ปัญหาทางกฎหมายในการบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ กับการคุ้มครองสิทธิและเสรีภาพตามรัฐธรรมนูญ

Legal Problems in Enforcing the Cybersecurity Act with the Protection of Rights and Freedoms According to the Constitution

Received: 23 February 2024
Revised: 16 March 2024
Accepted: 18 March 2024

จักรพงศ์ ลิ้มสุวรรณ[1*] และณิชาพรรณ ป้องขวาเลา[2]
Chakrapong Limsuwan[1*] and Nichapan Pongkhualao[2]
[1*,2]อาจารย์ คณะนิติศาสตร์ มหาวิทยาลัยราชภัฏมหาสารคาม
[1*,2]Lecturer from the Faculty of Law Rajabhat Maha sarakham University
*Corresponding Author Email: chakrapong.li@ rmu.ac.th

บทคัดย่อ

บทความวิชาการนี้ มีวัตถุประสงค์เพื่อนำเสนอปัญหาทางกฎหมายจากการบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จากการศึกษาเอกสารทางวิชาการที่เกี่ยวข้อง ได้แก่ หนังสือ ตำรา งานวิจัย บทความวิชาการ และการวิเคราะห์เปรียบเทียบกับกฎหมายต่างประเทศ พบว่า 1) กฎหมายฉบับดังกล่าวมีวัตถุประสงค์ในการป้องกัน ระงับ ยับยั้ง ภัยความมั่นคงทางไซเบอร์อันอาจก่อให้เกิดผลกระทบกับสารสนเทศพื้นฐานสำคัญของรัฐ หรือความมั่นคงของรัฐ หรือความสงบเรียบร้อยของสังคม ซึ่งเป็นกฎหมายที่มีความจำเป็นแต่ในขณะเดียวกันก็มีลักษณะเป็นกฎหมายที่มุ่งควบคุมและปราบปรามอาชญากรรมเป็นสำคัญ จนอาจมีบางกรณีที่อาจนำไปสู่การละเมิดต่อสิทธิและเสรีภาพของประชาชนจนเกินสมควรได้ 2) เมื่อเกิดภัยความมั่นคงทางไซเบอร์ในระดับวิกฤติพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้จะมีอำนาจเด็ดขาดในการกำหนดมาตรการที่เห็นว่าจำเป็นเพื่อดำเนินการให้บรรลุวัตถุประสงค์ของกฎหมาย โดยไม่จำเป็นต้องมีคำสั่งศาลก่อนการใช้อำนาจ นอกจากนี้ ผู้ที่ต้องอยู่ใต้บังคับของคำสั่งของคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติยังไม่อาจอุทธรณ์คำสั่งดังกล่าวได้อีกด้วย 3) เมื่อเกิดภัยความมั่นคงทางไซเบอร์ในระดับร้ายแรง แม้ว่ากฎหมายจะกำหนดให้พนักงานเจ้าหน้าที่จะต้องได้รับคำสั่งจากศาลก่อนการใช้อำนาจตามมาตรา 66 แต่ผู้ที่ต้องอยู่ใต้บังคับของคำสั่งของคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติก็ไม่อาจอุทธรณ์คำสั่งได้ และ 4) บทบัญญัติมาตรา 68 ที่ให้อำนาจเด็ดขาดแก่พนักงานเจ้าหน้าที่ และการห้ามมิให้อุทธรณ์ ตามมาตรา 69 เป็นบทบัญญัติที่ขัดต่อรัฐธรรมนูญ มาตรา 26 เนื่องจาก ขัดต่อหลักความได้สัดส่วนอันเป็นองค์ประกอบหนึ่งของหลักนิติรัฐ (นิติธรรม)

คำสำคัญ: กฎหมายไซเบอร์, สิทธิและเสรีภาพ, ความมั่นคงไซเบอร์

Abstract

This academic article aims to present legal issues arising from the enforcement of the Cyber Security Act B.E. 2562 by studying relevant academic documents, including books, textbooks, research papers, academic articles, and comparative analyses with foreign laws. It was found that: 1) The aforementioned law aims to prevent, suppress, and mitigate cyber threats that may impact critical information infrastructure or the security, peace, and order of society. While necessary, it also has characteristics of controlling and combating crimes, which may sometimes lead to violations of people's rights and freedoms beyond reasonable limits. 2) In a cyber crisis situation, officials under this Act have decisive power to implement necessary measures to achieve

the law's objectives without the need for court orders. Furthermore, those subject to the authority of the National Cyber Security Committee's orders cannot appeal these orders. 3) Even though the law requires officials to obtain court orders before exercising power under Article 66, individuals subject to the National Cyber Security Committee's orders cannot appeal them, particularly in severe cyber threat situations. And 4) Provisions like Article 68, granting officials decisive power and prohibiting appeal orders according to Article 69, is contrary to the constitution of Article 26, as they violate the principle of proportionality, which is one of the components of the rule of law.

Keywords: Cyber Law, Rights and Freedoms, Cyber Security

บทนำ

การรักษาเอกราช ความมั่นคง และความสงบภายในชาติเป็นภารกิจอันสำคัญยิ่งประการหนึ่งของรัฐบาล แต่ละรัฐซึ่งในอดีตแนวคิดเกี่ยวกับความมั่นคงของรัฐมักเกิดขึ้นจากแนวคิดทางการเมืองและสังคมวิทยา สอดคล้องกับแนวคิดของโธมัส ฮ็อบส์ (Thomas Hobbes) (เกรียงไกร เจริญธนาวัฒน์, 2564, น.79-82) ที่มองว่ารัฐจำเป็นจะต้องเป็นผู้ผูกขาดอำนาจในการปกครองและการใช้กำลัง เนื่องจากมนุษย์มีความจำเป็นจะต้องหลีกหนีจากสภาวะตามธรรมชาติซึ่งต่างก็พยายามทุกวิถีทางเพื่อให้ได้มาซึ่งสิ่งที่ตนปรารถนา สภาวะเช่นนี้จึงนำไปสู่ความไม่เป็นระเบียบในสังคมและนำไปสู่สงครามในที่สุด ประชาชนทั้งหลายจึงยินยอมพร้อมใจกันมอบอำนาจที่ตนมีอยู่ให้แก่ผู้ปกครองในลักษณะที่เป็นสัญญาสวามิภักดิ์ รัฐจึงเป็นผู้มีอำนาจสูงสุดเด็ดขาดเหนือทุก ๆ คนในประชาคม ปัญหาด้านความมั่นคงในอดีตจึงผูกติดอยู่กับความมั่นคงและการดำรงอยู่ของรัฐ กล่าวคือ ความมั่นคงในอธิปไตยเหนือดินแดน การคงอยู่ของระบอบการปกครอง หรือความเชื่อทางการเมือง

ปัจจุบันมุมมองด้านความมั่นคงของรัฐสมัยใหม่ได้เปลี่ยนจากเดิมซึ่งผูกติดกับการคงอยู่ของรัฐเป็นสำคัญ ไปสู่การให้ความสำคัญกับความมั่นคงอันมีมนุษย์เป็นวัตถุประสงค์แห่งการคุ้มครอง นับตั้งแต่ปี ค.ศ. 2000 เป็นต้นมา องค์การสหประชาชาติให้ความสำคัญกับการพัฒนาความมั่นคงของมนุษย์ (Human Security) มากขึ้นเรื่อย ๆ โดยมุมมองเรื่องความมั่นคงของมนุษย์จะตั้งอยู่บนพื้นฐานของภัยคุกคามที่มีผลกระทบต่อมนุษย์ เช่น ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางอาหาร ความมั่นคงทางสุขภาพ ความมั่นคงทางสิ่งแวดล้อม ความมั่นคงส่วนบุคคล ความมั่นคงของชุมชน และความมั่นคงทางการเมือง (United Nations Development Program, 2022, p.3-7) เป็นต้น ดังนั้น เมื่อภัยคุกคามความมั่นคงของมนุษย์ดังกล่าวข้างต้นล้วนแต่สามารถเกิดขึ้นได้โดยอาศัยการโจมตีทางไซเบอร์ เช่น การเจาะระบบคอมพิวเตอร์ของรัฐเพื่อขโมยข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของรัฐเพื่อนำไปหลอกลวงหรือก่ออาชญากรรมกับประชาชนทั่วไปได้ ปัจจุบันพันธกิจด้านความมั่นคงของรัฐในปัจจุบันจึงขยายขอบเขตออกไปจากกรอบความคิดเกี่ยวกับความมั่นคงแบบดั้งเดิมมาก

