บทความวิจัย

มาตรการทางกฎหมายในการคุ้มครอง ป้องกันการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์*

LEGAL MEASURES TO PROTECT AND PREVENT THE IMPORTATION OF PERSONAL DATA VIA COMPUTERS IN ACCORDANCE WITH THE LAW ON COMPUTER CRIME

เกียรติเฉลิม รักษ์งาม*, สังเวียน เทพผา
Kiatchaloem Raknga*, Sungwian Theppha
คณะนิติศาสตร์ มหาวิทยาลัยปทุมธานี ปทุมธานี ประเทศไทย
Doctor of Laws, Pathumthani University, Pathum Thani, Thailand
*Corresponding author E-mail: c.hal.oem@hotmail.com

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ 1) วิเคราะห์ความแตกต่างของมาตรการทางกฎหมายของต่างประเทศและประเทศไทยที่เกี่ยวข้องกับการคุ้มครองการนำเข้าข้อมูลทางคอมพิวเตอร์ 2) ศึกษาปัญหาอุปสรรคและข้อจำกัดของมาตรการทางกฎหมายในการคุ้มครองการนำเข้าข้อมูลทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ 3) เสนอแนวทางการแก้ไขมาตรการทางกฎหมายในการคุ้มครองการนำเข้าข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ โดยใช้วิธีการวิจัยเชิงคุณภาพ ประกอบด้วย การวิเคราะห์เอกสาร และการสัมภาษณ์เชิงลึก ผู้เชี่ยวชาญด้านกฎหมาย จำนวน 12 ท่าน ผลการวิจัยพบว่า กฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของต่างประเทศ เน้นการคุ้มครองข้อมูลส่วนบุคคล การกระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นอาชญากรรม เป็นภัยร้ายแรงต่อเศรษฐกิจสังคม และความมั่นคงของประเทศ ระดับการคุ้มครองสูงกว่ากฎหมายของประเทศไทย ตระหนักถึงความรุนแรงของผลที่ตามมา มีบทลงโทษตามระดับความเสียหาย มีค่าปรับสูง แต่กฎหมายของประเทศไทยมองว่าอาชญากรรมทางคอมพิวเตอร์เป็นปัญหาเฉพาะกลุ่ม ไม่ส่งผลกระทบในวงกว้าง เน้นความเสียหายที่เกิดขึ้นจริง บทลงโทษเน้นการจำคุก ปัญหาของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ได้แก่ คำจำกัดข้อมูลส่วนบุคคลไม่ชัดเจน สร้างความสับสนกับองค์กรในการนำเข้าข้อมูล ยากต่อการบังคับใช้กฎหมาย มีการบัญญัติถึงการนำเข้าข้อมูลคอมพิวเตอร์ แต่ไม่เน้นการคุ้มครองข้อมูลส่วนบุคคล บทลงโทษไม่รุนแรง ไม่สามารถยับยั้งการละเมิดกฎหมายได้ แนวทางการแก้ไขกฎหมายในการคุ้มครองการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์ คือ ควรการแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ให้มีความชัดเจน เพิ่มบทลงโทษให้รุนแรงขึ้น พัฒนากลไกการติดตามและตรวจสอบประสิทธิภาพ และส่งเสริมความร่วมมือระหว่างประเทศ

คำสำคัญ: มาตรการทางกฎหมาย การนำเข้าข้อมูลทางคอมพิวเตอร์ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

Abstract

The purposes of this research are to 1) analyze the differences in legal measures of foreign countries and Thailand related to the protection of computer data imports, 2) study the

* Received 3 March 2024; Revised 20 March 2024; Accepted 23 March 2024

problems, obstacles and limitations of legal measures to protect the import of computer data on computers according to the Computer Crimes Act and 3) propose guidelines for revising legal measures to protect the import of computer data according to the Computer Crimes Act. Using qualitative research methods including document analysis. and in-depth interviews Legal experts, 12 people. The research results found that Laws regarding foreign computer crimes Focus on protecting personal information Computer crimes are crimes. It is a serious threat to the economy, society, and national security. The level of protection is higher than Thai law. Realize the severity of the consequences. There are penalties based on the level of damage and high fines, but Thai law views computer crime as a specific problem. It does not have a wide impact. Focus on actual damage. The punishment emphasizes imprisonment. Problems with the Computer Crime Act include: The definition of personal data is unclear. It creates confusion for organizations when importing data, difficult to enforce the law there are provisions regarding the importation of computer data. But it does not focus on protecting personal information. The punishment is not severe. Unable to stop violations of the law guidelines for amending the law to protect the import of personal data via computer is to amend the Computer Crime Act (No. 2) B.E. 2017 to make it clear. Increase the severity of the punishment Develop a mechanism for tracking and monitoring performance, and promote international cooperationใ

Keywords: Legal Measures, Importing Data Via Computer, Computer Crime Act

บทนำ

วิวัฒนาการทางเทคโนโลยีสารสนเทศที่ก้าวไปอย่างรวดเร็ว ทำให้ผู้คนจำนวนมากหันมาใช้เครือข่ายสังคมออนไลน์กันอย่างแพร่หลาย โดยสร้างบัญชีการใช้งานเครือข่ายสังคมออนไลน์เพื่อการติดต่อสื่อสาร การส่งต่อข้อมูล การซื้อขายและการโฆษณาสินค้า เช่น เฟสบุ๊ค ยูทูบ วอสแอ๊บ วีแชท อินสตาแกรม ติ๊กต๊อก และ ทวิตเตอร์ เป็นต้น ทำให้การติดต่อสื่อสารสะดวกรวดเร็วมากยิ่งขึ้น ซึ่งการติดตั้งแอบพลิเคชั่นดังกล่าวได้มีการรวบรวม ใช้และการเปิดเผยข้อมูลส่วนบุคคล การกระทำดังกล่าวจะมีทั้งผู้ให้บริการและผู้ใช้งานเครือข่ายออนไลน์ที่ทำให้เกิดความเดือดร้อนรำคาญ รวมถึงสร้างความเสียหายให้กับเจ้าของข้อมูล อีกทั้งยังมีการนำข้อมูลส่วนบุคคลไปแสวงหาผลประโยชน์ หรือนำมาเปิดเผยโดยที่เจ้าของข้อมูลไม่ได้ยินยอม และไม่ทราบล่วงหน้าว่ามีบุคคลอื่นนำข้อมูลไปเผยแพร่ ซึ่งการนำข้อมูลไปใช้ ขโมยตัวตน การละเมิดความเป็นส่วนตัวทำให้เจ้าของข้อมูลไม่ได้รับความปลอดภัยต่อข้อมูลของตนเอง (ปัทมา มัญชุนากร, 2565) การใช้งานเทคโนโลยีสารสนเทศและการสื่อสารโดยใช้อินเทอร์เน็ตเป็นสื่อกลางในการเชื่อต่อสังคมและโลกเข้าด้วยกันทำให้เกิดประโยชน์กับการติอต่อสื่อสาร การติดตามสถานการณ์ต่าง ๆ ที่เกิดขึ้นในสังคมอย่างง่ายดาย การดำเนินชีวิตของประชาชนเริ่มเปลี่ยนไปจากโลกจริง หันมาสนใจใช้ชีวิตบนโลกไซเบอร์มากขึ้น ไม่ว่าจะเพื่อซื้อสินค้า หรือการใช้บริการต่าง ๆ เช่น การพาณิชย์อิเล็กทรอนิกส์ (e-commerce) การรับส่งไปรษณีย์อิเล็กทรอนิกส์ (e-mail) รวมถึงการใช้เครือข่ายสังคมออนไลน์ที่นับวันเข้ามาเป็นส่วนหนึ่งของการใช้ชีวิตของคนในสังคมโดยไม่รู้ตัว การใช้เครือข่ายสังคมออนไลน์จะมีทั้งการใช้อย่างสร้างสรรค์และเป็นประโยชน์เพื่อใช้ข้อมูลข่าวสารเกี่ยวกับภัยพิบัติที่จะเกิดขึ้น และการใช้ในการร่วมมือกับกลุ่มมิจฉาชีพสำหรับหลอกลวงผู้อื่น (รุ่งอรุณ รุ่งทองคำกุล, 2558) อีกทั้ง อาชญากรรมไซเบอร์เป็นเรื่องใกล้ตัว เป็นเพราะเทคโนโลยีเข้ามามีบทบาทในการใช้ชีวิตของประชาชนมากขึ้น ซึ่งอาชญากรรมทางไซเบอร์ เป็นอาชญากรที่ประกอบอาชญากรรมที่ฉลาดมากขึ้น สามารถใช้เทคโนโลยีที่ล้ำหน้ากว่าเจ้าหน้าที่ไปมาก จึงไม่ควรประเมิน

