ปัญหาทางกฎหมายตามพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562[1]

สุมิตร สีหาฤทธิ์[2]

การเปลี่ยนผ่านจากยุคหนึ่งสู่อีกยุคหนึ่งนั้นมีจุดหมายที่มีนัยยะสำคัญเป็นของตัวมันเอง ปัจจุบันมนุษย์เราสามารถเชื่อมโยงกับผู้คน สังคม และระบบโครงสร้างพื้นฐานของประเทศได้อย่างสะดวก ง่ายดาย และรวดเร็วขึ้นกว่าแต่ก่อนมาก เช่น การส่งผ่านข้อความ เสียงสนทนาพร้อมใบหน้า หรือติดตามข่าวสารผ่านทางการใช้งานแอปพลิเคชั่นด้าน Social Network ต่าง ๆ ได้อย่างไร้ขอบเขต เราไม่ต้องเสียเวลาไปทำธุรกรรมทางการเงินที่ธนาคาร เนื่องจากสามารถสั่งดำเนินการผ่านแอปพลิเคชั่นด้าน Internet Banking ได้อย่างสะดวกและรวดเร็ว เราไม่ต้องเดินทางไปสั่งอาหาร รอคิวร้านค้าหรือออกไปยืนรอรถแท็กซี่ เพราะเราสามารถดำเนินการผ่านแอปพลิเคชั่นด้านโลจิสติกส์ต่าง ๆ ได้อย่างไร้ข้อจำกัด บริบทของรูปแบบการดำเนินชีวิตที่เปลี่ยนไปในภาคประชาชนเช่นนี้ สะท้อนให้เห็นได้ว่ากลไกที่ถูกวางบทบาทไว้เติมเต็มช่องว่างระหว่างยุคสมัย เพื่อก่อให้เกิดการเชื่อมโยงระหว่างกันและกันที่เรียกว่า ระบบดิจิทัล (Digital system) ซึ่งระบบดิจิทัลนี้ได้เข้ามาพลิกโฉมรูปแบบการดำเนินชีวิตของผู้คน และเข้ามามีบทบาทร่วมกับการใช้ชีวิตประจำวันของเรามากขึ้นอย่างเห็นได้ชัดในช่วงระยะเวลาไม่กี่ปีที่ผ่านมา โยทั้งภาครัฐและภาคเอกชนต่างก็นำระบบดิจิทัลมาใช้เพื่อเดินหน้าปรับปรุงโครงสร้างองค์กรของตนเองอย่างต่อเนื่อง เพื่อเป็นกลไกหนึ่งที่สำคัญในการดำเนินงานก่อให้เกิดการปรับปรุงมาตรฐานด้านการบริการและการใช้งานที่ดีขึ้นสะดวกสบายขึ้น เป็นการเตรียมความพร้อมที่จะรองรับ

ประเทศไทยเป็นประเทศหนึ่งที่มีการพัฒนาของระบบดิจิทัลและเทคโนโลยีอย่างก้าวกระโดด ซึ่งสามารถสังเกตได้จากปริมาณการใช้อินเตอร์เน็ตที่เพิ่มขึ้นอย่างเป็นนัยสำคัญภายใน 2-3 ปีที่ผ่านมา ทำให้ประเทศก้าวสู่ยุค 4.0 ได้อย่างเต็มรูปแบบจึงจำเป็นที่จะต้องทำความเข้าใจและร่วมกันพัฒนาการรักษาความมั่นคงปลอดภัยของโลกไซเบอร์ไปพร้อม ๆ กับการพัฒนาประเทศ เนื่องมาจากระบบไซเบอร์ (Cyber) เป็นการสื่อสารด้วยระบบอินเทอร์เน็ตที่สร้างประโยชน์ในการติดต่อสื่อสารที่สะดวก รวดเร็ว และแม่นยำ ก่อให้เกิดการสร้างประสิทธิภาพของการทำงานทางธุรกิจ การพัฒนาประเทศ และการสร้างคุณภาพชีวิตที่ดีของประชาชน แต่ปัจจุบันกลับพบว่าภัยคุกคามทางไซเบอร์มีจำนวนที่เพิ่มสูงขึ้นและทวีความรุนแรงขึ้นตามลำดับ ส่งผลกระทบและสร้างความเสียหาย ทั้งต่อระดับปัจเจกชนและระดับประเทศ ซึ่งนานาประเทศ

