิดเผยระบุว่า NSA ได้ เก็บรวบรวมข้อมูลการโทรศัพท์ (metadata) ของพลเมืองอเมริกันจำนวนมาก โดยไม่จำเป็นต้องมีหมายศาล นอกจากนี้ ยังมีโครงการ PRISM ที่อนุญาตให้ NSA เข้าถึงข้อมูลส่วนบุคคลโดยตรงจากเซิร์ฟเวอร์ของบริษัทเทคโนโลยีรายใหญ่ เช่น Google, Facebook และ Apple ด้วย (Greenwald, 2014)

จำนวนพลเมืองอเมริกันที่ตกเป็นเป้าถูกดักฟังโดยตรงนั้นเป็นข้อมูลที่ไม่ได้รับการเปิดเผยอย่างเป็นทางการทั้งหมด อย่างไรก็ตาม การเก็บรวบรวมข้อมูลอย่างกว้างขวางหมายความว่า ข้อมูลการสื่อสารของชาวอเมริกันหลายล้านคนถูกเก็บไว้ การขยายอำนาจการเฝ้าระวังเช่นนี้ถูกมองว่ามีความจำเป็นโดยรัฐบาลและหน่วยงานความมั่นคงเพื่อ "เชื่อมโยงจุดต่างๆ" (connect the dots) และป้องกันการโจมตีที่อาจเกิดขึ้น อย่างไรก็ตาม นักวิจารณ์และองค์กรสิทธิพลเมืองได้เตือนถึงอันตรายของการให้อำนาจรัฐมากเกินไป ซึ่งอาจนำไปสู่การ ละเมิดสิทธิในความเป็นส่วนตัว การจำกัดเสรีภาพในการแสดงความคิดเห็น และการสร้างบรรยากาศแห่งความหวาดระแวงและการควบคุม

แม้ว่ามาตรการเหล่านี้มีเป้าหมายเพื่อความมั่นคง แต่บางครั้งการดำเนินการก็ล้ำเส้นสิทธิและเสรีภาพของประชาชนจนเป็นที่วิพากษ์วิจารณ์อย่างกว้างขวาง การเฝ้าระวังแบบ "เหวี่ยงแห" (Mass Surveillance) การเก็บรวบรวมและวิเคราะห์ข้อมูลการสื่อสารของประชาชนจำนวนมากโดยไม่มีเหตุอันควรสงสัยเฉพาะเจาะจง ถือเป็นการละเมิดสิทธิในความเป็นส่วนตัวอย่างร้ายแรง ตัวอย่างเช่น โครงการ PRISM ของสำนักงานความมั่นคงแห่งชาติสหรัฐอเมริกา (NSA) ที่ถูกเปิดเผยโดย Edward Snowden แสดงให้เห็นถึงการเข้าถึงข้อมูลผู้ใช้งานจากบริษัทเทคโนโลยีรายใหญ่โดยรัฐบาล (Greenwald, 2014) ซึ่งได้วิเคราะห์ถึงการเกิดขึ้นของ "ทุนนิยมเฝ้าระวัง" ที่บริษัทเทคโนโลยีและรัฐบาลเก็บรวบรวมและวิเคราะห์

ข้อมูลส่วนบุคคลในระดับที่ไม่เคยมีมาก่อน ซึ่งส่งผลกระทบต่อความเป็นอิสระและเสรีภาพของมนุษย์ (Zuboff, 2019)

การสร้างความมั่นคงปลอดภัยไซเบอร์ในต่างประเทศ

จากหน่ออ่อน 911 กระทั่งเมื่อเทคโนโลยีสารสนเทศและอินเทอร์เน็ตเข้ามามีบทบาทในทุกมิติของชีวิตสมัยใหม่ ความมั่นคงจึงเปลี่ยนรูปแบบจากสนามรบสู่โลกออนไลน์ การคุกคามไม่จำเป็นต้องใช้ในลักษณะก่อการร้ายเสมอไป แต่อาจอยู่ในรูปของการแฮกข้อมูลระบบรัฐ การแพร่ข่าวปลอม หรือการโจมตีโครงสร้างพื้นฐานผ่านระบบไซเบอร์ ดังนั้นแนวคิดความมั่นคงไซเบอร์ (cybersecurity) จึงขยายตัวขึ้นอย่างรวดเร็ว รัฐบาลต่าง ๆ เริ่มออกกฎหมายและจัดตั้งหน่วยงานพิเศษเพื่อควบคุมภัยคุกคามไซเบอร์ แต่ในขณะเดียวกัน อำนาจใหม่ที่รัฐได้รับก็กลายเป็นดาบสองคม เพราะมักมาพร้อมกับการละเมิดสิทธิเสรีภาพของประชาชนภายใต้ข้ออ้างด้าน “ความมั่นคง”

