**ปัญหาทางกฎหมายในการคุ้มครองสิทธิของบุคคลตามพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562**

สุจิตรา เปรมจิตต์1, อาจารย์ภาวิตา ค้าขาย2

1สาขาวิชานิติศาสตร์ คณะมนุษยศาสตร์และสังคมศาสตร์, E-mail : s59123440087@ssru.ac.th

2อาจารย์ที่ปรึกษาประจำสาขาวิชานิติศาสตร์ คณะมนุษยศาสตร์และสังคมศาสตร์, E-mail pawita.ka@ssru.ac.th

**บทคัดย่อ**

การวิจัยเรื่องนี้มีวัตถุประสงค์เพื่อวิเคราะห์ปัญหาทางกฎหมายจากการบังคับใช้พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 และเสนอแนะแนวทางในการปรับปรุงข้อกฎหมายที่เกี่ยวกับการคุ้มครองสิทธิของบุคคลในกรณีของการบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 โดยศึกษาเกี่ยวกับการคุ้มครองสิทธิในข้อมูลของบุคคล ทั้งนี้มีกฎหมายที่ประกาศใช้เกี่ยวกับการคุ้มครองสิทธิของบุคคลเกี่ยวกับข้อมูลส่วนบุคคลอยู่หลายฉบับ เพื่อมิให้บุคคลผู้เก็บรักษาข้อมูลนำข้อมูลซึ่งเจ้าของมิได้อนุญาตไปเผยแพร่ ซึ่งบุคคลนั้นมีสิทธิที่จะได้รับความคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นสิทธิขั้นพื้นฐานหรือสิทธิตามธรรมชาติของมนุษย์ที่ได้มีการบัญญัติไว้ในมาตรา 32 รัฐธรรมนูญแห่งราชอาณาจักไทย 2560

จากการศึกษาพบว่าแม้จะมีกฎหมายออกมาคุ้มครองสิทธิของบุคคลในกรณีข้อมูลส่วนบุคล แต่ก็มีกฎหมายที่ออกมาเป็นข้อยกเว้นในการละเมิดข้อมูลส่วนบุคคลนั้นได้ ทั้งที่ความผิดนั้นมีกฎหมายอื่นออกมารองรับในการกระทำความผิดนั้นอยู่แล้ว เช่น พระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์2560

**คำสำคัญ :** สิทธิส่วนบุคคล, ข้อมูลส่วนบุคคล, ความมั่นคงปลอดภัยไซเบอร์

 **บทนำ**

 **ความเป็นมาและความสำคัญของปัญหา**

เทคโนโลยีในโลกปัจจุบันนี้มีความก้าวหน้าและเปลี่ยนแปลงไปอย่างรวดเร็ว และในปัจจุบันประเทศไทยกำลังเข้าสู่ยุคอิเล็กทรอนิกส์ทำให้การจัดเก็บข้อมูลไม่ว่าจะเป็นข้อมูลส่วนตัว ข้อมูลการทำธุรกรรม ข้อมูลธุรกิจต่าง ๆ ล้วนถูกเก็บไว้ในระบบคอมพิวเตอร์ หรือในโลกออนไลน์ เช่น **internet Banking** คำสั่งซื้อของจากเว็บออนไลน์ จะเห็นได้อินเตอร์เน็ตได้เข้ามามีบทบาทในการประกอบธุรกิจและอยู่ในชีวิตประจำวันของเรา เป็นอย่างมาก จึงทำให้มีความเสี่ยงที่จะถูกคุกคามหรือถูกละเมิดด้านไซเบอร์อย่างหลีกเลี่ยงไม่ได้

 ภัยคุกคามทางไซเบอร์ เป็นการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลที่เกี่ยวข้อง (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 ) และเป็นภัยคุกคามที่ส่งผลกระทบในหลายภาคส่วน ไม่ว่าจะเป็น สิทธิส่วนบุคคล ผลกระทบทางเศรษฐกิจ โดยในปี 2560 ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย ได้บันทึกสถิติภัยคุกคามพบว่าประเทศไทย มีสถิติการคุกคามทางไซเบอร์ตลอดทั้งปีผลโดยรวมทั้งหมด 3237 ครั้ง ในปี 2561 ตั้งแต่เดือนมกราคม ถึงเดือน ธันวาคม มีการคุกคามทางไซเบอร์ที่ได้บันทึกไว้ในสถิติแล้วจำนวนทั้งหมด 2520 ครั้ง โดยการคุกคามที่มากสูงสุดเป็นอันดับหนึ่งของปีนี้คือ “ความพยายามจะบุกรุกเข้าระบบ” ที่บันทึกไว้ได้จำนวน 1102 ครั้ง ซึ่งมากกว่าสถิติที่บันทึกได้ตลอดปี 2560 ถึง 163 ครั้ง (ไทยเซิร์ต, 2562) ซึ่งการกระทำดังกล่าวนั้นถือได้ว่าเป็นการกระทำที่ผิดกฎหมายโดยเกี่ยวข้องกับการใช้งานคอมพิวเตอร์หรือโครงข่ายโทรคมนาคม

ในปัจจุบันมีการกฎหมายออกมาเพื่อคุ้มครองรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นฉบับแรกมีชื่อว่าพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์2562 เป็นกฎหมายที่ใช้การแก้ปัญหาความมั่นคงปลอดภัยไซเบอร์ด้วยกฎหมายใหม่นี้รัฐมีอำนาจอย่างมากในการติดตามความเสี่ยงและภัยคุกคามที่เกี่ยวกับความปลอดภัยทางไซเบอร์ แต่การรักษาความมั่นคงปลอดภัยไซเบอร์นั้นก็ต้องอยู่ในหลักสากล คือไม่เป็นการเป็นการละเมิดสิทธิส่วนบุคคลซึ่งสิทธิในความเป็นส่วนตัวหรือสิทธิส่วนบุคคลนี้เป็นสิทธิขั้นพื้นฐานมีบัญญัติไว้ใน[รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 25](https://th.wikipedia.org/wiki/%E0%B8%A3%E0%B8%B1%E0%B8%90%E0%B8%98%E0%B8%A3%E0%B8%A3%E0%B8%A1%E0%B8%99%E0%B8%B9%E0%B8%8D%E0%B9%81%E0%B8%AB%E0%B9%88%E0%B8%87%E0%B8%A3%E0%B8%B2%E0%B8%8A%E0%B8%AD%E0%B8%B2%E0%B8%93%E0%B8%B2%E0%B8%88%E0%B8%B1%E0%B8%81%E0%B8%A3%E0%B9%84%E0%B8%97%E0%B8%A2_%E0%B8%9E%E0%B8%B8%E0%B8%97%E0%B8%98%E0%B8%A8%E0%B8%B1%E0%B8%81%E0%B8%A3%E0%B8%B2%E0%B8%8A_2550)60 ดังนั้นหน่วยงานที่รับผิดชอบจะต้องใช้อำนาจของตนไม่ให้กระทบต่อความเป็นส่วนตัว และมีการรักษาความปลอดภัยอย่างเหมาะสม

พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ เริ่มมีการประกาศใช้ในปี พ.ศ.2562 และมีเนื้อหาในกฎหมายที่ยังไม่ชัดเจน ในประเด็นตามมาตรา 61 นั้นเมื่อเกิดหรือคาดว่าจะเกิดภัยคุกคามขึ้นในการรวบรวมพยานหลักฐานหรือระงับการคุกคามไซเบอร์ สามารถขอข้อมูลจากผู้ครอบครองข้อมูลได้ แต่เนื่องจากคำว่า ข้อมูล ในพระราชบัญญัตินี้ มิได้บัญญัติคำนิยามไว้ จึงตีความหมายได้กว้าง การได้มาซึ่งข้อมูลเพื่อหาภัยคุกคามอาจได้ข้อมูลในส่วนอื่นไปด้วย และในมาตรา 62 วรรคสอง กฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ให้อำนาจขอข้อมูลผู้ประกอบการได้ หากผู้ประกอบการให้ข้อมูลลูกค้าก็จะถือว่าไม่เป็นการละเมิดหรือผิดสัญญา ซึ่งอาจจะกระทบต่อการลงทุนและข้อมูลสิทธิส่วนบุคคลเป็นอย่างมาก

ผู้อำนวยการสถาบันกฎหมายสื่อดิจิทัลฯ ให้ความเห็นว่า “กฎหมายไซเบอร์ให้อำนาจขอข้อมูลผู้ประกอบการธุรกิจได้ หากผู้ประกอบการให้ข้อมูลลูกค้าจะไม่เอาผิด นั่นเท่ากับไปทำลายระบบกฎหมายข้อมูลส่วนบุคคล ยกตัวอย่างเช่น เจ้าหน้าที่จะขอเข้ามาดูการสนทนาในมือถือโดยปกติแล้วหากค่ายมือถือยอมเปิดเผยข้อมูลถือว่าผิดสัญญา แต่ถ้าคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์สั่งถือว่าเป็นการยกเว้นความผิด นั่นเท่ากับว่าเราไปยกเว้นกฎหมายสัญญากับการละเมิด” และอำนาจในการสั่งให้เอกชนต้องให้ข้อมูล หรือต้องปฏิบัติตามที่เลขาธิการสั่งนั้นไม่มีกรอบในการใช้อำนาจ เลขาธิการทำได้เพียงเพราะสงสัยว่าจะมีภัย ซึ่งองค์กรแทบทุกองค์กรที่เชื่อมต่ออินเตอร์เน็ตอยู่นั้น เห็นได้ว่าเสี่ยงที่จะมีภัยตลอดเวลา และหลายองค์กรโดนโจมตีจากภัยไซเบอร์ทุกวัน การจะอ้างถึงการเชื่อได้ว่าจะมีภัยนั้น ดูจะเป็นอำนาจที่กว้างขวางเกินไป (คณาธิป ทองรวีวงศ์: ภูมิ ภูมิรัตน์, 2562)

โดยกรรมการสิทธิมนุษยชนแห่งชาติ ก็ได้ให้ความเห็นว่าข้อกังวลคือเรื่องการให้อำนาจเจ้าหน้าที่เข้าไปตรวจค้นได้โดยไม่ต้องมีหมายศาลนี้เป็นการให้อำนาจเจ้าหน้าที่รัฐมากเกินไป ดังนั้นตรงนี้จึงบอกไม่ได้ว่าจะทำอย่างไร เนื่องจากเป็นเรื่องของการใช้ดุลพินิจในการพิจารณาว่าสิ่งใดเป็นภัยไม่ร้ายแรง (อังคณา นีละไพจิตร) และในมาตรา 66(4) ให้อำนาจเจ้าหน้าที่ยึดหรืออายัดคอมพิวเตอร์ได้ไม่เกิน 30 วันเพื่อตรวจสอบหรือวิเคราะห์หากเกิดความเสียหาย อาจทำให้เอกชนไม่มั่นใจที่จะลงทุนในกิจกรดิจิตอลในไทย (อธึก อัศวานันท์, 2562)

ดังนั้น ผู้ศึกษามุ่งเน้นที่จะศึกษาสภาพปัญหาและผลกระทบที่จะเกิดขึ้นต่อประชาชน หน่วยงานเอกชน และเสนอแนะแนวทางในการเยียวยาผู้ถูกละเมิดสิทธิและเสรีภาพส่วนบุคคลจากการบังคับใช้กฎหมายดังกล่าว

**วัตถุประสงค์ของการวิจัย**

1. เพื่อวิเคราะห์ปัญหาทางกฎหมายจากการบังคับใช้พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562

2. เพื่อเสนอแนะแนวทางในการปรับปรุงข้อกฎหมายที่เกี่ยวกับการคุ้มครองสิทธิของบุคคลในกรณีของการบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562

**เนื้อเรื่อง/การทบทวนวรรณกรรม**

การวิจัยเรื่องนี้ ผู้วิจัยได้ศึกษาแนวคิดทฤษฎีเอกสารทางวิชาการในประเด็นดังต่อไปนี้ (1) ความหมายของการรักษาความมั่นคงความปลอดภัยทางไซเบอร์ (2) ศึกษาเรื่องแนวคิดและวิวัฒนาการเกี่ยวกับสิทธิมนุษยชน (3) แนวคิดทฤษฎีเรื่องการคุ้มครองสิทธิส่วนบุคคล (4) แนวคิดเรื่องข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคล (5) หลักนิติรัฐและหลักนิติธรรม

1)ความหมายของการรักษาความมั่นคงความปลอดภัยทางไซเบอร์

ประเทศสิงคโปร์ ให้ความหมาย การรักษาความมั่นคงความปลอดภัยทางไซเบอร์ หมายถึง สถานะที่คอมพิวเตอร์หรือระบบคอมพิวเตอร์ได้รับการปกป้องจากการเข้าถึงหรือการโจมตีที่ไม่ได้รับอนุญาต (Cybersecurity Act, 2018)

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ในมาตรา 3 ได้ให้ความหมาย การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า “มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ”

 และ ให้ความหมายของคำว่า ภัยคุกคามทางไซเบอร์ หมายความว่า “การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง” (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562)