---

[1]บทความนี้เรียบเรียงจากการศึกษาอิสระ เรื่อง ปัญหาทางกฎหมายตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีอาจารย์ที่ปรึกษา คือ รองศาสตราจารย์ ดร.ณฐ สันตาสว่าง และคณะกรรมการสอบ คือ รองศาสตราจารย์จุฑามาศ นิศารัตน์ และรองศาสตราจารย์ประเทือง ธนิยผล

[2]นักศึกษาปริญญาโท หลักสูตรนิติศาสตร์มหาบัณฑิต (วิทยาเขตบางนา) คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง

ต่างให้ความสำคัญในการดำเนินงานเพื่อรับมือกับปัญหาภัยคุกคามดังกล่าวอย่างมาก ประเทศไทยเป็นประเทศหนึ่งที่ถูกภัยคุกคามทางไซเบอร์เล่นงาน และถูกคุกคามทางไซเบอร์เป็นจำนวนมากในแต่ละปี คิดเป็นอันดับสองในอาเซียน รองจากอินโดนีเซีย โดยเฉพาะเว็บไซต์หน่วยงานภาครัฐซึ่งโดนโจมตีมากที่สุด เนื่องจากขาดการเฝ้าระวังและขาดแคลนบุคลากรในการปฏิบัติงานด้านรักษาความปลอดภัยในส่วนนี้

แต่รัฐบาลไทยก็ไม่ได้นิ่งนอนใจกับปัญหานี้ โดยให้ความสำคัญและกำหนดมาตรการการรักษาความมั่นคงปลอดภัยด้านไซเบอร์อย่างมากพร้อมมาตรการด้านกฎหมาย และกำหนดประเด็นยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขันภายใต้หัวข้ออุตสาหกรรมความมั่นคงของประเทศ โดยการสร้างอุตสาหกรรมที่ส่งเสริมความมั่นคงปลอดภัยไซเบอร์ เพื่อลดผลกระทบจากภัยคุกคามไซเบอร์ต่อเศรษฐกิจและสังคมและปกป้องอธิปไตยทางไซเบอร์ เพื่อรักษาผลประโยชน์ของชาติจากการทำธุรกิจดิจิทัล จึงได้มีการบัญญัติพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 โดยการนำเสนอร่างของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อกำหนดหลักเกณฑ์ แนวทางและมาตรการต่าง ๆ ที่เกี่ยวข้องอย่างเป็นรูปธรรม ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุมคามทางไซเบอร์ ซึ่งมีการประสานความร่วมมือระหว่างผู้เกี่ยวข้อง พัฒนาความรู้ความสามารถของบุคลากร และผู้เชี่ยวชาญ รวมถึงการให้ความรู้และความตระหนักถึงภัยไซเบอร์อีกด้วย ซึ่งกฎหมายฉบับนี้ถูกบังคับใช้กับหน่วยงานของรัฐหรือหน่วยงานเอกชนซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศรวมทั้งสิ้น 8 กลุ่ม ได้แก่ ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุข และด้านอื่น ๆ ตามที่คณะกรรมการฯ ประกาศกำหนดเพิ่มเติม

จากการศึกษาพระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ 2562 เพื่อเป็นแนวทางในการจัดการ การป้องกัน การรับมือ และการลดความเสี่ยงทางไซเบอร์ โดยศึกษาตั้งแต่ความเป็นมาและความสำคัญ และทฤษฎีเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ผู้ศึกษาเล็งเห็นช่องโหว่ของกฎหมายบางประการที่จำเป็นต้องมีศึกษา และแก้ไขปรับปรุงเพื่อให้เหมาะสมกับสภาพการณ์ในปัจจุบันให้มากขึ้นอย่างเช่นปัญหาดังต่อไปนี้

