การสร้างสมดุลระหว่างความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองสิทธิมนุษยชนผ่านแนวทางฐานสิทธิมนุษยชน

BALANCING CYBERSECURITY AND HUMAN RIAHTS PROTECTION THROUGH THE HUMAN RIGTHS BASED APPROACH

[1]อมรรัตน์ อินนุมาตร

[1]AMORNRAT INNUMAT

[1]มหาวิทยาลัยธรรมศาสตร์, ประเทศไทย

[1]Thammasat University, Thailand

[1]nakichan@hotmail.com

Received: October 20,2024; **Revised** :November 2, 2024; **Accepted** :December 28,2024

บทคัดย่อ

ในโลกปัจจุบันที่เชื่อมต่อถึงกัน ความก้าวหน้าอย่างรวดเร็วของเทคโนโลยีได้นำมาซึ่งทั้งโอกาส และความท้าทาย เมื่อการพึ่งพาโครงสร้างพื้นฐานดิจิทัลเติบโตขึ้น ความต้องการมาตรการรักษาความปลอดภัยทางไซเบอร์ที่แข็งแกร่งก็เพิ่มขึ้นเช่นกัน เพื่อปกป้องข้อมูลที่ละเอียดอ่อน และระบบที่สำคัญ อย่างไรก็ตาม ในขณะที่รัฐบาลและองค์กรต่างๆ เข้มงวดกับการรักษาความปลอดภัยทางไซเบอร์ มีความกังวลเกี่ยวกับการละเมิดสิทธิมนุษยชนที่อาจเกิดขึ้นได้ บทความนี้มีจุดมุ่งหมายเพื่อสำรวจความสัมพันธ์ที่ซับซ้อน และกำลังพัฒนาระหว่างกฎหมายความมั่นคงปลอดภัยไซเบอร์กับสิทธิมนุษยชน และความสำคัญของการสร้างสมดุลที่ละเอียดอ่อนระหว่างมิติทั้งสอง ผ่านการศึกษากฎหมายภายในของประเทศต่างๆ และแนวทางในระดับระหว่างประเทศที่น่าสนใจ รวมถึงข้อเสนอแนะที่จะนำแนวทางฐานสิทธิมนุษยชนมาเป็นกรอบในการจัดทำกฎหมาย นโยบายหรือมาตรการต่างๆ ด้านความมั่นคงปลอดภัยไซเบอร์

คำสำคัญ : ความมั่นคงปลอดภัยไซเบอร์, สิทธิมนุษยชน, แนวทางฐานสิทธิมนุษยชน, ดิจิทัล

---

[1]นักศึกษา หลักสูตรนิติศาสตรมหาบัณฑิต สาขากฎหมายระหว่างประเทศ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

Abstract

In today's interconnected world, the rapid advancement of technology has brought both opportunities and challenges. As the reliance on digital infrastructure grows, so does the need for robust cybersecurity measures to protect sensitive information and critical systems. However, as governments and organizations tighten their grip on cybersecurity, concerns about potential infringements on human rights have emerged. This article aims to explore the complex and evolving relationship between cybersecurity law and human rights, and the importance of striking a delicate equilibrium between the two. Through the study of the internal laws of different countries and an interesting international approach. Including suggestions to adopt a human rights-based approach as a framework for drafting laws, policies or measures on cyber security.

Keywords : Cybersecurity, Human Rights, Human Rights-based Approach, Digital

บทนำ

ยุคดิจิทัลได้นำความก้าวหน้าที่ไม่เคยมีมาก่อน ปฏิวัติวิธีการสื่อสาร การทำงาน และการใช้ชีวิตของมนุษย์ จากการเพิ่มจำนวนของสมาร์ทโฟน และแพลตฟอร์มโซเชียลมีเดีย ไปจนถึง Internet of Things (IoT) และคลาวด์คอมพิวติ้ง (Cloud Computing) โลกของเราเชื่อมโยงถึงกันมากขึ้นกว่าที่เคยเป็นมา อย่างไรก็ตาม การเชื่อมต่อนี้ยังทำให้เราเผชิญกับภัยคุกคามทางไซเบอร์ที่ก่อให้เกิดความเสี่ยงอย่างมากต่อบุคคล องค์กร และแม้แต่ประเทศชาติ ความก้าวหน้าอย่างรวดเร็วของเทคโนโลยีทำให้เกิดวิวัฒนาการของภัยคุกคามทางไซเบอร์ ทุกวันนี้ทั้งในระดับประเทศ และระดับโลกต้องเผชิญกับการโจมตีที่ซับซ้อนมากมาย ส่งผลให้ประเทศต่าง ๆ มีการพัฒนามาตรการและบัญญัติกฎหมาย เพื่อรับมือกับภัยคุกคามทางไซเบอร์ รวมไปถึงการสร้างความร่วมมือในระดับระหว่างประเทศเพื่อร่วมกันวางแนวปฏิบัติที่เป็นมาตรฐาน ให้คำแนะนำในการเฝ้าระวัง และต่อสู้กับภัยคุกคามดังกล่าว สำหรับในระดับประเทศนั้น ประเทศต่าง ๆ มีการบัญญัติกฎหมายเกี่ยวกับอาชญากรรมไซเบอร์ และความมั่นคงทางไซเบอร์กันออกมาเป็นจำนวนมาก รวมไปถึงนโยบายและแผนระดับชาติอีกด้วย แต่กฎหมาย มาตรการ และนโยบายด้านความมั่นคงไซเบอร์เหล่านั้นส่งผลกระทบโดยตรงกับสิทธิมนุษยชน เช่น สิทธิในความเป็นส่วนตัว (Right to Privacy) เสรีภาพในการแสดงออก (Freedom of Expression) สิทธิในการเข้าถึงข้อมูลข่าวสาร (Right to Access to Information) เป็นต้น โดยผู้มีอำนาจกำหนดนโยบาย หรือผู้มีอำนาจตรากฎหมายมี

วัตถุประสงค์เพื่อจะปกป้องโลกไซเบอร์ ตลอดจนระบบเทคโนโลยีสารสนเทศจากการกระทำในทางไม่พึงประสงค์ มาตรการต่าง ๆ ที่ออกมาให้น้ำหนักไปในเรื่องความมั่นคงเป็นหลัก โดยใช้แนวทางความมั่นคงของรัฐเป็นศูนย์กลาง (National security-centric approach) จนทำให้กฎเกณฑ์ในเรื่องความมั่นคงทางไซเบอร์ในประเทศต่าง ๆ มีมากมาย และกว้างเกินไป ขาดความชัดเจน และปราศจากการตรวจสอบถ่วงดุล หรือกลไกความรับผิดต่อระบอบ (regime) อื่น ๆ การเยียวยาผู้ได้รับผลกระทบจากการบังคับใช้มาตรการต่าง ๆ เหล่านั้น ซึ่งสามารถนำไปสู่การละเมิดสิทธิมนุษยชนได้

ในกรณีของประเทศไทยได้มีการตราพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งประกาศในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562 และมีผลใช้บังคับตั้งแต่วันที่ 28 พฤษภาคม 2562 ซึ่งพระราชบัญญัติฉบับนี้ถูกวิพากษ์วิจารณ์โดยภาคส่วนต่าง ๆ ในสังคมอย่างกว้างขวาง ด้วยความวิตกกังวลว่าจะก่อให้เกิดการละเมิดสิทธิมนุษยชน เพราะความไม่ชัดเจนในการให้นิยามของคำสำคัญในบทบัญญัติต่าง ๆ รวมไปถึงการใช้ดุลพินิจของเจ้าหน้าที่ผู้มีอำนาจหน้าที่ในการบังคับใช้กฎหมายดังกล่าว