จีน เป็นหนึ่งในตัวอย่างที่เด่นชัดที่สุดในการใช้กฎหมายไซเบอร์เพื่อควบคุมข้อมูลของประชาชนอย่างเป็นระบบ กฎหมาย Cybersecurity Law ที่มีผลบังคับใช้ในปี 2017 บังคับให้บริษัทเทคโนโลยีภายในประเทศต้องจัดเก็บข้อมูลผู้ใช้งานไว้ภายในประเทศ และให้รัฐสามารถเข้าถึงข้อมูลเหล่านี้ได้โดยไม่มีข้อจำกัดทางกฎหมายที่ชัดเจน นอกจากนี้ยังสามารถสั่งลบหรือจำกัดการเผยแพร่เนื้อหาที่ถือว่า “เป็นภัยต่อความมั่นคง” ได้อย่างกว้างขวาง (Creemers, 2017) การดำเนินนโยบายเช่นนี้ทำให้จีนสามารถควบคุมโซเชียลมีเดียและแหล่งข่าวออนไลน์ได้อย่างเบ็ดเสร็จ และกลายเป็นกรอบควบคุมที่จำกัดเสรีภาพในการแสดงออกของพลเมืองจีนในระดับลึก นอกจากนี้ จีนยังมีการใช้อำนาจรัฐในการควบคุมและสอดส่องข้อมูลของประชาชนอย่างเข้มงวด ผ่านระบบ Great Firewall ที่ควบคุมการเข้าถึงอินเทอร์เน็ตและระบบ “Social Credit” ที่เก็บรวบรวมข้อมูลพฤติกรรมของประชาชนเพื่อประเมินความน่าเชื่อถือ (Kostka, 2019) แนวทางนี้ถูกวิจารณ์ว่าเป็นการละเมิดความเป็นส่วนตัวและเสรีภาพของประชาชน แต่รัฐบาลจีนมองว่าเป็นวิธีการในการรักษาความสงบเรียบร้อยและความมั่นคงของชาติ

รัสเซีย รัฐบาลได้ผ่านกฎหมายชุดหนึ่งที่รู้จักกันในชื่อ Yarovaya Law เมื่อปี 2016 ซึ่งเป็นส่วนหนึ่งของความพยายามในการต่อต้านการก่อการร้าย แต่กลับให้อำนาจรัฐในการสอดส่องและจัดเก็บข้อมูลของประชาชนอย่างเข้มงวด กฎหมายฉบับนี้กำหนดให้ผู้ให้บริการโทรคมนาคมต้องเก็บข้อมูลทั้งหมดของผู้ใช้งานไว้นานถึง 6 เดือน และอนุญาตให้หน่วยงานความมั่นคงสามารถร้องขอให้เข้าถึงข้อมูลและระบบสื่อสารได้ รวมถึงการขอให้บริษัทถอดรหัสข้อความแบบเข้ารหัส เช่น ข้อความจากแอปพลิเคชันสื่อสารต่าง ๆ (Human Rights Watch, 2016) แน่นอนว่าแนวทางนี้สร้างความกังวลด้านสิทธิในความเป็นส่วนตัวและการแสดงออก โดยเฉพาะในหมู่นักเคลื่อนไหวและสื่ออิสระ

ยิ่งไปกว่านั้น รัสเซียได้พัฒนาแนวคิด "อธิปไตยทางอินเทอร์เน็ต" (Sovereign Internet) โดยทดสอบการตัดขาดจากอินเทอร์เน็ตโลกเพื่อสร้างเครือข่ายภายในประเทศของตนเอง (RuNet) (The standard, 2019) รัฐบาลได้รวมเอาที่อยู่ IP ของประเทศกว่าครึ่งหนึ่งไว้กับผู้ให้บริการอินเทอร์เน็ต 7 ราย ที่รัฐบาลเกี่ยวข้อง (Human Rights Watch, 2025) ซึ่งทำให้รัฐบาลมีอำนาจในการบล็อกและควบคุมการรับส่งข้อมูลอย่างกว้างขวาง แม้ว่า VPN จะได้รับความนิยมอย่างสูงในรัสเซีย โดยมีการดาวน์โหลดถึง 33.5 ล้านครั้ง ในปี 2022 (The Jamestown Foundation, 2024) แต่รัฐบาลก็พยายามอย่างต่อเนื่องที่จะบล็อก VPN และออกกฎหมายที่ลงโทษผู้ให้บริการที่ไม่ยอมปฏิบัติตามคำสั่งของรัฐ (The Moscow Times, 2025)

อินเดีย ในปี 2021 ได้ออกกฎหมายควบคุมแพลตฟอร์มดิจิทัลภายใต้ชื่อ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules หรือ IT Rules 2021 กฎหมายฉบับนี้บังคับให้แพลตฟอร์มโซเชียลมีเดีย เช่น Facebook และ Twitter ลบเนื้อหาที่ไม่เหมาะสม ภายใน 36 ชั่วโมงหลังจากได้รับคำร้องจากรัฐ และในกรณีที่เกี่ยวข้องกับความมั่นคงแห่งชาติ แพลตฟอร์มจะต้องเปิดเผยตัวตนของผู้ส่งข้อความต้นทาง เช่น ข้อความจาก WhatsApp ซึ่งเป็นแอปพลิเคชันที่เน้นความเป็นส่วนตัวและการเข้ารหัสแบบ end-to-end (Freedom House, 2021) ข้อกำหนดเช่นนี้ถูกวิพากษ์วิจารณ์ว่าเปิดช่องให้รัฐละเมิดเสรีภาพในการสื่อสารและความเป็นส่วนตัวของพลเมือง

