



การบังคับใช้กฎหมายเกี่ยวกับการกำหนดโทษทางอาญาศึกษา กรณีการซื้อขายข้อมูลส่วนบุคคล
โดยมิชอบด้วยกฎหมาย
Law Enforcement Regarding Criminal Sanctions A Case Study of Unlawfully
Selling Personal Data

พัชรกิม สุขอนันต์^{1*} และศิวพร เสาวคนธ์²

Patchrapeem Sukanan^{1*} and Siwaporn Saowakon²

^{1*}นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม

²อาจารย์ ประจำหลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม

^{1*}Master Student of laws Program the Faculty of Law Sripatum University

²Lecturer from the Master of Laws Program Faculty of Law Sripatum University

*Corresponding author email: patchrapeem@gmail.com

Received: 8 May 2025

Revised: 25 May 2025

Accepted: 28 May 2025

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์ 1. เพื่อศึกษาแนวคิด ทฤษฎี และหลักการเกี่ยวกับการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย 2. เพื่อศึกษามาตรการการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมายของระหว่างประเทศต่างประเทศและประเทศไทย 3. เพื่อวิเคราะห์ปัญหาการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย และ 4. เพื่อให้ศึกษาแนวทางในการแก้ไขปัญหาเกี่ยวกับการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย เป็นการวิจัยแบบเชิงคุณภาพ โดยการศึกษาวิจัยจากเอกสาร อาทิ หนังสือ ตำรา เอกสารวิชาการ งานวิจัย และสื่ออิเล็กทรอนิกส์ที่เกี่ยวข้อง แล้วนำข้อมูลที่รวบรวมได้จากเอกสารต่าง ๆ ที่เกี่ยวข้องมาวิเคราะห์ในเชิงเนื้อหา ผลการวิจัยพบว่า 1) แนวคิด ทฤษฎีและหลักการที่จะนำมาใช้บังคับกฎหมายเกี่ยวกับการกำหนดโทษ ได้แก่ แนวคิดการคุ้มครองข้อมูลส่วนบุคคล แนวคิดเกี่ยวกับการกำกับดูแล แนวคิดการกำหนดโทษทางอาญา ทฤษฎีการลงโทษทางอาญา รวมทั้งมาตรฐานสากลด้านการคุ้มครองข้อมูลส่วนบุคคล การละเมิดความปลอดภัยของข้อมูลส่วนบุคคล และปัจจัยที่พิจารณาการกำหนดโทษทางอาญา 2) หากประเทศไทยสามารถปรับปรุงมาตรการทางกฎหมายให้ครอบคลุมถึงการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบ และเสริมสร้างกลไกการบังคับใช้กฎหมายที่มีประสิทธิภาพมากขึ้น จะช่วยลดปัญหาการละเมิดข้อมูลส่วนบุคคล อำนวยความเป็นธรรมให้กับเจ้าของข้อมูลและเพิ่มศักยภาพในการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในระยะยาว 3) การกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคล โดยมิชอบด้วยกฎหมาย ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ไม่ครอบคลุมถึงบุคคลธรรมดา ซึ่งทำการซื้อขายข้อมูลลักษณะของการกระทำความผิด บทลงโทษ รวมถึงการนำข้อมูลส่วนบุคคลไปแสวงหาผลประโยชน์โดยมิชอบบนเว็บไซต์หรือแพลตฟอร์ม ส่งผลให้ขาด



มาตรการในการควบคุมและปราบปรามการซื้อขายข้อมูลส่วนบุคคลที่มีประสิทธิภาพ และมีการนำข้อมูลไปใช้เพื่อแสวงหาผลประโยชน์เชิงพาณิชย์โดยปราศจากความยินยอมของเจ้าของข้อมูล และ 4) เสนอให้เพิ่มเติมบทบัญญัติในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ในส่วนของบทลงโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย

คำสำคัญ: การพัฒนากฎหมาย, อุตสาหกรรมขนาดเล็ก, ชุมชน

Abstract

This research consists purposes were 1. to study the concepts, theories, and principles related to the criminal penalties for the illegal buying and selling of personal data 2. to examine the criminal penalty measures regarding the illegal buying and selling of personal data in international, foreign, and Thai legal contexts 3. to analyze the problems associated with imposing criminal penalties in cases involving the illegal buying and selling of personal data and 4. to explore potential solutions to the issues related to the imposition of criminal penalties for the illegal trading of personal data. This is a qualitative research study conducted through a review of relevant literature, including books, textbooks, academic papers, research studies, and electronic media. The data collected from these various sources will be analyzed using content analysis. The results of the study found that 1) Concepts, theories and principles to be applied to enforce the law on penalties include the concept of personal data protection, the concept of supervision, the concept of criminal penalties, the theory of criminal punishment, including international standards on personal data protection, violations of personal data security and factors considering criminal penalties 2) If Thailand can improve legal measures to cover the illegal trading of personal data and strengthen the effective law enforcement mechanism, it will help reduce the problem of personal data violations, provide justice for data owners and increase the potential to prevent and suppress cybercrimes related to personal data in the long term 3) Criminal penalties in cases of illegal trading of personal data under the Personal Data Protection Act B.E. 2562 and the Computer Crime Act B.E. 2550 and amendments do not cover individuals who trade data. The nature of the offense, penalties, and the use of personal data for illegal gain on websites or platforms result in a lack of effective measures to control and suppress the trading of personal data and the use of data for commercial gain without the consent of the data owner and 4) It is proposed to add provisions in the Personal Data Protection Act B.E. 2562 and the Computer Crime Act B.E. 2550 and amendments. In terms of criminal penalties in cases of unlawful trading of personal data



Keywords: Legal Development, Small Industry, Community

บทนำ

ในยุคที่เทคโนโลยีดิจิทัลมีความก้าวหน้าอย่างรวดเร็ว การคุ้มครองข้อมูลส่วนบุคคลได้กลายเป็นประเด็นสำคัญที่ได้รับความสนใจทั่วโลก เนื่องจากการแลกเปลี่ยนข้อมูลผ่านระบบออนไลน์และอุปกรณ์ดิจิทัลมีปริมาณเพิ่มสูงขึ้นอย่างต่อเนื่อง การละเมิดข้อมูลส่วนบุคคลจึงอาจนำไปสู่ผลกระทบร้ายแรงทั้งในด้านการเงิน ชื่อเสียง ความมั่นคง และสิทธิในความเป็นส่วนตัวของประชาชน หลายประเทศจึงได้ออกกฎหมายเพื่อกำกับดูแลและปกป้องข้อมูลส่วนบุคคลอย่างเข้มงวด เช่น GDPR ของสหภาพยุโรป, CCPA ของสหรัฐอเมริกา และ Data Protection Act 2018 ของสหราชอาณาจักร ซึ่งล้วนมีบทบัญญัติที่ชัดเจนและบทลงโทษที่เหมาะสมในการรับมือกับการละเมิดข้อมูล สำหรับประเทศไทยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลบังคับใช้เมื่อวันที่ 1 มิถุนายน 2565 (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 2567) โดยมุ่งหมายคุ้มครองสิทธิในความเป็นส่วนตัวของบุคคล และกำหนดมาตรฐานในการเก็บ รวบรวม ใช้เปิดเผย หรือโอนข้อมูลส่วนบุคคลให้มีความปลอดภัยและเป็นธรรม อย่างไรก็ตาม แม้จะมีการกำหนดโทษทั้งทางปกครองและทางอาญา แต่ในทางปฏิบัติยังคงพบปัญหาการละเมิดข้อมูลส่วนบุคคลอย่างแพร่หลาย โดยเฉพาะการซื้อขายข้อมูลโดยมิชอบด้วยกฎหมาย (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 2567)