ความสามารถของคนกลุ่มนี้ต่ำเกินไป และเป็นอาชญากรรมที่ไม่มีเชื้อชาติ ไม่มีขอบเขตของประเทศ (พัฒนะ ศุกรสุต, 2563)

การละเมิดข้อมูลส่วนบุคคลเป็นปัญหาที่เกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศและการสื่อสาร เพราะมีการใช้บริการบนอินเทอร์เน็ตเป็นตัวเชื่อมต่อระบบการสื่อสาร ทำให้อินเทอร์เน็ตได้กลายเป็นส่วนสำคัญในชีวิตประจำวันของบุคคลทุกเพศทุกวัย เช่น การซื้อขายสินค้าและบริการด้วยระบบออนไลน์อีกทั้งผู้ให้บริการมักเรียกร้องให้มีการสมัครใช้บริการ หรือลงทะเบียนเป็นสมาชิก โดยให้ผู้ใช้บริการกรอกรายละเอียดส่วนตัว เช่น ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ ที่อยู่จดหมายอิเล็กทรอนิกส์ รวมทั้งหมายเลขบัตรประจำตัวประชาชน ที่มีการจัดเก็บประมวลผล หรือนำไปใช้ หรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล และอาจทำให้บุคคลที่เป็นเจ้าของข้อมูลได้รับความเสียหาย หรือข้อมูลส่วนบุคคลอาจถูกนำไปเผยแพร่ยังสื่อสังคมออนไลน์ อีกทั้งปัญหาการก่ออาชญากรรมที่เกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศและการสื่อสารนับว่าเป็นการยากลำบากในการติดตาม การกระทำดังกล่าวถ้ารัฐบาลไม่มีกฎเกณฑ์หรือมาตรการใด ๆ มารองรับ ไม่ก้าวให้ทันเทคโนโลยี ความโกลาหลก็ย่อมจะเกิดขึ้น ยิ่งคอมพิวเตอร์มีความสำคัญและเข้ามาเกี่ยวข้องกับชีวิตประจำวันของคนมากขึ้นเท่าไร ความเสียหายจากการก่ออาชญากรรมทางคอมพิวเตอร์ก็จะทีวีคูณความรุนแรงมากขึ้นเป็นเงาตามตัว เพื่อป้องกันความเสียหายอันจะเกิดจากกรณีดังกล่าว และปราบปรามผู้กระทำความผิด กระทั่งเป็นการป้องกันอธิปไตยของประเทศทางเครือข่ายคอมพิวเตอร์ รัฐบาลจึงต้องตรากฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ขึ้น อีกทั้งการได้มาซึ่งข้อมูลส่วนบุคคลในปัจจุบันนั้นมีช่องทางค้นหาได้อย่างง่ายดายจากผู้ซึ่งมีความรู้ในด้านคอมพิวเตอร์ รวมทั้งบุคคลที่ทำหน้าที่เก็บข้อมูลของลูกค้า หรือบุคคลทั่วไปที่สามารถโจรกรรมข้อมูลจากระบบอินเทอร์เน็ต ซึ่งมักจะนำข้อมูลส่วนบุคคลของคนอื่นไปแอบอ้างทำธุรกรรมโดยที่เจ้าของมิได้อนุญาต หรือแม้กระทั่งหมายเลขโทรศัพท์เพื่อโทรมาก่อกวนสร้างความรำคาญหรือข่มขู่เจ้าของข้อมูลเพื่อเรียกร้องค่าเสียหาย โดยแอบอ้างว่าเป็นเจ้าหน้าที่ธนาคาร ตำรวจ กล่าวอ้างว่าเจ้าของข้อมูลนั้นกระทำความผิด ไปกู้ยืมเงิน หรือไปทำสิ่งผิดกฎหมาย ใช้โทรศัพท์ติดต่อมารบกวน ทำให้เจ้าของข้อมูลนั้นได้รับผลกระทบ เช่น สูญเสียเงินทอง หรือเกิดความรำคาญ แม้ว่าเหตุการณ์เหล่านี้จะเกิดขึ้นกับประชาชนเพิ่มมากขึ้น แต่ก็ไม่สามารถที่จะจับตัวผู้กระทำความผิดได้ (สุนทร เปลี่ยนสี, 2551)

ปัญหาจากการจัดเก็บและเผยแพร่ข้อมูลส่วนบุคคลบนโลกออนไลน์ที่ส่งผลกระทบต่อผู้ใช้บริการที่เป็นเจ้าของข้อมูล ที่ผ่านมาการทำความเข้าใจความเป็นส่วนตัวออนไลน์ในสังคมไทยมักมีข้อจำกัด แม้ว่าประเทศไทยมีกฎหมายคุ้มครองข้อมูลในภาคบริการต่าง ๆ เช่น การคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความดูแลของรัฐตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พุทธศักราช 2540 การคุ้มครองข้อมูลผู้ป่วยตามพระราชบัญญัติสุขภาพแห่งชาติ พุทธศักราช 2550 การคุ้มครองข้อมูลเครดิตตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พุทธศักราช 2545 (ปรับปรุง พ.ศ. 2551) แต่ก็ยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เป็นการเฉพาะสำหรับการนำเข้าข้อมูลทางคอมพิวเตอร์ ถึงแม้ว่าอินเทอร์เน็ตจะเข้ามามีบทบาทในชีวิตของผู้คนในหลายมิติ ทำให้เกิดปัญหาเกี่ยวกับการนำเข้าข้อมูลส่วนบุคคลทางอินเทอร์เน็ตเพื่อกลั่นแกล้งกัน โดยข้อมูลส่วนบุคคลที่มีการเผยแพร่ในเว็บไซต์ ได้แก่ ชื่อ นามสกุล เลขประจำตัวประชาชน ที่อยู่ ภาพถ่าย อีเมล หมายเลขโทรศัพท์ สถานที่ทำงาน เลขบัญชีธนาคาร ข้อมูลการเดินทาง ตำแหน่งที่ตั้ง ผลการเรียน สิ่งเหล่านี้ล้วนเป็นข้อมูลที่กระจายในพื้นที่ต่าง ๆ บนเครือข่ายอินเทอร์เน็ต ทั้งธนาคาร สถานศึกษา หน่วยงานราชการ และภาคธุรกิจ อย่างไรก็ตาม พื้นที่ส่วนใหญ่ที่มีข้อมูลดังกล่าวกระจายอยู่นั้นจะมีลักษณะการใช้งานที่เอื้อต่อการส่งผ่านข้อมูลได้ง่าย โดยใช้ปุ่มเดียวก็สามารถกระจายภาพได้ จึงเป็นเครื่องมือที่เปิดโอกาสให้ผู้ใช้เป็นผู้ผลิต เผยแพร่ข้อความ และรูปภาพต่าง ๆ ด้วยตนเอง รวมทั้งความสามารถในการเข้าถึงได้จากอุปกรณ์สื่อสารหลายประเภท (เครือข่ายพลเมืองเน็ต, 2557) เมื่ออินเทอร์เน็ตเข้ามามีบทบาทต่อชีวิตคนอย่างมาก ตั้งแต่การมีตัวตนบนสื่อสังคมออนไลน์ การสื่อสาร ธุรกรรมการเงิน จนกระทั่งการสร้างพื้นที่เสมือนจริง ถึงแม้ว่าจะทำให้มีความสะดวกสบาย แต่สิ่งที่เกิดขึ้นตามมาคือ การ