ประเด็นที่หนึ่งปัญหาเกี่ยวกับความหมายของ “ภัยคุกคามไซเบอร์”

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 บัญญัติคำนิยามไว้ในมาตรา 3 ว่า “ภัยคุกคามไซเบอร์” คือ “การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง”

เมื่อพิจารณาตามบทนิยามดังกล่าวนี้ จะเห็นได้ว่ากฎหมายได้ให้ความหมายที่กว้างเกินไป จากตัวบทบัญญัติมุ่งเกี่ยวกับการโจมตีระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องเป็นหลัก โดยตีความหมายที่กว้างรวมไปถึงในส่วนของอุปกรณ์คอมพิวเตอร์ แต่เนื่องจากบทนิยามดังกล่าวใช้คำว่า

การกระทำหรือการดำเนินการใด ๆ ทำให้ผู้ใช้กฎหมายสามารถตีความหมายได้กว้าง ซึ่งเป็นการตีกรอบให้คำว่าภัยคุกคามไซเบอร์มีความหมายที่บ่งบอกไปถึงเนื้อหาในระบบออนไลน์ไปด้วยขึ้นอยู่กับเจตนารมณ์การตีความของผู้ใช้กฎหมายนั้น ๆ ซึ่งกฎหมายให้อำนาจคณะกรรมการมั่นคงปลอดภัยไซเบอร์ในการพิจารณาตีความโดยใช้ดุลพินิจ ซึ่งอาจทำให้เนื้อหาบนโลกออนไลน์อาจกลายเป็นความผิดได้ เช่น การแสดงความคิดเห็นในการวิพากษ์วิจารณ์การทำงานรัฐบาล หรือวิจารณ์ศาลรัฐธรรมนูญ เนื่องจากถือเป็นการกระทำหรือการดำเนินการใด ๆ ดังที่บัญญัติไว้ในมาตรา 3 นี้ ซึ่งเป็นการปิดกั้นความคิดเห็นของประชาชนโดยการใช้กฎหมายเป็นเครื่องมือเพื่อเอาผิดก็ได้ ดังนั้นแล้วการเขียนกฎหมายในลักษณะเช่นนี้มีความเสี่ยงที่ในอนาคตอาจมีผู้เจตนาไม่ดีใช้กฎหมายเป็นเครื่องมือตีความคำว่า “ภัยคุกคามไซเบอร์” ครอบคลุมถึงประเด็น “เนื้อหา” บนโลกออนไลน์มากกว่าเรื่องระบบ ข้อมูล โปรแกรมดังเจตนารมณ์แห่งพระราชบัญญัติฉบับนี้และหากตีความที่ผิดเพี้ยนแปลกไปจะทำให้การใช้บังคับในมาตรา 60 จะไม่สอดคล้องกันไปด้วย เนื่องจากมาตรา 60 ได้แบ่งออกระดับภัยคุกคามทางไซเบอร์ออกเป็น 3 ระดับอย่างชัดเจน คือ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ดังนั้นจากบทนิยามตามมาตรา 3 นี้จะต้องให้ความหมายไว้อย่างกระชับ และชัดเจน เพื่อจะได้สอดคล้องกับบทมาตราอื่น ๆ

ประเด็นที่สองปัญหาเกี่ยวกับการใช้อำนาจของรัฐในการขอข้อมูลจากบุคคลที่เกี่ยวข้อง เพื่อประโยชน์ในการทำงาน

ข้อมูลส่วนบุคคล เป็นข้อมูลประเภทหนึ่งที่เกี่ยวข้องกับตัวบุคคลหรือทำให้สามารถเชื่อมโยงไปยังเจ้าของข้อมูลได้ง่าย นอกจากนี้แล้วคำว่าข้อมูลส่วนบุคคล ยังหมายรวมถึงข้อมูลอื่น ๆ ที่สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม เนื่องด้วยเหตุนี้จึงมีการผลักดันให้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพื่อเป็นการให้หลักประกันที่ดีเพียงพอต่อการคุ้มครองความเป็นส่วนตัวของพลเมือง การให้ความคุ้มครองข้อมูลส่วนบุคคลจะต้องรักษาดุลยภาพระหว่างสิทธิขั้นพื้นฐานในความเป็นส่วนตัวและความมั่นคงของรัฐ