อียิปต์ ออกกฎหมาย Cybercrime Law ในปี 2018 โดยมีสาระสำคัญคือให้อำนาจรัฐในการบล็อกเว็บไซต์หรือเนื้อหาที่ “เป็นภัยต่อความมั่นคง” หรือ “ขัดต่อศีลธรรม” ของรัฐ รวมถึงลงโทษผู้ใช้งานที่แชร์ข้อมูลเท็จหรือปลุกปั่นสังคม กฎหมายฉบับนี้ถูกใช้เป็นเครื่องมือสำคัญในการควบคุมโลกออนไลน์ ซึ่งในทางปฏิบัติได้ส่งผลให้มีการจับกุมผู้ใช้โซเชียลมีเดียจำนวนมาก รวมถึงนักเคลื่อนไหวและนักข่าวที่วิจารณ์รัฐบาล (Amnesty International, 2018) กฎหมายดังกล่าวจึงกลายเป็นสิ่งที่ลดทอนเสรีภาพในการแสดงออกอย่างรุนแรงภายใต้ข้ออ้างด้านความมั่นคง

การรักษาสมดุลเสรีภาพของพลเมืองกับความมั่งคงปลอดภัยแห่งรัฐ

สำหรับประเทศที่ยอมรับได้ว่ามีความก้าวหน้าในเชิงกฎหมายด้านการคุ้มครองเสรีภาพและข้อมูลส่วนบุคคลของพลเมืองมากที่สุด นั่นก็คือกลุ่มประเทศใน**สหภาพยุโรป** (EU) โดยมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือ General Data Protection Regulation (GDPR) ซึ่งถือเป็นตัวอย่างที่โดดเด่นของความพยายามในการสร้างสมดุลระหว่างความมั่นคง และเสรีภาพอย่างเป็นรูปธรรม

GDPR ซึ่งมีผลบังคับใช้เมื่อปี 2018 ได้รับการยกย่องว่าเป็นหนึ่งในกฎหมายที่เข้มงวดและทันสมัยที่สุดในโลกด้านการคุ้มครองข้อมูลส่วนบุคคล โดยมีจุดมุ่งหมายเพื่อคืนอำนาจในการควบคุมข้อมูล

ให้แก่เจ้าของข้อมูล พร้อมทั้งกำหนดข้อบังคับอย่างเข้มงวดต่อผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล ทั้งในและนอกเขต EU (Voigt & Von dem Bussche, 2017) กฎหมายฉบับนี้เกิดขึ้นจากการตระหนักว่าแม้รัฐและองค์กรจะมีความจำเป็นในการใช้ข้อมูลเพื่อความมั่นคง เศรษฐกิจ และการบริการประชาชน แต่สิทธิส่วนบุคคลไม่ควรถูกละเลยหรือใช้เป็นข้ออ้างในการเฝ้าระวังโดยไม่จำกัดขอบเขต

แนวคิดเรื่องสมดุลใน GDPR สะท้อนชัดในหลักการ “proportionality” และ “necessity” ซึ่งกำหนดว่าการเก็บและใช้ข้อมูลต้องมีวัตถุประสงค์ชัดเจน อยู่ในขอบเขตที่จำเป็น และไม่เกินกว่าเหตุ เช่น รัฐไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้โดยไม่มีกฎหมายที่เหมาะสม หรือในกรณีของหน่วยงานด้านความมั่นคง ก็ยังต้องปฏิบัติตามกรอบสิทธิขั้นพื้นฐานของประชาชนที่ระบุไว้ในกฎบัตรแห่งสิทธิพื้นฐานของสหภาพยุโรป (Charter of Fundamental Rights of the EU, 2012) สิ่งนี้สะท้อนให้เห็นว่า EU ไม่ได้ปฏิเสธความจำเป็นด้านความมั่นคง แต่เลือกออกแบบระบบที่ให้ “อำนาจภายใต้การตรวจสอบ” แทนการใช้อำนาจแบบไร้ขอบเขต

อีกตัวอย่างคือ การอนุญาตให้มีการเก็บข้อมูล metadata ของการสื่อสารเพื่อวัตถุประสงค์ด้านความมั่นคง แต่ต้องอยู่ภายใต้การกำกับของศาลหรือองค์กรอิสระ และต้องมีมาตรการป้องกันการนำข้อมูลไปใช้ในทางที่ละเมิดสิทธิ (European Court of Justice, 2016) นั่นทำให้ GDPR กลายเป็นเครื่องมือสร้าง “ความไว้วางใจ” ระหว่างรัฐ องค์กร และประชาชน ซึ่งถือเป็นองค์ประกอบสำคัญของระบบประชาธิปไตยที่โปร่งใส

กรณีของสหภาพยุโรปจึงสะท้อนแนวคิดที่ว่า ความมั่นคงและเสรีภาพไม่จำเป็นต้องเป็นศัตรูกัน หากแต่สามารถดำรงอยู่ร่วมกันได้ผ่านกลไกทางกฎหมายและสถาบันที่รอบคอบ และตรวจสอบได้ การมีความมั่นคงโดยที่ประชาชนยังคงมีสิทธิและเสรีภาพในโลกดิจิทัลอย่างแท้จริง จึงไม่ใช่เพียงอุดมคติ แต่เป็นแนวปฏิบัติที่จับต้องได้ภายใต้กรอบคิดแบบยุโรป