**2) แนวคิดและวิวัฒนาการเกี่ยวกับสิทธิมนุษยชน**

เรื่องสิทธิมนุษยชนถูกนำมาให้ความสำคัญค่อนข้างมากในช่วงปลายคริสต์ศตวรรษที่ 18 ซึ่งแนวคิดเรื่อง สิทธิมนุษยชนหมายถึงสิทธิของมนุษย์ทุกคน คือ ผู้เป็นมนุษย์ย่อมมีสิทธิดังกล่าวตั้งแต่เกิดจนตายโดยปราศจากเงื่อนไขหรือข้อจำกัดทางกฎหมาย และความมุ่งหมายของหลักสิทธิมนุษยชนก็คือเพื่อเป็นหลักที่ปกป้องสิทธิขั้นพื้นฐานของมนุษย์ที่มีมาแต่กำเนิด เป็นสิทธิที่เท่าเทียมกัน ไม่สามารถแบ่งแยกเพิกถอนหรือจำหน่ายจ่ายโอนได้ ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชนที่นา ๆ ประเทศทำให้เกิดขึ้นเพื่อให้การส่งเสริมคุ้มครองสิทธิมนุษยชนของประชาชนทั่วโลก โดยเป็นผลลัพธ์จากความสูญเสียที่เกิดขึ้นในสงครามโลกครั้งที่ 2 ซึ่งประชาคมระหว่างประเทศได้ตั้งปณิธานว่าจะไม่ให้มีเหตุการณ์ขัดแย้งดังเช่นสงครามโลกครั้งที่ 2 เกิดขึ้นอีก สหประชาชาติได้ถูกจัดตั้งขึ้นโดยมีแนวคิดและโครงสร้างตามที่ระบุไว้ในกฎบัตรสหประชาชาติ ซึ่งกฎบัตรสหประชาชาติเองก็ได้ระบุไว้ถึงการยืนยันความศรัทธาในสิทธิมนุษยชนขั้นพื้นฐาน ในศักดิ์ศรีและคุณค่าของมนุษย์ หลังจากนั้นจึงได้เกิดการเจรจาเอกสารที่จะระบุถึงรายการสิทธิที่ควรได้รับความคุ้มครอง ซึ่งในขณะนั้นเรียกกันว่าเป็นร่างแรกของตราสารระหว่างประเทศว่าด้วยสิทธิมนุษยชน ต่อมาสหประชาชาติได้รับรองปฏิญญาสากลว่าด้วยสิทธิมนุษยชน โดยข้อมติสหประชาชาติ 217 เอ (III) เมื่อวันที่ 10 ธันวาคม พ.ศ.2491ในที่ประชุมสมัชชาสหประชาชาติ สมัยสามัญ สมัยที่ 3 ปฏิญญาสากลว่าด้วยสิทธิมนุษยชนจึงถือได้ว่าเป็นเอกสารประวัติศาสตร์ในการวางรากฐาน ด้านสิทธิมนุษยชนระหว่างประเทศฉบับแรกของโลกและเป็นพื้นฐานของกฎหมายระหว่างประเทศด้านสิทธิมนุษยชนทุกกฉบับที่มีอยู่ในปัจจุบัน (ธนา เวสโกสิทธิ์, 2559,หน้า102-109)

**3) แนวคิดทฤษฎีเรื่องการคุ้มครองสิทธิส่วนบุคคล**

 **3.1) ความเป็นมาของสิทธิ**

ในยุคเริ่มแรกเมื่อมีการก่อตั้งรัฐ มีความเห็นกันว่าสิทธิและเสรีภาพเป็นเรื่องที่ไม่สำคัญ และไม่ใช้เนื้อหาสาระของรัฐธรรมนูญเพราะรัฐธรรมนูญเป็นกฎหมายที่กำหนดโครงสร้างและกลไกในการปกครองของรัฐ แต่ต่อมาในยุคประชาธิปไตย ได้มีการให้ความสำคัญกับสิทธิของประชาชนเป็นอย่างมาก รัฐธรรมนูญลายลักอักษรของประเทศต่าง ๆ จึงได้มีการบัญญัติเรื่อสิทธิของประชาชนไว้ในรัฐธรรมนูญ เพื่อเป็นหลักประกันไม่ให้รัฐใช้อำนาจก้าวล่วงเข้าไปลุกล้ำสิทธิและเสรีภาพของประชาชนมากจนเกินสมควร

**3.2) ความหมายของสิทธิ (Right)**

สิทธิ หรือ สิทธิ์ ตามพจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ.2542 หมายถึง อำนาจอันชอบธรรม รวมถึงอำนาจที่จะกระทำการใด ๆ ได้อย่างอิสระโดยได้รับการรับรองจากกฎหมาย (พจนานุกรมฉบับราชบัณฑิตยสถาน , 2542)

รองศาสตราจารย์มานิต จุมปา ได้ให้ความหมายของคำว่าสิทธิว่า สิทธิ คือ “ประโยชน์ที่กฎหมายรับรองและคุ้มครองให้แก่บุคคลในอันที่จะกระทำการเกี่ยวกับทรัพย์สินหรือบุคคลอื่น เช่น สิทธิในทรัพย์สิน สิทธิในชีวิตและร่างกายเป็นต้น” (มานิตย์ จุมปา, 2557,หน้า 82)

จากความหมายดังกล่าวจะเห็นได้ว่า สิทธิ (Right) หมายถึงอำนาจและความชอบธรรมที่มีกฎหมายรับรองไว้ บุคคลจะกระทำการหรือไม่กระทำการใดก็ได้ และสิทธิดังกล่าวทำให้เกิดสิทธิเรียกร้องที่จะไม่ให้บุคคลใดแทรกแซงสิทธิของตนตามรัฐธรรมนูญ

**3.3) สิทธิส่วนบุคคล** (Right of Privacy) เป็นส่วนหนึ่งของสิทธิมนุษยชน ซึ่งเป็นสิทธิขั้นพื้นที่ทุกคนพึงมี และได้รับการคุ้มครอง มนุษย์ทุกคนย่อมมีสิทธิเสรีภาพในชีวิตร่างกายและจิตใจ มีสิทธิในการดำรงชีวิตความเป็นอยู่ของตนได้อย่างอิสระ และมีสิทธิที่จะเลือกอยู่โดยลำพังโดยไม่ถูกแทรกแซงและมีความเสมอภาคที่จะไม่ให้ผู้ใดมาล่วงละเมิดทำร้ายร่างกายหรือจิตใจ (คณาธิป ทองรวีวงศ์, 2555)

 อย่างไรก็ตามการเก็บรักษาข้อมูลไว้เป็นความลับในปัจจุบันมีความยากขึ้น เนื่องจากปัจจุบันมีการเก็บรวบรวมข้อมูล เพื่อไปใช้ เช่น การเก็บข้อมูลของลูกค้าในธนาคาร การเก็บข้อมูลของคนไข้ในโรงพยาบาล การเก็บข้อมูลจากการซื้อขายออนไลน์ เป็นต้น ดังนั้น แนวคิดเกี่ยวกับความเป็นอยู่ส่วนตัวที่ยอมรับและเหมาะสมในยุคปัจจุบัน คือหลักการที่ว่าบุคคลจะมีความเป็นอยู่ส่วนตัวได้ต่อเมื่อสามารถควบคุมข้อมูลข่าวสารเกี่ยวกับตัวเองได้ หรือควบคุมในการเผยแพร่และใช้ข้อมูลที่เกี่ยวข้องกับชีวิตตนเองโดยบุคคลอื่นได้

**4) แนวคิดทฤษฎีเรื่องข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคล**

เมื่อสิทธิความเป็นอยู่ส่วนตัวเป็นสิทธิขั้นพื้นฐานอย่างหนึ่งที่บุคคลพึงมี จึงทำให้เกิดแนวคิดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อคุ้มครองข้อมูลมิให้บุคคลอื่นนำไปใช้โดยมิได้รับความยินยอมจากเจ้าของข้อมูล กฎบัตรสิทธิขั้นพื้นฐานของสหภาพยุโรป ได้กล่าวถึงการคุ้มครองความเป็นอยู่ส่วนตัว โดยการคุ้มครองข้อมูลส่วนบุคคลไว้ว่า บุคคลทุกคนมีสิทธิได้รับการคุ้มครองในข้อมูลส่วนบุคคลของตนเอง (ดาวัลย์ ขาวสนิท, 2561, น.7-8)