วิทยานิพนธ์ฉบับนี้จึงมุ่งพิจารณาแนวทางการสร้างสมดุลระหว่างความมั่นคงปลอดภัยไซเบอร์ และสิทธิมนุษยชนผ่านแนวทางฐานสิทธิมนุษยชน (Human Rights-Based Approach) โดยศึกษากฎหมายระหว่างประเทศ มาตรฐาน และแนวปฏิบัติที่ได้รับการยอมรับในปัจจุบัน ตลอดจนศึกษากฎหมายว่าด้วยความมั่นคงทางไซเบอร์ของประเทศต่าง ๆ และของประเทศไทย ในการวิเคราะห์ว่ากฎหมายที่ตราขึ้นใช้เพื่อรักษาความมั่นคงทางไซเบอร์นั้น มีการสร้างความสมดุลกับมิติด้านสิทธิมนุษยชน หรือไม่ เพื่อเป็นแนวทางในการปรับปรุงกฎหมายว่าด้วยความมั่นคงไซเบอร์ของประเทศไทยให้มีความเหมาะสม มีมาตรฐานในระดับสากล บรรลุเจตนารมณ์ในการรักษาความมั่นคงทางไซเบอร์ ในขณะเดียวกันก็ส่งเสริม และปกป้องสิทธิมนุษยชนด้วย

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาลักษณะของความมั่นคงปลอดภัยทางไซเบอร์ ประเภทของภัยคุกคาม เพื่อทำความเข้าใจเหตุผลในการออกมาตรการทางกฎหมายเพื่อรับมือกับภัยคุกคามทางไซเบอร์

2. เพื่อศึกษาว่าสิทธิมนุษยชนด้านใดบ้างที่อาจถูกกระทบจากการบังคับใช้กฎหมายว่าด้วยความมั่นคงทางไซเบอร์

3.เพื่อศึกษาแนวทางฐานสิทธิมนุษยชนที่จะใช้สร้างสมดุลในการพัฒนานโยบาย และมาตรการทางกฎหมายด้านความมั่นคงทางไซเบอร์

4. เพื่อศึกษากฎหมาย มาตรฐาน และแนวปฏิบัติในทางระหว่างประเทศที่ได้รับการยอมรับอย่างกว้างขวางในปัจจุบัน ตลอดจนกฎหมายภายในประเทศต่างๆ ที่น่าสนใจเพื่อเปรียบเทียบมาตรการการรักษาความมั่นคงทางไซเบอร์ และมาตรการในการคุ้มครองสิทธิมนุษยชนในกฎหมายเหล่านั้น

5. เพื่อศึกษาพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ในเรื่องความสมดุลของมิติด้านความมั่นคง และมิติด้านสิทธิมนุษยชน เพื่อให้สามารถเสนอแนะแนวทางในการปรับปรุงกฎหมายดังกล่าวให้เกิดความสมดุลต่อไป

วิธีดำเนินการวิจัย

วิทยานิพนธ์นี้เป็นการศึกษาวิจัยทางเอกสารโดยศึกษา และวิเคราะห์จากหนังสือ วารสาร บทความ งานวิจัย ตราสารระหว่างประเทศ ตัวบทกฎหมาย และข้อมูลอิเล็กทรอนิกส์ทั้งของประเทศไทย และต่างประเทศ และวิเคราะห์เพื่อเสนอแนวทางในการปรับปรุงกฎหมายว่าด้วยการรักษาความมั่นคงทางไซเบอร์โดยไม่ละเลยมิติด้านสิทธิมนุษยชน

ผลการวิจัย

รัฐมีหน้าที่ในการปกป้องส่งเสริมสิทธิเสรีภาพขั้นพื้นฐานของประชาชน ซึ่งสิทธิต่างๆ ได้มีการรับรองไว้ทั้งในกฎหมายภายในของประเทศ เช่น รัฐธรรมนูญ พระราชบัญญัติ ตลอดจนกฎหมายลำดับรองต่าง ๆ และรับรองไว้โดยกฎหมายระหว่างประเทศ ทั้งที่เป็น Soft Law เช่น ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights: UDHR) และที่เป็นความตกลงระหว่างประเทศที่มีค่าบังคับ เช่น กติการะหว่างประเทศว่าด้วยสิทธิพลเมือง และสิทธิทางการเมือง (International Covenant on Civil and Political Rights: ICCPR) กติการะหว่างประเทศว่าด้วยสิทธิทางเศรษฐกิจ สังคมและวัฒนธรรม (International Covenant on Economic, Social and Cultural Rights: ICESCR) เป็นต้น

1. ลักษณะของความมั่นคงปลอดภัยทางไซเบอร์ ประเภทของภัยคุกคาม เพื่อทำความเข้าใจเหตุผลในการออกมาตรการทางกฎหมายเพื่อรับมือกับภัยคุกคามทางไซเบอร์ สรุปได้ดังนี้ ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็นเพื่อทำให้องค์กรและผู้ใช้ปราศจากความเสี่ยงและความเสียหายต่อระบบและข้อมูลในทุกรูปแบบ รวมถึงการระวังป้องกันการโจมตี การบ่อนทำลาย การบุกรุก การจารกรรม และความ

ผิดพลาดต่าง ๆ โดยคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล 3 ประการ ได้แก่ การรักษาความลับ ความสมบูรณ์ของข้อมูล และความพร้อมใช้งาน

ภัยคุกคามทางไซเบอร์ (Cyber Threat) คือ ภัยอันตรายที่อาจเกิดขึ้นต่อระบบคอมพิวเตอร์ หรือเครือข่าย ซึ่งอาจส่งผลให้ระบบหรือเครือข่ายดังกล่าวไม่สามารถใช้งานได้ตามปกติ หรือถูกขโมย ทำลาย หรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต โดยภัยคุกคามทางไซเบอร์สามารถจำแนกออกเป็น 9 ประเภท ได้แก่ เนื้อหาที่เป็นภัยคุกคาม การโจมตีสภาพความพร้อมใช้งานของระบบ การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ ความพยายามรวบรวมข้อมูลของระบบ การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต ความพยายามจะบุกรุกเข้าระบบ การบุกรุกหรือเจาะระบบได้สำเร็จ โปรแกรมไม่พึงประสงค์ และภัยคุกคามอื่น ๆ นอกเหนือจากที่กล่าวไว้ข้างต้น โดยภัยคุกคามเหล่านี้อาจมาจาก 5 แหล่ง ได้แก่ รัฐบาลแห่งชาติ ผู้ก่อการร้าย สายลับของเอกชนและองค์กรอาชญากรรม แฮกทิวิส และแฮกเกอร์ ซึ่งสามารถก่อให้เกิดความเสียหายได้หลายระดับ ตั้งแต่ระดับบุคคลธรรมดาไปจนถึงระดับประเทศ

