มหาวิทยาลัยนอร์ทกรุงเทพ
NORTH BANGKOK UNIVERSITY

การประชุมวิชาการระดับชาติการวิจัยประยุกต์ ครั้งที่ 5 ประจำปี 2566

National Conference in Applied Research

NCAR NBU

มิติใหม่ของโลกภายหลังจากการแพร่ระบาด ของเชื้อไวรัสโคโรนา 2019 : ความท้าทายและโอกาส

New Global Perspectives in the post- pandemic: Challenges and Opportunities

วันศุกร์ที่ 24 มีนาคม 2566 ณ มหาวิทยาลัยนอร์ทกรุงเทพ

ด้านสังคมศึกษา ฉบับที่ 2/2

www.northbkk.ac.th

S0032L: มาตรการทางกฎหมายเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์: ศึกษาเปรียบเทียบกฎหมายไทยกับกฎหมายสหรัฐอเมริกา

LEGAL MEASURES RELATING TO ONLINE IDENTITY THEFT: A COMPARATIVE STUDY OF THAI AND THE U.S. LAWS

คณาธิป ทองรวีวงศ์ [1]

[1] รองศาสตราจารย์ คณะนิติศาสตร์ มหาวิทยาลัยเกษมบัณฑิต

บทคัดย่อ

การวิจัยมีวัตถุประสงค์ 1) ศึกษาการจำแนกรูปแบบพฤติกรรมของการกระทำของการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ 2) ศึกษามาตรการทางกฎหมายของไทยและสหรัฐอเมริกาเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคล ในกรอบกฎหมาย 3 กลุ่ม ตามขอบเขตการวิจัย และ 3) ศึกษาการตีความและปรับใช้กฎหมายไทยและสหรัฐอเมริกากับการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ โดยจำแนกวิเคราะห์ตามกรอบการจำแนกรูปแบบพฤติกรรม การวิจัยนี้ใช้วิธีวิจัยเชิงคุณภาพ โดยวิเคราะห์เอกสาร ตัวบทกฎหมาย วรรณกรรมทางกฎหมาย ของไทยเปรียบเทียบกับสหรัฐอเมริกา

ผลการวิจัย พบว่า 1) การโจรกรรมข้อมูลส่วนบุคคล มีขั้นตอนการกระทำที่สำคัญ 3 ขั้นตอน คือ การได้มาซึ่งข้อมูล การกระทำต่อข้อมูลก่อนนำไปใช้ และการนำข้อมูลส่วนบุคคลไปใช้ 2) ปัจจุบันไทยไม่มีกฎหมายโดยเฉพาะสำหรับการโจรกรรมข้อมูลส่วนบุคคล ซึ่งต่างจากสหรัฐอเมริกาที่กำหนดกฎหมายเฉพาะสำหรับการโจรกรรมข้อมูลส่วนบุคคล และ 3) พระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์สามารถนำมาปรับใช้กับขั้นตอนการได้มาซึ่งข้อมูล แต่มีข้อจำกัดในแง่องค์ประกอบการกระทำไม่ครอบคลุมการกระทำในขั้นตอนการกระทำต่อข้อมูลก่อนนำไปใช้ และขั้นตอนการนำข้อมูลไปใช้ แต่สหรัฐอเมริกากำหนดความผิดดังกล่าวโดยมีองค์ประกอบความผิดครอบคลุมการโจรกรรมข้อมูลส่วนบุคคลทั้ง 3 ขั้นตอน ผู้วิจัยจึงมีข้อเสนอแนะเชิงนโยบายในการปรับปรุงแก้ไขกฎหมายตามแนวทางตัวแบบกฎหมายสหรัฐอเมริกา

คำสำคัญ: ข้อมูลส่วนบุคคล, การโจรกรรมข้อมูลส่วนบุคคล, กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์, กฎหมายคุ้มครองข้อมูลส่วนบุคคล

Abstract

The aims of this study were 1) to study the classification of behavioral patterns of online identity theft of personal data. 2) study the legal measures of Thailand and the United States regarding online identity theft of personal data according to 3 groups of laws according to the scope of the research 3) study the interpretation and application of Thai and US laws on online identity theft of personal data by using frame work of behavioral pattern of this crime. This qualitative research used documentary analysis by comparing content of laws, articles and literatures of Thai and The U.S. laws.

The research finding.

The results indicated that 1) Online identity theft of personal data could be classified into 3 stages: acquisition of data, interference or manipulation of data and use of personal data 2) Thailand legal system currently does not have a specific law for online identity theft of personal data in contrast with the United States which enacted specific laws for this crime. 3) The Computer Crimes Act can be applied to certain stages especially data acquisition but the results is a limitation in terms of action elements, not covering actions in the action on the data before use and the use of the data. But the United States defines such offenses with an offense component covering all 3 steps of identity theft. Therefore, the researcher proposes policy suggestions for amending the law by using the United States law as a model in order to cover the 3 steps of online identity theft.