เมื่อพิจารณาตามมาตรา 62 แล้ว พบว่าใน (1) และ (2) นั้น บุคคลผู้เป็นเจ้าของข้อมูลจำต้องให้ข้อมูลตามที่กฎหมายให้อำนาจเลขาธิการสั่งให้เจ้าหน้าที่สามารถเข้าขอข้อมูลจากบุคคลที่เกี่ยวข้อง เพื่อประโยชน์ในการทำงานได้ โดยผู้ให้ข้อมูลจะได้รับความคุ้มครองและไม่ถือว่าเป็นการละเมิดหรือผิดสัญญา หากผู้ให้ข้อมูลนั้นกระทำโดยสุจริต และหากบุคคลใดไม่ให้ความร่วมมือจะถือเป็นการการกระทำความผิดมีทาตามมาตรา 74 จึงกลายเป็นประเด็นปัญหาว่า ในการขอความร่วมมือของเจ้าหน้าที่นั้น เจ้าของข้อมูลจำเป็นจะต้องให้ข้อมูลแก่เจ้าหน้าที่ทุกกรณีที่ขอไปหรือทุกครั้งที่ขอไปหรือไม่ เพราะคำว่า “ขอความร่วมมือ” นั้นย่อมหมายถึง การวิงวอนให้ผู้อื่นกระทำหรือช่วยเหลือด้วยความเต็มใจ อีกทั้งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ยังได้ให้สิทธิแก่เจ้าของข้อมูลไว้ว่าเป็นสิทธิในความเป็นส่วนตัวหรือสิทธิส่วนบุคคลซึ่งเจ้าของข้อมูลย่อมมีสิทธิในข้อมูลของตน โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนได้ เว้นแต่ถูกจำกัดสิทธิโดยกฎหมายหรือสัญญาที่ให้ประโยชน์

แก่เจ้าของข้อมูลส่วนบุคคล และหากการถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

ดังนั้น จากที่กล่าวมากลับพบว่าสองมาตรานี้มีความขัดแย้งในตัวบทกฎหมาย ควรมีการบัญญัติให้ มีความชัดเจนว่ามาตรา 62 (1) และ (2) นั้นเป็นการบังคับให้ต้องปฏิบัติตามคำสั่ง ทั้งนี้เพื่อเป็นการป้องกันการละเมิดสิทธิของบุคคลในการใช้ดุลพินิจของเจ้าหน้าที่ที่ขอข้อมูลเกินความจำเป็นด้วย

ประเด็นที่สามปัญหาการใช้อำนาจเจ้าหน้าที่ ในการยึด-ค้น-เจาะระบบ-ทำสำเนา ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