ด้วยเหตุนี้ ประเทศต่างๆ ทั่วโลกจึงตื่นตัวในการพัฒนามาตรการและกฎหมายเพื่อรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงสร้างความร่วมมือระหว่างประเทศเพื่อร่วมกันวางแนวปฏิบัติในการเฝ้าระวังและต่อสู้กับภัยคุกคามดังกล่าว เช่น สหประชาชาติได้จัดตั้ง UNGGE เพื่อเสาะหาแนวทางในการสร้างความเข้มแข็งให้แก่สันติภาพและความมั่นคงของโลก ตลอดจนมีมาตรการที่สร้างความมั่นใจให้เกิดขึ้นในโลกไซเบอร์ โดยการพัฒนาบรรทัดฐานหรือมาตรฐานสำหรับพฤติกรรมที่มีความรับผิดชอบของรัฐในโลกไซเบอร์

2. สิทธิมนุษยชนด้านต่าง ๆ ที่อาจถูกกระทบจากการบังคับใช้กฎหมายว่าด้วยความมั่นคงทางไซเบอร์ สรุปได้ดังนี้

2.1 สิทธิในความเป็นส่วนตัว (Right to Privacy) กฎหมายความมั่นคงทางไซเบอร์มักอนุญาตให้หน่วยงานรัฐหรือหน่วยงานที่เกี่ยวข้องสามารถเข้าถึงและเก็บข้อมูลส่วนบุคคลของประชาชน โดยไม่ได้รับความยินยอมอย่างชัดเจนอาจละเมิดสิทธิในความเป็นส่วนตัว และก่อให้เกิดความเสี่ยงต่อความปลอดภัยของข้อมูลส่วนบุคคล

2.2 เสรีภาพในการแสดงออก (Freedom of Expression) กฎหมายความมั่นคงทางไซเบอร์อาจนำไปสู่การควบคุมหรือเซ็นเซอร์เนื้อหาที่เผยแพร่ทางอินเทอร์เน็ต ซึ่งอาจละเมิดเสรีภาพในการแสดงออกของประชาชนและสื่อมวลชน

2.3 สิทธิในการเข้าถึงข้อมูล (Right to Access Information) กฎหมายอาจกำหนดข้อจำกัดในการเข้าถึงข้อมูลที่ถือว่าเป็นภัยต่อความมั่นคง การบังคับใช้กฎหมายโดยไม่มีการเปิดเผย

ข้อมูลเกี่ยวกับวิธีการตรวจสอบหรือมาตรการที่ใช้ อาจส่งผลให้ประชาชนขาดความเข้าใจเกี่ยวกับสิทธิในการเข้าถึงข้อมูล และขาดความโปร่งใสในการดำเนินงานของรัฐ

2.4 สิทธิในเสรีภาพและความมั่นคงของบุคคล (Right to Liberty and Security) การใช้มาตรการทางไซเบอร์เพื่อตรวจสอบและเฝ้าระวังการกระทำของบุคคลอาจส่งผลต่อสิทธิในการเสรีภาพและความมั่นคงของบุคคล มาตรการบางอย่างอาจถูกดำเนินการโดยไม่มีการตรวจสอบที่เป็นอิสระ ทำให้เกิดความเสี่ยงต่อการใช้อำนาจอย่างไม่เป็นธรรมและละเมิดสิทธิของบุคคล

2.5 สิทธิในการพิจารณาคดีที่เป็นธรรม (Right to a Fair Trial) ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมภายใต้กฎหมายความมั่นคงทางไซเบอร์อาจถูกใช้ในการดำเนินคดีกับบุคคล โดยไม่มีการป้องกันสิทธิในการพิจารณาคดีที่เป็นธรรม

2.6 สิทธิในการรวมกลุ่มและการสมาคม (Right to Freedom of Assembly and Association) กฎหมายความมั่นคงทางไซเบอร์อาจมีมาตรการที่ละเมิดสิทธิในการรวมกลุ่มและการสมาคมของบุคคลในบริบทของการใช้เทคโนโลยีดิจิทัล

3. แนวทางฐานสิทธิมนุษยชนที่จะใช้สร้างสมดุลในการพัฒนานโยบายและมาตรการทางกฎหมายด้านความมั่นคงทางไซเบอร์ สรุปได้ดังนี้

3.1 หลักการความจำเป็นและได้สัดส่วน (Principle of Necessity and Proportionality) การดำเนินมาตรการควรมีพื้นฐานจากการประเมินความจำเป็นในการป้องกันหรือรับมือกับภัยคุกคามทางไซเบอร์ เพื่อให้มั่นใจว่ามาตรการที่ใช้จะไม่เกินความจำเป็นในการบรรลุวัตถุประสงค์ทางความมั่นคง นอกจากนี้มาตรการควรมีสัดส่วนกับระดับของภัยคุกคามและผลกระทบที่อาจเกิดขึ้น โดยควรเลือกใช้มาตรการที่ส่งผลกระทบต่อสิทธิมนุษยชนให้น้อยที่สุด

3.2 ความโปร่งใสและความรับผิดชอบ (Transparency and Accountability) นโยบายและมาตรการควรมีความโปร่งใส โดยมีการเปิดเผยข้อมูลเกี่ยวกับวัตถุประสงค์ วิธีการและกระบวนการในการดำเนินมาตรการเพื่อให้ประชาชนเข้าใจและสามารถตรวจสอบได้

3.3 การปกป้องสิทธิในความเป็นส่วนตัว (Protection of Privacy) ควรมีการกำหนดข้อกำหนดที่ชัดเจนในการเก็บรวบรวม การจัดเก็บ การใช้ และการแบ่งปันข้อมูลส่วนบุคคล เพื่อป้องกันการเข้าถึงและการใช้ข้อมูลโดยไม่ได้รับอนุญาต และเพื่อคุ้มครองความเป็นส่วนตัวของบุคคล

3.4 เสรีภาพในการแสดงออกและการเข้าถึงข้อมูล (Freedom of Expression and Access to Information) มาตรการควรให้ความเคารพเสรีภาพในการแสดงออก โดยการกำหนดมาตรการที่ไม่ก่อให้เกิดการเซ็นเซอร์หรือจำกัดการเผยแพร่ความคิดเห็นที่ไม่จำเป็น

3.5 การให้ความรู้และการสร้างความตระหนัก (Education and Awareness) การสร้างความตระหนักและการให้ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีการป้องกันตัวเองให้กับประชาชนและองค์กร เพื่อเสริมสร้างความสามารถในการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์

3.6 การสร้างกลไกในการพิจารณาข้อร้องเรียน (Complaint Mechanisms) ควรมีกลไกในการรับเรื่องร้องเรียนจากบุคคลที่เห็นว่ามาตรการด้านความมั่นคงทางไซเบอร์ได้ละเมิดสิทธิมนุษยชนของตน เพื่อให้สามารถตรวจสอบและดำเนินการแก้ไขได้อย่างเป็นธรรม

3.7 การส่งเสริมความร่วมมือระหว่างประเทศ (International Cooperation) ควรส่งเสริมความร่วมมือระหว่างประเทศในการแบ่งปันข้อมูล ประสบการณ์ และแนวทางที่ดีที่สุดในการจัดการกับภัยคุกคามทางไซเบอร์ เพื่อเพิ่มประสิทธิภาพในการป้องกันและรับมือกับภัยคุกคามในระดับโลก ควรมีการพัฒนามาตรฐานสากลที่สอดคล้องกับหลักการสิทธิมนุษยชน เพื่อให้การดำเนินงานด้านความมั่นคงทางไซเบอร์ในทุกประเทศสามารถคุ้มครองสิทธิมนุษยชนได้อย่างเหมาะสม