การคุ้มครองข้อมูลส่วนบุคคลในไทยนั้น มีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 2562 ซึ่งกำหนดสิทธิของเจ้าของข้อมูล และหน้าที่ของผู้เก็บ ใช้ และเผยแพร่ข้อมูล ให้ต้องรับผิดชอบต่อเจ้าของข้อมูล พระราชบัญญัตินี้จึงมีความเกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์เพราะพระราชบัญญัตินี้กำหนดหน้าที่ให้ผู้ควบคุมหรือผู้ใช้ข้อมูล ต้องดูแลไม่ให้ข้อมูลรั่วไหลออกไป เพื่อปกป้องความเป็นส่วนตัวของเจ้าของข้อมูล

ข้อมูลส่วนบุคคล (Personal information) นั้นมีความหมายที่กว้างและกฎหมายฉบับต่าง ๆ ในแต่ละประเทศก็ให้ความหมายที่ต่างกันออกไป ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 2562 ข้อมูลส่วนบุคคล หมายความว่า “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวตนบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลผู้ถึงแก่กรรมโดยเฉพาะ”

ความหมายตาม EU Directive ข้อมูลส่วนบุคคล หมายถึง ข้อความใดๆที่เกี่ยวกับบุคคลธรรมดา อันระบุตัว หรืออาจรระบุตัวบุคคลนั้นได้ ซึ่งบุคคลที่อาจถูกระบุตัวได้ไม่ว่าโดยตรงหรือโดยอ้อม รวมถึงข้อมูลที่แสดงถึงเอกลักษณ์ทางวัฒนธรรมและสังคมของบุคคลนั้นเป็นต้น (ETDA, 2560)

ในการคุ้มครองสิทธิส่วนบุคคลในประเด็นของข้อมูลส่วนบุคคลนั้น ข้อมูลสามารถแบ่งออกได้เป็น 2 ประเภท คือ ข้อมูลมี่ทีลักษณะทั่วไป ข้อมูลที่เกี่ยวข้องบุคคลผู้เป็นเจ้าของข้อมูล เช่น ชื่อ ที่อยู่ อาชีพ อายุ เบอร์โทรศัพท์ สถานภาพในการสมรส การศึกษา เป็นต้น ข้อมูลดังกล่าวเป็นข้อมูลที่อาจเก็บรวบรวม เปิดเผย หรือใช้ได้ ทั้งนี้ต้องเป็นไปตามที่กฎหมายบัญญัติไว้ และ ข้อมูลที่มีความอ่อนไหว คือ ข้อมูลที่เกี่ยวกับบุคคลซึ่งถือเป็นเรื่องเฉพาะตัว หากมีการนำไปเปิดเผยอาจก่อให้เกิดผลกระทบต่อความรู้สึก ชื่อเสียงของเจ้าของข้อมูลได้ หรืออาจก่อให้เกิดการเลือกปฏิบัติหรือเกิดอันตรายต่อเจ้าของข้อมูล โดยข้อมูลประเภทนี้เจ้าของข้อมูลต้องการที่จะเก็บข้อมูลนี้เป็นความลับและไม่ต้องการให้เปิดเผยข้อมูล เช่น ข้อมูลเกี่ยวกับความคิดเห็นทางการเมือง ความเชื่อเกี่ยวกับลัทธิ ศาสนา ประวัติสุขภาพประวัติอาชญากรรม สถานะทางการเงิน หรือข้อมูลการใช้อินเตอร์เน็ต เป็นต้น (อธิพร สิทธิธีรรัตน์, 2558, น.17)

**5) หลักนิติรัฐ (Legal state: Rechtsstaat)**

คำว่า นิติรัฐ เป็นคำที่ใช้กันในประเทศที่ใช้ระบบประมวลกฎหมาย มีพื้นฐานและวิวัฒนาการมาจากประเทศเยอรมณี ได้มีการศึกษาทางวิชาการในปลายศตวรรษที่ 19 และตั้งแต่กลางศตวรรษที่ 19 ก็ได้มีการใช้คำนี้อย่างแพร่หลาย ในช่วงต้นของศตวรรษที่19 นิติรัฐ หมายถึง รัฐที่ออกกฎหมายอย่างมีเหตุมีผล ในศตวรรษที่ 19 นี้นิติรัฐมิได้หมายถึงเป้าหมายหรือเนื้อหาของรัฐ แต่หมายถึงวิธีการหรือลักษณะของการกระทำเป้าหมายหรือเนื้อหาของรัฐให้เป็นรูปธรรม (กมลชัย รัตนสกาววงศ์, 2537, น.92) มีผู้ให้คำนิยามความหมายของนิติรัฐไว้หลายท่าน อาทิ

 สมยศ เชื้อ ให้คำนิยามคำว่านิติรัฐ หมายถึง รัฐซึ่งยอมรับรองและให้ความคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานของราษฎรไว้ในรัฐธรรมนูญ เพื่อให้ราษฎรใช้สิทธิและเสรีภาพเช่นว่านั้น พัฒนาบุคลิกภาพของตนได้ ดังนั้น รัฐประเภทนี้จึงเป็นรัฐที่มีการจำกัดอำนาจโดยยอมอยู่ภายใต้กฎหมายของตนอย่างเคร่งครัด (สมยศ เชื้อไทย, 2535, น.127)

    หลักนิติรัฐนั้นมีความสำคัญในการขจัดการใช้อำนาจของเจ้าหน้าที่ไม่ให้ใช้อำนาจเป็นไปตามอำเภอใจ จึงมีความเกี่ยวข้องกับสิทธิของบุคคลถือได้ว่าเป็นพื้นฐานของศักดิ์ศรีความเป็นมนุษย์ เพื่อความเป็นอิสระของปัจเจกบุคคลในการพัฒนาบุคลิกภาพของแต่ละบุคคล รัฐจึงต้องให้ความเคารพต่อขอบเขตของสิทธิและเสรีภาพของบุคคล จะแทรกแซงสิทธิและเสรีภาพนั้นมิได้ จะกระทำได้ต่อเมื่อมีกฎหมายซึ่งผ่านความเห็นชอบจากตัวแทนของประชาชนตามหลักความชอบธรรมในทางประชาธิปไตยได้ให้ความเห็นชอบแล้วเท่านั้น จึงจะสามารถกระทำได้ เพื่อให้การคุ้มครองสิทธิของบุคคลมีผลในทางปฏิบัติอย่างแท้จริง (บรรเจิด สิงคะเนติ, 2547)

 ศาสตราจารย์ บุญศรี มีวงศ์อุโฆษ ได้อธิบายว่าประเทศที่มีการใช้หลักนิติรัฐนั้นจะต้องมีลักษณะดังนี้

 1.หลักการแบ่งแยกอำนาจ ไม่ให้อำนาจรัฐแก่ผู้ใดผู้หนึ่งใช้อำนาจเป็นผู้เดียว ให้มีการตรวจสอบถ่วงดุลซึ่งกันและกัน 2. ต้องมีการคุ้มครองสิทธิมนุษยชน ศักดิ์ศรีความเป็นมนุษย์ คือต้องมีมาตรการในการให้ความคุ้มครองสิทธิเสรีภาพของประชาชน 3. กฎหมายจะต้องมีลักษณะที่แน่นอน ชัดเจน ไม่คลุมเครือ 4. ประชาชนมีสิทธิฟ้องร้องหน่วยงานของรัฐให้รับผิดชอบ (ธาริณี มณีรอด, 2559, น.17-18)