นับว่าปัจจุบันกฎหมายที่ใช้บังคับเกี่ยวกับการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบยังไม่สามารถตอบสนองต่อปัญหาที่เกิดขึ้นได้อย่างมีประสิทธิภาพ ประเทศไทยยังไม่มีบทบัญญัติกฎหมายเฉพาะที่ครอบคลุมการกระทำความผิดของบุคคลธรรมดาที่มีพฤติกรรมซื้อขายหรือแสวงหาประโยชน์จากข้อมูลส่วนบุคคลโดยมิชอบ ส่งผลให้เกิดช่องว่างทางกฎหมาย และทำให้การบังคับใช้กฎหมายในทางปฏิบัติไม่ครอบคลุมต่อพฤติกรรมที่เกิดขึ้นจริง เนื่องจากการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบเป็นปัญหาในระดับประเทศที่ก่อให้เกิดความเสียหายอย่างร้ายแรง ทั้งในมิติของความปลอดภัย ทรัพย์สิน และสิทธิความเป็นส่วนตัวของประชาชน (คณาธิป ทองรวีวงศ์, 2566) การควบคุมปัญหาดังกล่าวจึงจำเป็นต้องมีมาตรการทางกฎหมายที่ชัดเจน โดยเฉพาะบทบัญญัติเกี่ยวกับโทษทางอาญาที่เฉพาะเจาะจง เพื่อให้สามารถป้องกันและปราบปรามการกระทำความผิดในลักษณะนี้ได้เป็นอย่างดี และสร้างมาตรฐานในการจัดการข้อมูลส่วนบุคคลที่มีประสิทธิภาพมากยิ่งขึ้น ยกตัวอย่างเช่น ปัญหาการบังคับใช้กฎหมายในกรณีซื้อขายข้อมูลส่วนบุคคล ซึ่งในประเด็นนี้เห็นว่า มาตรา 80 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดโทษทางอาญาสำหรับผู้ล่วงรู้ข้อมูล ส่วนบุคคลจากการปฏิบัติหน้าที่แล้วนำไปเปิดเผยโดยมิชอบ แต่ยกเว้นความผิดในบางกรณี เช่น การเปิดเผยตามหน้าที่หรือได้รับความยินยอมจากเจ้าของข้อมูล อย่างไรก็ตาม การบังคับใช้บทบัญญัตินี้ยังมีข้อจำกัด โดยเฉพาะในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยบุคคลทั่วไป ซึ่งไม่ได้อยู่ในขอบเขตของผู้มีหน้าที่ตามกฎหมาย ส่งผลให้ผู้กระทำความผิดสามารถเลี่ยงโทษทางอาญาได้ และทำให้มาตรการทางกฎหมายไม่สามารถควบคุมพฤติกรรมดังกล่าวได้อย่างมีประสิทธิภาพ รวมทั้งปัญหากำหนดลักษณะการกระทำความผิดในกรณีที่บุคคลธรรมดาซื้อขายข้อมูลส่วนบุคคล (พิทยา บรรลือทรัพย์, 2562) ซึ่งในประเด็นนี้เห็นว่า มาตรา 80 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นบทบัญญัติที่กำหนดโทษทางอาญาสำหรับบุคคลที่มีหน้าที่เกี่ยวข้องกับการบังคับใช้กฎหมายคุ้มครองข้อมูล เช่น พนักงานเจ้าหน้าที่หรือคณะกรรมการที่เปิดเผยข้อมูลโดยมิชอบ อย่างไรก็ตาม เนื่องจากกฎหมายอาญาดำเนินการโดยเคร่งครัดเพื่อคุ้มครองสิทธิของประชาชน การ



ตีความคำว่า “ผู้ใด” ในมาตรานี้จึงต้องจำกัดขอบเขตให้ชัดเจนเฉพาะบุคคลตามที่กฎหมายกำหนด (นิรนาท แก้วประเสริฐ, 2557) หากตีความขยายให้ครอบคลุมถึงบุคคลทั่วไปที่ไม่มีหน้าที่โดยตรง อาจก่อให้เกิดความไม่แน่นอนทางกฎหมาย กระทบต่อหลักนิติรัฐ และสร้างความกังวลเกินควรต่อผู้ปฏิบัติงาน จนอาจลดประสิทธิภาพในการบังคับใช้กฎหมาย (สำนักงานคณะกรรมการกฤษฎีกา, 2561) ในทางกลับกัน มาตรา 80 ยังไม่ครอบคลุมถึงกรณีที่บุคคลธรรมดาซื้อขายข้อมูลส่วนบุคคลโดยมิชอบ ซึ่งถือเป็นช่องว่างสำคัญในทางกฎหมาย และส่งผลให้การปราบปรามอาชญากรรมไซเบอร์ขาดประสิทธิภาพ ดังนั้น จึงควรมีการปรับปรุงกฎหมายให้ครอบคลุมการกระทำของบุคคลทั่วไป เพื่อให้สามารถคุ้มครองข้อมูลส่วนบุคคลและสิทธิของประชาชนได้อย่างเหมาะสม

นับว่าปัจจุบันกฎหมายที่ใช้บังคับเกี่ยวกับการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบยังไม่สามารถตอบสนองต่อปัญหาที่เกิดขึ้นได้อย่างมีประสิทธิภาพ ประเทศไทยยังไม่มีบทบัญญัติกฎหมายเฉพาะที่ครอบคลุมการกระทำความผิดของบุคคลธรรมดาที่มีพฤติกรรมซื้อขายหรือแสวงหาประโยชน์จากข้อมูลส่วนบุคคลโดยมิชอบ ส่งผลให้เกิดช่องว่างทางกฎหมาย และทำให้การบังคับใช้กฎหมายในทางปฏิบัติไม่ครอบคลุมต่อพฤติกรรมที่เกิดขึ้นจริง เนื่องจากการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบเป็นปัญหาในระดับประเทศที่ก่อให้เกิดความเสียหายอย่างร้ายแรง ทั้งในมิติของความปลอดภัย ทรัพย์สิน และสิทธิความเป็นส่วนตัวของประชาชน การควบคุมปัญหาดังกล่าวจึงจำเป็นต้องมีมาตรการทางกฎหมายที่ชัดเจน โดยเฉพาะบทบัญญัติเกี่ยวกับโทษทางอาญาที่เฉพาะเจาะจง เพื่อให้สามารถป้องกันและปราบปรามการกระทำความผิดในลักษณะนี้ได้อย่างเป็นรูปธรรม และสร้างมาตรฐานในการจัดการข้อมูลส่วนบุคคลที่มีประสิทธิภาพมากยิ่งขึ้น

ดังนั้น จากสภาพปัญหาที่กล่าวมาข้างต้นจึงได้มีการศึกษาการบังคับใช้กฎหมายเกี่ยวกับการกำหนดโทษทางอาญา ศึกษากรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย โดยศึกษากฎหมายของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร Data Protection Act 2018 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ที่มีการบัญญัติมาตรการเกี่ยวกับการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมายไว้โดยเฉพาะเป็นแนวทาง และนำไปสู่เสนอแนวทาง การกำหนดโทษทางอาญาในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมายต่อไปในอนาคต

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาแนวคิด ทฤษฎี และหลักการเกี่ยวกับการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย
2. เพื่อศึกษามาตรการการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคล โดยมิชอบด้วยกฎหมายของระหว่างประเทศต่างประเทศและประเทศไทย
3. เพื่อศึกษาวิเคราะห์ปัญหาการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคล โดยมิชอบด้วยกฎหมาย
4. เพื่อศึกษาแนวทางในการแก้ไขปัญหาเกี่ยวกับการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย



การทบทวนวรรณกรรม

การวิจัยนี้ ได้ทำการศึกษาการบังคับใช้กฎหมายเกี่ยวกับการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย โดยศึกษารัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ประมวลกฎหมายอาญา พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงประกาศ ระเบียบ และข้อบังคับที่เกี่ยวข้อง นอกจากนี้ได้มีการศึกษากฎหมายที่เกี่ยวข้องกับการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย เพื่อนำมาวิเคราะห์เปรียบเทียบปัญหาต่าง ๆ และหาแนวทางแก้ไขปัญหายุ่งยากเกี่ยวกับการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย ซึ่งวรรณกรรมที่เกี่ยวข้องกับการบังคับใช้กฎหมายเกี่ยวกับการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย สามารถแบ่งออกเป็น 4 ประเด็นหลัก ได้แก่ แนวคิด ทฤษฎี และหลักการทางกฎหมายอาญา ซึ่งประกอบด้วยทฤษฎีการลงโทษ เช่น ทฤษฎีตอบแทน (Retributive Theory) ทฤษฎีป้องปราม (Deterrence Theory) และทฤษฎีฟื้นฟู (Rehabilitation Theory) รวมถึงหลักการสำคัญในการกำหนดโทษ เช่น หลักความได้สัดส่วน (Proportionality) หลักความชอบด้วยกฎหมาย (Legality) และหลักความยุติธรรม (Justice) ประเด็นต่อมาคือเรื่องข้อมูลส่วนบุคคลและการซื้อขายโดยมิชอบ โดยข้อมูลส่วนบุคคลหมายถึงข้อมูลที่สามารถระบุตัวบุคคลได้ เช่น ชื่อ-สกุล หมายเลขบัตรประจำตัวประชาชน หรือข้อมูลทางการเงิน โดยในปัจจุบันมีการลักลอบซื้อขายข้อมูลเหล่านี้ผ่านช่องทางออนไลน์โดยมิชอบ ซึ่งสร้างความเสียหายให้กับเจ้าของข้อมูลและสังคมโดยรวม ส่วนประเด็นเรื่องการกำหนดโทษและมาตรการทางกฎหมาย พบว่า ประเทศไทยมีการบัญญัติบทลงโทษทั้งทางอาญาและทางปกครองไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเฉพาะในหมวดบทกำหนดโทษ มาตรา 72-74 ขณะเดียวกันในต่างประเทศ เช่น สหภาพยุโรป มีการใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (GDPR) ซึ่งแม้จะเน้นบทลงโทษทางปกครอง แต่ก็มีความเข้มงวดและเป็นแบบอย่างสำคัญในการออกแบบมาตรการป้องกันการละเมิดข้อมูลส่วนบุคคล สุดท้ายคือประเด็นปัญหาและข้อจำกัดในการบังคับใช้กฎหมาย ทั้งในเชิงนโยบาย การตีความกฎหมาย ความพร้อมของหน่วยงานที่เกี่ยวข้อง และการบังคับใช้จริงในทางปฏิบัติ ซึ่งเป็นโจทย์สำคัญที่ควรศึกษาเพิ่มเติมเพื่อหาแนวทางปรับปรุงแก้ไขให้มีประสิทธิภาพยิ่งขึ้น

วิธีดำเนินการวิจัย

การวิจัยนี้ เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีวิธีการดำเนินการวิจัย ดังนี้

1. แหล่งข้อมูลการวิจัย ได้แก่ การวิจัยเอกสาร (Documentary Research) ประกอบด้วย การค้นคว้าและเก็บรวบรวมข้อมูลจากเอกสารวิชาการทั้งภาษาไทยและภาษาต่างประเทศจากแหล่งข้อมูลที่มีความน่าเชื่อถือมาใช้ประกอบการวิจัย อาทิ หนังสือ บทความ รายงานการการศึกษาจากสถาบันต่าง ๆ ที่เกี่ยวข้อง เป็นต้น

2. การเก็บรวบรวมข้อมูล ได้แก่ การเก็บรวบรวมข้อมูลปฐมภูมิ (Primary Data) คือ ข้อมูลที่ได้จากการรวบรวมข้อมูลเอกสารต่าง ๆ (Document Research) ด้วยการทบทวนวรรณกรรมจากตำรา เอกสาร รายงานการวิจัย การประชุม สัมมนา วิทยานิพนธ์และบทความ รวมทั้งเอกสารอื่น ๆ ที่เกี่ยวข้อง



3. การวิเคราะห์ข้อมูล ได้แก่ เป็นการนำข้อมูลที่ได้จากการรวบรวมข้อมูลตามระเบียบวิธีวิจัยที่กำหนดไว้มาวิเคราะห์ร่วมกัน แล้วนำเสนอเป็นความเรียง (Descriptive) เพื่อให้ได้คำตอบเชิงเปรียบเทียบที่เป็นข้อค้นพบของงานวิจัย แล้วนำมาวิเคราะห์ในเชิงเนื้อหา (Content Analysis)

ผลการวิจัย

การศึกษานี้ ผู้วิจัยสามารถจำแนกผลได้ ดังนี้

1. การศึกษาแนวคิด ทฤษฎี และหลักการเกี่ยวกับการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย

ผลการวิจัยพบว่า ในสถานการณ์ปัจจุบันที่มีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย กลายเป็นปัญหาที่ส่งผลกระทบต่อความปลอดภัยของประชาชน เช่น การกระทำของแก๊งคอลเซ็นเตอร์ที่หลอกลวงประชาชน แม้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจะมีการกำหนดโทษทางปกครอง แต่ก็ไม่สามารถทำให้ผู้กระทำความผิดเกรงกลัวต่อการปรับเงิน เนื่องจากแก๊งคอลเซ็นเตอร์ไม่ถือว่าตนเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือถึงแม้จะถูกตัดสินว่ามีความผิดทางปกครอง การปรับเงินก็ไม่ได้เป็นสิ่งที่ทำให้อาชญากรทางไซเบอร์หวาดกลัว การกำหนดโทษทางอาญาที่มีการปรับ การจำคุก หรือทั้งจำทั้งปรับ สำหรับการกระทำความผิดเกี่ยวกับการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย จะช่วยเพิ่มประสิทธิภาพในการบังคับใช้กฎหมาย และทำให้เกิดความชัดเจนว่าผู้กระทำความผิดในลักษณะดังกล่าวจะได้รับโทษทางอาญาอย่างแน่นอน ดังนั้น การทำวิทยานิพนธ์ในครั้งนี้จึงได้ศึกษาแนวคิด หลักการ และทฤษฎีที่เกี่ยวข้องกับการกำหนดโทษทางอาญาในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย ซึ่งซึ่งการศึกษานี้มีการทบทวนงานวรรณกรรม ได้แก่ แนวคิดการคุ้มครองข้อมูลส่วนบุคคล แนวคิดเกี่ยวกับการกำกับดูแล แนวคิดการกำหนดโทษทางอาญา ทฤษฎีการลงโทษทางอาญา รวมทั้งมาตรฐานสากลด้านการคุ้มครองข้อมูลส่วนบุคคล การละเมิดความปลอดภัยของข้อมูลส่วนบุคคล และปัจจัยที่พิจารณาการกำหนดโทษทางอาญา ซึ่งเกี่ยวข้องโดยตรงกับการบังคับใช้กฎหมายเกี่ยวกับการกำหนดโทษทางอาญา ศึกษากรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย

2. การศึกษามาตรการการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคล โดยมิชอบด้วยกฎหมายของระหว่างประเทศต่างประเทศและประเทศไทย

ผลการวิจัยพบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) มีประเด็นสำคัญที่เป็นอุปสรรคต่อการบังคับใช้กฎหมายในการควบคุมการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบ ได้แก่ ช่องว่างทางกฎหมายที่ทำให้การลงโทษผู้กระทำผิดไม่มีประสิทธิภาพเพียงพอ โดยเฉพาะในมาตรา 80 PDPA ซึ่งกำหนดโทษทางอาญาเฉพาะกรณีที่บุคคลซึ่งมีหน้าที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเปิดเผยข้อมูลโดยมิชอบ แต่ไม่ได้ครอบคลุมถึงการซื้อขายข้อมูลส่วนบุคคลโดยบุคคลทั่วไป ส่งผลให้ผู้กระทำความผิดสามารถหลีกเลี่ยงการถูกดำเนินคดีอาญาได้ง่าย นอกจากนี้ PDPA ของประเทศไทยยังเน้นการลงโทษทางแพ่งและทางปกครองมากกว่าการกำหนดโทษทางอาญา ทำให้มาตรการลงโทษขาดประสิทธิภาพในการป้องปราม (deterrence) การซื้อขายข้อมูลส่วนบุคคลซึ่งก่อให้เกิดผลกระทบอย่างร้ายแรงต่อสิทธิของเจ้าของข้อมูล อีกทั้งการดำเนินคดีในกรณีดังกล่าวยังมีข้อจำกัดในทางปฏิบัติ เนื่องจาก การพิสูจน์ความผิดในกรณีการซื้อขายข้อมูลส่วนบุคคลมีความซับซ้อน อันเป็นผลมาจากการที่ธุรกรรมดังกล่าวมัก



ดำเนินการผ่านช่องทางออนไลน์หรือแพลตฟอร์มดิจิทัลที่มีลักษณะกระจายตัว ทำให้ยากต่อการตรวจสอบและรวบรวมพยานหลักฐาน

อุปสรรคต่อมา ในการกำกับดูแลและการบังคับใช้กฎหมายข้ามพรมแดน เป็นปัญหาที่พบในหลายประเทศ โดยเฉพาะเมื่อผู้กระทำความผิดหรือแพลตฟอร์มที่ใช้สำหรับซื้อขายข้อมูลส่วนบุคคลตั้งอยู่ในต่างประเทศ การดำเนินคดีข้ามพรมแดนต้องอาศัยความร่วมมือระหว่างประเทศและกระบวนการทางกฎหมายที่ซับซ้อน ส่งผลให้การบังคับใช้กฎหมายเป็นไปอย่างล่าช้าและไม่มีประสิทธิภาพ เมื่อพิจารณาเปรียบเทียบกับแนวทางของต่างประเทศ พบว่า กฎหมายของสหราชอาณาจักรภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2561 (DPA 2018) กำหนดให้การเสนอขายหรือจำหน่ายข้อมูลส่วนบุคคลที่ได้มาโดยมิชอบเป็นความผิดทางอาญา ซึ่งช่วยให้หน่วยงานกำกับดูแลสามารถดำเนินคดีและใช้มาตรการลงโทษที่เข้มงวดขึ้น ขณะที่ในสหรัฐอเมริกา กฎหมายที่เกี่ยวข้อง เช่น California Consumer Privacy Act (CCPA) และ Computer Fraud and Abuse Act (CFAA) กำหนดกลไกที่อนุญาตให้ผู้บริโภคดำเนินการฟ้องร้องต่อองค์กรที่ละเมิดสิทธิของตน ซึ่งเป็นแนวทางที่ช่วยเสริมสร้างความเข้มแข็งให้กับการคุ้มครองข้อมูลส่วนบุคคลผ่านการดำเนินคดีโดยผู้เสียหาย ซึ่งจากผลการวิเคราะห์เปรียบเทียบกฎหมายของต่างประเทศนั้น ประเทศไทยต้องมีการปรับปรุงมาตรการทางกฎหมายให้ครอบคลุมถึงการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบ โดยอาจพิจารณาเพิ่มบทบัญญัติที่กำหนดให้การซื้อขายหรือการเสนอขายข้อมูลส่วนบุคคลที่ได้มาโดยมิชอบเป็นความผิดทางอาญา รวมถึงการพัฒนาแนวทางการบังคับใช้กฎหมายที่สามารถรับมือกับความซับซ้อนของธุรกรรมดิจิทัลและการกำกับดูแลข้ามพรมแดนได้อย่างมีประสิทธิภาพ ดังนั้น หากประเทศไทยสามารถปรับปรุง มาตรการทางกฎหมายให้ครอบคลุมถึงการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบ และเสริมสร้างกลไกการบังคับใช้กฎหมายที่มีประสิทธิภาพมากขึ้น จะช่วยลดปัญหาการละเมิดข้อมูลส่วนบุคคล อำนวยความเป็นธรรมให้กับเจ้าของข้อมูลและเพิ่มศักยภาพในการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในระยะยาว

3. การศึกษาวิเคราะห์ปัญหาการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคล โดยมิชอบด้วยกฎหมาย

ผลการวิจัยพบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม พบว่าทั้งสองฉบับมีบทบาทสำคัญในการกำกับดูแลการใช้ข้อมูลส่วนบุคคลและควบคุมการกระทำความผิดที่เกี่ยวข้องกับข้อมูลในระบบดิจิทัล อย่างไรก็ตาม บทบัญญัติในกฎหมายทั้งสองฉบับ ยังขาดความครอบคลุมในประเด็นการซื้อขายข้อมูลส่วนบุคคลโดยบุคคลธรรมดา และการนำข้อมูลส่วนบุคคลไปแสวงหาผลประโยชน์โดยมิชอบผ่านแพลตฟอร์มออนไลน์หรือ Dark Web ซึ่งส่งผลให้เกิดช่องว่างทางกฎหมายที่ทำให้การดำเนินคดีกับผู้กระทำผิดเป็นไปได้ยากจำกัด ในกรณีของ PDPA มาตรา 80 กำหนดโทษทางอาญาสำหรับ “ผู้ใด” ที่เปิดเผยหรือใช้ข้อมูลส่วนบุคคลโดยมิชอบ อย่างไรก็ตาม ข้อความของมาตราดังกล่าวไม่ได้ระบุอย่างชัดเจนว่าการซื้อขายข้อมูลส่วนบุคคล โดยบุคคลธรรมดาจะถือเป็นความผิดหรือไม่ ซึ่งส่งผลให้เกิดข้อถกเถียงเกี่ยวกับการตีความขอบเขตของบทลงโทษและทำให้การดำเนินคดีกับบุคคลที่ซื้อขายหรือแสวงหาผลประโยชน์จากข้อมูลส่วนบุคคลโดยมิชอบเป็นไปได้ยาก นอกจากนี้ PDPA มุ่งเน้นการกำกับดูแลผู้ควบคุมข้อมูล (Data Controller) และผู้ประมวลผลข้อมูล (Data Processor) มากกว่าการควบคุมพฤติกรรมของบุคคลธรรมดาที่ซื้อขายข้อมูลส่วนบุคคล ส่งผลให้การซื้อขายข้อมูลในตลาดมืด (Black Market) หรือผ่านแพลตฟอร์มออนไลน์ที่ไม่สามารถตรวจสอบได้ ยังคงเป็นปัญหาที่ไม่ได้รับการแก้ไขอย่างมีประสิทธิภาพ ในขณะเดียวกัน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ



คอมพิวเตอร์ฯ มาตรา 14 กำหนดโทษสำหรับการนำเข้าสู่ข้อมูลอันเป็นเท็จที่อาจก่อให้เกิดความเสียหายต่อบุคคลหรือประชาชน อย่างไรก็ตาม เนื่องจาก ข้อมูลส่วนบุคคลโดยทั่วไปไม่ใช่ข้อมูลอันเป็นเท็จ จึงไม่อยู่ภายใต้ขอบเขตของมาตราดังกล่าว ส่งผลให้บุคคลที่ซื้อขายข้อมูลส่วนบุคคลโดยมิชอบไม่สามารถถูกดำเนินคดีภายใต้กฎหมายฉบับนี้ นอกจากนี้ มาตรา 22 ของกฎหมายฉบับเดียวกัน ใช้ถ้อยคำว่า “พนักงานเจ้าหน้าที่” ซึ่งจำกัดขอบเขตของบุคคลที่อยู่ภายใต้บทบัญญัตินี้ หมายความว่ากฎหมายฉบับนี้มุ่งเน้นไปที่การควบคุมการใช้ข้อมูลของเจ้าหน้าที่รัฐ มากกว่าการกำกับดูแลการกระทำของบุคคลทั่วไป ส่งผลให้บุคคลธรรมดาที่ซื้อขายข้อมูลส่วนบุคคลสามารถหลีกเลี่ยงความรับผิดทางกฎหมายได้