ก่ออาชญากรรม ข้อมูลจาก Statista ชี้ให้เห็นว่าเมื่อปี ค.ศ. 2022 (พ.ศ. 2565) สถิติการก่ออาชญากรรมบนโลกออนไลน์มีมากกว่า 650,000 คดีทั่วโลก คดีที่เกิดขึ้นมากที่สุด 3 อันดับแรก คือ 1) การหลอกลวงโดยแอบอ้างตนเองเพื่อการเข้าถึงข้อมูลส่วนบุคคล 2) การละเมิดข้อมูลส่วนบุคคล และ 3) การโกงการซื้อขายทางออนไลน์ เช่น ได้รับเงินแล้ว แต่ไม่มีการจัดส่งสินค้าตามที่ตกลง ซึ่งความเสียหายที่เกิดขึ้นนี้หน่วยงานรวบรวมข้อมูลความปลอดภัยไซเบอร์ (Cybersecurity Ventures) คาดการณ์ว่าระหว่างปี ค.ศ. 2021-2025 (พ.ศ. 2564-2568) ค่าใช้จ่ายสำหรับการป้องกันการโจมตีทางไซเบอร์ทั่วโลกจะมีมูลค่าสูงถึง 1.75 ล้านล้านดอลลาร์สหรัฐฯ หรือเพิ่มขึ้นร้อยละ 15 ต่อปี ส่งผลให้โลกออนไลน์กลายเป็นพื้นที่สำหรับอาชญากรรม ดังที่มีทฤษฎีทางอาชญาวิทยาเข้ามาเกี่ยวข้อง คือ 1) ทฤษฎีไร้ตัวตน ระบุว่า การที่คนกล้าทำความผิดบนโลกออนไลน์ ส่วนหนึ่งเป็นเพราะการไร้ตัวตน ความนิรนามบนโลกออนไลน์ที่ไม่สามารถระบุตัวตนของผู้กระทำความผิดได้ จึงทำให้เกิดความเชื่อมั่นว่าสามารถหลบหนีจากความผิดได้ จึงเป็นเหตุผลให้คนกล้าก่ออาชญากรรมมากขึ้น 2) ทฤษฎีเปลี่ยนพื้นที่ ที่มีสมมติฐานเกี่ยวกับพัฒนาการทางเทคโนโลยี กิจกรรมต่าง ๆ ที่ถูกย้ายจากโลกจริงเข้าไปสู่โลกเสมือนที่ไม่หยุดนิ่ง มีการเคลื่อนไหวตลอดเวลา ส่งผลให้อาชญากรรมไม่ต้องแบกรับสถานภาพบางอย่างแบบเดียวกับโลกจริง เช่น สถานะทางสังคม ความมีชื่อเสียง จนทำให้ผู้คนตัดสินใจก่ออาชญากรรมบนโลกออนไลน์มากยิ่งขึ้น (สาวิตรี สุขศรี และปวีร์ เจนวีระนนท์, 2566)

ด้วยเหตุผลดังกล่าว ผู้วิจัยได้เล็งเห็นถึงปัญหาและความสำคัญที่จะเกิดขึ้นในอนาคต จึงสนใจศึกษามาตรการทางกฎหมายเกี่ยวกับในการคุ้มครองข้อมูลส่วนบุคคลในการนำเข้าข้อมูลคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ทั้งนี้ผลที่ได้อาจนำไปใช้เป็นแนวทางสำหรับพิจารณาเพื่อการปรับปรุงมาตรการทางกฎหมายให้ครอบคลุมถึงประชาชนทั่วไป เพื่อให้เกิดความปลอดภัยจากการใช้เทคโนโลยีดิจิทัลและการสื่อการผ่านอินเทอร์เน็ต และทำให้ประชาชนจะได้รับประโยชน์จากการทางกฎหมายที่สามารถเรียกร้องค่าเสียหายในกรณีที่ถูกนำข้อมูลส่วนบุคคลของเจ้าของข้อมูลไปใช้ในทางที่ไม่ถูกต้อง

วัตถุประสงค์ของการวิจัย

1. เพื่อวิเคราะห์ความแตกต่างของมาตรการทางกฎหมายของต่างประเทศและประเทศไทยที่เกี่ยวข้องกับการคุ้มครองการนำเข้าข้อมูลทางคอมพิวเตอร์
2. เพื่อศึกษาปัญหาอุปสรรคและข้อจำกัดของมาตรการทางกฎหมายในการคุ้มครองในการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
3. เพื่อเสนอแนวทางการแก้ไขปัญหาทางกฎหมายในการคุ้มครองในการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) ผู้วิจัยดำเนินการวิจัยโดยใช้วิธีการวิจัยเอกสาร (Documentary Research) ด้วยการศึกษาและวิเคราะห์ข้อมูลที่ได้จากแนวคิด ทฤษฎีที่เกี่ยวข้องกับมาตรการทางกฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ การคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ทำการสืบค้นข้อมูลทางอินเทอร์เน็ต บทความทางวิชาการ รวมทั้งการเก็บรวบรวมข้อมูลภาคสนามโดยใช้การสัมภาษณ์ผู้ทรงคุณวุฒิทางด้านกฎหมาย และนักวิชาการด้านกฎหมาย ตลอดจนเจ้าหน้าที่ที่ทำหน้าที่ในการควบคุมดูแลการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ โดยเครื่องมือที่ใช้เก็บรวบรวมข้อมูลแบ่งออกเป็น 2 ประเภท ดังนี้

1. ข้อมูลปฐมภูมิ เป็นข้อมูลที่ได้จากการสัมภาษณ์เชิงลึก ด้วยการออกแบบสัมภาษณ์แบบมีโครงร่าง โดยกำหนดประเด็นการสัมภาษณ์เพื่อให้ผู้สัมภาษณ์มีอิสระในการให้ข้อมูลและแสดงความคิดเห็นเกี่ยวกับ

มาตรการทางกฎหมายในการคุ้มครองและป้องกันการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์ และเพื่อให้ได้ข้อมูลเชิงลึกที่เหมาะสมในการนำไปสู่แนวทางการพัฒนามาตรการทางกฎหมาย

2. ข้อมูลทุติยภูมิ เป็นข้อมูลที่ได้จากเอกสารโดยการรวบรวมจาก แนวคิด และทฤษฎี ผลงานวิจัยที่เกี่ยวข้อง รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 และตัวบทกฎหมายที่เกี่ยวข้อง หนังสือ ตำรา เอกสารวิชาการด้านกฎหมาย คำพิพากษาศาลฎีกา และเอกสารที่เกี่ยวข้องกับการกระทำความผิดต่อข้อมูลอิเล็กทรอนิกส์

ผลการวิจัย

1. การวิเคราะห์ความแตกต่างของมาตรการทางกฎหมายของต่างประเทศและประเทศไทยที่เกี่ยวข้องกับการคุ้มครองการนำเข้าข้อมูลทางคอมพิวเตอร์

