ปัญหาทางกฎหมายตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 : ศึกษาเฉพาะกรณี การละเมิดสิทธิส่วนบุคคล[1]

บุษกร เอี่ยมสอาด[2]

จากการศึกษาพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 แล้ว พบว่า ในปัจจุบันการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียมมีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังนั้น เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที สมควรกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและหน่วยงานเอกชน ที่จะต้องมีการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรงตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ อย่างไรก็ตามการบัญญัติกฎหมายหรือการแก้ไขบทบัญญัติแห่งกฎหมายจะต้องคำนึงสิทธิของประชาชนเป็นสำคัญตามปฏิญญาสากลว่าด้วยสิทธิมนุษยชน แม้รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560ได้บัญญัติยกเว้นการดำเนินการของรัฐบางอย่างหากจะบรรลุผลจะต้องตรากฎหมายที่ก้าวล่วงสิทธิและเสรีภาพของประชาชนบ้าง แต่การละเมิดสิทธินั้นจะต้องชั่งน้ำหนักระหว่างประโยชน์สาธารณะที่พึงมีพึงได้จากการละเมิดสิทธิเหล่านั้น เป็นไปตามหลักความจำเป็นและพอสมควรแก่เหตุ แม้เรื่องไซเบอร์สเปซเป็นเรื่องค่อนข้างใหม่ ประชาชนอาจยังไม่เข้าใจ หรือเข้าถึงภัยคุกคามนี้มากนั้น จึงยังไม่ทราบถึงการยินยอมที่ต้องให้ข้อมูลให้เจ้าหน้าที่เข้าถึงความเป็นส่วนตัวมากน้อยเพียงใด

---

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

[2] นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต (ส่วนกลาง) คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง

จากการศึกษาทำให้ทราบว่า พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีบทบัญญัติทางกฎหมายที่มีปัญหาในทางปฏิบัติอยู่หลายประการอันส่งผลต่อการละเมิดสิทธิส่วนบุคคล ซึ่งสามารถพิจารณาได้จาก 4 ประเด็นปัญหา ดังต่อไปนี้

ประเด็นปัญหาที่หนึ่ง ปัญหาเกี่ยวกับความหมายของ “ภัยคุกคามทางไซเบอร์” ตามมาตรา 3 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้บัญญัติเกี่ยวกับคำนิยามคำว่า “ภัยคุกคามทางไซเบอร์” หมายความว่า “การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องและเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง” ซึ่งเป็นการขยายความให้ครอบคลุมถึงข้อมูลอื่นที่เกี่ยวข้อง ถือว่าเป็นการนิยามความหมายที่กว้าง ซึ่งอาจเกิดการตีความอันการละเมิดสิทธิส่วนบุคคลได้ ในขณะที่เมื่อเทียบเคียงกับกฎหมายเกี่ยวกับการรักษาความปลอดภัยไซเบอร์ในลักษณะเดียวกันนี้ของประเทศสิงคโปร์และประเทศสหรัฐอเมริกา พบว่า มีการนิยามความหมายของภัยคุกคามทางไซเบอร์ที่ชัดเจนว่าเหตุการณ์ใดก็ตามที่ส่งผลกระทบทางลบต่อความมั่นคงปลอดภัยของเครือข่ายและระบบข้อมูลสถานการณ์หรือเหตุการณ์ใดก็ตามที่น่าจะส่งผลกระทบทางลบต่อความมั่นคงปลอดภัยของเครือข่ายและระบบข้อมูล ซึ่งมุ่งเน้นภัยคุกคามที่เกิดขึ้นกับเรือข่ายหรือระบบข้อมูลเท่านั้น นอกจากนี้มาตรา 60 แห่งพระราชบัญญัติฉบับเดียวกัน ได้แบ่งภัยคุกคามไซเบอร์ ออกเป็น 3 ระดับ คือ ระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤติ ถือว่าเป็นการเปิดโอกาสให้ ตีความ “ขยาย” ความหมายของภัยคุกคามไซเบอร์ให้กว้างขึ้น ซึ่งไม่เพียงแต่การขยายความหมายเท่านั้น แต่เป็นการขยายขอบเขตการตีความของของคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) ตามมาตรา 13 (6) ซึ่งบัญญัติให้ กกม. มีหน้าที่และอำนาจในการกำหนดระดับของภัยคุกคามทางไซเบอร์ พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับเสนอต่อคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ดังนั้น การให้ความหมายของภัยคุกคามทางไซเบอร์ และการกำหนดระดับ รวมทั้งรายละเอียดของลักษณะภัยคุกคามทางไซเบอร์แต่ละระดับอาจเป็นการตีความในทางเป็นโทษที่เป็นลักษณะของการละเมิดสิทธิส่วนบุคคลได้