สำหรับ**ประเทศไทย** มีกฎหมายที่เกี่ยวข้องที่สำคัญอย่างน้อย 3 ฉบับ ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีความพยายามในการสร้างสมดุลระหว่างความมั่นคงทางไซเบอร์กับการคุ้มครองสิทธิพลเมือง อย่างไรก็ตาม การบังคับใช้กฎหมายและความชัดเจนของขอบเขตอำนาจรัฐยังคงเป็นประเด็นที่ต้องติดตามและทบทวน (อ่านต่อใน เหรียญสองด้าน เสรีภาพประชาชนและความมั่นคงไซเบอร์ในบริบทไทย)

ดังนั้น จากการเปรียบเทียบจะเห็นได้ว่าประเทศต่าง ๆ มีแนวทางที่แตกต่างกันในการสร้างสมดุลระหว่างอำนาจรัฐและความเป็นส่วนตัว โดยเฉพาะอย่างยิ่งในสหภาพยุโรปที่ให้ความสำคัญกับความเป็นส่วนตัวผ่านกฎหมายที่เข้มงวด และอีกหลายประเทศพยายามหาสมดุลระหว่างสองด้านนี้ แต่ยังคง

เผชิญกับการวิพากษ์วิจารณ์ การสร้างสมดุลที่เหมาะสมจำเป็นต้องคำนึงถึงบริบททางสังคม วัฒนธรรม และความต้องการของประชาชนในแต่ละประเทศ

เหรียญสองด้าน เสรีภาพประชาชนและความมั่นคงไซเบอร์ในบริบทไทย

ประเทศไทยเป็นอีกหนึ่งประเทศที่ตระหนักถึงความสำคัญของทั้งเสรีภาพของประชาชนและความมั่นคงปลอดภัยไซเบอร์ ในด้านการคุ้มครองเสรีภาพและความเป็นส่วนตัว รัฐธรรมนูญแห่งราชอาณาจักรไทยได้รับรองสิทธิในความเป็นส่วนตัวและการสื่อสารถึงกันโดยทางใดๆ จะกระทำมิได้ (Constitution of the Kingdom of Thailand, 2017, Section 32) นอกจากนี้ ประเทศไทยได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ซึ่งมีเจตนารมณ์ในการให้ความคุ้มครองข้อมูลส่วนบุคคลของประชาชนและกำหนดหลักเกณฑ์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

อย่างไรก็ตาม ในขณะเดียวกัน ประเทศไทยก็มีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม รวมถึงพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 ซึ่งให้อำนาจแก่หน่วยงานของรัฐในการเฝ้าระวัง ตรวจสอบ และเข้าถึงข้อมูลทางคอมพิวเตอร์ในบางกรณีเพื่อวัตถุประสงค์ด้านความมั่นคงแห่งชาติ ความมั่นคงของรัฐ เศรษฐกิจของประเทศ หรือความสงบเรียบร้อยของประชาชน กฎหมายเหล่านี้ แม้จะมีเจตนาเพื่อป้องกันภัยคุกคามทางไซเบอร์ แต่ก็ถูกวิพากษ์วิจารณ์ถึงขอบเขตอำนาจที่กว้างขวางและการอาจกระทบต่อสิทธิความเป็นส่วนตัวและการแสดงความคิดเห็นของประชาชน

ตัวอย่างที่เห็นได้ชัดคือการบังคับให้ผู้ให้บริการอินเทอร์เน็ตเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) เป็นระยะเวลานาน ซึ่งอาจเป็นการรุกล้ำความเป็นส่วนตัวของผู้ใช้งานโดยไม่มีเหตุอันควร นอกจากนี้ การตีความและบังคับใช้กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ยังเป็นประเด็นที่ต้องจับตามองอย่างใกล้ชิด เพื่อให้มั่นใจว่าการใช้อำนาจของรัฐเป็นไปอย่างสมเหตุสมผลและไม่กระทบต่อเสรีภาพของประชาชนเกินความจำเป็น

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม พ.ศ. 2560 กฎหมายฉบับนี้มีจุดมุ่งหมายหลักในการลงโทษผู้กระทำความผิดเกี่ยวกับระบบคอมพิวเตอร์และข้อมูลทางคอมพิวเตอร์ ครอบคลุมความผิดหลากหลายรูปแบบ เช่น การเข้าถึงระบบโดยมิชอบ การทำให้ระบบขัดข้อง การดักรับข้อมูล การเผยแพร่ข้อมูลเท็จ และความผิดที่เกี่ยวข้องกับความมั่นคงของระบบ

ข้อเท็จจริงที่ปรากฏ มีการบังคับใช้ พ.ร.บ. คอมพิวเตอร์ฯ อย่างต่อเนื่องในคดีอาชญากรรมทางเทคโนโลยีต่างๆ อย่างไรก็ตาม กฎหมายนี้ถูกวิพากษ์วิจารณ์ในบางครั้งถึงความคลุมเครือของบทบัญญัติบางประการ โดยเฉพาะอย่างยิ่ง มาตรา 14 ที่เกี่ยวข้องกับการเผยแพร่ข้อมูลอันเป็นเท็จ ซึ่งถูกมองว่าอาจ