อาชญากรรมทางไซเบอร์เป็นการก่ออาชญากรรมรูปแบบใหม่ในยุคปัจจุบันซึ่งรัฐจะต้องปรับตัวให้ทันต่อความเปลี่ยนแปลงของก่ออาชญากรรมทั้งในแง่ของรูปแบบในการกระทำความผิด และพื้นที่ซึ่งเกิดการกระทำ กล่าวคือ นอกจากองค์ประกอบความผิดที่มีการเปลี่ยนแปลงไปมากจนกฎหมายในรูปแบบเดิมที่เคยมีไม่อาจนำมาตีความและบังคับใช้ได้อีกต่อไปแล้ว ยังมีความแตกต่างทั้งในเรื่องของพื้นที่ซึ่งเกิดการกระทำความผิดได้อย่างไร้พรมแดน หรือระบุตัวตนผู้กระทำความผิดได้ยากหรือถึงขั้นไม่อาจระบุตัวตนได้เลย อีกทั้งเครื่องมือที่ใช้ในการกระทำความผิดก็มีความเปลี่ยนแปลงไปมากด้วยเช่นกัน (สาวตรี สุขศรี , 2563, น.73) โดยการก่ออาชญากรรมทางไซเบอร์อาจเกิดขึ้นในรูปแบบของการเจาะระบบคอมพิวเตอร์ให้เกิดความเสียหาย ขัดข้องจนไม่สามารถทำงานได้ หรือการโจรกรรมข้อมูลหรือทำลายข้อมูลคอมพิวเตอร์ ซึ่งอาจมีเป้าหมายการโจมตีตั้งแต่ระดับปัจเจกบุคคลหรือองค์กร หรืออาจกระทบต่อความมั่นคงของรัฐหรือความปลอดภัยสาธารณะได้ เช่น เมื่อปี ค.ศ. 2010 ได้เกิดการโจมตีโรงไฟฟ้า

นิวเคลียร์ของประเทศอิหร่านด้วยหนอนไวรัส ชื่อว่า สตั๊กเน็ต (Stuxnet) โดยการโจมตีครั้งดังกล่าวก่อให้เกิดความผิดปกติของอุปกรณ์ที่สำคัญภายในโรงไฟฟ้านิวเคลียร์ส่งผลให้ความสามารถในการผลิตไฟฟ้าน้อยลงจนถึงไม่สามารถผลิตไฟฟ้าได้เลย (Marie Baezner, Patrice Robin, 2017) แม้ว่าการโจมตีครั้งดังกล่าวจะยังไม่เกิดความเสียหายต่อชีวิตและทรัพย์สินที่มีมูลค่ามหาศาล เนื่องจากสามารถยับยั้งการทำงานของหนอนไวรัสดังกล่าวได้ทันเวลา อย่างไรก็ตามการโจมตีครั้งดังกล่าวถือว่าเป็นการโจมตีทางไซเบอร์ที่ส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญของรัฐครั้งใหญ่ที่รู้จักกันอย่างกว้างขวางเป็นครั้งแรกของโลก (Josh Fruhlinger, 2022)

ผลกระทบจากการโจมตีทางไซเบอร์ข้างต้นที่สามารถส่งผลกระทบต่อทั้งประชาชนทั่วไปหรือต่อความสงบเรียบร้อยของสังคม ตลอดจนความมั่นคงของรัฐ ปัจจุบันปัญหาการโจมตีทางไซเบอร์จึงถูกจัดว่าเป็นภัยคุกคามที่กระทบต่อความมั่นคงของรัฐ รัฐทั้งหลายจึงต้องปรับตัวให้ทันต่อภัยความมั่นคงรูปแบบใหม่ที่เปลี่ยนแปลงไปจากอดีตมาก โดยสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ได้กำหนดตัวชี้วัดความพร้อมต่อการป้องกันภัยทางไซเบอร์เอาไว้ 5 ด้าน ได้แก่ ความพร้อมทางกฎหมาย ความพร้อมทางเทคนิค ความพร้อมในด้านนโยบายและการบริหารจัดการ ความพร้อมด้านศักยภาพในการพัฒนา และความพร้อมในด้านความร่วมมือระหว่างประเทศหรือองค์กรอื่นทั้งภายในและต่างประเทศ จากการศึกษาตัวชี้วัดของ ITU ข้างต้นประเทศไทยจัดอยู่ในอันดับที่ 44 จาก 194 ประเทศทั่วโลก โดยหากพิจารณาถึงความพร้อมทางด้านกฎหมายแล้วประเทศไทยจัดอยู่ในกลุ่มประเทศที่มีความพร้อมด้านกฎหมายในระดับที่สูงมาก (19.11 จาก 20 คะแนน) โดยมีจุดที่ต้องพัฒนาคือความสามารถทางเทคนิค (15.57 จาก 20 คะแนน) และศักยภาพในการพัฒนา (16.94 จาก 20 คะแนน) (International Telecommunication Union: ITU, 2020)

หากพิจารณาจากข้อมูลข้างต้นจะเห็นได้ว่าประเทศไทยจัดเป็นประเทศที่มีความพร้อมด้านกฎหมายในระดับสูงมาก กล่าวคือมีกฎหมายที่จัดตั้งหน่วยงานรัฐให้มีหน้าที่และอำนาจเฉพาะเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ นอกจากนี้ยังมีกฎหมายที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์สำหรับป้องกันและควบคุมการใช้เทคโนโลยีเพื่อกระทำความผิดทั้งในระดับหน่วยงานของรัฐและประชาชนทั่วไปด้วย โดยหากใช้วัตถุประสงค์ในการคุ้มครองของกฎหมายเป็นเกณฑ์ในการพิจารณา จะสามารถแบ่งออกเป็น 2 ลักษณะใหญ่ ๆ ได้แก่ การคุ้มครองความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และการคุ้มครองหรือควบคุมตรวจสอบความเหมาะสมของข้อมูลคอมพิวเตอร์ โดยในปัจจุบันมีกฎหมายที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ที่สำคัญอยู่ 3 ฉบับ ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ฉบับที่ 2 พ.ศ. 2560) และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

อนึ่ง แม้ประเทศไทยจะมีความพร้อมด้านกฎหมายในระดับที่สูงมากจากข้อพิจารณาข้างต้น แต่หากวิเคราะห์ต่อไปถึงขอบเขตในการศึกษาจะพบว่าความพร้อมดังกล่าวเป็นความพร้อมในเชิงรูปแบบเท่านั้น กล่าวคือ งานวิจัยดังกล่าวเป็นเพียงการสำรวจถึงความพร้อมทางกฎหมายในลักษณะที่ว่ามีหรือไม่มีกฎหมายที่เกี่ยวข้องตามตัวชี้วัดที่กำหนด แต่ไม่ได้ศึกษาถึงประสิทธิภาพของกฎหมายที่มีต่อการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ ตลอดจนไม่ได้มีการศึกษาเกี่ยวกับผลกระทบต่อสิทธิและเสรีภาพของประชาชนที่อาจเกิดจากการบังคับใช้กฎหมายดังกล่าวแต่อย่างใด

บทความฉบับนี้จึงจะได้ศึกษาถึงปัญหาและผลกระทบที่เกิดขึ้นจากการบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เปรียบเทียบกับกฎหมายต่างประเทศ และหลักประกันสิทธิและเสรีภาพตามรัฐธรรมนูญ ทั้งนี้ เพื่อเสนอแนะแนวทางการแก้ไขเพิ่มเติมกฎหมายให้ได้ดุลยภาพระหว่างการรักษาความมั่นคงทางไซเบอร์กับสิทธิและเสรีภาพของประชาชนให้เหมาะสมต่อไป

บทวิเคราะห์

ปัจจุบันนานาอารยประเทศโดยเฉพาะประเทศที่ปกครองในระบอบประชาธิปไตย เช่นในทวีปยุโรปหรือสหรัฐอเมริกา ไม่มีกฎหมายที่มีลักษณะคล้ายคลึงกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กล่าวคือ เป็นกฎหมายที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์เป็นการเฉพาะในฉบับเดียว โดยสหรัฐอเมริกาได้ตรารัฐบัญญัติชื่อว่า Strengthening American Cybersecurity Act of 2022 แต่ก็เป็นเพียงกฎหมายที่มีลักษณะเป็นการกำหนดการดำเนินการระหว่างหน่วยงานของรัฐเป็นสำคัญ โดยกฎหมายฉบับดังกล่าวเป็นการรวมกันของกฎหมาย 3 ฉบับ ได้แก่ (1) Federal Information Security Modernization Actซึ่งเกี่ยวกับการปรับปรุงความปลอดภัยข้อมูลระดับสหพันธรัฐ (2) Cyber Incident Reporting Act ซึ่งเกี่ยวกับการรายงานเหตุการณ์ทางไซเบอร์ และ (3) Federal Secure Cloud Improvement and Jobs Act ซึ่งเกี่ยวกับการปรับปรุงมาตรฐานระบบคราวด์ระดับสหพันธรัฐ นอกจากนี้ ยังมีการดำเนินการภายใต้กฎหมายอีกหลายฉบับซึ่งจะเป็นการกำหนดมาตรฐานความปลอดภัยและหน้าที่ของรัฐเป็นสำคัญ เช่น Health Insurance Portability and Accountability Act (HIPAA) ซึ่งเป็นกฎหมายกำหนดมาตรฐานความปลอดภัยเพื่อการคุ้มครองข้อมูลด้านสุขภาพของผู้ป่วย หรืออยู่ในรูปของกรอบในการปฏิบัติด้านความปลอดภัยทางไซเบอร์ โดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology: NIST) ซึ่งก็เป็นเพียงการกำหนดมาตรฐานด้านความปลอดภัยทางเทคโนโลยีเพื่อให้หน่วยงานของรัฐและเอกชนนำไปเป็นแนวปฏิบัติเพื่อป้องกันและลดความเสี่ยงในการโจมตีทางไซเบอร์ เป็นต้น ส่วนกรณีของสหราชอาณาจักร ปัจจุบันมีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (The Data Protection Act 2018) ซึ่งเป็นกฎหมายที่มุ่งคุ้มครองข้อมูลส่วนบุคคลของประชาชน และยังมีการกำหนดกรอบกรอบในการปฏิบัติด้านความปลอดภัยทางไซเบอร์ซึ่งมีลักษณะคล้ายคลึงกับของสหรัฐอเมริกา (Michael Brands, 2023) จะเห็นได้ว่ากลุ่มประเทศดังกล่าวข้างต้นมิได้มีกฎหมายเฉพาะในลักษณะที่ใช้กฎหมายเพียงฉบับเดียว เพื่อกำหนดหน้าที่และอำนาจแก่หน่วยงานและเจ้าหน้าที่ของรัฐให้ดำเนินการเกี่ยวกับปัญหาทางไซเบอร์ครอบคลุมในทุกกรณี