ในเชิงปฏิบัติ สำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์นั้น ไม่เพียงแต่เฉพาะหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเท่านั้นที่จะต้องตระหนักและปฏิบัติตามแนวทางที่คณะกรรมการกำหนด แต่เป็นหน้าที่ของประชาชนทุกคนที่ต้องช่วยกันเฝ้าระวังภัยให้ข้อมูลที่เป็นประโยชน์ ช่วยอำนวยความสะดวกต่อการทำงานของรัฐ รวมถึงให้เบาะแสเพื่อการป้องกันแก้ไขอย่างทันท่วงที เพื่อเป็นการปิดช่องโหว่ที่อาจส่งผลกระทบให้เกิดความเสียหายต่อประเทศชาติบ้านเมือง เมื่อพิจารณาตามมาตรา 66 กฎหมายให้อำนาจเจ้าหน้าที่และศาลในการใช้ดุลพินิจในเรื่องการยึด-ค้น-เจาะระบบ-ทำสำเนา ระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ตามที่บัญญัติไว้ใน (2) - (4) และให้อำนาจศาลใช้ดุลพินิจตามคำร้องของ กกม. ตามมาตรา 66 วรรคสอง ดุลพินิจถือเป็นอำนาจพิเศษและเป็นองค์ประกอบสำคัญที่จะทำให้กฎหมายดำเนินการไปด้วยความราบรื่นและยุติธรรมในการพิจารณาร่วมกับพยานหลักฐานและข้อเท็จจริงและข้อกฎหมาย แม้ว่าจะเป็นอำนาจที่พิเศษและถือเป็นที่สุด แต่ความผิดพลาดในการใช้ดุลพินิจก็อาจเกิดขึ้นได้ เพราะโดยธรรมชาติของความเป็นมนุษย์ย่อมเกิดขึ้นได้อยู่ตลอดเวลา ดังนั้นจึงกลายเป็นเป็นช่องโหว่ของกฎหมายฉบับนี้ เนื่องจากในการให้อำนาจเจ้าหน้าที่ในระดับร้ายแรงเพื่อการยึด-ค้น-เจาะระบบ-ทำสำเนาระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ ตามมาตรา 66 เป็นการละเมิดสิทธิขั้นพื้นฐานของเจ้าของข้อมูลกับทั้งกฎหมายให้อำนาจแก่เจ้าหน้าที่ผู้เกี่ยวข้องโดยไม่มีขอบจำกัดในการใช้อำนาจ แม้ว่าพระราชบัญญัติจะระบุไว้ว่ามีบทบัญญัติบางประการขัดต่อหลักประชาธิปไตยและละเมิดสิทธิและเสรีของบุคคล แต่ก็ยังคงอยู่ภายใต้เงื่อนไขตามมาตรา 26 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย แม้ว่ารัฐจะสามารถตรากฎหมายขึ้นจำกัดสิทธิและเสรีภาพของประชาชน แต่ทว่า รัฐย่อมไม่สามารถตัดหรือเพิกถอนสิทธิและเสรีภาพไปด้วยได้ทั้งเป็นการเพิ่มภาระแก่ของบุคคลเกินควร ซึ่งไม่เป็นไปตามมาตรา 26 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยที่ระบุไว้

ประเด็นที่สี่ปัญหาเกี่ยวกับการที่เจ้าหน้าที่ สามารถใช้อำนาจโดยไม่ต้องขอหมายศาล ในสถานการณ์เร่งด่วน ตามมาตรา 68 ขัดกับมาตรา 66

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. 2562 แบ่งประเภทของภัยคุกคามไว้ 3 ระดับ ไว้ในมาตรา 60 คือ กรณีที่เป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง เป็นหน้าที่ของหน่วยงานนั้น ๆ และหน่วยงานกำกับดูแลต้องดำเนินการตามมาตรฐานที่กำหนดไว้ กรณีที่เป็นภัยคุกคามระดับร้ายแรงเป็นหน้าที่ของสำนักงานคณะกรรมการรักษาความมั่นคงไซเบอร์จะให้ความช่วยเหลือในการแก้ปัญหา

โดยการเข้าไปในสถานที่ หรือเข้าไปตรวจ โดยเจ้าหน้าที่จะต้องขอหมายศาลก่อนดำเนินการ ตามมาตรา 66 (2) (3) และ (4) และในกรณีเป็นภัยระดับวิกฤติเป็นไปตามมาตรา 68 สามารถใช้อำนาจตามกฎหมายด้านการรักษาความมั่นคงได้ โดยในมาตรา 68 วรรคหนึ่งนั้น ไม่จำเป็นต้องยื่นคำร้องต่อศาลเพื่อให้ศาลมีคำสั่งตามคำร้องของพนักงานเจ้าหน้าที่