4. กฎหมาย มาตรฐาน และแนวปฏิบัติในทางระหว่างประเทศที่ได้รับการยอมรับอย่างกว้างขวางในปัจจุบัน ตลอดจนกฎหมายภายในประเทศต่างๆ ที่น่าสนใจเพื่อเปรียบเทียบมาตรการการรักษาความมั่นคงทางไซเบอร์ และมาตรการในการคุ้มครองสิทธิมนุษยชน สรุปได้ดังนี้

กฎหมายของประเทศไทย และสิงคโปร์ มีความใกล้เคียงกันในเรื่องการมุ่งเน้นปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สำหรับประเทศจีน มีการขยายขอบเขตไปถึงการควบคุมการใช้อินเทอร์เน็ตด้วย โดยกฎหมายของทั้งไทย จีน และสิงคโปร์ มีลักษณะเป็นการบังคับให้ต้องปฏิบัติตามบทบัญญัติในกฎหมาย หากไม่ปฏิบัติตามจะมีความผิด และมีโทษแล้วแต่กรณี ในขณะที่กฎหมายของสหรัฐอเมริกา เป็นการสร้างระบบสมัครใจสำหรับการแบ่งปันข้อมูลตัวบ่งชี้ภัยคุกคามทางไซเบอร์ระหว่างหน่วยงานของรัฐ และเอกชน สำหรับแนวบรรทัดฐานของสหประชาชาติ และอาเซียน เป็นแนวบรรทัดฐานที่ไม่มีสภาพบังคับ เน้นให้เกิดระบบสมัครใจที่ประเทศต่าง ๆ จะปฏิบัติร่วมมือกัน ซึ่งหากสามารถทำให้เกิดการยอมรับ นำไปปฏิบัติอย่างกว้างขวาง และต่อเนื่อง อาจพัฒนาไปสู่การเป็นกฎหมายจารีตประเพณีได้ในอนาคต สำหรับสหภาพยุโรปเป็นกฎและระเบียบที่มุ่งเน้นการสร้างขีดความสามารถของประเทศสมาชิกและเพิ่มความร่วมมือระหว่างกันเพื่อให้เกิดการดำเนินการที่มีมาตรฐานเดียวกันทั่วทั้งภูมิภาค

หน่วยงานหรือองค์กรหลักที่ทำหน้าที่ภายใต้กฎหมาย สำหรับสหประชาชาติ และอาเซียนไม่ได้มีหน่วยงานเพื่อกำกับดูแลการปฏิบัติตามแนวบรรทัดฐาน แต่ในการประชุมในระดับต่าง ๆ มีการติดตามความคืบหน้าในการปฏิบัติ หรือการดำเนินการของรัฐสมาชิกว่าได้นำเอาบรรทัดฐานต่าง ๆ

ไปใช้มากน้อยเพียงใด สำหรับสหภาพยุโรปมีกลไกของการบังคับใช้กฎหมายของสหภาพซึ่งแตกต่างจากองค์การระหว่างประเทศของภูมิภาคอื่นๆ อยู่แล้ว และมี ENISA เป็นหน่วยงานหลักในการต่อต้านภัยคุกคามด้านความมั่นคงทางไซเบอร์ สำหรับกฎหมายของประเทศสหรัฐอเมริกา หน่วยงานที่ทำหน้าที่หลักเป็นหน่วยงานที่มีอยู่เดิม เช่น กระทรวงความมั่นคงแห่งมาตุภูมิ กระทรวงกลาโหม สำนักงานข่าวกรองแห่งชาติ เป็นต้น ในขณะที่กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ของประเทศจีน สิงคโปร์ และไทย มีการตั้งหน่วยงาน หรือคณะกรรมการขึ้นใหม่ ทั้งนี้ หน่วยงานของสิงคโปร์ และของไทยมีหน้าที่ และอำนาจที่คล้ายคลึงกัน กล่าวคือ กำหนดหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกำหนดหน้าที่ให้แก่หน่วยงานเหล่านั้น ตลอดจนหน่วยงานกำกับดูแล รวมถึงการวางแนวปฏิบัติและมาตรฐานต่าง ๆ

มาตรการสำคัญของกฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของสหรัฐอเมริกาคือการแบ่งปันข้อมูล โดยเน้นระบบสมัครใจ ไม่ได้กำหนดเป็นหน้าที่ ในขณะที่กฎหมายของจีนมีบทบัญญัติที่ค่อนข้างเข้มงวด และมีการเปิดช่องให้หน่วยงานที่ทำหน้าที่หลัก คือ CAC กำหนดกฎหมายเพิ่มเติมได้ ลักษณะเดียวกับการให้อำนาจคณะกรรมการต่าง ๆ ในกฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของไทยสามารถใช้อำนาจและดุลพินิจกำหนดรายละเอียดและหลักเกณฑ์ในเรื่องต่างๆ ซึ่งทั้งประเทศจีน ไทย และสิงคโปร์ ต่างให้ความสำคัญกับการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศเช่นเดียวกัน โดยมีการกำหนดมาตรฐาน และหน้าที่ให้ผู้รับผิดชอบหน่วยงานเหล่านั้นต้องปฏิบัติตาม

มิติด้านสิทธิมนุษยชนในกฎหมาย บรรทัดฐานความรับผิดชอบของรัฐบนโลกไซเบอร์ของสหประชาชาติ ข้อ 5 เน้นย้ำให้รัฐเคารพข้อมติคณะมนตรีสิทธิมนุษยชนที่ 20/8 และ 26/13 ว่าด้วยการส่งเสริม การคุ้มครอง และการใช้สิทธิมนุษยชนบนอินเทอร์เน็ต เช่นเดียวกับมติสมัชชาใหญ่ที่ 68/167 และ 69/166 ว่าด้วยสิทธิในความเป็นส่วนตัวในยุคดิจิทัล เพื่อรับประกันการเคารพสิทธิมนุษยชนอย่างเต็มที่ สำหรับการให้ความสำคัญด้านสิทธิมนุษยชนของสหภาพยุโรปในกฎหมาย กฎข้อบังคับต่าง ๆ ปรากฏให้เห็นผ่านกลไก และสถาบันด้านสิทธิมนุษยชนของสหภาพยุโรป สำหรับกฎหมายความมั่นคงปลอดภัยไซเบอร์ของสหรัฐอเมริกา จีน สิงคโปร์ และไทย มีการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยกฎหมายของสหรัฐอเมริกากำหนดให้หน่วยงานเอกชนระบุ และลบข้อมูลส่วนบุคคลที่ไม่เกี่ยวข้องโดยตรงกับภัยคุกคามความปลอดภัยทางไซเบอร์ ก่อนที่จะแบ่งปันข้อมูลภายใต้กฎหมาย รวมถึงกำหนดให้มีการพัฒนาขั้นตอนเพื่อระบุ และลบข้อมูลที่ไม่เกี่ยวข้องโดยตรงกับภัยคุกคามความปลอดภัยทางไซเบอร์ที่หน่วยงานของรัฐบาลกลางทราบในขณะที่แบ่งปันข้อมูล ว่าเป็นข้อมูลส่วนบุคคล หรือข้อมูลที่เฉพาะเจาะจง นอกจากนี้ยังมีขั้นตอนการแจ้ง