 ทั้งนี้บทบัญญัติมาตรานี้ชี้ให้เห็นถึงรากฐานความคิดของหลักนิติรัฐ ในกรณีที่องค์กรนิติบัญญัติสามารถตรากฎหมายจำกัดสิทธิและเสรีภาพของบุคคลไดตามที่รัฐธรรมนูญให้อำนาจองค์กรนิติบัญญัติต้องดำเนินการตรากฎหมายให้สอดคลองกับเงื่อนไขต่าง ๆ อาทิ

 **หลักความได้สัดส่วนพอสมควรแกเหตุ (Principle of proportionality)**

ในการตรากฎหมายจำกัดสิทธิเสรีภาพของบุคคลนั้นในรัฐธรรมนูญ กล่าวว่า จะต้องกระทําไดเท่าที่เป็น การที่รัฐธรรมนูญบัญญัติหลักในเรื่องความจำเป็นไวนี้แสดงให้เห็นว่า เป็นไปตามหลักนิติรัฐและการยอมรับหลักพอสมควรแกเหตุ หลักความพอสมควรแกเหตุนั้นเป็นหลักที่มีการจำกัดอำนาจรัฐไม่ให้เป็นไปโดยอำเภอใจ องค์กรนิติบัญญัติแม้วาโดยสภาพไมใช่เป็นองค์กรที่ใช้อำนาจปกครองล่วงล้ำสิทธิและเสรีภาพของประชาชนโดยตรง แต่องค์กรนิติบัญญัติก็อาจใช้อำนาจรัฐในการตรากฎหมายซึ่งอาจมีผลกระทบต่อสิทธิและเสรีภาพของประชาชนได (วรเจตน ภาคีรัตน์, ม.ป.ป.) ในการตรวจสอบความชอบด้วยกฎหมาย ยังคงมีหลักอื่น ๆ อีกมากมายที่มิได้มีการบัญญัติไว้เป็นลายลักษณ์อักษร เช่น กฎหมายที่ตราขึ้นจำกัดสิทธิและเสรีภาพของปัจเจกชนจะต้องชัดเจนและมีความแน่นอน เป็นต้น

**กฎหมายที่เกี่ยวข้องในเรื่องสิทธิส่วนบุคคลกับการรักษาความมั่นคงปลอดภัยไซเบอร์**

นอกจากผู้ให้บริการอินเตอร์เน็ตจะสามารถรู้ข้อมูลการใช้งานอินเตอร์เน็ต การสื่อสาร ของลูกค้าได้แล้ว ในประเทศไทยยังมีกฎหมายที่ให้อำนาจเจ้าหน้าที่รัฐสามารถเข้ามาขอข้อมูลของประชาชนได้ แต่อำนาจเหล่านี้ก็ต้องมีหลักเกณฑ์การใช้อำนาจที่รอบคอบ มีขอบเขตชัดเจน และถูกตรวจสอบได้ (I law, 2562) กฎหมายฉบับที่ให้รัฐสามารถขอข้อมูลได้คือพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรา62 และมาตรา 66 ในการรวบรวมข้อมูล สามารถขอข้อมูล เข้าถึงข้อมูล เพื่อประโยชน์ในการดำเนินการเพื่อวิเคราะห์สถานการณ์และประเมินผลกระทบภัยคุกคามทางไซเบอร์ และในกรณีเร่งด่วน ตามมาตรา 68 สามารถขอข้อมูลปัจจุบันและต่อเนื่อง และในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ 2560 มาตรา 18 ที่ให้เจ้าหน้าที่รัฐมีอำนาจเข้าถึงข้อมูลอะไรได้บ้าง และในมาตรา 19 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลสามารถเปิดเผยข้อมูลได้ หากมีกฎหมายอื่นบัญญัติให้กระทำได้

 **วิธีดำเนินการวิจัย**

**1. ระเบียบวิธีวิจัย**

การวิจัยฉบับนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative research) โดยได้ทำการศึกษาค้นคว้าจากหนังสือ บทความวิชาการ ข้อมูลข่าวสารจากอินเตอร์เน็ต บทกฎหมายที่เกี่ยวข้อง ตำราทางกฎหมายและทางวิชาการ ที่เกี่ยวข้องกับสิทธิในข้อมูลส่วนบุคคล ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 เพื่อเป็นข้อมูลในการวิเคราะห์ปัญหา สรุปและข้อเสนอแนะ

**2. ขั้นตอนการวิจัย**

ผู้วิจัยกำหนดประเด็นปัญหาเรื่องการละเมิดสิทธิของบุคคลตามมาตรา 62 มาตรา 66 และ มาตรา 68 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 และค้นคว้ากฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล สิทธิมนุษยชนขั้นพื้นฐาน แนวคิดเรื่องการคุ้มครองสิทธิส่วนบุคคลในเรื่องข้อมูลส่วนบุคคล และศึกษาหลักนิติรัฐ เพื่อใช้ในการตีความตัวบทกฎหมายไม่ให้ขัดต่อเจตนารมณ์ของกฎหมาย

**3. การเก็บรวบรวมข้อมูล**

ในการเก็บรวบรวมข้อมูลสำหรับการวิจัยในครั้งนี้ ใช้การเก็บข้อมูลจากแห่งปฐมภูมิที่ได้มาจาก

เอกสารต่าง ๆ เช่น กฎหมายที่เกี่ยวกับการละเมิดสิทธิของบุคคลตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 และแหล่งข้อมูลทุติยภูมิ ได้แก่ หนังสือ บทความวิชาการ วารสารทางกฎหมาย ข้อมูลข่าวสารจากอินเตอร์เน็ต

**4. การวิเคราะห์ข้อมูล**

การวิเคราะห์ข้อมูลในรูปแบบการวิเคราะห์เนื้อหา จากแหล่งปฐมภูมิ ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 และแหล่งข้อมูลทุติยภูมิได้แก่ หนังสือ วารสารทางกฎหมาย ตำรา ข้อมูลข่าวสารจากอินเตอร์เน็ต การคุกคามไซเบอร์ในประเทศไทย แนวคิดและทฤษฎีที่เกี่ยวข้องเพื่อใช้ในการพิจารณาการละเมิดสิทธิของบุคคล และใช้ในการตีความตัวบทกฎหมายเพื่อไม่ให้เป็นการใช้อำนาจเกินขอบเขต

**ผลการวิจัย**

 งานวิจัยเริ่มศึกษาเรื่องการรักษาความปลอดภัยไซเบอร์ นั้นถือกำเนิดจากอินเตอร์เน็ต เทคโนโลยีสารสนเทศและการสื่อสาร จึงตองมีการพัฒนาอย่างมาก การรักษาความปลอดภัยจึงเป็นเรื่องที่สำคัญเพราะความปลอดภัยในโลกไซเบอร์มีความซับซ้อนมากยิ่งขึ้น วิธีการแบบดั้งเดิมจึงไม่ได้คำนึงถึงปัญหาที่เกี่ยวข้องกับการรักษาความปลอดภัยขอมูลขององค์กรและการจัดการกับความเป็นส่วนตัวในปัจจุบัน (borwell, 2018)