แต่เนื่องจากตามมาตรา 60 ได้แบ่งประเภทภัยคุกคามไว้เพียงแค่ 3 ระดับเท่านั้น โดยกฎหมายไม่ได้การระบุความหมายหรือคำนิยามในกรณีที่เป็นเหตุจำเป็นเร่งด่วน ตามมาตรา 68 ไว้ ผู้ศึกษาเห็นว่า ตามมาตรา 66 และมาตรา 68 เป็นกรณีที่ไม่สอดคล้องกัน อันเนื่องจากในกรณีเหตุร้ายแรงตามมาตรา 68 กฎหมายไม่ได้ระบุขอบเขตของการใช้อำนาจในกรณีจำเป็นเร่งด่วนเอาไว้ ดังนั้นการใช้ดุลพินิจในการใช้อำนาจของพนักงานเจ้าหน้าที่จึงเป็นช่องโหว่ในการยกมาเป็นข้ออ้าง เพื่อไม่ต้องยื่นคำร้องต่อศาลได้ ดังนั้นพนักงานเจ้าหน้าที่จะนำมาตรา 68 วรรคหนึ่งมาใช้ในทุกกรณี ซึ่งโดยหลักความเป็นจริงในทางปฏิบัติโดยทั่วไปพนักงานเจ้าหน้าที่ผู้มีอำนาจจะใช้อำนาจเกินขอบเขต เพื่อความสะดวกของตนจนทำให้เจ้าของข้อมูลรับภาระเกินความจำเป็นโดยใช้กฎหมายปิดปากเจ้าของข้อมูลปัญหานี้เป็นการเป็นช่องโหว่ของกฎหมายที่สมควรแก่การแก้ไขอย่างเร่งด่วน

จากการศึกษาปัญหาทางกฎหมายตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ผู้ศึกษาขอเสนอแนะแนวทางแก้ไขปัญหา ดังต่อไปนี้

ประเด็นที่หนึ่งปัญหาเกี่ยวกับความหมายของ “ภัยคุกคามไซเบอร์”

แก้ไขมาตรา 3 นิยาม “ภัยคุกคามไซเบอร์” เป็น

ภัยคุกคามไซเบอร์ หมายถึง การกระทำหรือการดำเนินการใด ๆ เกี่ยวกับไซเบอร์ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง *“ไม่รวมถึงเนื้อหาบนโลกออนไลน์โดยทั่วไป ซึ่งเป็นการให้ความหมายที่กะทัดรัดมากขึ้น เพื่อให้เกิดความชัดเจนและการตีความกฎหมายที่เป็นไปในทิศทางเดียวกัน”*

ประเด็นที่สองปัญหาเกี่ยวกับการใช้อำนาจของรัฐในการขอข้อมูลจากบุคคลที่เกี่ยวข้องเพื่อประโยชน์ในการทำงาน

แก้ไขมาตรา 62 เป็น

“ในการดำเนินการตามมาตรา 61 เพื่อประโยชน์ในการวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ ให้เลขาธิการสั่งให้พนักงานเจ้าหน้าที่มีอำนาจหน้าที่ดำเนินการดังต่อไปนี้

(1) *“มีหนังสือให้”* บุคคลที่เกี่ยวข้องเพื่อมาให้ข้อมูลภายในระยะเวลาที่เหมาะสมและตามสถานที่ที่กำหนด หรือให้ข้อมูลเป็นหนังสือเกี่ยวกับภัยคุกคามทางไซเบอร์

(2) *"มีหนังสือให้บุคคลนำ"* ข้อมูล เอกสาร หรือสำเนาข้อมูลหรือเอกสารซึ่งอยู่ในความครอบครองของผู้อื่นอันเป็นประโยชน์แก่การดำเนินการ

(3) สอบถามบุคคลผู้มีความรู้ความเข้าใจเกี่ยวกับข้อเท็จจริงและสถานการณ์ที่มีความเกี่ยวพันกับภัยคุกคามทางไซเบอร์

(4) เข้าไปในอสังหาริมทรัพย์หรือสถานประกอบการที่เกี่ยวข้องหรือคาดว่ามีส่วนเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ของบุคคลหรือหน่วยงานที่เกี่ยวข้อง โดยได้รับความยินยอมจากผู้ครอบครองสถานที่นั้น