กฎหมายต่างประเทศที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ได้แก่ General Data Protection Regulation (GDPR) เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป มีผลบังคับใช้ตั้งแต่วันที่ 25 พฤษภาคม 2561 กำหนดหลักเกณฑ์และวิธีการในการนำเข้าข้อมูลส่วนบุคคลจากประเทศนอกสหภาพยุโรป กฎหมายฉบับนี้ออกโดยสหภาพยุโรป (EU) กำหนดหลักเกณฑ์และวิธีการในการนำเข้าข้อมูลส่วนบุคคล โดยให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล ต้องปฏิบัติตามหลักเกณฑ์ในการเก็บ รวบรวม ใช้ เปิดเผย วิเคราะห์ และลบข้อมูลส่วนบุคคลรวมถึงสิทธิของเจ้าของข้อมูล องค์กรที่นำเข้าข้อมูลต้องปฏิบัติตาม GDPR อย่างเคร่งครัด มิฉะนั้นจะต้องเผชิญกับบทลงโทษที่รุนแรง สำหรับ EU-U.S. Privacy Shield กรอบความร่วมมือระหว่างสหภาพยุโรปและสหรัฐอเมริกา กำหนดมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลสำหรับบริษัทในสหรัฐอเมริกาที่รับข้อมูลส่วนบุคคลจากสหภาพยุโรป ส่วนกฎหมายของสหรัฐอเมริกา CCPA (California Consumer Privacy Act) เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของรัฐแคลิฟอร์เนีย คล้ายกับ GDPR แต่มีขอบเขตจำกัดเฉพาะในรัฐแคลิฟอร์เนีย สหรัฐอเมริกาให้สิทธิแก่ผู้บริโภคในการเข้าถึงข้อมูลส่วนบุคคลของตน ขอให้ลบข้อมูลส่วนบุคคลและปฏิเสธการขายข้อมูลส่วนบุคคล นอกจากนี้กฎหมายของประเทศสเปน คือ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales: กฎหมายนี้ปรับปรุงกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับ GDPR ของ EU เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เข้มงวด องค์กรต้องได้รับความยินยอมจากบุคคลก่อนเก็บหรือประมวลผลข้อมูลส่วนบุคคล มีการกำหนดโทษสำหรับอาชญากรรมทางคอมพิวเตอร์ เช่น การแฮ็ก การโจมตีไซเบอร์ และการเผยแพร่เนื้อหาที่ผิดกฎหมาย เนื้อหาลามกอนาจาร เนื้อหาปลุกระดมความเกลียดชัง และเนื้อหาเกี่ยวกับการก่อการร้าย การละเมิดลิขสิทธิ์ถือว่าเป็นอาชญากรรม ผู้กระทำผิดอาจถูกปรับหรือจำคุก

กฎหมายของประเทศไทย ประกอบด้วย พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พุทธศักราช 2545 กำหนดให้บริษัทข้อมูลเครดิตต้องเก็บรักษาข้อมูลเครดิตของบุคคลอย่างปลอดภัย และเปิดเผยข้อมูลเครดิตได้เฉพาะกรณีที่มีกฎหมายกำหนด พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 เป็นกฎหมายหลักที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในประเทศไทย มีบทบัญญัติเกี่ยวกับการนำเข้าข้อมูลคอมพิวเตอร์ที่ผิดกฎหมาย และเน้นการป้องกันการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ มีบทลงโทษสำหรับผู้ที่นำเข้าข้อมูลคอมพิวเตอร์โดยมิชอบ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ไม่ได้กำหนดรายละเอียดเกี่ยวกับวิธีการนำเข้าข้อมูลส่วนบุคคล พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 (PDPA) เป็นกฎหมายฉบับแรกของไทยที่คุ้มครองข้อมูลส่วนบุคคล กำหนดหลักเกณฑ์และวิธีการในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล องค์กรที่นำเข้าข้อมูลส่วนบุคคลต้องปฏิบัติตาม PDPA อย่างเคร่งครัด มิฉะนั้นจะต้องเผชิญกับบทลงโทษ นอกจากนี้ยังมี กฎหมายอื่น ๆ กฎหมายของประเทศไทยบางฉบับมีบทบัญญัติ

เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เช่น ประมวลกฎหมายอาญา ประมวลกฎหมายแพ่งและพาณิชย์ พระราชบัญญัติการประกอบธุรกิจข้อมูลข่าวสาร พุทธศักราช 2540

การวิเคราะห์ความแตกต่าง พบว่า GDPR และ CCPA มุ่งเน้นการคุ้มครองข้อมูลส่วนบุคคล ส่วนพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 มุ่งเน้นไปที่การป้องกันอาชญากรรมทางคอมพิวเตอร์ ระดับการคุ้มครองของ GDPR และ CCPA ให้ระดับการคุ้มครองข้อมูลส่วนบุคคลสูงกว่าพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 อีกทั้งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ไม่ได้กำหนดรายละเอียดเกี่ยวกับวิธีการนำเข้าข้อมูลส่วนบุคคล ส่วนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 (PDPA) เป็นกฎหมายใหม่ที่กล่าวถึงประเด็นการถ่ายโอนข้อมูลส่วนบุคคลไปต่างประเทศโดยเฉพาะ รวมถึงข้อกำหนดในการได้รับความยินยอมและการรับรองการคุ้มครองที่เหมาะสม และองค์กรที่นำเข้าข้อมูลส่วนบุคคลเข้ามาในประเทศไทยต้องปฏิบัติตาม PDPA ด้วย

2. ปัญหาอุปสรรคและข้อจำกัดของมาตรการทางกฎหมายในการคุ้มครองการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ผู้ให้ข้อมูลส่วนใหญ่มีความคิดเห็นคล้ายกันว่า ปัญหาอุปสรรคและข้อจำกัดของมาตรการทางกฎหมายในการคุ้มครองในการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ประกอบด้วย 1) ความคลุมเครือของกฎหมาย ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 มุ่งเน้นไปที่การป้องกันอาชญากรรมทางคอมพิวเตอร์ มากกว่าการคุ้มครองข้อมูลส่วนบุคคล ไม่ได้ให้คำจำกัดความที่ชัดเจนเกี่ยวกับ “ข้อมูลส่วนบุคคล” ทำให้เกิดความสับสนกับองค์กรในการนำเข้าข้อมูล ยากต่อการบังคับใช้กฎหมาย 2) ความครอบคลุมกฎหมายไม่ได้กำหนดนิยามของ “ข้อมูลส่วนบุคคล” ไว้อย่างชัดเจน อีกทั้งไม่ได้กำหนดรายละเอียดเกี่ยวกับวิธีการนำเข้าข้อมูลส่วนบุคคล รวมถึงกฎหมายยังไม่ได้กำหนดบทลงโทษสำหรับผู้ที่ละเมิดกฎหมายเกี่ยวกับการนำเข้าข้อมูลส่วนบุคคล 3) ความซับซ้อนของกฎหมายเนื่องจากกฎหมายเกี่ยวกับการนำเข้าข้อมูลส่วนบุคคลมีหลายฉบับ กระจายอยู่ในหลายหน่วยงาน บางฉบับมีความซับซ้อน ยากต่อการเข้าใจ 4) ความยุ่งยาก กฎหมายมีขั้นตอนและวิธีการยุ่งยากสำหรับองค์กรที่ต้องการนำเข้าข้อมูลส่วนบุคคล องค์กรต้องขออนุญาตจากหน่วยงานที่เกี่ยวข้องก่อนนำเข้าข้อมูล ต้องจัดทำเอกสารประกอบจำนวนมาก และต้องเสียค่าธรรมเนียมในการของอนุญาต 5) บทลงโทษ บทลงโทษสำหรับการนำเข้าข้อมูลส่วนบุคคลโดยมิชอบไม่รุนแรงพอ ไม่สามารถยับยั้งการละเมิดกฎหมายได้ อีกทั้งบทลงโทษเน้นไปที่การป้องกันอาชญากรรมทางคอมพิวเตอร์ 6) กลไกการบังคับใช้ที่อ่อนแอ หน่วยงานที่รับผิดชอบในการบังคับใช้กฎหมายมีทรัพยากรจำกัดในการตรวจสอบและควบคุมการนำเข้าข้อมูลส่วนบุคคล เจ้าหน้าที่ที่เกี่ยวข้องอาจไม่มีความรู้ความเข้าใจเกี่ยวกับกฎหมายและเทคโนโลยีใหม่ ๆ ทำให้ยากต่อการตรวจสอบและดำเนินคดีกับผู้กระทำความผิด 7) เทคโนโลยีมีการพัฒนาอย่างรวดเร็ว ทำให้กฎหมายของประเทศไทยตามไม่ทัน ยังไม่ได้รองรับเทคโนโลยีใหม่ ๆ ที่เกิดขึ้น กฎหมายยังไม่ได้รับการแก้ไขให้ทันสมัยอยู่เสมอ การบังคับใช้กฎหมายมีความยากลำบาก อีกทั้งเกิดช่องโหว่ที่ผู้กระทำผิดสามารถใช้ประโยชน์ได้ องค์กรและประชาชนทั่วไปยังไม่มีความตระหนักรู้ถึงกฎหมายเกี่ยวกับการนำเข้าข้อมูลส่วนบุคคล และ 8) มีอุปสรรคในการแลกเปลี่ยนข้อมูลและหลักฐานเพราะกฎหมายของประเทศไทยยังไม่ได้มีการสร้างความร่วมมือระหว่างประเทศ