บุคคลที่ได้รับทราบข้อมูล หรือพิจารณาแล้วว่าถูกแบ่งปันโดยละเมิดกฎหมาย แต่ไม่มีบทกำหนดโทษที่ประกันการเยียวยา กรณีเกิดความผิดพลาดในการจัดการข้อมูลส่วนบุคคล

อนึ่ง กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของทั้ง 4 ประเทศ ยังมีปัญหาคล้ายคลึงกันในเรื่องการมีบทบัญญัติบางส่วนที่มีความกำกวม อาจทำให้เกิดการตีความอย่างกว้างขวางจนกระทบต่อสิทธิมนุษยชน

5. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ในเรื่องความสมดุลของมิติด้านความมั่นคง และมิติด้านสิทธิมนุษยชน เพื่อให้สามารถเสนอแนะแนวทางในการปรับปรุงกฎหมายดังกล่าวให้เกิดความสมดุล สรุปได้ดังนี้

จากการศึกษาพบว่าพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ.2562 เป็นกฎหมายที่มีวัตถุประสงค์หลักมุ่งไปที่การป้องกันความปลอดภัยทางไซเบอร์ของประเทศ และปกป้องโครงสร้างพื้นฐานข้อมูลที่สำคัญจากภัยคุกคามทางไซเบอร์ โดยวางกรอบในลักษณะกว้างๆ โดยให้อำนาจคณะกรรมการต่างๆ ที่ตั้งขึ้นตามพระราชบัญญัติฉบับนี้มีอำนาจในการออกกฎหมายลำดับรองเพื่อกำหนดรายละเอียดของหลักเกณฑ์ ประมวลแนวทางปฏิบัติ กรอบมาตรฐานต่างๆ ตลอดจนประเภทของภัยคุกคาม และระดับของภัยคุกคาม ซึ่งทำให้พระราชบัญญัติที่ประกาศใช้มีลักษณะเป็นบทบัญญัติที่ไม่ชัดเจน มีถ้อยคำที่ตีความได้อย่างกว้างขวาง และเปิดโอกาสให้คณะกรรมการต่าง ๆ ใช้ดุลพินิจมากเกินไป การตั้งคณะกรรมการหลายชุดที่อาจมีการทำงานที่ซ้ำซ้อน และมีอำนาจมาก การกำหนดหลักเกณฑ์ ประมวลแนวปฏิบัติ กรอบมาตรฐาน ประเภท และระดับภัยคุกคาม ไม่ผ่านการรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียอย่างกว้างขวาง ทำให้ขาดการตรวจสอบ ถ่วงดุล แม้กฎหมายจะมีเจตนารมณ์ที่ดีในการป้องกัน และแก้ปัญหาภัยคุกคามทางไซเบอร์ แต่กฎหมายมุ่งไปที่ประเด็นด้านความมั่นคงเป็นหลัก โดยยังไม่ได้ให้ความสำคัญด้านสิทธิมนุษยชน การปกป้องสิทธิขั้นพื้นฐาน และการมีส่วนร่วมของประชาชนเท่าที่ควรจะเป็น

กฎหมายฉบับนี้มีบทกำหนดโทษในกรณีที่พนักงานเจ้าหน้าที่จงใจ หรือประมาทเลินเล่อในการเปิดเผยข้อมูลหรือทำให้ผู้อื่นล่วงรู้ข้อมูลที่ได้จากการปฏิบัติหน้าที่ แต่ไม่มีบทบัญญัติที่ประกันการเยียวยาความเสียหายในกรณีอื่นๆ หากการใช้ดุลพินิจ หรือการปฏิบัติงานของพนักงานเจ้าหน้าที่ก่อให้เกิดความเสียหายทั้งต่อความเป็นส่วนตัว ทรัพย์สิน หรือสิทธิมนุษยชนด้านอื่นๆ จะได้รับการคุ้มครอง หรือให้การช่วยเหลือเยียวยาอย่างไร อีกทั้งยังมีปัญหาเกี่ยวกับการอุทธรณ์คำสั่งในกรณีภัยคุกคามทางไซเบอร์ในระดับร้ายแรงและระดับวิกฤติ ตามที่บัญญัติไว้ในมาตรา 69 ให้ผู้ได้รับคำสั่งเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ อาจอุทธรณ์คำสั่งได้เฉพาะที่เป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงเท่านั้น ซึ่งการดำเนินการรับมือภัยคุกคามทางไซเบอร์ในระดับร้ายแรงหลายมาตรา ขาดพยานหลักฐานที่ชัดเจนเพียงพอในการจำกัดสิทธิเสรีภาพส่วนบุคคล เช่น

มาตรา 66 การให้ กกม. มีอำนาจปฏิบัติการ หรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ โดยเข้าไปตรวจสอบสถานที่ เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทดสอบการทำงานของคอมพิวเตอร์ ยึด หรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใดๆ แม้ว่าจะให้ยื่นคำร้องต่อศาลเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการ แต่ใน (1) ซึ่งเป็นการเข้าตรวจสอบสถานที่ ไม่อยู่ในบังคับที่จะต้องยื่นคำร้องต่อศาลก่อนการปฏิบัติ ไม่ได้กำหนดให้มีหมายค้น เพียงให้มีหนังสือแจ้งเหตุอันสมควรไปยังเจ้าของ หรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น ทำให้เห็นว่าสัดส่วนของมิติด้านสิทธิมนุษยชนมีน้ำหนักน้อยมากในกฎหมายฉบับนี้ เมื่อเทียบกับมิติด้านความมั่นคง

อภิปรายผล

จากการศึกษาพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และการสร้างสมดุลระหว่างความมั่นคงปลอดภัยไซเบอร์กับการคุ้มครองสิทธิมนุษยชน สามารถอภิปรายผลการวิจัยได้ในประเด็นต่าง ๆ ดังนี้

1. ภัยคุกคามทางไซเบอร์เป็นภัยอันตรายที่ส่งผลกระทบต่อระบบคอมพิวเตอร์ เครือข่ายและข้อมูล ซึ่งอาจสร้างความเสียหายได้ตั้งแต่ระดับบุคคลไปจนถึงระดับประเทศ โครงสร้างพื้นฐานที่สำคัญทางสารสนเทศมีความเสี่ยงสูงต่อการถูกโจมตีทางไซเบอร์ ซึ่งอาจส่งผลกระทบต่อความมั่นคงของประเทศในด้านต่าง ๆ เหตุการณ์ไม่พึงประสงค์ทางไซเบอร์ที่เกิดขึ้นทั่วโลกแสดงให้เห็นถึงความเสียหายร้ายแรงที่อาจเกิดขึ้นจากภัยคุกคามเหล่านี้ เป็นเหตุให้ประเทศต่าง ๆ มีความตื่นตัวในการพัฒนากฎหมายและมาตรการ รวมถึงความร่วมมือระหว่างประเทศเพื่อรับมือกับภัยคุกคามทางไซเบอร์ การดำเนินการเหล่านี้มีจุดมุ่งหมายเพื่อเสริมสร้างสันติภาพ ความมั่นคง และความไว้วางใจในโลกไซเบอร์ นอกจากนี้ ยังมีการพัฒนาบรรทัดฐานและแนวปฏิบัติเพื่อส่งเสริมพฤติกรรมที่มีความรับผิดชอบของรัฐในโลกไซเบอร์อีกด้วย