ถูกใช้เพื่อจำกัดเสรีภาพในการแสดงความคิดเห็นและการวิพากษ์วิจารณ์ (Human Rights Watch, 2020) มีกรณีการดำเนินคดีกับนักกิจกรรมและประชาชนที่แสดงความคิดเห็นออนไลน์ ซึ่งถูกตีความว่าเป็นการเผยแพร่ข้อมูลเท็จที่กระทบต่อความมั่นคงหรือความสงบเรียบร้อย ส่วนในด้านความสัมพันธ์เชิงอำนาจ กฎหมายนี้ให้อำนาจแก่เจ้าหน้าที่รัฐในการสืบสวน สอบสวน และดำเนินคดีกับผู้กระทำความผิด ซึ่งอาจนำไปสู่การใช้อำนาจที่ไม่สมดุลและกระทบต่อสิทธิของผู้ถูกกล่าวหาได้

2. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 กฎหมายฉบับนี้มีเป้าหมายหลักในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อความมั่นคงแห่งชาติ ความมั่นคงทางเศรษฐกิจ และความสงบเรียบร้อยของประชาชน กฎหมายให้อำนาจแก่คณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (กมช.) และ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (สกมช.) ในการกำหนดมาตรการ เฝ้าระวัง ตรวจสอบ และสั่งการหน่วยงานต่างๆ ที่เกี่ยวข้อง ทว่าข้อเท็จจริงที่ปรากฏ การบังคับใช้ พ.ร.บ. ความมั่นคงไซเบอร์ฯ ยังอยู่ในช่วงเริ่มต้น แต่ได้ก่อให้เกิดความกังวลในวงกว้างเกี่ยวกับขอบเขตอำนาจที่กว้างขวางของเจ้าหน้าที่รัฐในการเข้าถึงข้อมูลและการสั่งการ โดยเฉพาะอย่างยิ่ง มาตรา 60 ที่ให้อำนาจ สกมช. ในการเข้าถึงข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์โดยไม่ต้องมีหมายศาลในกรณีที่มี "ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ" ซึ่งถูกมองว่าอาจเป็นการรุกล้ำความเป็นส่วนตัวโดยไม่มีการตรวจสอบที่เพียงพอ (iLaw, 2019) นอกจากนี้ การกำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อาจนำไปสู่การเพิ่มการควบคุมและตรวจสอบกิจกรรมออนไลน์ของประชาชนที่ใช้บริการเหล่านั้น และกฎหมายนี้ยังเป็นการเสริมสร้างอำนาจของรัฐในการควบคุมและจัดการพื้นที่ไซเบอร์อย่างมีนัยสำคัญ โดยมีข้อกังวลว่าอาจนำไปสู่การลดทอนเสรีภาพในการแสดงความคิดเห็นและการเข้าถึงข้อมูล หากไม่มีการใช้ดุลพินิจและการตรวจสอบอย่างเหมาะสม

3. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พ.ร.บ. PDPA) กฎหมายฉบับนี้มีจุดมุ่งหมายในการให้ความคุ้มครองข้อมูลส่วนบุคคลของประชาชน กำหนดหลักเกณฑ์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และให้สิทธิแก่เจ้าของข้อมูลในการควบคุมข้อมูลของตน ข้อเท็จจริงที่ปรากฏ พ.ร.บ. PDPA มีผลบังคับใช้แล้ว และหลายหน่วยงานทั้งภาครัฐและเอกชนกำลังปรับตัวเพื่อให้สอดคล้องกับกฎหมาย อย่างไรก็ตาม ยังมีความท้าทายในการบังคับใช้กฎหมายอย่างมีประสิทธิภาพ และมีข้อกังวลว่า ข้อยกเว้นในกฎหมายที่อนุญาตให้เปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ด้านความมั่นคงแห่งชาติและความมั่นคงของรัฐ อาจถูกตีความและนำไปใช้ในวงกว้าง จนลดทอนการคุ้มครองสิทธิในความเป็นส่วนตัวที่กฎหมายต้องการให้กฎหมายนี้พยายามสร้างสมดุลระหว่างสิทธิของเจ้าของข้อมูลกับ

ความจำเป็นในการใช้ข้อมูลเพื่อวัตถุประสงค์ต่างๆ รวมถึงความมั่นคง อย่างไรก็ตาม การตีความและการบังคับใช้ข้อยกเว้นยังคงเป็นประเด็นสำคัญที่ต้องจับตามอง

จากข้อเท็จจริงที่ปรากฏ กฎหมายไทยด้านความมั่นคงปลอดภัยทางไซเบอร์และการคุ้มครองเสรีภาพพลเมืองยังคงอยู่ในสภาวะที่มีความตึงเครียดและต้องมีการปรับปรุงอย่างต่อเนื่อง แม้ว่า พ.ร.บ. PDPA จะเป็นก้าวสำคัญในการคุ้มครองสิทธิในความเป็นส่วนตัว แต่อำนาจที่กว้างขวางที่มอบให้กับรัฐภายใต้ พ.ร.บ. คอมพิวเตอร์ฯ และ พ.ร.บ. ความมั่นคงไซเบอร์ฯ โดยเฉพาะอย่างยิ่งในประเด็นการเข้าถึงข้อมูลและการควบคุมเนื้อหาออนไลน์ยังคงเป็นข้อกังวลหลัก