ผู้เขียนจึงได้ทำการศึกษาบทบัญญัติของกฎหมายที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อวิเคราะห์เปรียบเทียบกับรัฐบัญญัติความมั่นคงไซเบอร์ (Security Act 2018) ของสาธารณรัฐสิงคโปร์ ซึ่งเป็นกฎหมายที่มีอิทธิพลต่อการยกร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย และมีสาระสำคัญที่คล้ายคลึงกันหลายประการ แล้วนำมาวิเคราะห์เปรียบเทียบกับหลักการจำกัดสิทธิและเสรีภาพโดยชอบธรรมตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 เพื่อเสนอแนะแนวทางในการสร้างดุลยภาพระหว่างประโยชน์สาธารณะ กล่าวคือ ความมั่นคงปลอดภัยทางไซเบอร์ กับสิทธิและเสรีภาพบางประการที่รัฐธรรมนูญให้การคุ้มครอง โดยแบ่งการวิเคราะห์ออกเป็น 3 ส่วน ดังนี้

1. อำนาจของพนักงานเจ้าหน้าที่ซึ่งมีลักษณะที่เป็นกระทบกระเทือนต่อสิทธิและเสรีภาพของประชาชน

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ได้กำหนดกลไกในการป้องกัน ระงับ ยับยั้ง ความเสียหายที่อาจเกิดขึ้นจากการโจมตีทางไซเบอร์ ซึ่งมีความคล้ายคลึงกันในเชิงรูปแบบกับรัฐบัญญัติบัญญัติความมั่นคงไซเบอร์ของสาธารณรัฐสิงคโปร์ โดยได้แบ่งความรุนแรงของภัยคุกคามทางไซเบอร์เป็น 3 ระดับ เช่นเดียวกับสาธารณรัฐสิงคโปร์ ได้แก่ ภัยคุกคามระดับไม่ร้ายแรง ภัยคุกคามระดับร้ายแรง และภัยคุกคามระดับวิกฤติ ซึ่งในแต่ละระดับนั้นจะมีขอบเขตของหน้าที่และอำนาจของพนักงานเจ้าหน้าที่ที่แตกต่างกันออกไป กล่าวคือ ยิ่งสถานการณ์มีความรุนแรงและเร่งด่วนมากเพียงใด ขอบเขตของหน้าที่และอำนาจของเจ้าพนักงานยิ่งกว้างขวางและมีขั้นตอนที่น้อยลงเพื่อทันต่อสถานการณ์มากขึ้นด้วย โดยเฉพาะภัยคุกคามในระดับร้ายแรงและระดับวิกฤติซึ่งอาจส่งผลกระทบต่อความมั่นคงทางเทคโนโลยีสารสนเทศ หรือความมั่นคงของรัฐ หรือความสงบสุขของสังคมในวงกว้างได้ เช่น ในกรณีที่เกิดภัยคุกคามในระดับวิกฤติ สภาความมั่นคงแห่งชาติสามารถให้มอบหมายให้เลขาธิการมีอำนาจดำเนินการใด ๆ ก็ได้เท่าที่เห็นว่าจำเป็น เพื่อป้องกันและเยียวยาความเสียหาย โดยไม่จำต้องมีคำสั่งศาลก่อน ตามมาตรา 68 ส่วนในกรณีการเกิดภัย

คุกคามในระดับร้ายแรง พนักงานเจ้าหน้าที่อาจเข้าตรวจสอบสถานที่ เข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ยึดหรืออายัดคอมพิวเตอร์และอุปกรณ์ใด ๆ ที่เกี่ยวข้องได้เท่าที่จำเป็น โดยจะต้องมีคำสั่งศาลก่อน ตามมาตรา 66 เป็นต้น กรณีดังกล่าวจึงถือเป็นบทบัญญัติแห่งกฎหมายที่ให้อำนาจแก่พนักงานเจ้าหน้าที่ให้สามารถปฏิบัติการที่จำเป็นได้แม้จะกระทบกระเทือนต่อสิทธิและเสรีภาพของประชาชนซึ่งรัฐธรรมนูญให้การคุ้มครองหลายประการ เช่น การเข้าไปในเคหะสถานเพื่อตรวจค้น เข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ กับเสรีภาพในเคหสถานที่รัฐธรรมนูญรับรอง ตามมาตรา 33 การสกัดหรือคัดกรองข้อมูลคอมพิวเตอร์ กับเสรีภาพในการสื่อสารที่รัฐธรรมนูญรับรอง ตามมาตรา 36 เป็นต้น

2. การควบคุมตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่

การตรวจสอบการใช้อำนาจรัฐโดยองค์กรตุลาการนั้นเป็นหลักการพื้นฐานสำคัญประการหนึ่งของหลักนิติรัฐ เนื่องจากศาลเป็นองค์กรผู้ใช้อำนาจอธิปไตยที่มีหลักประกันความเป็นอิสระ (บรรเจิด สิงคะเนติ, 2555, น.293) สูงที่สุดในบรรดาองค์กรผู้ใช้อำนาจอธิปไตยด้วยกันเอง เพื่อควบคุมตรวจสอบการใช้อำนาจของรัฐว่ามีการละเมิดสิทธิหรือเสรีภาพของประชาชนเกินสมควรหรือไม่ ในการวิเคราะห์เกี่ยวกับการควบคุมตรวจสอบโดยองค์กรตุลาการนี้ผู้เขียนได้แบ่งการวิเคราะห์ออกเป็น 2 กรณี ดังนี้

2.1 การตรวจสอบกรณีภัยคุกคามทางไซเบอร์ระดับร้ายแรง

ในการตรวจสอบการใช้อำนาจและดุลพินิจของพนักงานเจ้าหน้าที่สำหรับกรณีที่มีภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กฎหมายได้กำหนดให้องค์กรตุลาการทำหน้าที่ตรวจสอบการใช้ดุลพินิจของพนักงานเจ้าหน้าที่ในการใช้อำนาจตามมาตรา 66 (2) – (4) โดยกำหนดให้คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์จะต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจ เพื่อให้ศาลสั่งให้พนักงานเจ้าหน้าที่สามารถดำเนินการได้ตามคำร้อง นอกจากนี้ ในการพิจารณาอนุญาตของศาลจะต้องพิจารณาถึงเหตุอันควรเชื่อได้ว่ามีบุคคลใด บุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับ ร้ายแรงขึ้น ศาลจึงจะพิจารณามีคำสั่งอนุญาตได้ กลไกดังกล่าวจึงถือได้ว่ามีกระบวนการคุ้มครองสิทธิและเสรีภาพในเบื้องต้นแล้ว

เมื่อพิจารณาต่อไปถึงบทบัญญัติมาตรา 69 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งบัญญัติไว้ว่า “ผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่งได้เฉพาะที่เป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงเท่านั้น” หรืออาจกล่าวได้อีกนัยว่าในกรณีที่เกิดภัยคุกคามทั้งในระดับร้ายแรง และระดับวิกฤติ ผู้ได้รับคำสั่งอันเกี่ยวกับมาตรการจำเป็นเพื่อรับมือภัยคุกคามระดับร้ายแรงหรือระดับวิกฤติแล้วแต่กรณี ต้องห้ามมิให้อุทธรณ์คำสั่งนั้น คงมีเพียงกรณีภัยคุกคามระดับไม่ร้ายแรงเท่านั้นที่สามารถอุทธรณ์ได้ จึงเป็นกรณีที่กฎหมายไม่เปิดโอกาสแก่ผู้ที่ต้องตกอยู่ภายใต้คำสั่งดังกล่าว ให้สามารถใช้สิทธิโต้แย้งถึงเหตุอันควรเชื่อซึ่งพนักงานเจ้าหน้าที่ได้ยกขึ้นอ้างต่อศาลได้ จึงอาจนำมาซึ่งการกระทำกระเทือนต่อสิทธิและเสรีภาพหลายประการของผู้ได้รับคำสั่งอันเกี่ยวกับมาตรการจำเป็นเพื่อรับมือภัยคุกคามดังที่ได้วิเคราะห์ไปแล้วในข้อ 1