2. กฎหมายว่าด้วยความมั่นคงทางไซเบอร์ แม้จะมีจุดมุ่งหมายเพื่อปกป้องความมั่นคงของรัฐและระบบ แต่ก็อาจมีผลกระทบต่อสิทธิมนุษยชนในหลายด้าน ได้แก่ สิทธิในความเป็นส่วนตัว เสรีภาพในการแสดงออก สิทธิในการเข้าถึงข้อมูล สิทธิในเสรีภาพและความมั่นคงของบุคคล สิทธิในการพิจารณาคดีที่เป็นธรรม สิทธิในการรวมกลุ่มและการสมาคม ประเด็นสำคัญคือ กฎหมายความมั่นคงทางไซเบอร์เป็นดาบสองคม ในขณะที่สามารถใช้เพื่อปกป้องสิทธิมนุษยชนจากภัยคุกคามไซเบอร์ แต่ก็อาจถูกนำมาใช้เพื่อละเมิดสิทธิมนุษยชนได้เช่นกัน ปัญหานี้มักเกิดขึ้นเมื่อผู้มี

อำนาจให้ความสำคัญกับความมั่นคงของรัฐมากกว่าสิทธิของประชาชน และไม่ได้คำนึงถึงผลกระทบที่อาจเกิดขึ้นกับบุคคล ดังนั้น การออกแบบและบังคับใช้กฎหมายความมั่นคงทางไซเบอร์จึงควรคำนึงถึงสมดุลระหว่างความมั่นคงและสิทธิมนุษยชนอย่างรอบคอบ การรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสีย และการสร้างความโปร่งใสในการดำเนินงานของรัฐ จะช่วยให้กฎหมายได้รับการยอมรับและมีประสิทธิภาพในการปกป้องทั้งความมั่นคงและสิทธิเสรีภาพของประชาชน

3. แนวทางฐานสิทธิมนุษยชนเพื่อความมั่นคงปลอดภัยไซเบอร์ จะทำให้การคุ้มครองสิทธิมนุษยชนเป็นแกนหลักของนโยบาย และแนวปฏิบัติด้านความปลอดภัยทางไซเบอร์ โดยตระหนักดีว่าปัจเจกบุคคลมีสิทธิโดยกำเนิดทั้งแบบออฟไลน์ และออนไลน์ และสิทธิเหล่านี้ควรได้รับการเคารพ ปกป้อง และปฏิบัติตามในบริบทของมาตรการรักษาความปลอดภัยทางไซเบอร์ แนวทางนี้รับทราบถึงสิทธิขั้นพื้นฐานในความเป็นส่วนตัว และการปกป้องข้อมูลซึ่งความเป็นส่วนตัวเป็นสิทธิมนุษยชนขั้นพื้นฐานที่ต้องได้รับการคุ้มครองในโลกไซเบอร์ เสรีภาพในการแสดงออก ทำให้บุคคลสามารถแสดงความคิดเห็น และเข้าถึงข้อมูลได้ ซึ่งมาตรการความปลอดภัยทางไซเบอร์ต้องไม่ทำให้เกิดการจำกัดเสรีภาพในการแสดงออก และต้องมีกระบวนการที่โปร่งใส และรับผิดชอบกระบวนการอันชอบธรรม และการกำกับดูแลของฝ่ายตุลาการ รวมถึงการไม่เลือกปฏิบัติต่อกลุ่มใดกลุ่มหนึ่งอย่างไม่เหมาะสม เพื่อให้มั่นใจว่าทุกคนได้รับการปฏิบัติอย่างเท่าเทียมกัน และเป็นธรรม

4. การรักษาความมั่นคงปลอดภัยไซเบอร์เปรียบเทียบกฎหมายไทยกับแนวบรรทัดฐานระหว่างประเทศและกฎหมายต่างประเทศในด้านต่าง ๆ กฎหมายของประเทศไทยและสิงคโปร์เน้นการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure, CII) ซึ่งกฎหมายของไทย จีน และสิงคโปร์มีสภาพบังคับ ซึ่งถ้าไม่ปฏิบัติตามจะมีบทลงโทษที่แตกต่างกันออกไป โดยที่กฎหมายของจีนขยายขอบเขตไปถึงการควบคุมการใช้อินเทอร์เน็ตด้วย แต่กฎหมายของสหรัฐอเมริกาเน้นการสร้างระบบสมัครใจในการแบ่งปันข้อมูลภัยคุกคามไซเบอร์ระหว่างหน่วยงานรัฐและเอกชน โดยไม่มีบทลงโทษที่บังคับใช้ สำหรับแนวบรรทัดฐานของสหประชาชาติและอาเซียนเป็นระบบสมัครใจไม่มีสภาพบังคับ เน้นการร่วมมือกันอย่างสมัครใจ ซึ่งต่างจากสหภาพยุโรปที่มีระบบกฎหมายและระเบียบที่มุ่งเน้นการสร้างขีดความสามารถของสมาชิกและความร่วมมือระหว่างประเทศสมาชิกเพื่อมาตรฐานเดียวกันทั่วภูมิภาค

มาตรการที่สำคัญในการใช้รักษาความมั่นคงปลอดภัยทางไซเบอร์ กฎหมายของจีน ไทย และสิงคโปร์เน้นการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยมีการกำหนดมาตรฐานและหน้าที่ให้ผู้รับผิดชอบหน่วยงานเหล่านั้นต้องปฏิบัติตาม ซึ่งทั้งประเทศจีนและไทยมีระบบการแบ่งระดับภัยคุกคามที่กำหนดให้หน่วยงานสามารถใช้อำนาจและดุลพินิจกำหนดรายละเอียดต่าง ๆ ได้ และจีนมีกฎหมายที่เข้มงวดและเปิดช่องให้หน่วยงาน CAC สามารถกำหนดกฎหมายเพิ่มเติมได้

การเปรียบเทียบนี้แสดงให้เห็นว่ากฎหมายความมั่นคงปลอดภัยไซเบอร์ในแต่ละประเทศมีความแตกต่างกันในแง่ของวัตถุประสงค์ หน่วยงานหลัก มาตรการสำคัญ และการคุ้มครองสิทธิมนุษยชน ซึ่งสะท้อนถึงบริบททางสังคม การเมือง และความต้องการด้านความมั่นคงที่แตกต่างกันในแต่ละประเทศ

5. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ในเรื่องความสมดุลของมิติด้านความมั่นคง และมิติด้านสิทธิมนุษยชน มีบทบัญญัติหลายส่วนที่ขาดการคำนึงถึงสิทธิมนุษยชน และมุ่งเน้นด้านความมั่นคง ทำให้ข้อเสนอแนะในการปรับปรุงแก้ไขต้องนำแนวทางฐานสิทธิมนุษยชนเพื่อความมั่นคงปลอดภัยทางไซเบอร์ (Human Rights-Based Approach to Cybersecurity) มาเป็นกรอบในการปรับปรุงกฎหมาย โดยบทบัญญัติที่ควรเร่งปรับปรุงแก้ไขในพระราชบัญญัติฉบับนี้หลัก ๆ 6 ประการ ดังต่อไปนี้