ประเด็นสำคัญอีกประการหนึ่ง คือ การนำข้อมูลส่วนบุคคลไปใช้แสวงหาผลประโยชน์โดยมิชอบผ่านแพลตฟอร์มใต้ดิน (Dark Web) หรือเว็บไซต์ที่มีลักษณะปกปิดตัวตน ซึ่งเป็นช่องทางที่นิยมใช้สำหรับการดำเนินกิจกรรมผิดกฎหมาย เช่น การซื้อขายข้อมูลบัตรเครดิต ข้อมูลบัญชีธนาคาร และข้อมูลส่วนบุคคลที่สามารถนำไปใช้ในการแอบอ้างตัวตนหรือฉ้อโกงทางออนไลน์ แม้ว่ากฎหมายไทยจะมีบทบัญญัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลและการกระทำความผิดทางไซเบอร์ แต่ยังไม่มีความมาตรการที่ครอบคลุมโดยตรงเกี่ยวกับการซื้อขายข้อมูลส่วนบุคคลบนแพลตฟอร์มใต้ดิน ซึ่งทำให้การดำเนินคดีในกรณีดังกล่าวเป็นไปได้ยาก ดังนั้น เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยมีประสิทธิภาพมากขึ้น ควรมีการปรับปรุง PDPA ให้สามารถดำเนินคดีกับบุคคลธรรมดาที่ซื้อขายหรือใช้ข้อมูลส่วนบุคคลโดยมิชอบบนแพลตฟอร์มออนไลน์ได้

4. การศึกษาแนวทางในการแก้ไขปัญหาเกี่ยวกับการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย

ผลการวิจัยพบว่า เมื่อมาตรการลงโทษที่กำหนดไว้ในกฎหมายยังไม่มีผลเชิงป้องปรามที่จะเป็นมาตรการป้องปรามการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบ ส่งผลให้การกระทำผิดในลักษณะดังกล่าวยังคงเกิดขึ้นอย่างต่อเนื่อง โดยเฉพาะในกรณีที่ข้อมูลส่วนบุคคลถูกซื้อขายในตลาดมืด (Dark Web) หรือถูกนำไปใช้เพื่อแสวงหาผลประโยชน์ในเชิงพาณิชย์โดยปราศจากความยินยอมของเจ้าของข้อมูล แม้ว่ามาตรา 80 ของ PDPA จะกำหนดโทษทางอาญาสำหรับการละเมิดข้อมูลส่วนบุคคลโดยมิชอบ แต่โทษที่กำหนดไว้คือ จำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ ซึ่งเมื่อเปรียบเทียบกับผลกำไรที่อาชญากรไซเบอร์หรือองค์กรธุรกิจสามารถได้รับจากการซื้อขายข้อมูลส่วนบุคคลแล้ว บทลงโทษดังกล่าวยังถือว่าไม่เพียงพอในการป้องปรามพฤติกรรมดังกล่าวให้หมดไป เมื่อพิจารณากฎหมายของประเทศที่มีมาตรการควบคุมการซื้อขายข้อมูลส่วนบุคคลที่เข้มงวดกว่าพบว่า สหราชอาณาจักรมีมาตรา 170 แห่ง DPA 2018 ซึ่งกำหนดให้การได้มา เปิดเผย หรือครอบครองข้อมูลส่วนบุคคลโดยมิชอบเป็นความผิดอาญาที่มีโทษจำคุกสูงสุดถึง 5 ปี หรือค่าปรับแบบไม่จำกัด (Unlimited Fine) ซึ่งแตกต่างจาก PDPA ของไทยที่กำหนดโทษจำคุกสูงสุดเพียง 1 ปี หรือปรับไม่เกิน 1 ล้านบาท นอกจากนี้ DPA 2018 ยังมีมาตรา 171 ซึ่งกำหนดให้การเสนอหรือรับสินบนเพื่อให้เปิดเผยข้อมูลส่วนบุคคลโดยมิชอบเป็นความผิดทางอาญาโดยตรง ในสหรัฐอเมริกา แม้ว่าจะไม่มีพระราชบัญญัติกลางที่ควบคุมข้อมูลส่วนบุคคลในทุกกรณี แต่ California Consumer Privacy Act (CCPA) และกฎหมายเฉพาะภาคอุตสาหกรรม เช่น Health Insurance Portability and Accountability Act (HIPAA) กำหนดบทลงโทษที่รุนแรงขึ้น โดยเฉพาะอย่างยิ่ง Federal Trade Commission (FTC) มีอำนาจในการสั่งปรับองค์กรที่ละเมิดข้อมูลส่วนบุคคลเป็นจำนวนมาก ตัวอย่างเช่น กรณีที่ Facebook ถูกปรับ 5,000 ล้านดอลลาร์สหรัฐ ภายใต้กฎหมายของ FTC หรือการลงโทษจำคุกในกรณีที่มีการละเมิดข้อมูลสุขภาพโดยมิชอบ ดังนั้น การกำหนดบทลงโทษที่รุนแรงขึ้นในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบเป็นสิ่งจำเป็นเพื่อให้



สามารถควบคุมและป้องปรามพฤติกรรมดังกล่าวได้อย่างมีประสิทธิภาพ PDPA ของไทยยังมีช่องโหว่สำคัญในการกำหนดโทษทางอาญาสำหรับบุคคลที่ซื้อขายข้อมูลส่วนบุคคลโดยมิชอบ ซึ่งแตกต่างจากกฎหมายของสหราชอาณาจักรและสหรัฐอเมริกาที่กำหนดโทษที่เข้มงวดกว่า ดังนั้น การเพิ่มโทษทางอาญาให้สอดคล้องกับมูลค่าความเสียหายที่เกิดขึ้น รวมถึงการให้อำนาจแก่ PDPC ในการดำเนินคดีโดยตรง จะช่วยให้การบังคับใช้กฎหมายเป็นไปอย่างมีประสิทธิภาพมากขึ้น นอกจากนี้ การจัดตั้งหน่วยงานเฉพาะทางและเสริมสร้างความร่วมมือระหว่างภาครัฐและเอกชนจะช่วยให้ประเทศไทยสามารถรับมือกับปัญหาการละเมิดข้อมูลส่วนบุคคลในบริบทของเศรษฐกิจดิจิทัลได้อย่างเหมาะสมและสอดคล้องกับมาตรฐานสากลมากยิ่งขึ้น ดังนั้น แนวทางในการแก้ไขปัญหาเกี่ยวกับการกำหนดโทษทางอาญาในกรณีการซื้อขาย ข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมายเสนอให้เพิ่มเติมบทบัญญัติในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติมในส่วนของบทลงโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย

สรุปผลการวิจัย

การวิจัยนี้ ผู้วิจัยสามารถสรุปผลการวิจัยตามวัตถุประสงค์ได้ ดังนี้

1. เพื่อศึกษาแนวคิด ทฤษฎี และหลักการเกี่ยวกับการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย พบว่า การศึกษาแนวคิด ทฤษฎีและหลักการเกี่ยวกับการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย สามารถสรุปแนวคิด ทฤษฎีและหลักการที่จะนำมาใช้บังคับกฎหมายเกี่ยวกับการกำหนดโทษ ได้แก่ แนวคิดการคุ้มครองข้อมูลส่วนบุคคล แนวคิดเกี่ยวกับการกำกับดูแล แนวคิดการกำหนดโทษทางอาญา ทฤษฎีการลงโทษทางอาญา รวมทั้งมาตรฐานสากลด้านคุ้มครองข้อมูลส่วนบุคคล การละเมิดความปลอดภัยของข้อมูลส่วนบุคคล และปัจจัยที่พิจารณาการกำหนดโทษทางอาญา