จากการสัมภาษณ์ดังกล่าวสรุปได้ว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ยังมีข้อจำกัดหลายประการในการคุ้มครองการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์ จำเป็นต้องมีการแก้ไขกฎหมายและพัฒนาระบบต่าง ๆ องค์กรและประชาชนควรตระหนักถึงกฎหมายและปฏิบัติตามอย่างเคร่งครัด รวมถึงเพิ่มประสิทธิภาพในการบังคับใช้กฎหมาย

3. เพื่อตอบวัตถุประสงค์การวิจัยข้อที่ 3 แนวทางการแก้ไขปัญหาทางกฎหมายในการคุ้มครองในการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จากผลการสัมภาษณ์มีข้อเสนอแนะสำหรับการแก้ไข สรุปได้ดังนี้ ควรมีการแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ให้ครอบคลุมถึงการคุ้มครองข้อมูลส่วนบุคคล มีการกำหนดนิยามของ “ข้อมูลส่วนบุคคล” กำหนดรายละเอียดเกี่ยวกับวิธีการนำเข้าข้อมูลส่วนบุคคล กำหนดบทลงโทษสำหรับผู้ที่ละเมิดกฎหมายเกี่ยวกับการนำเข้าข้อมูลส่วนบุคคลที่รุนแรงมากขึ้น สำหรับการนำเข้าข้อมูลส่วนบุคคลโดยมิชอบ เพิ่มทรัพยากรให้หน่วยงานที่รับผิดชอบในการบังคับใช้กฎหมาย พัฒนากลไกเยียวยาผู้เสียหาย ลดขั้นตอนและวิธีการให้ง่ายขึ้น ให้ความรู้แก่เจ้าหน้าที่ที่เกี่ยวข้องในเรื่องเทคโนโลยีสารสนเทศและการสื่อสารให้ทันต่อการเปลี่ยนแปลง องค์กรที่นำเข้าข้อมูลส่วนบุคคลควรทำการศึกษากฎหมายทั้งของต่างประเทศ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

อภิปรายผล

การวิเคราะห์ความแตกต่างของมาตรการทางกฎหมายของต่างประเทศและประเทศไทยที่เกี่ยวข้องกับการคุ้มครองการนำเข้าข้อมูลทางคอมพิวเตอร์ พบว่า กฎหมายของต่างประเทศ เช่น กฎหมายของสหภาพยุโรป หรือ GDPR และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของรัฐแคลิฟอร์เนีย หรือ CCPA มุ่งเน้นการคุ้มครองข้อมูลส่วนบุคคล ส่วนพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 มุ่งเน้นไปที่การป้องกันอาชญากรรมทางคอมพิวเตอร์ ระดับการคุ้มครองของ GDPR และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของรัฐแคลิฟอร์เนีย CCPA ให้ระดับการคุ้มครองข้อมูลส่วนบุคคลสูงกว่าพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 อีกทั้งในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฉบับนี้ ไม่ได้กำหนดรายละเอียดเกี่ยวกับวิธีการนำเข้าข้อมูลส่วนบุคคล เป็นเพราะว่า ต่างประเทศมองว่าอาชญากรรมทางคอมพิวเตอร์เป็นภัยคุกคามร้ายแรงต่อเศรษฐกิจ ความมั่นคง และสังคม อีกทั้งตระหนักถึงความรุนแรงที่ตามมา เช่น การโจรกรรมข้อมูล การโจมตีระบบไซเบอร์ สามารถสร้างความเสียหายได้ในวงกว้างและรวดเร็ว ยากต่อการพิสูจน์ ส่วนประเทศไทยยังมีมุมมองเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ค่อนข้างผ่อนคลาย มองว่าเป็นอาชญากรรมทั่วไป เป็นการละเมิดกฎหมายทั่วไป และยังไม่ให้ความสำคัญกับผลที่เกิดขึ้นในระยะยาว เพราะยังมองว่าเป็นปัญหาเฉพาะกลุ่ม ยังไม่ส่งผลในวงกว้าง สำหรับในต่างประเทศมีกฎหมายที่พัฒนาตามเทคโนโลยี มีบทลงโทษสำหรับอาชญากรรมรูปแบบใหม่ มีการเพิ่มประสิทธิภาพของระบบบังคับใช้กฎหมายด้วยการทุ่มเททรัพยากร มีหน่วยงานเฉพาะทาง อีกทั้งในต่างประเทศยังมีการร่วมลงนามสนธิสัญญาระหว่างประเทศในการใช้กฎหมายร่วมกัน กฎหมายของสหรัฐอเมริกา กำหนดบทลงโทษสหรับการโจมตีระบบคอมพิวเตอร์ของรัฐบาล จำคุก 20 ปี ปรับสูงสุด 250,000 เหรียญสหรัฐ ประเทศอังกฤษ จำคุก 14 ปี สำหรับการแฮ็กข้อมูลที่มีความละเอียดอ่อน และสหภาพยุโรป (GDPR) กำหนดบทลงโทษสูงสุดร้อยละ 4 ของรายได้ทั่วโลก หรือ 20 ล้านยูโร หรือขึ้นอยู่กับว่าจำนวนใดสูงกว่า ในขณะที่ประเทศไทยยังตามหลังเทคโนโลยี บทลงโทษยังไม่ครอบคลุม ทรัพยากรมีจำกัด กลไกบังคับใช้ยังไม่เต็มประสิทธิภาพ ขาดการผลักดันจากประชาสังคม บทลงโทษของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 กำหนดโทษจำคุกสูงสุด 5 ปี สำหรับการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต กฎหมายต่างประเทศเกี่ยวกับการทำผิดเกี่ยวกับคอมพิวเตอร์จึงมีมาตรการลงโทษที่หนักกว่า เพราะเป็นอาชญากรรม พิจารณาตามระดับความเสียหาย เน้นการป้องกัน และยังมีความร่วมมือระหว่างประเทศ ดังนั้นในต่างประเทศโดยเฉพาะประเทศในแถบยุโรปจะมีสถิติของอาชญากรรมทางคอมพิวเตอร์ลดลง ในทางกลับกันอาชญากรรมทางคอมพิวเตอร์ในประเทศไทยนับวันจะมีแนวโน้มเพิ่มขึ้น ดังผลการวิจัยของ ณัฐสุดา อัคราวัฒนา และธานี วรภัทร์ สรุปว่า ตามนิติวิธีของประมวลกฎหมาย (Civil Law) การกระทำใดที่เป็นความผิดทางอาญา และมีผลกระทบต่อคุณธรรมทางกฎหมายต้องบัญญัติความผิด