การตีความและการบังคับใช้กฎหมายเหล่านี้มีแนวโน้มที่จะให้น้ำหนักกับความมั่นคงของรัฐมากกว่าเสรีภาพของประชาชน ในหลายกรณี การดำเนินคดีภายใต้ พ.ร.บ. คอมพิวเตอร์ฯ ในข้อหาเผยแพร่ข้อมูลเท็จถูกมองว่าเป็นการจำกัดเสรีภาพในการแสดงความคิดเห็นและการวิพากษ์วิจารณ์มากกว่าที่จะเป็นการป้องกันภัยคุกคามที่แท้จริงต่อความมั่นคง นอกจากนี้ ความคลุมเครือของบทบัญญัติบางประการ ในกฎหมายทั้งสองฉบับเปิดโอกาสให้เจ้าหน้าที่รัฐสามารถใช้ดุลพินิจในวงกว้าง ซึ่งอาจนำไปสู่การเลือกปฏิบัติและการใช้อำนาจที่ไม่เป็นธรรม การขาดกลไกการตรวจสอบและถ่วงดุลที่มีประสิทธิภาพยังเป็นปัจจัยที่น่ากังวล

การสร้างความสมดุลความมั่นคงปลอดภัยไซเบอร์กับเสรีภาพพลเมือง

จากที่กล่าวมาข้างต้น เพื่อให้ความมั่นคงปลอดภัยไซเบอร์ที่ถูกสร้างโดยรัฐเกิดความสมดุลกับเสรีภาพพลเมืองที่ต้องได้รับความคุ้มครอง บทความนี้จึงพยายามเสนอ “หมุดยึด” 4 ประการ บนหลักการที่ว่า “ความมั่นคงและเสรีภาพไม่จำเป็นต้องเป็นปฏิปักษ์กัน แต่สามารถดำรงอยู่ร่วมกันได้ผ่านการจัดการอำนาจที่โปร่งใสและตรวจสอบได้” โดยมุ่งเน้นไปที่การสร้างกลไกการตรวจสอบและถ่วงดุลทางสถาบันและกฎหมาย เพื่อป้องกันมิให้รัฐใช้อำนาจเกินขอบเขตภายใต้ข้ออ้างด้านความมั่นคง หมุดยึดสำคัญ 4 ประการ ได้แก่

หมุดยึดที่ 1 กลไกการกำกับดูแลที่เป็นอิสระ คือการสร้าง องค์กรอิสระที่เข้มแข็ง และ ยึดโยงกับภาคประชาสังคม (Civil Society Linkage) องค์กรดังกล่าวต้องมีอำนาจในการตรวจสอบและควบคุมการเข้าถึงข้อมูลของหน่วยงานความมั่นคงได้อย่างแท้จริง โดยเน้นการป้องกันการใช้อำนาจเกินขอบเขตของรัฐ การมีส่วนร่วมของภาคประชาสังคมในกลไกนี้จะช่วยเสริมสร้าง ความไว้วางใจ และรับประกันว่าการตัดสินใจด้านความมั่นคงจะคำนึงถึงมุมมองด้านสิทธิมนุษยชน

หมุดยึดที่ 2 กรอบกฎหมายที่ชัดเจนและจำกัด คือเน้นการแก้ไขกฎหมายที่มีอยู่ (เช่น กฎหมายความมั่นคงปลอดภัยไซเบอร์) ให้มีขอบเขตการใช้อำนาจตรวจสอบที่ชัดเจน ไม่คลุมเครือ กฎหมายต้องระบุ คำจำกัดความ ของ "ภัยคุกคาม" และ "ระดับวิกฤติ" ที่แคบและจำกัดที่สุด เพื่อป้องกันการตีความที่

กว้างเกินไป นอกจากนี้ต้องมีข้อห้ามชัดเจนเกี่ยวกับการเฝ้าระวังแบบเหวี่ยงแห โดยกำหนดให้มาตรการสอดส่องข้อมูลส่วนบุคคลต้องกระทำเฉพาะเจาะจง (Targeted) และอยู่ภายใต้คำสั่งศาลเท่านั้น เพื่อคุ้มครองสิทธิในความเป็นส่วนตัว

หมุดยึดที่ 3 หลักการนิติรัฐเชิงสัดส่วน คือการยึดถือเอาหลักการสากลมาใช้ในทุกขั้นตอนของการจำกัดสิทธิ การคำนึงถึงความได้สัดส่วน (Proportionality) โดยบังคับให้รัฐบาลต้องพิสูจน์ว่ามาตรการใด ๆ ที่จำกัดสิทธิพลเมืองนั้น ต้องมีความจำเป็นอย่างยิ่ง และ ไม่เกินกว่าเหตุ เมื่อเทียบกับประโยชน์ด้านความมั่นคงที่คาดว่าจะได้รับ การกระทำของรัฐต้องมีฐานทางกฎหมาย และสามารถตรวจสอบย้อนกลับได้ เช่น จัดให้มีช่องทาง การร้องเรียนและการเยียวยา ที่เข้าถึงง่ายและเป็นอิสระสำหรับพลเมืองที่เชื่อว่าสิทธิในความเป็นส่วนตัวของตนถูกละเมิดโดยหน่วยงานของรัฐ เพื่อธำรงไว้ซึ่งหลักนิติรัฐและรับประกันว่าอำนาจของรัฐจะถูกใช้ไปอย่างมีเหตุผลและจำกัด