ผู้ให้ข้อมูลตามวรรคหนึ่ง ซึ่งกระทำโดยสุจริตย่อมได้รับการคุ้มครองและไม่ถือว่าเป็นการละเมิดหรือผิดสัญญา"

ประเด็นที่สามปัญหาการใช้อำนาจเจ้าหน้าที่ ในการยึด-ค้น-เจาะระบบ-ทำสำเนา ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

"เห็นควรให้ยกเลิกมาตรา 66"

ประเด็นที่สี่ปัญหาเกี่ยวกับการที่เจ้าหน้าที่ สามารถใช้อำนาจโดยไม่ต้องขอหมายศาล ในสถานการณ์เร่งด่วน ตามมาตรา 68 ขัดกับมาตรา 66

แก้ไขมาตรา 68 วรรคหนึ่ง เป็น

ควรแก้ไขมาตรา 68 วรรคหนึ่ง ระบุว่า ในกรณีที่เป็นเหตุจำเป็นเร่งด่วน และเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ คณะกรรมการอาจมอบหมายให้เลขาธิการมีอำนาจ *"ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำ หรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว"*

และเพิ่มคำนิยามในมาตรา 3 คำว่า *"เหตุจำเป็นเร่งด่วน หมายความว่า เป็นกรณีความจำเป็นเร่งด่วน ที่เกิดขึ้นโดยไม่ได้คาดหมายไว้ก่อน/และไม่อาจดำเนินการตามปกติได้ทัน เกี่ยวกับภัยคุกคามทางไซเบอร์"*

เอกสารอ้างอิง

กาญจนารัตน์ ลีวิโรจน์. "สิทธิและเสรีภาพของประชาชน: ความคุ้มครองที่อาจถูกจำกัดโดยกฎหมายและกฎ." **เอกสารวิชาการส่วนบุคคล (Individual Study)**. รายงานการฝึกอบรมหลักสูตรหลักนิติธรรมเพื่อประชาธิปไตยรุ่นที่ 1 วิทยาลัยรัฐธรรมนูญ. สำนักงานศาลรัฐธรรมนูญ.

กุสุมา เมฆเมฆา และอำนาจ เนตยสุภา. **"การตีความกฎหมายอาญาไทย." ในการใช้การตีความกฎหมาย**. พิมพ์ครั้งที่ 3, กรุงเทพมหานคร: กองทุนศาสตราจารย์จิตติ ติงศภัทิย์ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. 2552.

ข่าวไทยพีบีเอส. **เปิดร่าง พ.ร.บ.รักษาความมั่นคงปลอดภัย ขจัดอาชญากรไซเบอร์** [Online]. Available URL: https://news.thaipbs.or.th/content/278080. 2563 (มิ.ย., 15).

ข่าวเศรษฐกิจ ช่อง 3. **ไซแมนเทคเปิดสถิติ "ภัยคุกคาม" ปี 62 พบไทยติดอันดับ 7 ของเอเชีย** [Online]. Available URL: http://news.ch3thailand.com/economy/90756. 2563 (มิ.ย., 11).

ฉัตรชัย ศรีเมืองกาญจนา. "กรอบยุทธศาสตร์ชาติด้านความมั่นคง." **Legislative Institutional Repository of Thailand**. Issue พฤษภาคม 2561.

ธานินทร์ กรัยวิเชียร และวิชา มหาคุณ. **การตีความกฎหมาย**. พิมพ์ครั้งที่ 3. กรุงเทพมหานคร: โรงพิมพ์ชวนพิมพ์. 2539.

บรรเจิด สิงคะเนติ. **หลักพื้นฐานเกี่ยวกับสิทธิเสรีภาพและศักดิ์ศรีความเป็นมนุษย์**. กรุงเทพฯ : สำนักพิมพ์วิญญูชน. 2558.

สุรพงษ์ ชัยจันทร์. "แนวโน้มด้านความมั่นคงปลอดภัยของโลกไซเบอร์ Cyber Security Trend." **เอกสารทางวิชาการ**.