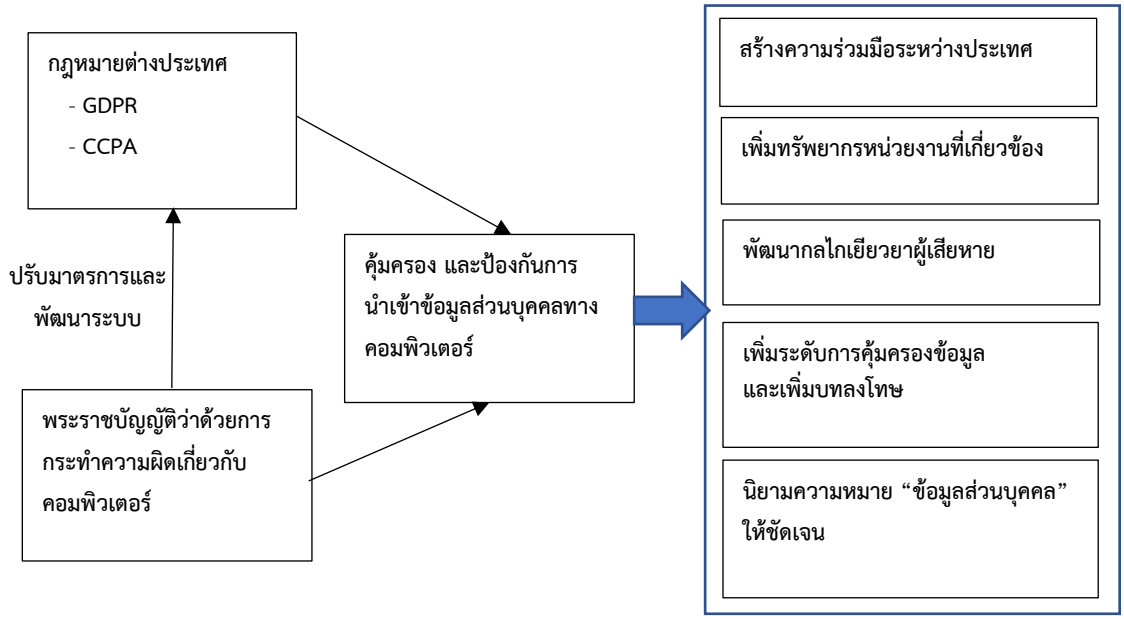
และมาตรการบัญญัติทางอาญา เนื่องจากกฎหมายอาญาต้องการหลักความชัดเจนแน่นอน ในสหพันธ์สาธารณรัฐเยอรมนี และสาธารณรัฐฝรั่งเศสได้บัญญัติความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์เพื่อขึ้นในประมวลกฎหมายอาญา โดยเป็นความผิดที่กระทำต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยตรง (ณัฐสุดา อัคราวัฒนา และธานี วรภัทร์, 2561)

ปัญหาอุปสรรคและข้อจำกัดของมาตรการทางกฎหมายในการคุ้มครองในการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พบว่า กฎหมายยังมีความคลุมเครือ มุ่งเน้นไปที่การคุ้มครองป้องกันอาชญากรรมทางคอมพิวเตอร์มากกว่า การป้องกันการนำเข้าข้อมูลส่วนบุคคลโดยมิชอบ เนื่องจากยังไม่มีการนิยามความหมายของคำว่า “ข้อมูลส่วนบุคคล” ไว้ในกฎหมายฉบับนี้ แต่จากข้อความในมาตรา 14 ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดา ซึ่งทำให้สามารถระบุตัวบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ นามสกุล เลขประจำตัวประชาชน ที่อยู่ เบอร์โทรศัพท์ ข้อมูลทางการเงิน ข้อมูลการศึกษา ข้อมูลสุขภาพ ข้อมูลทางพันธุกรรม ข้อมูลลายนิ้วมือ ข้อมูลเสียง รูปถ่าย หรือข้อมูลอื่นใด ทำให้เกิดความสับสนในการนำเข้าข้อมูลทางคอมพิวเตอร์ และยังเป็นเรื่องยากในการบังคับใช้กฎหมาย รวมถึงบทลงโทษตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ที่เกี่ยวข้องกับการนำเข้าข้อมูลส่วนบุคคลโดยมิชอบยังไม่รุนแรงพอ จึงไม่สามารถยับยั้งการละเมิดกฎหมายได้ อีกทั้งกฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยยังมีอุปสรรคในการแลกเปลี่ยนข้อมูลและหลักฐาน เป็นเพราะการบังคับใช้กฎหมายที่มีประสิทธิภาพจำเป็นต้องอาศัยความร่วมมือระหว่างประเทศ ซึ่งกฎหมายของต่างประเทศ เช่น กฎหมายของสหภาพยุโรป หรือ GDPR ที่มีข้อตกลงการบังคับใช้กฎหมายระหว่างประเทศที่เป็นสมาชิกของสหภาพยุโรป ซึ่งผลการวิจัยของ ปัทมา มัญชุนากร ระบุว่า การพัฒนาทางเทคโนโลยีและเครือข่ายสังคมออนไลน์ ทำให้การนำแนวคิดผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ในทางปฏิบัติมีความยากยิ่งขึ้น เนื่องจากมีปัญหาเรื่องความสับสนของการกำหนดฐานะของบุคคลที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จึงจำเป็นต้องกำหนดแนวทางปฏิบัติเกี่ยวกับการตีความหมายของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล อีกทั้งปัญหาความไม่ครอบคลุมของบทบัญญัติกรณีที่มีบุคคลหลายรายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล และอีกปัญหา คือ การจัดสรรหน้าที่และความรับผิดชอบระหว่างผู้ให้บริการและผู้ใช้งานเครือข่ายสังคมออนไลน์ ที่ทุกฝ่ายควรปฏิบัติตามหลักความรับผิดชอบครบทุกฝ่าย (ปัทมา มัญชุนากร, 2565) โดยผลการวิจัยของ Nwankwo, & Ukaoha พบว่า กฎหมายอาชญากรรมทางคอมพิวเตอร์ของประเทศไนจีเรีย มีช่องว่างบางอย่างที่ขัดขวางเป้าหมายของกฎหมาย ต้องมีการทบทวนกฎหมายอย่างรอบคอบ โดยนำมาเปรียบเทียบกับระดับสากล เพื่อให้กฎหมายเข้มงวดยิ่งขึ้นทั้งทางปฏิกิริยาและเชิงรุกในการส่งเสริมความปลอดภัยทางไซเบอร์ (Nwankwo, W., & Ukaoha, K. C., 2019) การป้องกันและต่อสู้กับอาชญากรรมทางอินเทอร์เน็ต ยังมีความกังวลเรื่องความปลอดภัยทางไซเบอร์ ที่เป็นภัยคุกคามต่อการป้องกันข้อมูลทางเทคโนโลยีสมัยใหม่ อีกทั้งยังเป็นอุปสรรคในการดำเนินคดี การบังคับใช้กฎหมายที่มีความยากลำบาก จึงต้องมีความเชี่ยวชาญในการบังคับใช้กฎหมายด้านอาชญากรรมทางคอมพิวเตอร์ (Atta Ul Haq, Q., 2021) และกฎหมายเกี่ยวกับการกำกับดูแลผู้ให้บริการอินเทอร์เน็ตยังไม่ครอบคลุมเนื้อหาการกลั่นแกล้งทางไซเบอร์ มีช่องว่างในการบังคับใช้ ควรมีการแก้ไขปรับปรุงในการกำกับดูแลเกี่ยวกับผู้ให้บริการอินเทอร์เน็ต มีการแจ้งเตือน ปิดกั้นหรือลบเนื้อหาข้อมูลคอมพิวเตอร์ และคุ้มครองสิทธิเด็กและเยาวชน และบุคคลทั่วไปที่ถูกกลั่นแกล้งผ่านไซเบอร์ (อุษณีย์ ตันสูงเนิน, 2565) อาชญากรรมไซเบอร์เป็นผลมาจากการใช้คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และเครือข่ายในทางที่ผิด การใช้งานของคอมพิวเตอร์ในทุกขอบเขต การประยุกต์ใช้เทคโนโลยีสารสนเทศในกิจกรรมทางสังคม และการโต้ตอบจำนวนมาก มีผลให้เกิดความอ่อนแอทางสังคม และพฤติกรรมที่ผิดกฎหมายบางรูปแบบและภัยคุกคามพื้นฐานบางประการ (Grujić, Z., & Blagić, P. D., 2019)