หมุดยึดที่ 4 ลำดับความสำคัญของเสรีภาพ หลักนี้คือการปรับเปลี่ยนกรอบความคิด โดยกำหนดให้เสรีภาพพลเมืองมีค่ามากกว่าความสะดวกของรัฐ ในการปฏิบัติงานด้านความมั่นคง รัฐบาลจึงต้องรับภาระในการพิสูจน์ความชอบธรรมในการจำกัดสิทธิพลเมือง และต้องสร้างความโปร่งใสในการใช้เทคโนโลยีเฝ้าระวัง เช่น การเปิดเผยรายงานความโปร่งใสประจำปี (Transparency Report) โดยเปิดเผยจำนวนครั้งของการร้องขอข้อมูลจากรัฐบาล (เช่น การดักฟัง, การขอเข้าถึงข้อมูลจราจร) ที่ถูกร้องขอและถูกปฏิเสธ เพื่อให้สาธารณะสามารถตรวจสอบการทำงานได้และป้องกันไม่ให้การแสวงหาความมั่นคงแปรสภาพเป็นเครื่องมือในการควบคุมพลเมือง และส่งเสริม เสรีภาพในการแสดงความคิดเห็นอย่างแท้จริง

บทสรุป

การสร้างสมดุลระหว่างอำนาจของรัฐในการรักษาความมั่นคงปลอดภัยไซเบอร์ กับสิทธิในความเป็นส่วนตัวของประชาชน เป็นประเด็นที่ต้องการความละเอียดอ่อนและการมีส่วนร่วมจากหลายภาคส่วน รัฐบาลจำเป็นต้องมีเครื่องมือในการป้องกันภัยคุกคามทางไซเบอร์ที่ซับซ้อนและเปลี่ยนแปลงตลอดเวลา เช่น การโจมตีระบบโครงสร้างพื้นฐานหรือการแพร่กระจายข้อมูลปลอม (disinformation) แต่ในขณะเดียวกันก็ต้องไม่ล่วงล้ำหรือใช้ข้อมูลส่วนบุคคลเกินขอบเขตที่จำเป็น เพราะอาจก่อให้เกิดผลกระทบต่อเสรีภาพในการแสดงออก ความเชื่อมั่นต่อรัฐ และบรรยากาศประชาธิปไตยโดยรวม

แม้ว่ากฎหมายการสร้างความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ จะถูกออกแบบมาภายใต้เงื่อนไขและบริบทของประเทศนั้นๆ จึงไม่สามารถวัดผลหรือกำหนดได้ด้วยค่าหรือสูตรตายตัว แต่มาตรการใดที่รัฐจะใช้นั้น ควรอยู่บนหลัก “ความจำเป็นและได้สัดส่วน” (necessity and proportionality) ตามหลักสิทธิมนุษยชนสากล พร้อมทั้งต้องมีระบบตรวจสอบและถ่วงดุลเพื่อป้องกันการใช้อำนาจในทางมิชอบ ความ

โปร่งใสในการจัดการข้อมูล และการให้สิทธิกับประชาชนในการรับรู้และโต้แย้ง จึงกลายเป็นหัวใจสำคัญของนโยบายความมั่นคงในยุคดิจิทัล ดังนั้น เพื่อวางรากฐานของสมดุลที่มั่นคงและยั่งยืน คำถามสำคัญต่อไปนี้ควรถูกหยิบยกขึ้นมาพิจารณา

รัฐควรมีขอบเขตมากน้อยเพียงใดในการเก็บข้อมูลส่วนบุคคลเพื่อความมั่นคง?

การกำหนดขอบเขตนี้ควรตั้งอยู่บนหลัก “ความจำเป็น” ในการใช้ข้อมูลอย่างเหมาะสม โดยต้องจำกัดการเก็บเฉพาะข้อมูลที่เกี่ยวข้องกับภัยคุกคามจริงเท่านั้น ไม่ใช่การสอดส่องพฤติกรรมของประชาชนทั่วไปอย่างครอบคลุมหรือไม่มีเป้าหมาย

การกำหนดขอบเขตที่ชัดเจนสามารถป้องกันการละเมิดสิทธิได้หรือไม่?

กฎหมายที่ชัดเจนไม่เพียงแต่กำหนดขอบเขตอำนาจของรัฐเท่านั้น แต่ยังเป็นกลไกตรวจสอบเชิงสถาบัน หากมีกระบวนการอิสระ เช่น ศาลหรือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเข้ามาอนุมัติการเข้าถึงข้อมูล จะสามารถจำกัดการใช้อำนาจเกินขอบเขต และสร้างบรรทัดฐานทางกฎหมายที่สมดุล เช่น แนวทางของ GDPR ในสหภาพยุโรปที่ให้ความสำคัญกับสิทธิของเจ้าของข้อมูล และวางระบบบทลงโทษที่ชัดเจนต่อผู้ละเมิด (Voigt & Von dem Bussche, 2017)

ประชาชนสามารถเชื่อมั่นได้หรือไม่ว่ารัฐจะใช้ข้อมูลอย่างถูกต้องและไม่ละเมิดความเป็นส่วนตัว?

คำถามนี้นำไปสู่ประเด็น “ความโปร่งใส” (Transparency) และ “ความไว้วางใจ” (trust) ซึ่งไม่สามารถเกิดขึ้นได้จากคำประกาศของรัฐเพียงลำพัง แต่ต้องมีกลไกตรวจสอบและการเปิดเผยข้อมูลต่อสาธารณะว่ามีการเก็บ ใช้ หรือแชร์ข้อมูลในลักษณะใดบ้าง เช่น การจัดทำรายงานความโปร่งใส (transparency report) หรือการมีช่องทางร้องเรียนที่มีประสิทธิภาพสำหรับผู้ที่เชื่อว่าตนถูกละเมิดสิทธิ

ประชาชนควรมีสิทธิในการตรวจสอบข้อมูลที่รัฐเก็บเกี่ยวกับตนเองหรือไม่?