5.1 การให้นิยามที่ชัดเจนของคำสำคัญเพื่อการบังคับใช้กฎหมายอย่างมีประสิทธิภาพ และหลีกเลี่ยงการตีความที่กว้างขวางโดยเจ้าหน้าที่ผู้ปฏิบัติ โดยในมาตรา 3 มีคำสำคัญหลายคำที่ควรต้องปรับปรุง เช่น “การรักษาความมั่นคงปลอดภัยไซเบอร์” ซึ่งมิได้ให้ความหมาย หรือขยายความ คำว่า ความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ ว่าหมายถึงสิ่งใดบ้าง “ภัยคุกคามทางไซเบอร์” ที่ให้ความหมายขยายไปถึง “ข้อมูลอื่นที่เกี่ยวข้อง” นอกเหนือจากความเสียหายที่เกิดกับการทำงานของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ ซึ่ง “ข้อมูลอื่นที่เกี่ยวข้อง” เป็นข้อความที่กว้าง และไม่สามารถระบุได้ว่าข้อมูลอย่างไรบ้างที่จัดว่าเกี่ยวข้อง ดังนั้น ควรตัดถ้อยคำที่กำกวมออก และเปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียทุกกลุ่มเข้าไปมีส่วนร่วมในการพิจารณากำหนดรายละเอียดภัยคุกคามรวมถึงมาตรการต่าง ๆ เพื่อหลีกเลี่ยงโอกาสที่จะทำให้เกิดการละเมิดสิทธิมนุษยชน

5.2 การใช้ดุลพินิจในกฎหมายต้องสอดคล้องกับพระราชบัญญัติหลักเกณฑ์การจัดทำร่างกฎหมาย และการประเมินผลสัมฤทธิ์ของกฎหมาย พ.ศ. 2562 เนื่องด้วยการใช้อำนาจของเจ้าหน้าที่ของรัฐมีที่มาจากบทบัญญัติของกฎหมายเป็นพื้นฐานสำคัญ เมื่อใดที่กฎหมายที่ให้อำนาจแก่เจ้าหน้าที่ของรัฐโดยมิได้กำหนดองค์ประกอบ หรือเงื่อนไขการใช้อำนาจไว้อย่างชัดเจนแล้ว ในการบังคับใช้กฎหมายย่อมจะทำให้เจ้าหน้าที่ของรัฐมีดุลพินิจในการใช้อำนาจในเรื่องนั้น ๆ ดังนั้น ดุลพินิจของเจ้าหน้าที่ของรัฐจึงเกิดขึ้นจากการที่ตัวบทกฎหมายเปิดโอกาสให้เจ้าหน้าที่ของรัฐ ใช้กฎหมายได้อย่างยืดหยุ่น และสอดคล้องกับข้อเท็จจริงเป็นการเฉพาะเรื่องเฉพาะราย เพื่อมิให้การใช้บทบัญญัติของกฎหมายแข็งกระด้าง และเพื่อมุ่งหมายให้เกิดความยุติธรรมขึ้นแก่เฉพาะเรื่องเฉพาะรายนั้นๆ ทั้งนี้ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 มี

บทบัญญัติจำนวนมากที่เปิดช่องให้คณะกรรมการคณะต่างๆ ในกฎหมาย เลขาธิการฯ ตลอดจนพนักงานเจ้าหน้าที่ใช้ดุลพินิจ

5.3 กรณีที่กฎหมายบัญญัติให้เป็นการขอความร่วมมือ ไม่ควรมีโทษทางอาญา โดยในมาตรา 61 (1) บัญญัติว่า เมื่อปรากฏแก่ กกม. ว่าเกิด หรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ กกม. ออกคำสั่งให้สำนักงานดำเนินการรวบรวมข้อมูล หรือพยานเอกสาร พยานบุคคล พยานวัตถุที่เกี่ยวข้องเพื่อวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคาม และมาตรา 62 (1) และ (2) บัญญัติว่า ในการดำเนินการตามมาตรา 61 เพื่อประโยชน์ในการวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ ให้เลขาธิการสั่งให้พนักงานเจ้าหน้าที่ดำเนินการมีหนังสือขอความร่วมมือจากบุคคลที่เกี่ยวข้องเพื่อมาให้ข้อมูลภายในระยะเวลาที่เหมาะสม และตามสถานที่ที่กำหนด หรือให้ข้อมูลเป็นหนังสือเกี่ยวกับภัยคุกคามทางไซเบอร์ และมีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูล หรือเอกสารซึ่งอยู่ในความครอบครองของผู้อื่นอันเป็นประโยชน์แก่การดำเนินการ ดังจะเห็นได้ว่าบทบัญญัติของกฎหมายให้เลขาธิการมีหนังสือขอความร่วมมือจากบุคคลที่เกี่ยวข้องมาให้ข้อมูล โดยในมาตรา 74 มีการกำหนดโทษของผู้ที่ไม่ปฏิบัติตามหนังสือเรียกของพนักงานเจ้าหน้าที่ หรือไม่ส่งข้อมูลให้แก่พนักงานเจ้าหน้าที่ตามมาตรา 62 (1) หรือ (2) โดยไม่มีเหตุอันสมควรแล้วแต่กรณี ต้องระวางโทษปรับไม่เกิน 100,000 บาท ซึ่งบทบัญญัติในมาตรา 62 (1) เป็นการทำหนังสือขอความร่วมมือ จึงไม่ควรถูกลงโทษทางอาญาเป็นค่าปรับสูงถึง 100,000 บาท กรณีหากจะบังคับให้ต้องปฏิบัติตาม ควรบัญญัติให้เป็นคำสั่งเรียกให้บุคคลที่เกี่ยวข้องมาให้ข้อมูลโดยระบุเหตุผลความจำเป็นเพื่อประโยชน์แก่การดำเนินการวิเคราะห์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง เพื่อไม่ให้เป็นการละเมิดสิทธิของบุคคลโดยไม่จำเป็น

5.4 การเข้าตรวจสอบสถานที่โดยไม่มีหมายค้น โดยในมาตรา 66(1) กำหนดให้พนักงานเจ้าหน้าที่โดยคำสั่งของ กกม. เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของ หรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่ โดยมีข้อสังเกตคือ การเข้าตรวจสอบสถานที่ตามมาตรานี้ มีลักษณะเดียวกับการค้นตามประมวลกฎหมายวิธีพิจารณาความอาญาหรือไม่ หากเป็นการเข้าไปในที่รโหฐานซึ่งมิใช่สถานที่ราชการ แต่เป็นสถานที่ของเอกชน ควรบัญญัติให้สอดคล้องกับกฎหมายวิธีพิจารณาความอาญา ซึ่งประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92 วรรคหนึ่ง ห้ามมิให้ค้นในที่รโหฐานโดยไม่มีหมายค้น หรือคำสั่งศาล เว้นแต่พนักงานฝ่ายปกครอง หรือตำรวจเป็นผู้ค้น ในกรณีตาม (1)–(5) นอกจากนั้นเพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 66 (2) (3) และ (4) ซึ่งกำหนดให้ กกม. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้อง

ต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำ หรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง รวมถึงเพื่อให้ได้สัดส่วนกับบทกำหนดโทษในมาตรา