นอกจากนี้ผลการวิจัยยังพบว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ยังมีข้อจำกัดหลายประการในการคุ้มครองการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์ จำเป็นต้องมีการแก้ไขกฎหมายให้มีความชัดเจน และเพิ่มบทลงโทษให้รุนแรงขึ้นตามผลกระทบที่เกิดขึ้น พัฒนากลไกการติดตามและตรวจสอบประสิทธิภาพ ส่งเสริมความร่วมมือระหว่างประเทศ สร้างตระหนักรู้ถึงกฎหมายและปฏิบัติตามอย่างเคร่งครัด รวมถึงเพิ่มประสิทธิภาพในการบังคับใช้กฎหมาย สอดคล้องกับผลการวิจัยของ อุษณีย์ ตันสูงเนิน ที่เสนอให้มีการแก้ไขปรับปรุงในเรื่องการกำกับดูแลผู้ให้บริการอินเทอร์เน็ต (อุษณีย์ ตันสูงเนิน, 2565) และผลการวิจัยของ ปัทมา มัญชุนากร เสนอให้เพิ่มเติมบทบัญญัติกรณีมีบุคคลหลายรายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล 2 กรณี 1) กำหนดหน้าที่ผู้ควบคุมข้อมูลร่วม ด้วยการเลือกเฉพาะผู้ควบคุมข้อมูลที่สามารถเป็นหลักประกันที่เพียงพอในการใช้มาตรการด้านเทคนิคและมาตรการเกี่ยวกับองค์กรที่เหมาะสม กำหนดหน้าที่ความรับผิดชอบของแต่ละคน กำหนดหน้าที่ความรับผิดชอบระหว่างผู้ควบคุมข้อมูลส่วนบุคคลร่วม โดยมีข้อตกลงที่แสดงถึงบทบาทและความสัมพันธ์ของผู้ควบคุมข้อมูลส่วนบุคคลร่วม ที่มีต่อเจ้าของข้อมูลส่วนบุคคลเป็นรายลักษณ์อักษร การเปิดเผยสาระสำคัญของข้อตกลงแก่เจ้าของข้อมูล ตลอดจนเจ้าของข้อมูลสามารถใช้สิทธิของตนภายใต้ข้อกำหนดของกฎหมายต่อผู้ควบคุมข้อมูลส่วนบุคคลร่วมได้โดยไม่ต้องคำนึงถึงข้อความในข้อตกลง (ปัทมา มัญชุนากร, 2565) สอดคล้องกับ นิกร โภคอุดม เสนอว่า เพื่อเป็นการป้องกันปัญหาเรื่องความเป็นส่วนตัวของข้อมูลรั่วไหลสหภาพยุโรปจึงได้ออกกฎหมายการคุ้มครองข้อมูลส่วนบุคคล เรียกว่า “GDPR” (EU General Data Protection Regulation--GDPR) เพื่อกำหนดให้องค์กรต่าง ๆ ต้องมีมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บไว้ ซึ่งประเทศไทยจึงนำกฎหมายนี้มาเป็นแนวทางสำหรับออกเป็นกฎหมายเพื่อการคุ้มครองข้อมูลส่วนบุคคลของประชาชน (นิกร โภคอุดม, 2563) นอกจากนี้ Atta Ul Haq ได้เสนอแนะว่า กลไกในการกำกับดูแลเกี่ยวกับอาชญากรรมบนโลกไซเบอร์ ต้องมีกลไกที่ชัดเจนควบคู่กับความเชี่ยวชาญด้านบังคับใช้กฎหมายในด้านอาชญากรรมทางอินเทอร์เน็ตและความสามารถในทางปฏิบัติของเจ้าหน้าที่และหน่วยงานที่เกี่ยวข้อง บทบาทของกฎหมายต้องสอดคล้องกับระดับภูมิภาค และระดับสากลในการป้องกันและต่อสู้กับอาชญากรรมทางอินเทอร์เน็ตที่ต้องมีการให้อำนาจการบริหารและความร่วมมือจากต่างประเทศในการควบคุมอาชญากรร (Atta Ul Haq, Q., 2021) นอกจากนี้ กฎหมายอาชญากรรมทางอินเทอร์เน็ตควรมีการทบทวนกฎหมายของประเทศ โดยเปรียบเทียบกับระดับสากล มีแนวปฏิบัติที่ดีที่สุด กฎหมายเกี่ยวกับอาชญากรรมทางอินเทอร์เน็ตต้องแก้ไขให้เข้มงวดมากขึ้น โดยจะเห็นได้จาก ประมวลกฎหมายแห่งสาธารณรัฐเซอร์เบีย ระบุบทบัญญัติเกี่ยวกับความผิดทางอาญาต่อความปลอดภัยของข้อมูลคอมพิวเตอร์ ให้ความคุ้มครองกับข้อมูลคอมพิวเตอร์และโปรแกรม รวมถึงห้ามใช้คอมพิวเตอร์และเครือข่ายคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Grujić, Z., & Blagić, P. D., 2019); (Nwankwo, W., & Ukaoha, K. C., 2019)

องค์ความรู้ใหม่

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 มีข้อจำกัดในการคุ้มครองการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์ ซึ่งยังขาดความชัดเจนเรื่องนิยามความหมายของคำว่า ข้อมูลส่วนบุคคล มีบทลงโทษที่ยังไม่หนักพอเมื่อเทียบกับบทลงโทษในกฎหมายต่างประเทศ การแก้ไขกฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ควรมีความชัดเจน อีกทั้งเพิ่มระดับการคุ้มครองโดยการเพิ่มอัตราค่าปรับให้สูงขึ้นตามระดับความรุนแรงของผลการกระทำ พัฒนากลไกเยียวยาผู้ได้รับผลกระทบ เพิ่มทรัพยากรแก่หน่วยงานที่รับผิดชอบในการบังคับใช้กฎหมาย และสร้างความร่วมมือระหว่างประเทส โดยสรุปองค์ความรู้ที่ได้จากการวิจัย ดังนี้