การให้สิทธิเข้าถึงและตรวจสอบข้อมูลที่รัฐถือครองเกี่ยวกับตนเอง เป็นหลักการพื้นฐานของสิทธิในข้อมูล (Data Subject Rights) และเป็นหัวใจของการสร้างสมดุลระหว่างอำนาจกับความรับผิดชอบ เช่น กฎหมาย GDPR กำหนดให้ประชาชนสามารถขอคัดลอก ลบ หรือโอนย้ายข้อมูลได้ตามสิทธิของเจ้าของข้อมูล ซึ่งช่วยลดความเสี่ยงจากการละเมิดสิทธิและเพิ่มพลังให้กับภาคประชาชนในการต่อรองกับรัฐและองค์กรขนาดใหญ่ (European Commission, 2020)

การเฝ้าระวังของรัฐในยุคดิจิทัลสามารถลดอาชญากรรมและการก่อการร้ายได้จริง หรือเป็นเพียงข้ออ้างในการควบคุมประชาชน?

คำถามนี้ชี้ให้เห็นถึงความจำเป็นของ “การประเมินผลกระทบ” (Impact Assessment) อย่างรอบด้าน โดยเฉพาะการนำมาตรการสอดส่องมาใช้ ต้องมีหลักฐานเชิงประจักษ์ว่ามาตรการเหล่านั้นส่งผล

ต่อการลดอาชญากรรมจริง มิใช่เป็นเพียงเครื่องมือควบคุมพลเมืองทางการเมืองหรือกลุ่มเห็นต่าง การใช้เทคโนโลยีเพื่อเฝ้าระวังควรอยู่ภายใต้กรอบกฎหมายที่โปร่งใส พร้อมการประเมินเชิงสิทธิมนุษยชนอย่างสม่ำเสมอ

การอ้างอิง

Amnesty International. (2018, July 16). Egypt: Cybercrime law is a fresh assault on freedom of expression. https://www.amnesty.org/en/latest/news/2018/07/egypt-proposed-laws-an-assault-on-online-freedoms/

Bennett, C. J., & Raab, C. D. (2006). The governance of privacy: Policy instruments in global perspective. Ashgate Publishing.

Charter of Fundamental Rights of the European Union. (2012). Official Journal of the European Union, C 326, 391–407.

Creemers, R. (2017, June 29). Translation: Cybersecurity law of the People's Republic of China (effective June 1, 2017). DigiChina, Stanford University. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

Constitution of the Kingdom of Thailand, B.E. 2560 (2017). Government Gazette, 134(40a), 1–98.

European Commission. (2020). What are your rights under the GDPR? https://commission.europa.eu/law/law-topic/data-protection/information-individuals_en

European Court of Justice. (2016, December 21). Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others [Judgment of the Court (Grand Chamber)]. http://curia.europa.eu/juris/document/document.jsf?docid=186492

Freedom House. (2021). Freedom on the net 2021: India. https://freedomhouse.org/country/india/freedom-net/2021

Freedom House. (2023). Freedom on the net 2023: United States. https://freedomhouse.org/country/united-states/freedom-net/2023

Freedom House. (2024). Freedom on the net 2024: The struggle for trust online. https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online

Greenwald, G. (2014). No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state. Metropolitan Books.

Human Rights Watch. (2016, July 7). Russia: Big brother law harms security, rights. https://www.hrw.org/news/2016/07/07/russia-big-brother-law-harms-security-rights

Human Rights Watch. (2020, February 26). Thailand: Cyber crime act tightens internet control. https://www.hrw.org/news/2020/02/26/thailand-cyber-crime-act-tightens-internet-control

Human Rights Watch. (2025, July 30). Russia: Internet blocking, disruptions and increasing isolation. https://www.hrw.org/news/2025/07/30/russia-internet-blocking-disruptions-and-increasing-isolation

iLaw. (2019). Cybersecurity Act, Section 60: Authorizes the NCSA to access information without a court warrant. http://ethesisarchive.library.tu.ac.th/thesis/2023/TU_2023_6101032511_18977_28857.pdf

Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society, 21*(7), 1565–1593. https://doi.org/10.1177/1461444819826402

Lyon, D. (2003). Surveillance after September 11. Polity Press.

Pew Research Center. (2019, November 15). Americans and privacy: Concerned, confused and feeling lack of control over their personal information. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

The Standard. (2019, December 25). Russia successfully tests disconnection from global internet system, aims to enhance domestic internet efficiency. https://thestandard.co/russia-successfully-disconnected-from-the-internet/

The Moscow Times. (2025, July 22). Explained: How Russia is cracking down on the internet and messaging apps. https://www.themoscowtimes.com/2025/07/22/explained-how-russia-is-cracking-down-on-the-internet-and-messaging-apps-a89893

The Jamestown Foundation. (2024, November 25). Russia ramps up internet censorship. https://jamestown.org/program/russia-ramps-up-internet-censorship/

Voigt, P., & Von dem Bussche, J. (2017). The EU General Data Protection Regulation (GDPR): *A practical guide. European Journal of Risk Regulation, 8*(1), 71-87.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.