ประเด็นปัญหาที่สอง ปัญหาเกี่ยวกับการอุทธรณ์คำสั่งภัยคุกคามทางไซเบอร์ในระดับร้ายแรงและระดับวิกฤต เนื่องจากมาตรา 69 แห่งพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562ได้บัญญัติให้ผู้ที่ได้รับคำสั่งเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ อาจอุทธรณ์คำสั่งได้เฉพาะที่เป็นภัยคุกคามทาง

ไซเบอร์ในระดับไม่ร้ายแรงเท่านั้น โดยการดำเนินการเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ระดับร้ายแรงนั้นต้องดำเนินการตามมาตรา 61 ถึงมาตรา 66 ส่วนการดำเนินการเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ระดับวิกฤต ต้องดำเนินการตามมาตรา 67 และมาตรา 68 ในหลายๆบทบัญญัติที่ดำเนินการเกี่ยวกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง มิได้มีพยานหลักฐานในการชัดเจนเพียงพอในการจำกัดสิทธิเสรีภาพส่วนบุคคล ดังเช่น มาตรา 65 กำหนดว่าในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการ เฝ้าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ตรวจสอบ รักษาสถานะของข้อมูล หรือเข้าถึงข้อมูลคอมพิวเตอร์เท่าที่จำเป็น เป็นต้น ซึ่งถือว่าเป็นเพียงเหตุอันควรเชื่อว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์และเป็นคำสั่งที่มีผลบังคับให้บุคคลกระทำการอย่างใดอย่างหนึ่งหรือห้ามมิให้กระทำการอย่างใดอย่างหนึ่ง การอนุญาตให้กระทำการหรือละเว้นกระทำการ หรือการยืนยันสิทธิที่มีผลบังคับเฉพาะกรณี ใดกรณีหนึ่งหรือบุคคลใดบุคคลหนึ่งเป็นการเฉพาะอันมีลักษณะเป็นคำสั่งทางปกครอง หากพิจารณาหลักความชอบด้วยกฎหมายและหลักการประกันความเป็นธรรมประกอบกัน การกระทำทั้งปวงขององค์กรฝ่ายปกครองต้องสอดคล้องกับหลักความชอบด้วยกฎหมาย หลักประกันความเป็นธรรม เพื่อให้สิทธิแก่เจ้าของกรรมสิทธิ์ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์มีสิทธิในการอุทธรณ์คำสั่งของคณะกรรมการ

ประเด็นปัญหาที่สาม ปัญหาเกี่ยวกับการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือข้อมูลอันที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็นเท่านั้นซึ่งอาจเป็นการละเมิดสิทธิส่วนบุคคล เมื่อพิจารณาจากบทบัญญัติตามมาตร 65 เป็นการจำกัดสิทธิในการดำเนินการหรือการเข้าถึงข้อมูลของบุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ บทบัญญัติดังกล่าวอาศัยเหตุอันเชื่อได้ว่าบุคคลดังกล่าวว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ ในการจำกัดสิทธิเสรีภาพของประชาชน และเมื่อพิจารณา ตามมาตร 65 (5) ที่กำหนดให้ กกม. สามารถออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์ ซึ่งคำว่า “เท่าที่จำเป็น” นี้ มิได้มีการกำหนดขอบเขตหรือลักษณะว่าแค่ไหนถือว่าเป็นการเข้าถึงที่จำเป็นเพียงพอแล้ว

จะเห็นได้ว่ากฎหมายกำหนดแต่เพียงว่าให้เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น และเป็นภัยคุกคามไซเบอร์ในระดับร้ายแรง ประเด็นที่ควรจะพิจารณาคือใครเป็นผู้กำหนดว่าข้อมูลเท่าใดถือเป็นว่าเป็นข้อมูลเท่าที่จำเป็นและการพิจารณาดังกล่าวถือเป็นดุลพินิจของเจ้าหน้าที่ผู้เกี่ยวข้อง แม้ว่าการออกกฎหมายในลักษณะนี้อาจทำให้การดำเนินการของเจ้าหน้าที่อยู่ ภายใต้หลักนิติธรรม กล่าวคือ เมื่อออกกฎหมายแล้วฝ่ายปกครองจึงจะมีอำนาจกระทำการใดๆ เท่าที่กฎหมายบัญญัติ อย่างไรก็ตาม ศาลรัฐธรรมนูญได้วางหลักการว่าการจำกัดสิทธิขั้นพื้นฐานของประชาชนนั้น แม้จะสามารถ กระทำได้โดยบทบัญญัติแห่งกฎหมาย แต่บทบัญญัติแห่งกฎหมายนั้นก็จะต้องได้สัดส่วนกันระหว่างการดำเนินมาตรการของรัฐ กับการคุ้มครองสิทธิเสรีภาพของประชาชน