2. เพื่อศึกษามาตรการการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคล โดยมิชอบด้วยกฎหมายของระหว่างประเทศต่างประเทศและประเทศไทย พบว่า มาตรการการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคล โดยมิชอบด้วยกฎหมายของระหว่างประเทศต่างประเทศและประเทศไทยหากประเทศไทยสามารถปรับปรุงมาตรการทางกฎหมายให้ครอบคลุมถึงการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบ และเสริมสร้างกลไกการบังคับใช้กฎหมายที่มีประสิทธิภาพมากขึ้น จะช่วยลดปัญหาการละเมิดข้อมูลส่วนบุคคล อำนวยความเป็นธรรมให้กับเจ้าของข้อมูลและเพิ่มศักยภาพในการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในระยะยาว

3. เพื่อศึกษาวิเคราะห์ปัญหาการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคล โดยมิชอบด้วยกฎหมาย พบว่า ปัญหาการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคล โดยมิชอบด้วยกฎหมายการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ไม่ครอบคลุมถึงบุคคลธรรมดา ซึ่งทำการซื้อขายข้อมูลลักษณะของการกระทำความผิด บทลงโทษ รวมถึงการนำข้อมูลส่วนบุคคลไปแสวงหาผลประโยชน์โดยมิชอบบนเว็บไซต์หรือแพลตฟอร์ม ส่งผลให้ขาดมาตรการในการควบคุมและปราบปรามการซื้อขายข้อมูลส่วนบุคคลที่มีประสิทธิภาพ และมีการนำข้อมูลไปใช้เพื่อแสวงหาผลประโยชน์เชิงพาณิชย์โดยปราศจากความยินยอมของเจ้าของข้อมูล



4. เพื่อศึกษาแนวทางในการแก้ไขปัญหาเกี่ยวกับการกำหนดโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย พบว่า แนวทางในการแก้ไขปัญหาเกี่ยวกับการกำหนดโทษทางอาญาในกรณีการซื้อขาย ข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย ซึ่งเสนอให้เพิ่มเติมบทบัญญัติในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ในส่วนของบทลงโทษทางอาญาในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย

การอภิปรายผล

การวิจัยนี้ ผู้วิจัยสามารถอภิปรายผลได้ ดังนี้

1. ปัญหาการบังคับใช้กฎหมายในกรณีซื้อขายข้อมูลส่วนบุคคลที่เกิดขึ้น แม้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) จะกำหนดบทลงโทษสำหรับการละเมิดข้อมูลส่วนบุคคล แต่ยังเผชิญข้อจำกัดในการบังคับใช้ โดยเฉพาะมาตรา 80 ซึ่งกำหนดโทษเฉพาะสำหรับผู้ที่มีหน้าที่ตามกฎหมายเท่านั้น มิได้ครอบคลุมถึงกรณีที่บุคคลทั่วไปกระทำการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบ ทำให้เกิดช่องว่างทางกฎหมายที่ส่งผลกระทบต่อประสิทธิภาพในการดำเนินคดี และเปิดโอกาสให้ผู้กระทำความผิดสามารถหลีกเลี่ยงความรับผิดได้ง่าย นอกจากนี้ โครงสร้างบทลงโทษภายใต้ PDPA ยังคงให้ความสำคัญกับการลงโทษทางแพ่ง และปกครองมากกว่าการใช้มาตรการทางอาญา ส่งผลให้ขาดพลังในการป้องปราม (Deterrence) พฤติกรรมการซื้อขายข้อมูลส่วนบุคคล ซึ่งเป็นพฤติกรรมที่ก่อให้เกิดความเสียหายอย่างร้ายแรงต่อสิทธิของเจ้าของข้อมูล อีกทั้งการดำเนินคดีในลักษณะดังกล่าวยังมีความซับซ้อนในทางปฏิบัติ เนื่องจากธุรกรรมมักดำเนินการผ่านช่องทางดิจิทัลที่มีลักษณะกระจายตัว ทำให้ยากต่อการตรวจสอบและรวบรวมพยานหลักฐาน (นिरนาท แก้วประเสริฐ, 2557) เมื่อพิจารณากฎหมายของต่างประเทศ เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร (Data Protection Act 2018) พบว่า ได้มีการกำหนดให้การเสนอขายหรือจำหน่ายข้อมูลที่ได้มาโดยมิชอบเป็นความผิดทางอาญาโดยเฉพาะ ซึ่งช่วยให้หน่วยงานกำกับดูแลสามารถดำเนินคดีได้อย่างเด็ดขาด ในขณะที่กฎหมายของสหรัฐอเมริกา เช่น CCPA และ CFAA ได้ให้อำนาจแก่ผู้บริโภคในการฟ้องร้ององค์กรที่ละเมิดสิทธิของตน ซึ่งเป็นกลไกเสริมที่ช่วยเพิ่มพลังให้แก่ระบบคุ้มครองข้อมูลส่วนบุคคลจากการเปรียบเทียบดังกล่าวยังสะท้อนว่า ประเทศไทยจำเป็นต้องปรับปรุงมาตรการทางกฎหมายให้ครอบคลุมถึงการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบ และควรพิจารณากำหนดให้การกระทำความผิดดังกล่าวเป็นความผิดทางอาญาโดยเฉพาะ ตลอดจนพัฒนากลไกการบังคับใช้กฎหมายที่มีประสิทธิภาพ ทั้งในระดับภายในประเทศและระหว่างประเทศ เพื่อให้สามารถรับมือกับธุรกรรมข้อมูลที่มีลักษณะไร้พรมแดน และสร้างความเชื่อมั่นในการคุ้มครองสิทธิส่วนบุคคลในยุคดิจิทัลได้อย่างยั่งยืน

2. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ยังมีข้อจำกัดสำคัญที่เป็นอุปสรรคต่อการบังคับใช้กฎหมายในกรณีการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบ โดยเฉพาะการขาดบทบัญญัติที่กำหนดลักษณะของการกระทำความผิดในกรณีที่บุคคลธรรมดาเป็นผู้กระทำความผิด มาตรา 80 ของ PDPA แม้จะบัญญัติโทษทางอาญาสำหรับการเปิดเผยข้อมูลโดยมิชอบ แต่กลับจำกัดขอบเขตไว้เฉพาะผู้ที่มีหน้าที่ตามกฎหมาย เช่น พนักงานเจ้าหน้าที่หรือคณะกรรมการที่เกี่ยวข้อง ส่งผลให้บุคคลธรรมดาซึ่งแสวงหาประโยชน์จากการซื้อขายข้อมูลโดยมิชอบไม่อยู่ในข่ายการรับโทษทางอาญาตามบทบัญญัติดังกล่าว ช่องโหว่นี้ส่งผลให้การควบคุมการซื้อขายข้อมูลส่วนบุคคลผ่านช่องทางออนไลน์หรือแพลตฟอร์มดิจิทัลยังขาดประสิทธิภาพ และอาจทำให้พฤติกรรม