 จากการศึกษากรอบแนวคิดทฤษฎีในเรื่อง สิทธิมนุษยชน นั้นเป็นที่รู้จักกันอย่างแพร่หลายนับตั้งแต่ได้มีการก่อตั้งองค์กรสหประชาชาติเป็นต้นมา และเป็นที่ยอมรับกันโดยทั่วไปว่าเป็นสิทธิธรรมชาติ ซึ่งมีความสัมพันธ์กับกฎหมายธรรมชาติ เป็นที่มาของสิทธิมนุษยชนในปัจจุบัน ภายหลังที่ได้มีการก่อตั้งองค์กรสหประชาชาติ ได้มีความร่วมมือในการจัดทำปฏิญญาสากลว่าด้วยสิทธิมนุษยชน และเนื้อหาในปฏิญญาสากลนั้นถือได้ว่าเป็นมาตรฐานของสิทธิมนุษยชนที่หลาย ๆ ประเทศยอมรับ (อุดมศักดิ์ สิทธิพงษ์, 2555, น.57)

 โดยกฎหมายที่เกี่ยวข้องกับการคุ้มครองสิทธิของบุคคล อาทิ ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ได้กล่าวถึงการคุ้มครองสิทธิไว้ใน ข้อ 12 ว่า “บุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย การสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น”

และประเทศไทยได้นำหลักการปฏิญญาสากลมาบรรจุลงไว้ในรัฐธรรมนูญ ว่าด้วยสิทธิและเสรีภาพของประชาชนชาวไทย มาตรา 26มีความว่าการตรากฎหมายที่มีผลเป็นการจำกัดสิทธิหรือเสรีภาพของบุคคลต้องเป็นไปตามเงื่อนไขที่บัญญัติไว้ในรัฐธรรมนูญ ในกรณีที่รัฐธรรมนูญมิได้บัญญัติเงื่อนไขไว้ กฎหมายดังกล่าวต้องไม่ขัดต่อหลักนิติธรรม ไม่เพิ่มภาระหรือจำกัดสิทธิหรือเสรีภาพของบุคคลเกินสมควรแก่เหตุ และจะกระทบต่อศักดิ์ศรีความเป็นมนุษย์ของบุคคลมิได้รวมทั้งต้องระบุเหตุผลความจำเป็นในการจำกัดสิทธิและเสรีภาพไว้ด้วย

มาตรา 32 มีความว่าบุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียงและครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่งหรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ

จากแนวคิดเรื่อง สิทธิมนุษยชนเห็นได้ว่าสิทธิของบุคคลในด้านข้อมูลส่วนบุคคลเป็นสิทธิที่ได้รับความคุ้มครอง การบังคับใช้กฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์นั้นเนื่องจากเป็นกฎหมายที่มีการจำกัดสิทธิเสรีภาพของประชาชน ถ้าหากการกระทำความผิดนั้น มีเหตุร้ายแรงกระทบต่อความปลอดภัยของประชาชน ความมั่นคงของรัฐ ก็เห็นได้มีความสำคัญที่จะมีกฎหมายการรักษาความมั่นคงปลอดภัยไวเบอร์นี้ เมื่อพิจารณาถึงกฎหมายที่เกี่ยวข้องกับสิทธิในข้อมูลส่วนบุคคล มีดังนี้

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับ 2560

ในมาตรา 18 กล่าวคือ “ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวน ในกรณีที่มีเหตุอันควรเชื่อได้ว่า มีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใดดังต่อไปนี้ เฉพาะที่จำเป็น เพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด และหาตัวผู้กระทำความผิด.. (2) เรียกข้อมูลจราจรทางคอมพิวเตอร์ จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ หรือจากบุคคลอื่นที่เกี่ยวข้อง

 (3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการ ให้แก่พนักงานเจ้าหน้าที่...”

**พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562**

มาตรา 62 ในการดำเนินการตามมาตรา 61 นั้นคือ การรวบรวมข้อมูล หรือพยานเอกสาร พยานวัตถุที่เกี่ยวข้อง เพื่อประโยชน์ในการวิเคราะห์สถานการณ์ (2) มีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูลหรือเอกสาร ซึ่งอยู่ในความครอบครองของผู้อื่น เพื่อประโยชน์ในการดำเนินการ และผู้ให้ข้อมูลตามวรรคหนึ่งนั้น ซึ่งกระทำโดยสุจริตย่อมได้รับการคุ้มครองและไม่ถือว่าเป็นการละเมิดหรือผิดสัญญา

และในมาตรา 66 (4) ในการ ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ ให้ กกม. ยื่นคำร้องต่อศาลให้เจ้าหน้าที่ สามารถยึด อายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามไซเบอร์

  แต่ทั้งนี้เมื่อพิจารณามาตรา 61 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 เป็นเรื่องของการที่จะต้องหาหลักฐานหรือระงับภัยคุกคามไซเบอร์ กฎหมายใช้ถ้อยคำในลักษณะคาดการณ์ คือ คาดว่าจะเกิดภัยคุกคาม เมื่อเกิดเหตุการณ์ที่คาดว่าจะเกิดขึ้นในอนาคต คณะกรรมการจึงใช้อำนาจเรียกขอข้อมูลจากผู้ให้บริการ เพื่อหาพยาน และประเมินผลกระทบจากภัยคุกคาม ทำให้ได้ไปทั้งข้อมูลเกี่ยวกับภัยคุกคาม รวมทั้งข้อมูลอื่นด้วย เช่น ข้อมูลจราจรคอมพิวเตอร์ และข้อมูลระบุตัวตนผู้ใช้งาน ทั้งนี้เมื่อผู้ให้บริการให้ข้อมูลไม่ต้องรับผิดในการละเมิดหรือผิดสัญญา (ภูมิ ภูมิรัตน์, 2562)

จากการศึกษาในพระราชบัญญัติมิได้มีการบัญญัติไว้ว่าในการใช้อำนาจตามมาตรานี้จะต้องมีการขอหมายศาลก่อน คณะกรรมการสามารถออกคำสั่งเลย ทั้งนี้ข้อมูลที่ได้ไปนั้นก็มีกฎหมายบัญญัติให้ความคุ้มครองเจ้าของข้อมูลคือ ห้ามเจ้าพนักงานที่ได้ข้อมูลไปเปิดเผยข้อมูลนั้นมีความผิดและมีโทษปรับและจำคุก แต่ว่าในกรณีที่เจ้าหน้าที่ได้ข้อมูลใดมาจากการใช้อำนาจมีข้อยกเว้นว่าหลักข้อห้ามนี้ “มิให้ใช้บังคับในการกระทำเพื่อประโยชน์ในการดำเนินคดีตามกฎหมายนี้หรือกฎหมายอื่น” การบัญญัติข้อยกเว้นไว้เช่นนั้นจะทำให้เกิดการจับกุมได้อย่างกว้าง