ประเด็นปัญหาที่สี่ ปัญหาการเข้าตรวจสอบสถานที่ในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ เมื่อพิจารณามาตรา 66 ที่กำหนดให้กกม. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ในเรื่องการเข้าตรวจสอบสถานที่ การเข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลที่เกี่ยวข้อง ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เฉพาะเท่าที่จำเป็นซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ โดยการดำเนินการตาม (2) (3) และ (4) ให้ กกม. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ซึ่งเป็นที่น่าสังเกตว่าเฉพาะการดำเนินการตาม (2) (3) และ (4) ให้ กกม. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้องส่วนการดำเนินการตาม (1) ที่กำหนดให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ ไม่ต้องยื่นคำร้องต่อศาลซึ่งไม่เป็นไปตาม มาตรา 33 แห่ง รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ที่กำหนดให้บุคคลย่อมมีเสรีภาพในเคหสถานการเข้าไปในเคหสถานโดยปราศจากความยินยอมของผู้ครอบครอง หรือการค้นเคหสถานหรือที่รโหฐานจะกระทำมิได้ เว้นแต่มีคำสั่งหรือหมายของศาลหรือมีเหตุอย่างอื่นตามที่กฎหมายบัญญัติ ซึ่งกรณีนี้แม้จะกำหนดข้อยกเว้นในการเข้าไปในเคหสถานของผู้ครอบครองได้โดยคำสั่งหรือหมายของศาล แต่คำสั่งดังกล่าวตามมาตรา 66 ที่ดำเนินการในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์นั้น ก็เป็นคำสั่งที่ผู้ครอบครองไม่อาจอุทธรณ์

คำสั่งทางปกครองดังกล่าวได้ตามมาตรา 69 แห่งพระราชบัญญัติเดียวกัน การดำเนินการตามมาตรา 66 (1) จึงถือว่าเป็นบทบัญญัติที่ไม่ชอบด้วยรัฐธรรมนูญ และไม่เป็นไปตามหลักในการอุทธรณ์คำสั่งทางปกครอง เป็นการละเมิดสิทธิบุคคลของประชาชนในการพิสูจน์ความบริสุทธิ์ของตน

จากการศึกษาปัญหาทางกฎหมายตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. 2562 ผู้ศึกษาจึงขอเสนอแนะแนวทางแก้ไขปัญหาดังกล่าว ดังนี้

ประเด็นปัญหาที่หนึ่ง ปัญหาเกี่ยวกับความหมายของ “ภัยคุกคามทางไซเบอร์”

ควรแก้ไขคำนิยามของ ภัยคุกคามทางไซเบอร์ มาตรา 3 เป็น “ ‘ภัยคุกคามทางไซเบอร์’ หมายความว่า การกระทำบนหรือผ่านระบบข้อมูลที่อาจส่งผลให้เกิดความพยายามโดยไม่ได้รับอนุญาตในการส่งผลกระทบต่อความปลอดภัย ความพร้อมใช้งาน และการรักษาความลับหรือความสมบูรณ์ของระบบข้อมูลหรือข้อมูลที่เก็บไว้ หรือถูกประมวลผลโดย หรือถูกโอนย้ายไปในระบบข้อมูล” เพื่อให้มุ่งเน้นผลกระทบที่อาจจะเกิดขึ้นจากระบบโดยตรง

ประเด็นปัญหาที่สอง ปัญหาเกี่ยวกับการอุทธรณ์คำสั่งภัยคุกคามทางไซเบอร์ในระดับร้ายแรงและระดับวิกฤต