การละเมิดข้อมูลส่วนบุคคลขยายตัวมากขึ้น โดยเฉพาะในบริบทของอาชญากรรมไซเบอร์ที่อาศัยข้อมูลส่วนบุคคลเป็นเครื่องมือในการกระทำความผิด เช่น การฉ้อโกงทางการเงิน การหลอกลวงทางออนไลน์ และการคุกคามความเป็นส่วนตัวในรูปแบบต่าง ๆ เมื่อเปรียบเทียบกับกฎหมายต่างประเทศ เช่น Data Protection Act 2018 ของสหราชอาณาจักร พบว่ามีบทบัญญัติที่ครอบคลุมการกระทำของบุคคลธรรมดาที่เข้าถึง ใช้เปิดเผย หรือจำหน่ายข้อมูลส่วนบุคคลโดยมิชอบไว้เป็นความผิดทางอาญาโดยเฉพาะ ขณะที่ California Consumer Privacy Act (CCPA) ของสหรัฐอเมริกา กำหนดมาตรฐานให้ทั้งองค์กรธุรกิจและบุคคลธรรมดาต้องปฏิบัติตามกฎหมาย และเปิดโอกาสให้เจ้าของข้อมูลสามารถฟ้องร้องผู้ละเมิดสิทธิของตนได้โดยตรง ซึ่งช่วยเสริมกลไกในการบังคับใช้กฎหมายอย่างเป็นรูปธรรม จากข้อจำกัดของ PDPA ในปัจจุบัน จึงมีความจำเป็นต้องมีการปรับปรุงกฎหมายให้ครอบคลุมการซื้อขายข้อมูลส่วนบุคคลโดยบุคคลธรรมดาอย่างชัดเจน โดยการเพิ่มบทบัญญัติที่กำหนดให้การกระทำความผิดทางอาญา พร้อมทั้งกำหนดโทษที่เหมาะสมกับมูลค่าความเสียหาย เพื่อเสริมสร้างกลไกการป้องปรามและการดำเนินคดีที่มีประสิทธิภาพ นอกจากนี้ ยังควรมีการกำหนดแนวทางการตีความมาตรา 80 ให้ชัดเจน เพื่อป้องกันไม่ให้เจ้าหน้าที่ผู้ปฏิบัติงานต้องรับภาระความรับผิดเกินสมควร อันจะช่วยเสริมความมั่นใจในการบังคับใช้กฎหมายและยกระดับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยให้มีมาตรฐานสอดคล้องกับหลักสากล

ข้อค้นพบ หรือองค์ความรู้ใหม่

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ซึ่งมีบทบาทสำคัญในการกำกับดูแลข้อมูลส่วนบุคคลและควบคุมการกระทำความผิดในระบบดิจิทัล แต่ในปัจจุบันยังขาดความครอบคลุมในการควบคุมการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบ โดยเฉพาะเมื่อผู้กระทำความผิดเป็นบุคคลธรรมดาที่ไม่ได้มีหน้าที่ตามกฎหมายโดยตรง มาตรา 80 แห่ง PDPA กำหนดโทษทางอาญาสำหรับการเปิดเผยหรือใช้ข้อมูลส่วนบุคคลโดยมิชอบ แต่ข้อบทดังกล่าวเน้นเฉพาะบุคคลที่มีหน้าที่ตามกฎหมาย เช่น พนักงานเจ้าหน้าที่หรือคณะกรรมการ จึงไม่สามารถบังคับใช้กับบุคคลทั่วไปที่ซื้อขายหรือแสวงหาผลประโยชน์จากข้อมูลส่วนบุคคลได้ ส่งผลให้เกิดข้อถกเถียงในทางตีความกฎหมาย และเปิดช่องว่างให้การละเมิดข้อมูลผ่านช่องทางออนไลน์ โดยเฉพาะในตลาดมืดดิจิทัล (Dark Web) สามารถดำเนินไปได้โดยปราศจากการควบคุมที่มีประสิทธิภาพ ในทำนองเดียวกัน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ มาตรา 14 และมาตรา 22 แม้จะมีเป้าหมายในการควบคุมการนำเข้าข้อมูลอันเป็นเท็จ และการใช้ข้อมูลโดยเจ้าหน้าที่รัฐ แต่ก็ไม่ครอบคลุมถึงกรณีของบุคคลธรรมดาที่ซื้อขายข้อมูลส่วนบุคคล เนื่องจากข้อมูลส่วนบุคคลตามปกติมิใช่ “ข้อมูลอันเป็นเท็จ” และผู้กระทำความผิดส่วนใหญ่มิใช่เจ้าหน้าที่ของรัฐ นอกจากนี้ การนำข้อมูลส่วนบุคคลไปใช้โดยมิชอบผ่านแพลตฟอร์มใต้ดิน เช่น Dark Web ยังคงเป็นปัญหาสำคัญ เนื่องจากเป็นช่องทางที่นิยมใช้ในการซื้อขายข้อมูลที่ละเอียดอ่อน เช่น ข้อมูลบัญชีธนาคาร บัตรเครดิต หรือข้อมูลที่สามารถใช้แอบอ้างตัวตนได้ แม้กฎหมายไทยจะมีบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและความผิดทางไซเบอร์ แต่ยังไม่มีความเฉพาะที่สามารถครอบคลุมถึงพฤติกรรมการซื้อขายข้อมูลบนแพลตฟอร์มดังกล่าวได้โดยตรง ดังนั้น เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยมีประสิทธิภาพมากยิ่งขึ้น จำเป็นต้องมีการปรับปรุงกฎหมาย โดยเฉพาะ PDPA ให้สามารถดำเนินคดีกับบุคคลธรรมดาที่มีพฤติกรรมซื้อขายหรือแสวงหาประโยชน์จากข้อมูลส่วนบุคคลโดยมิชอบผ่านแพลตฟอร์มออนไลน์ได้อย่างชัดเจน รวมถึงการกำหนดบทลงโทษที่เหมาะสมและสอดคล้องกับ



ลักษณะของความเสียหาย ตลอดจนการพัฒนาเครื่องมือทางกฎหมายที่สามารถรับมือกับรูปแบบอาชญากรรมไซเบอร์ที่ซับซ้อนในยุคดิจิทัลได้อย่างเป็นระบบ

ข้อเสนอแนะการวิจัย

1. ข้อเสนอแนะในการนำไปใช้ประโยชน์

1.1 ปัญหาการบังคับใช้กฎหมายในกรณีซื้อขายข้อมูลส่วนบุคคล เนื่องจากการบังคับใช้กฎหมายในการควบคุมการซื้อขายข้อมูลส่วนบุคคลโดยมิชอบยังมีช่องว่างทางกฎหมายที่ทำให้การลงโทษผู้กระทำผิดไม่มีประสิทธิภาพเพียงพอ โดยเฉพาะในมาตรา 80 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดโทษทางอาญาเฉพาะกรณีที่บุคคลซึ่งมีหน้าที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเปิดเผยข้อมูลโดยมิชอบ แต่ไม่ได้ครอบคลุมถึงการซื้อขายข้อมูลส่วนบุคคลโดยบุคคลทั่วไป ดังนั้น ในประเด็นนี้จึงเห็นควรเสนอให้เพิ่มเติมบทบัญญัติในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้ครอบคลุมถึงพฤติกรรมการซื้อขายหรือแลกเปลี่ยนข้อมูลส่วนบุคคลโดยมิชอบ และกำหนดให้เป็นความผิดทางอาญาที่สามารถดำเนินคดีและลงโทษผู้กระทำผิดได้โดยตรง

ให้เพิ่มเติมความต่อไปนี้ เป็น “มาตรา 80/1” แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ความว่า

“มาตรา 80/1 ผู้ใดกระทำการซื้อขาย เสนอให้ซื้อ เสนอขาย หรือดำเนินการใดเพื่อให้ได้มาหรือจำหน่ายไปซึ่งข้อมูลส่วนบุคคลโดยรู้หรือควรรู้ว่าเป็นข้อมูลส่วนบุคคลที่ได้มาจากการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ฝ่าฝืนพระราชบัญญัตินี้ หรือโดยประการอื่นที่มีขอบด้วยกฎหมาย ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินห้าล้านบาท หรือทั้งจำทั้งปรับ”