นอกจากนี้ มาตรการดังกล่าวข้างต้นไม่ได้เป็นมาตรการที่ใช้กับเฉพาะผู้กระทำความผิดเท่านั้น แต่ยังครอบคลุมไปถึงบุคคลบริษัทผู้ให้บริการอินเทอร์เน็ต หรือบริการคราวน์เซิร์ฟเวอร์ (Server) หรือระบบคอมพิวเตอร์ที่อาจเพียงถูกใช้เป็นเครื่องมือในการกระทำความผิด หรือเป็นเพียงทางผ่านในการนำไปสู่การกระทำความผิดด้วย โดยหากกรณีผู้ได้รับคำสั่งตามมาตรา 66 เป็นผู้ให้บริการซึ่งมีผู้ใช้งานเป็นจำนวนมากหากถูกยึดหรืออายัดอุปกรณ์เป็นเวลา 30 วัน ย่อมส่งผลกระทบต่อทั้งผู้ให้บริการในเรื่องของรายได้หรือความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์ซึ่งอาจมีการใช้เทคโนโลยีเฉพาะในการดูแล รวมไปถึงความลับทางการค้าบางประการด้วย นอกจากนี้ยังส่งผลกระทบในทางอ้อมต่อผู้ใช้บริการเป็นจำนวนมาก และปัญหาต่อการขับเคลื่อนเศรษฐกิจที่จะตามมา เป็นต้น ดังนั้น หากพนักงานเจ้าหน้าที่ตามกฎหมายใช้อำนาจดุลพินิจโดยปราศจากความรอบคอบ ไม่พิจารณาถึงผลกระทบที่อาจเกิดขึ้นจากกมาตรการที่กำหนดขึ้นอย่างถี่ถ้วน แม้จะสามารถป้องกันหรือยับยั้งภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้

แต่หากการดำเนินตามมาตรการที่กำหนดขึ้นนั้นก่อให้เกิดผลกระทบต่อประโยชน์สาธารณะด้านอื่น ๆ อย่างกว้างขวาง ย่อมนำมาซึ่งปัญหาการละเมิดสิทธิและเสรีภาพ ปัญหาทางเศรษฐกิจ หรือข้อพิพาทในสังคมตามมาได้

ส่วนกรณีเกิดภัยคุกคามระดับร้ายแรงในสาธารณรัฐสิงคโปร์ รัฐบัญญัติความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์ มาตรา 20 (1) และ (2) วางหลักไว้ว่า กรรมาธิการจะมีอำนาจดำเนินการในลักษณะคล้ายคลึงกับมาตรา 66 (2) – (4) ของไทย โดยไม่จำเป็นต้องขออนุญาตจากศาลก่อน ส่วนในสหรัฐอเมริกาแม้จะไม่ได้มีการกำหนดระดับความรุนแรงของภัยคุกคามทางไซเบอร์เหมือนในไทยและสาธารณรัฐสิงคโปร์ แต่ในการใช้อำนาจของรัฐนั้นก็จะเป็นไปตามหลักศุภนิติกระบวน (Due Process of Law) กล่าวคือ แม้การดำเนินการของพนักงานเจ้าหน้าที่ของรัฐจะเป็นการดำเนินการโดยอาศัยอำนาจตามกฎหมาย แต่หากเป็นกรณีที่มีผลเป็นการจำกัดสิทธิและเสรีภาพของประชาชนและมีบทลงโทษทางอาญา ก็จำเป็นจะต้องได้รับการตรวจสอบจากองค์กรตุลาการอีกชั้นหนึ่งด้วย เช่น ตามมาตรา 2244 ของ Strengthening American Cybersecurity Act of 2022 วางหลักไว้ว่า เมื่อพนักงานเจ้าหน้าที่ของรัฐได้รับรายงานเกี่ยวกับเหตุการณ์ทางไซเบอร์ (การโจมตีโดย Ransomware) เมื่อได้ร้องขอข้อมูลหรือความร่วมมือจากหน่วยงานที่ถูกโจมตีดังกล่าวแล้วแต่ได้รับการปฏิเสธหรือเพิกเฉย ก็สามารถขอคำสั่งจากศาลเพื่อบังคับให้เปิดเผยข้อมูลหรือให้ความร่วมมือได้ ทั้งนี้ จะต้องพิจารณาถึงผลกระทบต่อความมั่นคงของชาติ ความมั่นคงทางเศรษฐกิจ หรือสุขภาพและความปลอดภัยของประชาชนด้วย

2.2 การตรวจสอบกรณีภัยคุกคามทางไซเบอร์ระดับวิกฤติ

สำหรับกรณีการใช้อำนาจของพนักงานเจ้าหน้าที่ในกรณีเกิดภัยคุกคามทางไซเบอร์ระดับวิกฤตินั้น เป็นอำนาจเด็ดขาดในการใช้ดุลพินิจของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) คล้ายคลึงกับมาตรา 23 ของรัฐบัญญัติความมั่นคงปลอดภัยไซเบอร์ของสาธารณรัฐสิงคโปร์ โดยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ของไทยบัญญัติไว้ใน มาตรา 68 ว่า “ในกรณีที่เป็นเหตุจำเป็นเร่งด่วน และเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ คณะกรรมการอาจมอบหมายให้เลขาธิการมีอำนาจดำเนินการได้ทันทีเท่าที่จำเป็นเพื่อป้องกันและเยียวยา ความเสียหายก่อนล่วงหน้าได้โดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากการดำเนินการดังกล่าว ให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว”

จากถ้อยคำในบทบัญญัติดังกล่าวจะเห็นได้ว่า เมื่อเกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติขึ้น กมช. จะมีอำนาจดุลพินิจในการกำหนดมาตรการในการดำเนินการทั้งปวงตามที่เห็นว่าจำเป็นและเหมาะสม จึงเป็นบทบัญญัติที่ให้อำนาจในการใช้ดุลพินิจแก่ กมช. อย่างกว้างขวางมาก ทั้งยังเป็นอำนาจที่ไม่อาจยับยั้งในระหว่างการดำเนินการได้อีกด้วย เนื่องจาก แม้กฎหมายจะกำหนดให้องค์กรตุลาการเข้ามาเกี่ยวข้องกับการใช้อำนาจของ กมช. แต่ก็เป็นเพียงการแจ้งต่อศาลเพื่อทราบภายหลังจากการดำเนินการเสร็จสิ้นแล้วเท่านั้น ไม่ได้มีผลในต่อการตรวจสอบหรือเยียวยาผลกระทบจากการใช้อำนาจตามมาตรา 68 แต่อย่างใด การใช้อำนาจของ กมช. ในกรณีนี้จึงเป็นการใช้อำนาจในลักษณะที่เด็ดขาดที่ไม่อาจตรวจสอบได้เลย

นอกจากนี้ เมื่อพิจารณาประกอบกับบทบัญญัติมาตรา 69 ซึ่งห้ามมิผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อุทธรณ์คำสั่งของ กมช. ดังนั้น เมื่อเกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติขึ้นการใช้อำนาจของ กมช. ย่อมไม่อาจถูกตรวจสอบได้เลย ทั้งก่อนการดำเนินการและในระหว่างการดำเนินการ กรณีดังกล่าวจึงถือเป็นการตัดอำนาจตรวจสอบการใช้อำนาจรัฐโดยองค์กรตุลาการ อันเป็นหลักประกันด้านสิทธิพื้นฐานในกระบวนการยุติธรรม จึงอาจนำมาซึ่งการใช้อำนาจโดยมิชอบของพนักงานเจ้าหน้าที่ของรัฐ เช่น การบุกรุกเข้าไปในเคหสถาน การยึดอุปกรณ์คอมพิวเตอร์ การเจาะระบบ หรือเซิร์ฟเวอร์ของผู้ให้บริการ อันเป็นการละเมิดต่อสิทธิและเสรีภาพของประชาชนเกินสมควรได้

อนึ่ง เมื่อพิจารณาต่อไปถึงนิยามของภัยคุกคามทางไซเบอร์ระดับวิกฤติที่กำหนดไว้ในมาตรา 60 (3) ซึ่งแบ่งออกเป็น 2 ลักษณะ ได้แก่ (ก) เป็นภัยคุกคามที่ส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง

จนการทำงานล้มเหลวทั้งระบบและรัฐไม่สามารถควบคุมได้ ซึ่งมีความมุ่งหมายในการคุ้มครองการโจมตีที่อาจมีผลกระทบต่อการความปลอดภัยในลักษณะที่เป็นโครงสร้างพื้นฐานทางสารสนเทศอย่างแท้จริง และ (ข) เป็นภัยคุกคามอันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรือส่วนหนึ่งส่วนใดของประเทศตกอยู่ในภาวะคับขัน ... ผู้เขียนมีความเห็นว่า การบัญญัติคำว่า “อาจกระทบต่อความสงบเรียบร้อย หรือภัยต่อความมั่นคงของรัฐ” เป็นการใช้ถ้อยคำที่ก่อให้เกิดปัญหาในทางปฏิบัติเกี่ยวกับการตีความและบังคับใช้ในระบบกฎหมายของไทยมาโดยตลอด แม้ผู้เขียนจะเห็นพ้องกับคำวินิจฉัยศาลรัฐธรรมนูญซึ่งได้วางบรรทัดฐานไว้ในคำวินิจฉัยเกี่ยวกับถ้อยคำที่เกี่ยวข้องกับความมั่นคงตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ฉบับที่ 2 พ.ศ. 2560) มาตรา 14 ว่าการบัญญัติกฎหมายจะต้องมีความชัดเจนเพียงพอ และจะต้องไม่มุ่งเจาะจงเพียงกรณีใดกรณีหนึ่ง เพื่อให้ผู้บังคับใช้กฎหมายสามารถใช้ดุลพินิจนำไปปรับใช้แก่ข้อเท็จจริงเป็นเรื่อง ๆ ไปได้อย่างเหมาะสม (คำวินิจฉัยศาลรัฐธรรมนูญ ที่ 20/2566, 2566) ก็ตาม แต่ปัญหาทางกฎหมายดังกล่าวไม่ได้มีสาเหตุมาจากถ้อยคำของบทบัญญัติโดยลำพัง หากแต่เกิดจากการตีความหรือบังคับใช้กฎหมายเกี่ยวกับความสงบเรียบร้อยและความมั่นคงของรัฐในระบบกฎหมายของประเทศไทย มักขึ้นอยู่กับทัศนคติของผู้มีอำนาจบังคับใช้และตีความกฎหมายที่มีต่อแนวคิดเกี่ยวกับความมั่นคง ความสงบเรียบร้อย กับสิทธิและเสรีภาพ ซึ่งมีความไม่แน่นอน

การที่กฎหมายนิยามคำว่า “ภัยคุกคามทางไซเบอร์ ว่าหมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้าย ต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือ ข้อมูลอื่นที่เกี่ยวข้อง” เป็นการใช้ถ้อยคำที่มีขอบเขตที่ครอบคลุมการกระทำและผลของการกระทำที่กว้างขวางมาก เมื่อประกอบกับการนิยามคำว่าภัยคุกคามทางไซเบอร์ระดับวิกฤติ ตามมาตรา 60 (3) (ข) ในถ้อยคำว่าอาจกระทบต่อความสงบเรียบร้อย หรือภัยต่อความมั่นคงของรัฐ จากกรณีดังกล่าวข้างต้นจึงอาจก่อให้เกิดปัญหาการใช้ดุลพินิจเกินขอบเขต เพื่อควบคุมตรวจสอบเนื้อหาบางประการที่อาจเป็นเพียงกรณีที่ผู้กระทำความผิดใช้วิธีการทางเทคโนโลยีกระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญ แต่มิได้มีผลกระทบหรือน่าจะเกิดผลกระทบต่อความมั่นคงทางไซเบอร์อย่างแท้จริง เช่น การโจมตีโดยโทรจัน (Trojan) เพื่อทำการเปิดช่องโหว่ในเว็บไซต์ของหน่วยงานที่ถือว่าเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แล้วทำการการเผยแพร่ข้อมูลบางอย่างต่อลงไปบนเว็บไซต์หน่วยงานทั้งหลาย ซึ่งหากผู้มีอำนาจเห็นว่าข้อมูลดังกล่าวเป็นข้อมูลที่กระทบต่อความสงบเรียบร้อย กรณีดังกล่าวข้างต้นอาจถูกตีความว่าเป็นภัยคุกคามทางไซเบอร์ระดับวิกฤติตามมาตรา 60 (3) (ข) เพื่อใช้อำนาจตามมาตรา 68 ซึ่งไม่อาจตรวจสอบได้และอาจนำไปสู่การละเมิดต่อสิทธิและเสรีภาพของประชาชนดังที่ได้กล่าวมาแล้ว และยังเป็นการตีความบังคับใช้กฎหมายในลักษณะที่เป็นการมุ่งควบคุมตรวจสอบเนื้อหาที่ผู้มีอำนาจเห็นว่าไม่เหมาะสม แทนการมุ่งควบคุมและป้องกันการกระทำอันก่อให้เกิดผลกระทบต่อโครงสร้างพื้นฐานของรัฐ ความปลอดภัยสาธารณะ ระบบเศรษฐกิจ หรือสุขภาพของประชาชน อันเป็นเจตนารมณ์ที่แท้จริงของกฎหมายด้วย

3. หลักการจำกัดสิทธิและเสรีภาพโดยชอบธรรมตามหลักนิติรัฐ

ภายใต้การปกครองในระบอบประชาธิปไตยซึ่งถือว่าประชาชนต่างก็เป็นผู้ทรงสิทธิอันเป็นส่วนหนึ่งของอธิปไตยในรัฐ และด้วยเหตุนั้นสิทธิและเสรีภาพของประชาชนจึงเป็นสิ่งสูงค่าที่รัฐธรรมนูญลายลักษณ์อักษรในฐานะที่เป็นกฎหมายสูงสุด จะต้องบัญญัติไว้ให้มีความชัดเจนเพื่อสร้างกลไกในการคุ้มครองสิทธิและเสรีภาพของประชาชนให้ได้ดำรงอยู่อย่างเป็นรูปธรรม (เกรียงไกร เจริญธนาวัฒน์, 2561, น.176) การจะจำกัดสิทธิและเสรีภาพของประชาชนได้นั้นจึงจะต้องอาศัยอำนาจตามกฎหมาย ซึ่งกฎหมายนั้นก็จะต้องตราขึ้นโดยอาศัยอำนาจนิติบัญญัติที่ถือเป็นผู้แทนของปวงชนผู้เป็นเจ้าของอำนาจอธิปไตยด้วย กล่าวในอีกนัยหนึ่ง คือ ประชาชนในฐานะผู้ทรงสิทธิและเป็นส่วนหนึ่งของอำนาจอธิปไตยนั้นยินยอมจำกัดสิทธิและเสรีภาพที่ตนมีให้อยู่ภายใต้บทบัญญัติ

แห่งกฎหมายซึ่งตราขึ้นโดยฝ่ายนิติบัญญัติที่ถือเป็นผู้แทนของตนนั่นเอง (เกรียงไกร เจริญธนาวัฒน์, 2564, น.274–275) นอกจากหลักการพื้นฐานที่ว่าการจำกัดสิทธิและเสรีภาพของประชาชนนั้นจะต้องมาจากกฎหมายของฝ่ายนิติบัญญัติแล้ว ศาลสิทธิมนุษยชนแห่งยุโรปยังได้พัฒนาแนวทางในการวินิจฉัยว่าการจำกัดสิทธิและเสรีภาพของบุคคลในลักษณะใดจึงถือว่าเป็นการจัดสิทธิและเสรีภาพโดยชอบธรรม โดยมีหลักเกณฑ์ในการพิจารณา 3 ประการ ได้แก่ (1) การจำกัดสิทธิและเสรีภาพนั้นจะกระทำได้แต่โดยอาศัยอำนาจตามกฎหมายที่ตราขึ้นโดยฝ่ายนิติบัญญัติ (2) จะต้องมีเหตุผลความจำเป็นที่สามารถยอมรับได้ เช่น เพื่อรักษาความมั่นคงของชาติ ความสงบเรียบร้อยของสังคม หรือการรักษาสิทธิและเสรีภาพของผู้อื่น (3) มาตรการที่กฎหมายกำหนดหรือสิ่งที่กฎหมายลิดรอนสิทธิและเสรีภาพไปจากประชาชนนั้น เป็นมาตรการที่ได้สัดส่วนหรือไม่ (Donna Gomien, 1991, p.52-56) หลักการดังกล่าวข้างต้นถือเป็นพื้นฐานสำคัญซึ่งเป็นองค์ประกอบหนึ่งในหลักนิติรัฐ ซึ่งนานาอารยประเทศได้นำไปพัฒนาต่อยอดในการบัญญัติรับรองสิทธิและเสรีภาพแก่ประชาชนของตนเองจนถึงปัจจุบัน

สำหรับประเทศไทย ได้บัญญัติหลักการจำกัดสิทธิและเสรีภาพไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ดังนี้

“มาตรา 26 การตรากฎหมายที่มีผลเป็นการจำกัดสิทธิหรือเสรีภาพของบุคคลต้องเป็นไปตามเงื่อนไขที่บัญญัติไว้ในรัฐธรรมนูญ ในกรณีที่รัฐธรรมนูญมิได้บัญญัติเงื่อนไขไว้ กฎหมายดังกล่าวต้องไม่ขัดต่อหลักนิติธรรม ไม่เพิ่มภาระหรือจำกัดสิทธิหรือเสรีภาพของบุคคลเกินสมควรแก่เหตุ และจะกระทบต่อศักดิ์ศรีความเป็นมนุษย์ของบุคคลมิได้ รวมทั้งต้องระบุเหตุผลความจำเป็นในการจำกัดสิทธิและเสรีภาพไว้ด้วย