ควรแก้ไข มาตรา 69 เป็น “ผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์สามารถอุทธรณ์คำสั่งต่อคณะกรรมการการพิจารณาอุทธรณ์คำสั่งการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กอช.)” เพื่อเป็นหลักประกันความเป็นธรรมและให้โอกาสผู้ได้รับคำสั่งโต้แย้งคำสั่งทางปกครองนั้น เพื่อพิสูจน์ความบริสุทธิ์ของตน ดังเช่นการอุทธรณ์คำสั่งเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์ของประเทศสิงคโปร์ซึ่งกำหนดให้หน่วยงานที่ให้บริการด้านโครงสร้างพื้นฐานข้อมูลที่สำคัญ อาจอุทธรณ์คำสั่งต่อรัฐมนตรีในกรณีได้รับความเดือดร้อนเสียหายจากคำสั่งของเจ้าหน้าที่ผู้ทำคำสั่ง

ประเด็นปัญหาที่สาม ปัญหาเกี่ยวกับการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือข้อมูลอันที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็นเท่านั้นซึ่งอาจเป็นการละเมิดสิทธิส่วนบุคคล

สมควรปรับแก้ไขบทบัญญัติมาตรา 65 (5)และมาตรา 65 วรรคสอง โดยการ

1. จัดทำอนุบัญญัติโดยให้ทราบว่าผู้ใดเป็นผู้พิจารณาเหตุ “ความจำเป็น”ในการเข้าถึงข้อมูล ข้อมูลที่เข้าถึงนั้นเป็นข้อมูล “เท่าที่จำเป็น” เพียงใด

2. การจัดเก็บข้อมูลเหล่านั้นอยู่ในความดูแลของเจ้าหน้าที่หรือระบบที่เชื่อถือได้มากน้อยเพียงใด และระยะเวลาในการจัดเก็บข้อมูลเหล่านั้นจะจัดเก็บเพียงใด พ้นกำหนดระยะเวลาจะมีการส่งคืนหรือทำลาย

โดยไม่มีการทำสำเนาจัดเก็บไว้หรือไม่ เหล่านี้ล้วนเป็นความชัดเจนในการดำเนินการของเจ้าหน้าที่เพื่อสร้างความเชื่อมั่นต่อประชาชนหรือผู้ที่ถูกเข้าถึงข้อมูลทางคอมพิวเตอร์

3. สมควรกำหนดให้คณะกรรมการสิทธิมนุษยชนเป็นกรรมการโดยตำแหน่งของ กมช. และ กกม. เพื่อให้สามารถให้ความเห็นในการประชุมแต่ละครั้ง หรือในการออกกฎ ระเบียบ หรือกำหนดและหรือแก้ไขบทบัญญัติแห่งกฎหมายที่อาจเกิดการกระทบต่อสิทธิของประชาชน หรือเป็นภาระต่อประชาชนเกินสมควร

ประเด็นปัญหาที่สี่ ปัญหาการเข้าตรวจสอบสถานที่ในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

ควรแก้ไขมาตรา 66 วรรคสอง เป็น “ในการดำเนินการตาม (1) (2) (3) และ (4) ให้ กกม. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง...” เนื่องจากการที่พนักงานเจ้าหน้าที่สามารถเข้าไปในที่รโหฐานของประชาชนได้ โดยไม่ต้องขอหมายศาล ถือได้ว่าเป็นการขัดต่อหลักการเรื่องการค้นตามประมวลกฎหมายวิธีพิจารณาความอาญาและกฎหมายมิได้มีการวางมาตรการตรวจสอบถ่วงดุลใดๆ ไว้ ทำให้การใช้อำนาจไม่ได้รับการตรวจสอบ อาจทำให้เจ้าหน้าที่ใช้อำนาจในทางมิชอบและเป็นเหตุให้ประชาชนถูกก้าวล่วงในแดนแห่งสิทธิและเสรีภาพได้

เอกสารอ้างอิง

กุลพล พลวัน. **พัฒนาการแห่งลิทธิมนุษยชน**. พิมพ์ครั้งที่ 3. (กรุงเทพฯ: วิญญูชน, 2533).

จรัญ โฆษณานันท์. **สิทธิมนุษยชนไว้พรมแดน : ปรัชญา กฎหมายและความเป็นจริงทางสังคม**. พิมพ์ครั้งที่ 1. (กรุงเทพฯ : นิติธรรม, 2545).

บุญอนันต์ วรรณพานิชย์. **หลักกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง**. พิมพ์ครั้งที่ 1. (กรุงเทพฯ : สวัสดิการสำนักงานศาลปกครอง, 2544).

ปัญญา หอมอเนก. **ผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของชาติ : ปัญหาอธิปไตยไซเบอร์ และแนวทางการกำหนดยุทธศาสตร์ชาติ ตอนที่ 3** [Online]. Available URL: https://itgthailand.wordpress.com/tag/national-cybersecurity/(พฤษภาคม 2564)