1.2 ปัญหาการกำหนดลักษณะการกระทำความผิดในกรณีที่บุคคลธรรมดาซื้อขายข้อมูลส่วนบุคคล เนื่องจากมาตรา 80 ยังขาดบทบัญญัติที่กำหนดลักษณะของการกระทำความผิดในกรณีที่บุคคลธรรมดาซื้อขายข้อมูลส่วนบุคคลโดยมิชอบ ซึ่งส่งผลให้กฎหมายไทยไม่สามารถรับมือกับปัญหาการซื้อขายข้อมูลส่วนบุคคลที่เกิดขึ้นผ่านแพลตฟอร์มออนไลน์หรือในตลาดมืดดิจิทัลได้อย่างมีประสิทธิภาพ ดังนั้น ในประเด็นนี้จึงเห็นควรเสนอให้เพิ่มเติมบทบัญญัติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้ครอบคลุมถึงการกำหนดลักษณะการกระทำความผิดในกรณีที่บุคคลธรรมดาซื้อขายข้อมูลส่วนบุคคล ดังนี้

ให้เพิ่มเติมความต่อไปนี้ เป็น “มาตรา 80/2” แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ความว่า

“มาตรา 80/2 การกระทำใดตามมาตรา 80/1 เพื่อแสวงหาประโยชน์ในเชิงพาณิชย์ หรือเพื่อประโยชน์อันมิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น หรือเพื่อก่อความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล ผู้กระทำความผิดต้องระวางโทษจำคุกไม่เกินเจ็ดปี หรือปรับไม่เกินเจ็ดล้านบาท หรือทั้งจำทั้งปรับ”

2. ข้อเสนอแนะในการวิจัย

2.1 ปัญหาบทลงโทษในกรณีที่บุคคลธรรมดาซื้อขายข้อมูลส่วนบุคคลและการนำข้อมูลส่วนบุคคลไปแสวงหาผลประโยชน์โดยมิชอบบนเว็บไซต์หรือแพลตฟอร์ม ในประเด็นนี้เนื่องจากการนำข้อมูลส่วนบุคคลไปใช้แสวงหาผลประโยชน์โดยมิชอบผ่านแพลตฟอร์มใต้ดิน (Dark Web) หรือเว็บไซต์ที่มีลักษณะปกปิดตัวตน ซึ่งเป็นช่องทางที่นิยมใช้สำหรับการดำเนินกิจกรรมผิดกฎหมาย แต่กฎหมายยังขาดกฎหมายในการควบคุมเรื่องดังกล่าวอย่างมีประสิทธิภาพ ดังนั้น ในประเด็นนี้จึงเห็นควรแก้ไขเพิ่มเติมบทบัญญัติของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ดังนี้



ให้เพิ่มความต่อไปนี้เป็น “คำนิยาม” ของมาตรา 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ความว่า

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“แพลตฟอร์มใต้ดิน” หมายความว่า เครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือแพลตฟอร์มดิจิทัลที่ถูกออกแบบมาเพื่อปกปิดตัวตนของผู้ใช้งาน หรือปกปิดแหล่งที่มาของข้อมูลคอมพิวเตอร์ โดยเจตนาหลีกเลี่ยงการตรวจจับหรือการบังคับใช้กฎหมาย ซึ่งรวมถึงแต่ไม่จำกัดเพียงเครือข่ายที่เรียกว่า Dark Web หรือ Deep Web”

2.2 ปัญหาการกำหนดบทลงโทษที่รุนแรงขึ้นในกรณีการซื้อขายข้อมูลส่วนบุคคลที่มีขอบด้วยกฎหมาย เนื่องจากกฎหมายยังขาดกลไกควบคุมการใช้ข้อมูลส่วนบุคคลบนแพลตฟอร์มใต้ดิน ได้แก่ กำหนดให้การนำข้อมูลส่วนบุคคลไปขายหรือแจกจ่ายบนแพลตฟอร์มดิจิทัล หรือ Dark Web ซึ่งเป็นความผิดทางอาญาเพิ่มบทลงโทษสำหรับผู้ที่อำนวยความสะดวกหรือสนับสนุนการซื้อขายข้อมูลส่วนบุคคลในตลาดมืดทางออนไลน์ ดังนั้น ในประเด็นนี้จึงเห็นควรแก้ไขเพิ่มเติมบทบัญญัติของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ดังนี้

“มาตรา 16/3 ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลส่วนบุคคลของผู้อื่น โดยมีเจตนาเพื่อขาย เสนอขาย แจกจ่าย หรือเผยแพร่บนแพลตฟอร์มใต้ดิน โดยปราศจากความยินยอมจากเจ้าของข้อมูล ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ ถ้าการกระทำความผิดตามวรรคหนึ่ง เป็นเหตุให้ผู้อื่นได้รับความเสียหาย ถูกหลอกลวง ถูกฉ้อโกง หรือถูกละเมิดสิทธิส่วนบุคคลในลักษณะร้ายแรง ผู้กระทำความผิดต้องระวางโทษจำคุกไม่เกินเจ็ดปี หรือปรับไม่เกินหนึ่งแสนสี่หมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำความผิดตามวรรคหนึ่ง (1) กระทำต่อข้อมูลส่วนบุคคลของประชาชนเป็นจำนวนมากตั้งแต่หนึ่งร้อยคนขึ้นไป หรือ (2) กระทำเพื่อแสวงหาประโยชน์ทางการค้าหรือเพื่อประโยชน์ในการกระทำความผิดอาญาอื่น ผู้กระทำความผิดต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี หรือปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท หรือทั้งจำทั้งปรับ”

“มาตรา 16/4 ผู้ใดให้บริการ อำนวยความสะดวก หรือสนับสนุนการกระทำความผิดตามมาตรา 16/3 โดยรู้อยู่แล้วว่าเป็นการกระทำความผิด ต้องระวางโทษเช่นเดียวกับตัวการในความผิดนั้น

ผู้ให้บริการระบบคอมพิวเตอร์ที่จงใจสนับสนุนหรืออนุญาตให้มีการใช้ระบบคอมพิวเตอร์ในความควบคุมของตนเพื่อกระทำความผิดตามมาตรา 16/3 หรือรู้อยู่แล้วว่ามีกระทำความผิดดังกล่าวในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน แต่ไม่ดำเนินการระงับการกระทำความผิดหรือแจ้งเจ้าพนักงานทันทีที่ทราบ ต้องระวางโทษกึ่งหนึ่งของโทษที่กำหนดไว้สำหรับความผิดนั้น”

เอกสารอ้างอิง

คณาธิป ทองรวีวงศ์. (2563). กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1 ภาคกรอบความคิด ทฤษฎีและโครงสร้างฐาน

ความผิดและภาคความผิดต่อความมั่นคงปลอดภัยของระบบและข้อมูลคอมพิวเตอร์. กรุงเทพฯ: นิติธรรม.

นිරนาท แก้วประเสริฐ. (2557). ความหมายและการประยุกต์ใช้โทษอาญา. กรุงเทพฯ: สำนักพิมพ์แห่งมหาวิทยาลัยธรรมศาสตร์.



- พิทยา บรรลือทรัพย์. (2562). *มาตรการทางกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย*. (วิทยานิพนธ์หลักสูตรนิติศาสตรมหาบัณฑิต) คณะนิติศาสตร์ปริทัศน์ พนมยงค์ กรุงเทพมหานคร: มหาวิทยาลัยธุรกิจบัณฑิต.
- สำนักงานคณะกรรมการกฤษฎีกา. (2561). *ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ฉบับคณะกรรมการกฤษฎีกา (คณะที่ 11) ตรวจพิจารณา*. กรุงเทพฯ: สำนักงานคณะกรรมการกฤษฎีกา.
- สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2567). *สถิติเรื่องร้องเรียนด้านการคุ้มครองข้อมูลส่วนบุคคล*. สืบค้นเมื่อ 25 มีนาคม 2567, จาก <https://www.pdpc.or.th/wp-content/uploads/2024/03/-67-page-0001-scaled.jpg>.
- สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล. (2567). *สารานุกรมเกี่ยวกับ PDPA*. สืบค้นเมื่อ 25 มีนาคม 2567, จาก <https://www.pdpc.or.th/pdpc-book/pdpa-information/>.