ซึ่งโทษที่จะลงแก่ผู้ไม่ปฏิบัติตามคำสั่งของ กกม. หรือพนักงานเจ้าหน้าที่ซึ่งปฏิบัติตามคำสั่งของ กกม. ตามมาตรา 66 (1) บัญญัติไว้เท่ากันกับโทษของการไม่ปฏิบัติตามคำสั่งศาลตามมาตรา 66 (2) (3) และ (4) ดังนั้น การใช้อำนาจของ กกม. ในมาตรา 66 (1) จึงควรได้รับการตรวจสอบถ่วงดุลโดยศาลด้วย อันจะเป็นการสร้างหลักประกันความยุติธรรมให้แก่ประชาชนอีกชั้นหนึ่ง และเป็นการคุ้มครองสิทธิความเป็นส่วนตัว มิให้ถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร โดยต้องได้รับการคุ้มครองของกฎหมายจากการแทรกแซงสิทธิดังกล่าว

5.5 ปัญหาการอุทธรณ์คำสั่งในกรณีภัยคุกคามทางไซเบอร์ระดับร้ายแรง และระดับวิกฤติ ซึ่งบัญญัติไว้ในมาตรา 69 ควรแก้ไขเป็น “ผู้ที่ได้รับคำสั่งอันเกี่ยวกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่งต่อรัฐมนตรีได้” เพื่อเป็นหลักประกันความชอบด้วยกฎหมาย และให้สิทธิผู้ได้รับคำสั่งสามารถโต้แย้งคำสั่งทางปกครองนั้น ดังเช่นกฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ของประเทศสิงคโปร์ที่กฎหมายเปิดช่องให้ผู้ที่ได้รับคำสั่งจากผู้บัญชาการความปลอดภัยทางไซเบอร์ให้กระทำการใด ๆ สามารถอุทธรณ์คำสั่งไปยังรัฐมนตรีได้

5.6 การเพิ่มบทบัญญัติที่มีการประกันการเยียวยา และการชดเชยความเสียหายจากการดำเนินการของพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ซึ่งประเด็นนี้เป็นประการสำคัญที่ขาดหายไปจากพระราชบัญญัติฉบับนี้ ด้วยเหตุการณ์ภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ อาจเป็นกรณีเร่งด่วน และไม่อาจรอให้เนิ่นช้า หากเกิดการโจมตี หรือภัยคุกคามขึ้นจริง ก็อาจส่งผลให้เกิดความเสียหายอย่างร้ายแรงเป็นวงกว้าง และยากต่อการกู้คืนมาได้ หากมีกรณีใดที่กฎหมายไม่อาจใช้วิธีการตรวจสอบถ่วงดุลโดยศาล หรือใช้วิธีขอความร่วมมือได้ อันเนื่องมาจากเหตุจำเป็นเร่งด่วนอย่างแท้จริง ก็อาจให้มีการดำเนินการเพื่อป้องกันสถานการณ์ โดยต้องมีบทบัญญัติขึ้นมารองรับความเสียหายที่อาจเกิดขึ้นต่อสิทธิเสรีภาพของบุคคล การเยียวยาความเสียหายจากผลกระทบที่อาจเกิดขึ้นจากการดำเนินการดังกล่าว นอกจากจะต้องรายงานการดำเนินการต่อศาลแล้ว ยังต้องมีการประกันการเยียวยาให้แก่ผู้ได้รับความเสียหาย รวมถึงต้องกำหนดความรับผิดของเจ้าหน้าที่ในกรณีอื่นที่มีการกระทำเกินกว่าเหตุ หรือประมาทเลินเล่อให้เกิดความเสียหาย หรือละเมิดสิทธิของบุคคลเกินจำเป็นด้วย

องค์ความรู้ที่ได้จากการศึกษา

จากการศึกษาพบว่าการสร้างสมดุลระหว่างความมั่นคงปลอดภัยไซเบอร์ และสิทธิมนุษยชนมีความสำคัญอย่างยิ่งในภูมิทัศน์ดิจิทัลในปัจจุบัน โดยการให้ความสำคัญกับการปกป้องทั้งความปลอดภัยในโลกไซเบอร์ และสิทธิมนุษยชน ทำให้มั่นใจว่ามาตรการที่นำมาใช้นั้นมีสัดส่วน โปร่งใส และเคารพในความเป็นส่วนตัว การยอมรับแนวทางนี้ รัฐบาล และองค์กรต่าง ๆ สามารถสร้างสมดุลที่เหมาะสมในการปกป้องสิทธิส่วนบุคคลในขณะที่ต่อสู้กับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ ท้ายที่สุดแล้ว การส่งเสริมสิทธิมนุษยชนในขอบเขตของความปลอดภัยในโลกไซเบอร์นั้นเป็นสิ่งจำเป็นในการเสริมสร้างความไว้วางใจ รักษาคุณค่าทางประชาธิปไตย และส่งเสริมสภาพแวดล้อมดิจิทัลที่ปลอดภัย และครอบคลุม ทำให้เห็นว่าความปลอดภัย และสิทธิมนุษยชนไม่ได้ถูกแยกออกจากกัน แต่สามารถส่งเสริมซึ่งกันและกันได้

เอกสารอ้างอิง

กระทรวงการต่างประเทศ. *ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน* - Universal Declaration of Human Rights. สืบค้นเมื่อ 16 พฤษภาคม 2565 จาก https://shorturl.asia/lyueE

คณะทำงานศึกษา และยกร่างหลักเกณฑ์เกี่ยวกับการใช้ดุลพินิจของเจ้าหน้าที่ของรัฐ สำนักงานคณะกรรมการกฤษฎีกา. *ความเบื้องต้นเกี่ยวกับการใช้ดุลพินิจของเจ้าหน้าที่ของรัฐ*. สืบค้นเมื่อ 31 สิงหาคม 2565 จาก https://shorturl.asia/o2ndU

ราชกิจจานุเบกษา. *ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงาน หรือองค์กร หรือส่วนงานของหน่วยงาน หรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559*. สืบค้นเมื่อ 19 พฤษภาคม 2565 จาก https://shorturl.asia/rOJ94

ราชกิจจานุเบกษา. *พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562*. สืบค้นเมื่อ 27 พฤษภาคม 2562 จาก https://shorturl.asia/ob73S

Cyber Security Agency of Singapore. *Cybersecurity Act*. Retrieved May, 31, 2022, from : https://shorturl.asia/W14GN

European Parliament. *LEGISLATIVE TRAIN SCHEDULE: EU CYBERSECURITY AGENCY AND THE CYBERSECURITY ACT*. Retrieved May, 19, 2019, from : https://shorturl.asia/XOaWA

Freedom Online Coalition. *Recommendations for human rights based approaches to cybersecurity*. Retrieved May, 22, 2019, from : https://shorturl.asia/ZxoWb

Jacqueline Van De Velde. *The Law of Cyber Interference in Elections*. Retrieved February, 11, 2019, from : https://shorturl.asia/4JLGv

National People's Congress of the People's Republic of China. *中华人民共和国网络安全法 (The People's Republic of China Cyber Security Law)*. Retrieved May, 19, 2019, from : https://shorturl.asia/2hG0Z

UNDP. *Indicators for Human Rights Based Approaches to Development in UNDP Programming: A Users' Guide 2006*. Retrieved May, 29, 2019, from : https://shorturl.asia/xHhBE.

United Nations. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved March, 25, 2021, from : https://undocs.org/A/70/174.

United Nations Development Programme: UNDP. *Indicators for Human Rights Based Approaches to Development in UNDP Programming: A Users' Guide 2006*. Retrieved May, 29, 2019, from : https://shorturl.asia/w8n4m