กฎหมายตามวรรคหนึ่ง ต้องมีผลใช้บังคับเป็นการทั่วไป ไม่มุ่งหมายให้ใช้บังคับแก่กรณีใดกรณีหนึ่งหรือแก่บุคคลใดบุคคลหนึ่งเป็นการเจาะจง”

ดังจะเห็นได้ว่าหลักในการจำกัดสิทธิและเสรีภาพตามรัฐธรรมนูญของประเทศไทยประกอบไปด้วยหลักสำคัญตามแนวทางของศาลสิทธิมนุษยชนแห่งยุโรป 3 ประการ และยังมีการพัฒนาโดยการเพิ่มเติมหลักประกันสิทธิและเสรีภาพอีกหลายประการ กล่าวคือ หลักนิติธรรม หลักศักดิ์ศรีความเป็นมนุษย์ และหลักกฎหมายต้องบังคับใช้เป็นการทั่วไปเพิ่มเติมเข้ามาอีกด้วย

เมื่อพิจารณาถึงปัญหาเกี่ยวกับอำนาจของพนักงานเจ้าหน้าที่ซึ่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์มอบให้เพื่อปฏิบัติหน้าที่ และกลไกการควบคุมตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่ดังที่ได้วิเคราะห์ไปแล้วกับหลักเกณฑ์ในการพิจารณาความชอบธรรมในการจำกัดสิทธิและเสรีภาพ จะเห็นได้ว่ากฎหมายฉบับดังกล่าวนั้นเป็นกฎหมายระดับพระราชบัญญัติ ซึ่งอาศัยอำนาจนิติบัญญัติในการตรากฎหมายฉบับนี้ ภายใต้ความจำเป็นที่จะต้องจำกัดสิทธิและเสรีภาพบางประการของประชาชน โดยอาศัยเหตุผลอันสามารถยอมรับได้อย่างเป็นสากล กล่าวคือ ความจำเป็นต่อการรักษาความมั่นคงทางไซเบอร์ซึ่งเป็นภัยคุกคามรูปแบบใหม่ในโลกยุคปัจจุบัน นอกจากนี้ ยังไม่ถือเป็นการกระทบต่อศักดิ์ศรีความเป็นมนุษย์ และไม่ปรากฏว่ามีวัตถุประสงค์มุ่งหมายบังคับใช้แก่บุคคลหรือกลุ่มบุคคลในลักษณะที่เป็นการเลือกปฏิบัติแต่อย่างใด

อย่างไรก็ดี การที่กฎหมายให้อำนาจแก่พนักงานเจ้าหน้าที่ซึ่งอาจมีการใช้อำนาจหรือดุลพินิจที่กระทบกระเทือนต่อสิทธิและเสรีภาพของประชาชนไว้หลายประการ อีกทั้งยังไม่ได้กำหนดกลไกในการตรวจสอบการใช้อำนาจรัฐโดยองค์กรตุลาการสำหรับกรณีภัยคุกคามไซเบอร์ในระดับวิกฤติเอาไว้ ทั้งยังตัดสิทธิของผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์มิให้อุทธรณ์คำสั่งในกรณีที่เป็นภัยคุกคามไซเบอร์ในระดับร้ายแรงและระดับวิกฤติอีกด้วย กรณีดังกล่าวจึงเป็นบทบัญญัติแห่งกฎหมายที่จำกัดสิทธิหรือเสรีภาพของบุคคลเกินสมควรแก่เหตุ กล่าวคือ แม้กฎหมายจะมีเหตุผลความจำเป็นตามสมควรในการให้อำนาจแก่พนักงานเจ้าหน้าที่เพื่อให้ปฏิบัติหน้าที่บรรลุวัตถุประสงค์ของกฎหมายได้ก็ตาม แต่ไม่ได้หมายความว่าจะสามารถใช้ดุลพินิจอย่างเป็นอิสระจากข้อจำกัดทั้งปวง (นันทวัฒน์ บรมานันท์, 2560, น.315) พนักงานเจ้าหน้าที่ผู้ใช้อำนาจรัฐหรือดุลพินิจยังคงต้องผูกพันอยู่ภายใต้หลักความได้สัดส่วนหรือหลักความพอสมควรแก่เหตุ ซึ่งมีสาระสำคัญ 3 ประการ ได้แก่ (1) หลักความเหมาะสม กล่าวคือ

มาตรการที่อาจทำให้บรรลุวัตถุประสงค์ของกฎหมายได้จะถือว่าเป็นมาตรการที่เหมาะสม ในทางกลับกันมาตรการใดก็ตามที่ไม่อาจทำให้บรรลุวัตถุประสงค์ของกฎหมายได้ก็จะถือว่าเป็นมาตรการที่ไม่เหมาะสม (2) หลักความจำเป็น กล่าวคือ มาตรการของกฎหมายนั้นจะต้องเป็นมาตรการที่ก่อให้เกิดผลกระทบน้อยที่สุดเท่าที่จำเป็นซึ่งสามารถทำให้บรรลุวัตถุประสงค์ของกฎหมายได้ (3) หลักความได้สัดส่วนในความหมายอย่างแคบ กล่าวคือ มาตรการทั้งหลายที่กฎหมายกำหนดกำหนดขึ้นจะต้องอยู่ภายใต้ขอบเขตของความสัมพันธ์ที่เหมาะสมระหว่างวิธีการกับวัตถุประสงค์ของกฎหมาย (บรรเจิด สิงคะเนติ และคณะ, 2558, น.19-20)

จากข้อพิจารณาเกี่ยวกับสาระสำคัญของหลักความได้สัดส่วนข้างต้น จะเห็นได้ว่าวัตถุประสงค์ที่พระราชบัญญัติดังกล่าวนี้ คือ การป้องกัน และยับยั้งภัยความมั่นคงทางไซเบอร์ในระดับร้ายแรงและระดับวิกฤติอย่างทันท่วงที เพื่อมิให้เกิดความเสียหายต่อระบบสารสนเทศสำคัญของรัฐ หรือกระทบต่อความมั่นคงของรัฐ หรือความสงบเรียบร้อยของสังคม จึงได้กำหนดมาตรการเพื่อให้พนักงานเจ้าหน้าที่สามารถปฏิบัติงานได้อย่างรวดเร็ว โดยเฉพาะอย่างยิ่งกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติกฎหมายได้ให้อำนาจดุลพินิจในการกำหนดมาตรการใด ๆ ก็ได้ที่เห็นว่าจำเป็น ซึ่งเป็นการให้อำนาจใช้ดุลพินิจที่เด็ดขาดและไม่อาจตรวจสอบได้โดยองค์กรตุลาการทั้งก่อนและระหว่างการใช้อำนาจของพนักงานเจ้าหน้าที่ ซึ่งเป็นหลักพื้นฐานสำคัญของหลักนิติรัฐเกี่ยวกับกระบวนวิธีพิจารณาทั่วไป (บุญศรี มีวงศ์อุโฆษ, 2563 น.488-489) ประการหนึ่ง จึงอาจนำไปสู่การใช้อำนาจที่กระทบต่อสิทธิและเสรีภาพของประชาชนเกินสมควรได้ นอกจากนี้ การที่กฎหมายห้ามมิให้ผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อุทธรณ์คำสั่งได้สำหรับกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงและระดับวิกฤติ ตามมาตรา 69 ยังเป็นการปิดโอกาสของผู้ที่ได้รับผลกระทบจากการใช้อำนาจของรัฐมิให้ใช้สิทธิโต้แย้งดุลพินิจและการใช้อำนาจรัฐด้วย มาตรการดังกล่าวจึงเป็นมาตรการที่มีผลกระทบต่อสิทธิและเสรีภาพของประชาชนมากจนเกินสมควรจึงขัดต่อหลักความได้สัดส่วนและหลักนิติรัฐ (นิติธรรม) ตามมาตรา 26 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