นอกจากนั้นจากถ้อยคำในมาตรา 66(4) สามารถ ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เพื่อ ป้องกัน รับมือและลดความความเสี่ยง ผู้ประกอบการบางรายอาจกังวลในการใช้อำนาจของเจ้าหน้าที่ในการเข้าถึงหรือตรวจสอบข้อมูลเพราะกฎหมายมีลักษณะกว้าง ทั้งนี้ข้อมูลในระบบของผู้ประกอบการมีความหลากหลาย ทั้งข้อมูลทั่วไป ข้อมูลของลูกค้า ข้อมูลความลับทางการค้า ข้อมูลทรัพย์สินทางปัญญา ในทางธุรกิจนั้นก็ส่งผลให้นักลงทุนไม่มีความมั่นใจเนื่องจากการบังคับใช้กฎหมายเช่นนี้มีความเสี่ยงต่อข้อมูลของธุรกิจอย่างมาก แต่เมื่อพิจารณาถึงภัยคุกคามไซเบอร์ เป็นเหตุที่เกิดจากการกระทำความผิดต่อระบบคอมพิวเตอร์ การรับมือภัยคุกคามทางไซเบอร์ที่ได้ผล คือ การหยุดชุดคำสั่งของโปรแกรมที่ไม่พึงประสงค์มิใช่การไปหยุดบริการของผู้ประกอบการทางดิจิตอล (คณาธิป ทองรวีวงศ์, 2562)

 **อภิปรายผล**

 หลังจากที่มีการบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 ยังมีบทบัญญัติบางมาตราที่ยังไม่ชัดเจน โดยพิจารณาได้ดังนี้

1.จากบทบัญญัติในมาตรา 60 ที่ให้คณะกรรมการเป็นผู้กำหนดรายละเอียดของลักษณะภัยคุกคามไซเบอร์ เพียงแค่กำหนดว่าภัยนั้นร้ายแรงก็สามารถขอข้อมูลบุคคลได้โดยในมาตรา 62 (2) ให้อำนาจไว้โดยบัญญัติว่า “ในการดำเนินการตามมาตรา 61 เพื่อประโยชน์ในการวิเคราะห์สถานการณ์และประเมินผลผลกระทบจากภัยคุกคามไซเบอร์ ให้เลขาธิการสั่งให้พนักงานเจ้าหน้าที่ดำเนินการดังต่อไปนี้ (2) มีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูลหรือเอกสารที่อยู่ในความครอบครองของผู้อื่นอันเป็นประโยชน์ในการดำเนินการ คือ สามารถขอข้อมูลจากผู้ให้บริการได้ และมิได้มีการบัญญัติไว้ว่าการขอข้อมูลนั้นต้องขอหมายศาลเสียก่อน จึงมีปัญหาในเรื่องของการจำกัดความของคำว่า ข้อมูล ไม่ได้มีนิยามไว้ว่าอย่างไร ทั้งนี้ข้อมูลมีหลายประเภท และก็เป็นข้อมูลส่วนบุคคลที่ควรได้รับความคุ้มครองตามหลักสิทธิมนุษยชน รวมถึงข้อมูลทางการค้าซึ่งเป็นความลับของผู้ให้บริการ ซึ่งอาจเป็นการไปละเมิดสิทธิของเจ้าของข้อมูลเมื่อพิจารณาถึงแนวคิดตามปฏิญญาสากลว่าด้วยสิทธิมนุษยชนที่ว่า “บุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย การสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น” ผู้เขียนมีความเห็นว่าควรนิยามคำว่าข้อมูลไว้ว่ามีอย่างไรบ้างและให้ผู้ให้ข้อมูลเปิดเผยได้เฉพาะข้อมูลที่จำเป็น เพื่อไม่ให้เป็นการละเมิดสิทธิเสรีภาพขั้นพื้นฐานมากเกินไป และควรให้มีการบัญญัติในเรื่องการขอหมายศาลในการไปขอข้อมูล ให้เป็นไปตามหลักนิติรัฐเพื่อให้มีการตรวจสอบถ่วงดุลอำนาจซึ่งกัน เพื่อไม่ให้เกิดการใช้อำนาจตามอำเภอใจ

2.และในบทบัญญัติมาตรา 66 “ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ในระดับร้ายแรง กกม.มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการ.. (4) ยึดหรืออายัดคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามไซเบอร์” และสามารถยึดได้เป็นเวลาไม่เกิน 30 วัน ทั้งนี้หากพิจารณาถึงเจตนารมณ์ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามที่กระทำต่อระบบคอมพิวเตอร์ จึงไม่เห็นว่าเป็นการสมควรที่จะบัญญัติกฎหมายที่ให้อำนาจอย่างกว้างขวางให้เจ้าหน้าที่เช่นนี้ เมื่อพิจารณากฎหมาย Cybersecurity Act2018 ประเทศสิงคโปร์ ได้มีการอธิบายตัวอย่างของมาตรการแก้ไขในการป้องกันและกำจัดภัยคุกคามความปลอดภัยไซเบอร์ ได้แก่ มาตรา 20(2)(b) ที่บัญญัติถึงมาตรการให้การแก้ไขเมื่อได้รับผลกระทบจากเหตุการณ์ทางไซเบอร์ คือ

(a) การลบซอฟต์แวร์ที่เป็นอันตรายออกจากคอมพิวเตอร์

(b) การติดตั้งการอัพเดตซอฟต์แวร์เพื่อจัดการกับความปลอดภัยทางไซเบอร์

(c) ตัดการเชื่อมต่อคอมพิวเตอร์ที่ติดเชื้อชั่วคราวจากเครือข่ายคอมพิวเตอร์จนกระทั่งดำเนินการตามวรรค(a) หรือ(b)” เมื่อพิจารเปรียบเทียบกฎหมายสิงคโปร์เน้นไปที่การป้องกันต้นเหตุของการเกิดภัยคุกคามไซเบอร์แต่ของประเทศไทยเน้นไปที่การใช้อำนาจยึดอายัดเพื่อนำไปตรวจสอบหรือวิเคราะห์ ซึ่งอาจเกิดผลกระทบและอาจไดรับความเสียหายได้ การป้องกันไม่ให้ภัยไซเบอร์เกิดการคุกคามไปมากกว่าเดิมนั้นควรแก้ที่ชุดคำสั่งของโปรแกรมที่ไม่พึงประสงค์ที่เป็นปัญหา มิใช่ไปยึดคอมพิวเตอร์นั้น การยึดเครื่องคอมพิวเตอร์ทำให้เจ้าของระบบต้องหยุดการให้บริการจะเป็นการสร้างความเสียหายแก่ผู้บริโภคและผู้ให้บริการ ซึ่งการหยุดใช้บริการหลายวันจะทำให้เกิดความไม่เป็นธรรมแก่ผู้ประกอบการ และอาจเกิดการกลั่นแกล้งกันได้

**ข้อเสนอแนะ**

1.ผู้เขียนมีความเห็นว่าควรเพิ่มคำจำกัดความของคำว่าข้อมูลโดยการแบ่งข้อมูลเป็น 2 ประเภท ข้อมูลทั่วไป และข้อมูลประเภทที่มีความอ่อนไหว เพื่อที่เจ้าหน้าที่จะไม่ใช้อำนาจได้อย่างกว้างขวางให้เจ้าหน้าที่สามารถขอข้อมูลทั่วไปได้เท่านั้น และแก้ไขบทบัญญัติในมาตรา 62 โดยเพิ่มวรรคสามมีความว่า “ผู้ครอบครองข้อมูลต้องให้ความร่วมมือในการให้ข้อมูล และให้ความสะดวกตามมาตรา 61 แก่เจ้าหน้าที่ หากไม่ให้ข้อมูลก็ไม่เป็นความผิด และการดำเนินการตาม (2) ให้ กกม.ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง”