ภาพที่ 1 แนวทางการแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

สรุปและข้อเสนอแนะ

มาตรการทางกฎหมายในการคุ้มครองป้องกันการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ของประเทศไทย มีมาตรการที่ต้องได้รับการแก้ไขให้คล้ายกับกฎหมายของต่างประเทศ เช่น กฎหมายของสหภาพยุโรป หรือ GDPR และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของรัฐแคลิฟอร์เนีย หรือ CCPA มุ่งเน้นการคุ้มครองข้อมูลส่วนบุคคล ที่มองว่าอาชญากรรมทางคอมพิวเตอร์เป็นภัยคุกคามร้ายแรงต่อเศรษฐกิจ สังคม และความมั่นคง ปัญหาของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ขาดความชัดเจนของคำจำกัดความที่ชัดเจนของคำว่า “ข้อมูลส่วนบุคคล” มีบทลงโทษไม่รุนแรง และมองว่าอาชญากรรมทางคอมพิวเตอร์เป็นเพียงปัญหาเฉพาะกลุ่ม ดังนั้นแนวทางการแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฉบับนี้ คือ การให้คำจำกัดความที่ครอบคลุมและมีความชัดเจนของคำว่า “ข้อมูลส่วนบุคคล” เพิ่มบทลงโทษให้สูงขึ้นตามระดับความเสียหาย พัฒนากลไกการเยียวยาผู้เสียหาย สร้างความรู้ความเข้าใจให้กับหน่วยงานที่เกี่ยวข้อง และสร้างความร่วมมือระหว่างประเทศ จากผลการวิจัยดังกล่าว มีข้อเสนอแนะดังนี้ 1) จากการวิเคราะห์มาตรการทางกฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของต่างประเทศและกฎหมายของประเทศไทย พบว่า มาตรการทางกฎหมายของประเทศไทยยังไม่มีความชัดเจนของคำว่า “ข้อมูลส่วนบุคคล” ดังนั้น ผู้ที่มีส่วนเกี่ยวข้องกับการแก้ไขข้อกฎหมาย ควรนิยามความหมายให้ชัดเจนและครอบคลุม ทั้งบุคคลทั่วไปที่มีชีวิตอยู่ และผู้ที่ตายแล้ว โดยแยกให้ชัดเจนถึงมาตรการคุ้มครอง 2) มาตรการการคุ้มครองการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์ ควรมีการเพิ่มประเด็นข้อมูลที่มีความอ่อนไหว เพื่อให้การคุ้มครองเป็นพิเศษ เข้มข้นขึ้น และควรกำหนดบทลงโทษที่รุนแรงขึ้นโดยพิจารณาจากผลที่เกิดขึ้นจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ 3) การบังคับใช้กฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ให้มีประสิทธิภาพ ประเทศไทยควรสร้างความร่วมมือระหว่างประเทศ เพื่อให้เกิดการแลกเปลี่ยนข้อมูลและหลักฐาน ในกรณีที่มีอาชญากรรมทางคอมพิวเตอร์ข้ามชาติ และ 4) การปรับแก้ไขกฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ควรมีการศึกษาวิวัฒนาการของเทคโนโลยีใหม่ ๆ และดำเนินการให้ทันต่อเทคโนโลยีที่มีการเปลี่ยนแปลงอย่างรวดเร็ว เพื่อลดช่องว่างในการนำประโยชน์ไปใช้ สำหรับข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป ได้แก่ 1) ด้วยเหตุที่เทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็ว การวิจัยครั้ง

ต่อไปควรมีการศึกษาเกี่ยวกับกระบวนพิสูจน์เจตนาร้าย ความเสียหาย และความสัมพันธ์เชิงเหตุผล ในการนำเข้าข้อมูลทางคอมพิวเตอร์ และ 2) ควรมีการศึกษาเกี่ยวกับการสร้างกลไกการเข้าถึงพยานหลักฐานเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อนำไปสู่การเร่งรัดกระบวนการยุติธรรม และพัฒนาองค์ความรู้ให้กับผู้เกี่ยวข้องกับการพิจารณาคดีที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในกรณีการนำเข้าข้อมูลส่วนบุคคลทางคอมพิวเตอร์

เอกสารอ้างอิง

เครือข่ายพลเมืองเน็ต. (2557). การละเมิดความเป็นส่วนตัวออนไลน์ในสังคมไทย พ.ศ. 2556. เรียกใช้เมื่อ 13 ธันวาคม 2565 จาก https://thainetizen.org/wp-content/uploads/2014/03/ thainetizen-privacy-report-2013.pdf

ณัฐสุดา อัคราวัฒนา และธานี วรภัทร์. (2561). การกำหนดความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์. ใน วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขาวิชานิติศาสตร์. มหาวิทยาลัยธุรกิจบัณฑิตย์.

นิกร โภคอุดม. (2563). ความเป็นส่วนตัวในยุคดิจิทัล. วารสารมหาวิทยาลัยอีสเทิร์นเอเชีย ฉบับวิทยาศาสตร์และเทคโนโลยี, 14(2), 59-69.

ปัทมา มัญชุนากร. (2565). ปัญหากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในเครือข่ายสังคมออนไลน์: ศึกษากรณีผู้ควบคุมข้อมูลส่วนบุคคลหลายราย. วารสารรัชต์ภาคย์, 16(47), 89-107.

พัฒนะ ศุกรสุต. (2563). “ชีวิตวิถีใหม่” อยู่ภายใต้ภัยคุกคามทางไซเบอร์ แนะออกแบบระบบรองรับทำงานได้แม้ถูกโจมตีผู้จัดการออนไลน์ 2 มิถุนายน 2563. เรียกใช้เมื่อ 13 ธันวาคม 2565 จาก http://www.mgronline.com/onlinesection/detail/9630000063688

รุ่งอรุณ รุ่งทองคำกุล. (2558). ปัญหาทางกฎหมายอันเกิดจากการละเมิดสิทธิในความเป็นส่วนตัวและข้อมูลส่วนบุคคลของเด็กจากการใช้งานบนเครือข่ายอินเทอร์เน็ต. ใน วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขาวิชานิติศาสตร์. มหาวิทยาลัยธุรกิจบัณฑิตย์.

สาวิตรี สุขศรี และปวีร์ เจนวีระนนท์. (2566). ความรู้ทางกฎหมายหลากหลายและเข้าใจง่าย ชุดที่ 20: Cyber Crime เมื่อโลกออนไลน์เต็มไปด้วยอาชญากรรม: อาชญาวิทยาและบทบาทของกฎหมาย. ปทุมธานี: คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

สุนทร เปลี่ยนสี. (2551). แนวความคิดและหลักการของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์. กรุงเทพมหานคร: สำนักงานคณะกรรมการกฤษฎีกา.

อุษณีย์ ตันสูงเนิน. (2565). มาตรการทางกฎหมายในการกำกับดูแลผู้ให้บริการทางอินเทอร์เน็ต และการคุ้มครองเด็ก และเยาวชนที่ถูกกลั่นแกลงผ่านไซเบอร์. วารสารปัญญาปณิธาน, 7(1), 31-40.

Atta Ul Haq, Q. (2021). Cyber crime and their restriction through laws and techniques for protectingsecurity issues and privacy threats. In In Security Issues and Privacy Threats in Smart Ubiquitous Computing (pp. 31-63). Singapore: Springer.

Grujić, Z., & Blagić, P. D. (2019). Incriminations Against Security of Computer Data–Effectiveness of Criminal Justicemechanism Directed on Cyber Crime. Archibald Reiss Days, 8(1), 293-304.

Nwankwo, W., & Ukaoha, K. C. (2019). Socio-technical perspectives on cybersecurity: Nigeria’s cybercrime legislation in review. International Journal of Scientific and Technology Research, 8(9), 47-58.