ข้อค้นพบเชิงวิชาการ หรือองค์ความรู้ใหม่เชิงวิชาการ

บทความวิชาการฉบับนี้ ได้ข้อค้นพบทางวิชาการเกี่ยวกับปัญหาทางกฎหมายที่อาจเกิดขึ้นจากกลไกการป้องกันและยับยั้งภัยคุกคามทางไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งมีต้นแบบมาจากรัฐบัญญัติความมั่นคงปลอดภัยไซเบอร์ของสาธารณรัฐสิงคโปร์ โดยมีเนื้อหาที่เป็นไปเพื่อมุ่งเน้นการควบคุมอาชญากรรมเช่นเดียวกัน จนอาจนำไปสู่การใช้อำนาจในลักษณะที่กระทบกระเทือนต่อสิทธิและเสรีภาพของประชาชนเกินสมควร โดยเฉพาะอย่างยิ่งบทบัญญัติมาตรา 68 และมาตรา 69 ซึ่งเป็นการตัดและลดทอนการตรวจสอบการใช้อำนาจดุลพินิจจากองค์กรตุลาการ และสิทธิในการโต้แย้งของผู้ได้รับผลกระทบจากการใช้อำนาจของรัฐเป็นมาตรการทางกฎหมายที่ขัดต่อหลักความได้สัดส่วนตามรัฐธรรมนูญมาตรา 26 โดยมีข้อเสนอแนะให้แก้ไขเพิ่มเติมบทบัญญัติมาตรา 68 โดยกำหนดให้คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติสามารถดำเนินการใด ๆ เพื่อป้องกันและยับยั้งภัยคุกคามทางไซเบอร์ระดับวิกฤติตามความจำเป็นไปก่อนได้ โดยยังคงต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขออนุญาตดำเนินการ โดยหากไม่ได้รับอนุญาตจากศาลให้ดำเนินการ คำสั่งของคณะกรรมการเป็นอันสิ้นผลไป นอกจากนี้ ควรแก้ไขเพิ่มเติม มาตรา 69 โดยการให้สิทธิผู้ที่ต้องอยู่ภายใต้บังคับคำสั่งของคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำหรับกรณีที่มีภัยคุกคามทางไซเบอร์ระดับร้ายแรงและระดับวิกฤติ ให้สามารถอุทธรณ์คำสั่งได้ภายในเวลา 30 วัน นับแต่วันที่ได้รับคำสั่ง ทั้งนี้การอุทธรณ์คำสั่งดังกล่าวจะต้องไม่เป็นการทุเลาการบังคับหรือมีผลเป็นการยับยั้งการดำเนินการของพนักงานเจ้าหน้าที่ซึ่งปฏิบัติหน้าที่ตามคำสั่งของคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

บทสรุป

จากการศึกษาปัญหาทางกฎหมายในการบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์กับการคุ้มครองสิทธิและเสรีภาพตามรัฐธรรมนูญ ผู้เขียนสามารถสรุปผลการศึกษาและมีข้อเสนอแนะ ดังนี้

1. พระราชบัญญัติการรักษาความวามมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นกฎหมายที่มีความจำเป็นต่อการป้องกันและยับยั้งภัยคุกคามทางไซเบอร์ ซึ่งเป็นภัยต่อความมั่นคงรูปแบบใหม่ที่รัฐทั้งหลายจะต้องเผชิญมากขึ้นเรื่อย ๆ ในโลกยุคดิจิทัล การที่กฎหมายดังกล่าวได้ให้อำนาจหลายประการแก่พนักงานเจ้าหน้าที่ก็เพื่อให้สามารถปฏิบัติหน้าที่ให้บรรลุวัตถุประสงค์ของกฎหมายได้ การให้อำนาจบางประการที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของประชาชน เช่น การเข้าไปในเคหสถาน การยึดคอมพิวเตอร์หรืออุปกรณ์ การเข้าถึงข้อมูลคอมพิวเตอร์ ก็เป็นความจำเป็นอันมีเหตุผลสามารถยอมรับได้ ในแง่นี้จึงถือได้ว่าโดยเจตนารมณ์พื้นฐานของกฎหมายมีความชอบธรรมในการจำกัดสิทธิและเสรีภาพของประชาชนในเชิงรูปแบบ อย่างไรก็ดี เมื่อพิจารณาถึงมาตรการทางกฎหมายที่สร้างขึ้นส่งผลให้พระราชบัญญัติดังกล่าวมีลักษณะเป็นกฎหมายที่เอนเอียงไปในทางที่มุ่งควบคุมและปราบปรามอาชญากรรมเป็นสำคัญ จนอาจมีบางกรณีที่อาจนำไปสู่การละเมิดต่อสิทธิและเสรีภาพของประชาชนจนเกินสมควรได้

2. บทบัญญัติมาตรา 68 ของพระราชบัญญัติการรักษาความวามมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่กำหนดให้ กมช. มีอำนาจกำหนดมาตรการที่เห็นว่าจำเป็นเพื่อให้พนักงานเจ้าหน้าที่สามารถดำเนินการได้ในกรณีที่เกิดภัยความมั่นคงทางไซเบอร์ในระดับวิกฤติ โดยไม่ต้องขออนุญาตจากศาลก่อนนั้น แม้จะมีความจำเป็นเร่งด่วนซึ่งต้องอาศัยการดำเนินการอย่างฉับพลันให้สามารถยับยั้งหรือควบคุมผลกระทบอันเกิดจากการโจมตีทางไซเบอร์นั้นก็ตาม แต่การที่กฎหมายตัดทั้งอำนาจองค์กรตุลาการในการตรวจสอบการใช้ดุลพินิจของ กมช. ทั้งก่อนการดำเนินการและระหว่างการดำเนินการ ย่อมเป็นมาตรการที่กระทบต่อสิทธิและเสรีภาพของประชาชนเกินสมควร เนื่องจาก เป็นบทบัญญัติที่ขัดต่อหลักความได้สัดส่วน กล่าวคือ มาตรการที่กฎหมายใช้นั้นไม่ได้เป็นมาตรการที่ก่อให้เกิดผลกระทบน้อยที่สุดเท่าที่จำเป็นซึ่งสามารถทำให้บรรลุวัตถุประสงค์ของกฎหมายได้ บทบัญญัติดังกล่าวจึงขัดหรือแย้งต่อบทบัญญัติมาตรา 26 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

ผู้เขียนมีข้อเสนอแนะต่อประเด็นดังกล่าวว่า ควรมีการแก้ไขเพิ่มเติมบทบัญญัติมาตรา 68 ของพระราชบัญญัติการรักษาความวามมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อกำหนดมาตรการทางกฎหมายที่ก่อให้เกิดผลกระทบน้อยที่สุดเท่าที่จำเป็นแต่ยังสามารถทำให้บรรลุวัตถุประสงค์ของกฎหมายได้ โดยแบ่งการดำเนินการออกเป็น 3 ขั้นตอน (1) เมื่อเกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ซึ่งมีความจำเป็นต้องกำหนดมาตรการและดำเนินการเพื่อยับยั้งและควบคุมความเสียหายอย่างฉับพลันให้ กมช. สามารถกำหนดมาตรการที่จำเป็นเพื่อให้พนักงานเจ้าหน้าที่สามารถปฏิบัติการได้โดยเร็ว (2) ในระหว่างดำเนินการ กมช. จะต้องยื่นคำร้องต่อศาลเพื่อขออนุญาตเช่นเดียวกับการดำเนินการกรณีภัยคุกคามทางไซเบอร์ในระดับร้ายแรงตามมาตรา 66 (3) หากศาลพิจารณาแล้วเห็นว่ามีเหตุจำเป็นอันควรเชื่อได้ว่าเกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติจริงก็ให้พนักงานเจ้าหน้าที่ปฏิบัติหน้าที่ต่อไปจนบรรลุเป้าหมาย แต่หากเป็นกรณีที่ศาลเห็นว่าไม่ปรากฏเหตุจำเป็นอันควรเชื่อได้ว่าเกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติจริง ศาลอาจเพิกถอนคำสั่งและมาตรการใด ๆ ที่พนักงานเจ้าหน้าที่ดำเนินการไปตามคำสั่งของคณะกรรมการได้

3. บทบัญญัติมาตรา 69 ของพระราชบัญญัติการรักษาความวามมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่กำหนดห้ามมิให้ผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงในระดับวิกฤติอุทธรณ์คำสั่ง เมื่อพิจารณาประกอบกับมาตรา 68 ที่ให้อำนาจเด็ดขาดในการกำหนดมาตรการที่จำเป็นแก่ กมช. โดยปราศจากการตรวจสอบจากองค์กรตุลาการซึ่งแม้จะมีความจำเป็นเร่งด่วนซึ่งต้องอาศัยการดำเนินการอย่างฉับพลันดังที่ได้วิเคราะห์ไปแล้วก็ตาม แต่การที่กฎหมายห้ามมิให้ผู้ที่ได้รับผลกระทบใช้สิทธิโต้แย้งการใช้อำนาจและดุลพินิจของพนักงานเจ้าหน้าที่ เพื่อประโยชน์คือความสะดวกรวดเร็วในการดำเนินการเพื่อป้องกันหรือยับยั้งภัยคุกคามทางไซเบอร์ ก็ไม่ถือเป็นมาตรการที่ก่อให้เกิดผลกระทบน้อยที่สุดเท่าที่จำเป็นซึ่งสามารถทำให้บรรลุวัตถุประสงค์ของกฎหมายได้ บทบัญญัติดังกล่าวจึงขัดหรือแย้งต่อบทบัญญัติมาตรา 26 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ด้วยเช่นกัน

ผู้เขียนมีข้อเสนอแนะต่อประเด็นดังกล่าวว่า ควรมีการแก้ไขเพิ่มเติมบทบัญญัติมาตรา 69 ของพระราชบัญญัติการรักษาความวามมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อกำหนดมาตรการทางกฎหมายที่ก่อให้เกิดผลกระทบน้อยที่สุดเท่าที่จำเป็นแต่ยังสามารถทำให้บรรลุวัตถุประสงค์ของกฎหมายได้ โดยมีเงื่อนไขสำคัญ 2 ประการ (1) ในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงก็ดีหรือในระดับวิกฤติก็ดี ผู้ที่ได้รับผลกระทบจะต้องมีสิทธิอุทธรณ์คำสั่งได้ภายใน 30 วัน นับแต่วันที่ได้รับคำสั่ง (2) ในระหว่างอุทธรณ์นั้นจะต้องไม่เป็นเหตุทุเลาการบังคับหรือการดำเนินการใด ๆ ที่จำเป็น พนักงานเจ้าหน้าที่จะยังคงมีอำนาจในการดำเนินการตามความจำเป็นเพื่อให้บรรลุวัตถุประสงค์ในการป้องกันและยับยั้งภัยคุกคามทางไซเบอร์ต่อไป