2.แก้ไขบทบัญญัติมาตรา 66 “ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ในระดับร้ายแรง กกม.มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการ.. (4) ยึดหรืออายัดคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามไซเบอร์” เมื่อเปรียบเทียบจากมาตรการแก้ไขปัญญาของต่างประเทศควรยกเลิกบทบัญญัติในอนุมาตรานี้เสีย โดยบัญญัติใหม่ว่า “มาตรา 66 ในการป้องกัน รับมือ และลดความเสี่ยงและลดความเสี่ยงจากภัยคุกคามไซเบอร์ในระดับร้ายแรง กกม.มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการ.. (4) มีหนังสือแจ้งให้ผู้ครอบครองคอมพิวเตอร์ทำการลบซอฟต์แวร์ที่เป็นอันตรายออกจากคอมพิวเตอร์ และมีการติดตั้งการอัพเดตซอฟต์แวร์เพื่อจัดการกับความปลอดภัยทางไซเบอร์

 **กิตติกรรมประกาศ**

งานวิจัยนี้สำเร็จลุล่วงได้ด้วยความกรุณาจากอาจารย์ภาวิตา ค้าขาย อาจารย์ที่ปรึกษางานวิจัย ในการช่วยเหลือให้คำปรึกษาและชี้แนะแนวทางในการทำวิจัย อีกทั้งให้คำนำและข้อคิดเห็นต่าง ๆ อันเป็นคุณประโยชน์

และที่สำคัญผู้เขียนขอกราบขอบพระคุณบิดา มารดา ที่สนับสนุนผู้เขียนในทางการศึกษา ทั้งด้านกำลังในและทุนทรัพย์ตลอดมา

ผู้เขียนหวังว่า วิจัยฉบับนี้จะเป็นประโยชน์แก่การศึกษากฎหมายบ้าง ไม่มากก็น้อย หากมีข้อผิดพลาดประการใด ต้องขออภัยมา ณ ที่นี้ด้วย

  **เอกสารอ้างอิง**

**หนังสือภาษาไทย**

กมลชัย รัตนสกาววงศ์.(2537).**หลักกฎหมายปกครองเยอรมัน.**กรุงเทพฯ:สำนักพิมพ์นิติธรรม

บุญศรี มีวงศ์อุโฆษ.(2549).**หลักการใช้อำนาจขององค์กรที่ต้องคำนึงถึงศักดิ์ศรีความเป็นมนุษย์สิทธิ**

**และเสรีภาพ ตามรัฐธรรมนูญ(รายงานการวิจัย)**.กรุงเทพฯ:บริษัทพีเพรสจำกัด

**พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2525.** พิมพ์ครั้งที่ 1 : อักษรเจริญทัศน์. กรุงเทพฯ, 2525

มานิต จุมปา.(2557).**หลักกฎหมายรัฐธรรมนูญ พิมพ์ครั้งที่ 2**.กรุงเทพฯ:สำนักพิมพ์นิติธรรม

ธนา เวสโกสิทธิ์ (2559).**หลักสิทธิมนุษยชนกับหลักนิติธรรม**.วารสารศาลรัฐธรรมนูญ,18(52),102-105

สมยศ เชื้อไทย.(2535).**คำอธิบายหลักรัฐธรรมนูญทั่วไป พิมพ์ครั้งที่2**.กรุงเทพฯ:เรือนแก้วการพิมพ์.

อุดมศักดิ์ สินธิพงษ์.(2555).**สิทธิมนุษยชน พิมพ์ครั้งที่5**.กรุงเทพฯ:สำนักพิมพ์วิญญูชน

**เอกสารอิเล็กทรอนิกส์**

คณาธิป ทองรวีวงศ์.(2555).**มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว: ศึกษากรณีการรบกวนสิทธิในความเป็นอยู่ส่วนตัวจากการใช้เว็บไซต์เครือข่ายสังคม.วารสารวิชาการสมาคมสถาบันอุดมศึกษาเอกชนแห่งประเทศไทย)**, 18(2).สืบค้น 30 กรกฎาคม 2562 จาก [file:///C:/Users/User/Downloads/29726-Article%20Text-65383-1-10-20150128.pdf](file:///C%3A%5CUsers%5CUser%5CDownloads%5C29726-Article%20Text-65383-1-10-20150128.pdf)

ดาวัลย์ ขาวสนิท.(2561).**มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล:ศึกษาเฉพาะกรณี**

**ด้านการเงินการธนาคารของธนาคารพาณิชย์.(วิทยานิพนธ์มหาบัณฑิต) มหาวิทยาลัยธุรกิจบัณฑิตย์**. สืบค้นเมื่อ 20 กรกฎาคม 2562,จาก <http://libdoc.dpu.ac.th/thesis/Dawan.Kha.pdf>

บริษัทกสท.โทรคมนาคม จำกัด (มหาชน), **ภัยคุกคามทางไซเบอร์กับกฎหมายไซเบอร์ไทย** [online], 1 กรกฎาคม 2562, แหล่งที่มา <https://www.catcyfence.com/it-security/it-360/cybersecurity-threats-with-thai-laws/>

บรรเจิด สิงคะเนติ.(2547).**การควบคุมและตรวจสอบการใช้อำนาจของรัฐ**.สืบค้น 27 กรกฎาคม 2562

จาก <http://public-law.net/publaw/view.aspx?id=241>

ธาริณี มณีรอด.(2559).**ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล.**

**(วิทยานิพนธ์มหาบัณฑิต) มหาวิทยาลัยธุรกิจบัณฑิตย์** สืบค้นเมื่อ 20 กรกฎาคม 2562,จาก <http://libdoc.dpu.ac.th/thesis/159690>.pdf

วรเจตน ภาคีรัตน์.(ม.ป.ป.).**เงื่อนไขการตรากฎหมายจำกัดสิทธิและเสรีภาพของประชาชน : “มาตร” ในการควบคุมตรวจสอบความชอบด้วยรัฐธรรมนูญของกฎหมาย**.สืบค้น 30 กรกฎาคม 2562 จาก <http://lawwebservice.com/lawsearch/AcharnVorachet03.pdf>

อธิพร สิทธิธีรรัตน์.(2558).**ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์.(วิทยานิพนธ์มหาบัณฑิต)**.มหาวิทยาลัยธรรมศาสตร์ สืบค้นเมื่อ 1 สิงหาคม 2562 จาก <http://ethesisarchive.library.tu.ac.th/thesis/2015/TU_2015_5701033531_3922_2696.pdf>

Borwell.(2018).**The Evolution of Cyber Security**. Retrieved Sep 3, 2019, from <https://borwell.com/2018/11/08/the-evolution-of-cyber-security/>

ETDA.(2560). **Analytic, Intelligence & Response.**สืบค้น 10 กันยายน 2562, จาก [file:///C:/Users/User/Downloads/RSA%20Conference%202017%20Report%20%E0%B9%82%E0%B8%94%E0%B8%A2%20ETDA%20(3).pdf](file:///C%3A%5CUsers%5CUser%5CDownloads%5CRSA%20Conference%202017%20Report%20%E0%B9%82%E0%B8%94%E0%B8%A2%20ETDA%20%283%29.pdf)