4. แม้จากข้อมูลของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) จะจัดประเทศไทยอยู่ในกลุ่มประเทศที่มีความพร้อมด้านกฎหมายไซเบอร์ในระดับที่สูงมาก แต่ก็เป็นเพียงข้อพิจารณาเบื้องต้นในเชิงรูปแบบ เช่น การมีองค์กรผู้รับผิดชอบ ชัดเจน การมีนโยบายที่เกี่ยวข้อง การมีกฎหมายสารบัญญัติกำหนดสิทธิ หน้าที่ และความผิดของการกระทำต่าง ๆ ที่เกี่ยวข้องเอาไว้ มิได้เป็นข้อพิจารณาในเชิงเนื้อหาของกฎหมายแต่อย่างใด จากการศึกษาของผู้เขียนพบว่าการบังคับใช้กฎหมายไซเบอร์ในประเทศไทยมุ่งให้ความสำคัญกับการกระทำความผิดที่ใช้เทคโนโลยีในการโจมตีและก่อให้เกิดความเสียหายในปริมาณที่ไม่สูงมากนัก แต่กลับให้ความสำคัญกับการปราบปรามข้อมูลคอมพิวเตอร์ ซึ่งผู้มีอำนาจเห็นว่าเนื้อหานั้นกระทบต่อตัวผู้มีอำนาจ หรือความเชื่อทางการเมืองของผู้มีอำนาจ โดยอ้างเหตุเรื่องความมั่นคง หรือความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน ทั้งที่โดยเจตนารมณ์ของกฎหมายแล้วควรมุ่งควบคุมตรวจสอบข้อมูลคอมพิวเตอร์อันอาจส่งผลกระทบต่อความมั่นคงของรัฐ เช่น การนำเอาข้อมูลความลับทางการทหาร หรือกระทบต่อความมั่นคงทางเศรษฐกิจ เช่น การโจรกรรมหรือซื้อขายข้อมูลส่วนบุคคลของประชาชนจำนวนมาก นำไปสู่การฉ้อโกงประชาชนเป็นจำนวนมาก

นอกจากนี้ เพื่อป้องกันปัญหาข้อมูลส่วนบุคคลของประชาชนรั่วไหลจากหน่วยงานของรัฐ ดังเช่นกรณีที่ข้อมูลประชาชนกว่า 55 ล้านรายชื่อที่อยู่ในความครอบครองของกระทรวงสาธารณสุขรั่วไหลออกไปเผยแพร่บนเว็บไซต์สาธารณะ ในปี พ.ศ. 2566 (สุทธิพัฒน์ กนิษฐกุล, 2566) จึงสมควรแก้ไขเพิ่มเติมกฎหมายลำดับรองที่เกี่ยวกับการกำหนดมาตรฐานความปลอดภัยของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการดำเนินงานของหน่วยงานของรัฐให้มีมาตรฐานความปลอดภัยตามที่กำหนด โดยอาจกำหนดให้หน่วยงานใช้เทคโนโลยีและภาษาคอมพิวเตอร์ในการพัฒนาที่สอดคล้องกัน ซึ่งนอกจากจะกำหนดมาตรฐานเป็นกฎหมายลายลักษณ์อักษรแล้ว ควรกำหนดมาตรฐานการจัดทำระบบการจัดซื้อจัดจ้างของหน่วยงานของรัฐที่เกี่ยวข้องกับการจ้างสร้างหรือพัฒนาระบบคอมพิวเตอร์ เว็บไซต์ ซอฟต์แวร์ หรือฐานข้อมูลใด ๆ ในลักษณะที่เป็น code มาตรฐานซึ่งมีมาตรฐานเทคโนโลยีความปลอดภัยตามที่กำหนด เพื่อให้หน่วยงานของรัฐนำไปกำหนดเป็นมาตรฐานการจัดซื้อจัดจ้างของหน่วยงานของรัฐ เมื่อหน่วยงานของรัฐมีความจำเป็นจะต้องจ้างผู้ประกอบการในการพัฒนาระบบหรือซอฟต์แวร์ใด ๆ ให้กับหน่วยงานของรัฐ โดยผู้ประกอบการจะต้องนำเอาเทคโนโลยีที่กำหนดและ Code พื้นฐานนี้ไปประกอบการจัดทำข้อเสนอเพื่อยื่นต่อหน่วยงานของรัฐ และเมื่อผู้ประกอบการใดเป็นผู้ได้รับเลือกก็จะต้องพัฒนาระบบหรือซอฟต์แวร์นั้นให้ได้มาตรฐานตามที่กำหนดไว้แล้ว การกำหนดมาตรฐานและการรวมศูนย์ความปลอดภัยทางไซเบอร์ในลักษณะนี้จะช่วยให้การรักษาความปลอดภัยและการแก้ไขปัญหาของระบบและข้อมูลคอมพิวเตอร์ได้อย่างมีประสิทธิภาพและรวดเร็วมากขึ้น (Dave Packham, 2023) เมื่อเกิดภัยคุกคามทางไซเบอร์ซึ่งหน่วยงานราชการไม่สามารถแก้ไขปัญหาเองได้ พนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงไซเบอร์ พ.ศ. 2562 ก็จะสามารถเข้าไปดำเนินการยับยั้งหรือแก้ไขได้อย่างมีประสิทธิภาพและทันท่วงที

เอกสารอ้างอิง

เกรียงไกร เจริญธนาวัฒน์. (2564). *หลักพื้นฐานกฎหมายมหาชน*. (พิมพ์ครั้งที่ 7). กรุงเทพฯ: สำนักพิมพ์วิญญูชน.

_____. (2561). *รัฐ รัฐธรรมนูญและกฎหมาย*. (พิมพ์ครั้งที่ 9). กรุงเทพฯ: สำนักพิมพ์วิญญูชน.

นันทวัฒน์ บรมานันท์ (2560). *กฎหมายปกครอง*. (พิมพ์ครั้งที่ 5). กรุงเทพฯ: สำนักพิมพ์วิญญูชน.

บรรเจิด สิงคะเนติ และคณะ. (2558). *หลักความได้สัดส่วน (Principle of Proportionality) ในการตรวจสอบขอบเขตอำนาจรัฐตามมาตรา 29 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550*. (รายงานผลการวิจัย). กรุงเทพฯ: สำนักงานศาลรัฐธรรมนูญ.

_____. (2555). *หลักพื้นฐานเกี่ยวกับสิทธิเสรีภาพและศักดิ์ศรีความเป็นมนุษย์*. (พิมพ์ครั้งที่ 4). กรุงเทพฯ: สำนักพิมพ์วิญญูชน.

บุญศรี มีวงศ์อุโฆษ. (2563). *กฎหมายรัฐธรรมนูญ*. (พิมพ์ครั้งที่ 10). กรุงเทพฯ: สำนักพิมพ์วิญญูชน.

สาวตรี สุขศรี. (2563). *กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์*. (พิมพ์ครั้งที่ 2). กรุงเทพฯ: โรงพิมพ์เดือนตุลา.

สุทธิพัฒน์ กนิษฐกุล. (2566). *ความปลอดภัยทางไซเบอร์อยู่ที่ไหน ย้อนดูกรณีข้อมูลส่วนตัวหลุดจากหน่วยงานไทยในรอบ 4 ปี*. สืบค้นเมื่อ 15 เมษายน 2566, จาก https://thematter.co/quick-bite/qb-thai-leaked-informantion/200724.

Dave Packham. (2023). *Benefits of centralized cybersecurity tools in a university environment*. Retrieved 15 April 2023, from https://it.utah.edu/node4/posts/2023/october/cybersecurity-toolset.php

Donna Gomien. (1991). *Short guide to the European Convention on Human Rights*. Council of Europe.

International Telecommunication Union: ITU. (2020). *Global Cybersecurity Index 2020*. Retrieved 15 April 2023, from https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Josh Fruhlinger. (2022). *Stuxnet explained: The first known cyberweapon*. Retrieved 15 April 2023, from https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

Marie Baezner, Patrice Robin. (2017). *Stuxnet*. Retrieved 15 April 2023, from https://www.researchgate.net/publication/323199431_Stuxnet

Michael Brands. (2023). *Cybersecurity laws and legislation.* Retrieved 15 April 2023, from https://www.connectwise.com/blog/cybersecurity/cybersecurity-laws-and-legislation.

United Nations Development Program. (2022). *2022 Special Report on Human Security*. Retrieved 15 April 2023, from https://www.un-ilibrary.org/content/books/9789210014007#chapters.