Keywords: Personal data, Online-identity theft, Computer Crime Law, Personal Data Protection Law

บทนำและความสำคัญของปัญหาการวิจัย

การโจรกรรมข้อมูลระบุตัวบุคคลหรือข้อมูลส่วนบุคคล (Identity theft) โดยทั่วไปหมายถึง การที่บุคคลหนึ่งนำข้อมูลส่วนบุคคลของเหยื่อ เช่น ชื่อ หมายเลขประจำตัวประชาชน ชื่อ ภาพ ฯลฯ ไปแสดงตัวตนว่าเป็นเหยื่อ (Mitchison; Wilikens; Breitenbach; Urry; & Portesi. 2004) โดยอาจนำไปสู่การกระทำความผิดอาญาอื่น ๆ เช่น การฉ้อโกงหลอกลวงทางคอมพิวเตอร์ (Yvonne. 2010) ในทางวิชาการและกรอบความร่วมมือระหว่างประเทศมีการให้ความหมายของอาชญากรรมประเภทนี้แตกต่างกันไป เช่น องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนานิยามไว้ว่าหมายถึง “กิจกรรมที่ฝ่าฝืนกฎหมายซึ่งรวมถึงการได้มา โอน ประมวลผล หรือการใช้ข้อมูลส่วนบุคคลของบุคคลธรรมดาโดยปราศจากอำนาจ ด้วยเจตนาที่จะประกอบอาชญากรรมอื่น (Organization for Economic Cooperation and Development. 2008) ในสหรัฐอเมริกา คณะกรรมาธิการการค้า (Federal Trade Commission) ให้ความหมายว่า หมายถึง การที่บุคคลหนึ่งนำข้อมูลส่วนบุคคลของบุคคลอื่น เช่น ชื่อ หมายเลขที่บ่งระบุตัวบุคคล เช่น บัตรประชาชน ไปใช้โดยมิได้รับความยินยอม เพื่อการแสวงหาประโยชน์โดยมิชอบหรือใช้ในการประกอบอาชญากรรมอื่น (Chawki; & Abdel. 2006) เช่น ฉ้อโกง ปล้นทรัพย์ ก่อการร้าย ผู้กระทำการโจรกรรมข้อมูลเชิงเอกลักษณ์ อาจนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้ในการประกอบอาชญากรรมอื่นได้หลายรูปแบบ และส่งผลกระทบต่อเจ้าของข้อมูลในหลายมิติ เช่น ผลกระทบในด้านการเงิน โดยเฉพาะการนำไปใช้เกี่ยวกับบัญชีธนาคาร เช่น ใช้ข้อมูลของผู้อื่นเพื่อเปิดบัญชีใหม่ หรือ การเข้าไปสวมรอยในบัญชีการเงินของผู้อื่น เช่น การเจาะเข้าระบบบัญชีธนาคารออนไลน์ของผู้อื่นและใช้บัญชีของบุคคลนั้นทำธุรกรรม (Hoofnagle. 2007) การกระทำทั้งสองกรณีอาจทำขึ้นโดยที่ผู้เป็นเจ้าของข้อมูลอาจไม่รับรู้หรือรับทราบการกระทำดังกล่าวเลย นอกจากผลโดยตรงด้านการเงินที่เสียไปจากการโจรกรรมแล้ว ยังมีผลกระทบด้านอื่นเช่น เวลาที่เสียไปในการจัดการกับปัญหาที่เกิดขึ้น เวลาและค่าใช้จ่ายเกี่ยวกับการดำเนินคดีอันเป็นผลจากการถูกโจรกรรมข้อมูล (Listerman; & Romesberg. 2009) ผลกระทบที่ไม่เกี่ยวกับการเงินโดยตรง เช่น นำไปใช้สวมรอยประกอบอาชญากรรมภายใต้เอกลักษณ์ของผู้ที่ถูกโจรกรรม รวมทั้งอาจนำไปใช้ในการก่อการร้าย เช่น ในการ

วางแผนก่อการร้ายมีการใช้ข้อมูลของบุคคลอื่นเช่าห้องพัก เช่าสำนักงาน เช่ายานพาหนะ เปิดใช้โทรศัพท์ ใช้หนังสือเดินทางปลอม เปิดบัญชีทางการเงินโดยใช้ชื่อบุคคลอื่น (Biegelman. 2009)

จึงกล่าวได้ว่า การโจรกรรมข้อมูลส่วนบุคคล ส่งผลกระทบต่อเจ้าของข้อมูลหลายด้าน นอกจากผลกระทบทางการเงิน ยังรวมถึงผลกระทบต่อสิทธิเสรีภาพ เช่น ต้องตกเป็นผู้ต้องหาในคดีอาญาจากความผิดที่ตนไม่ได้ก่อขึ้น เพราะอาชญากรรมใช้ข้อมูลส่วนบุคคลของเหยื่อในการปกปิดการระบุตัวตนของผู้กระทำ เสียโอกาสในการประกอบอาชีพหรือการจ้างงานจากประวัติข้อมูลดังกล่าว รวมทั้งผลกระทบในมิติความรู้สึก สภาพอารมณ์และจิตใจ ซึ่งไม่อาจคำนวณเป็นเงินได้ นอกจากในระดับของบุคคลผู้ได้รับผลกระทบโดยตรงจากการโจรกรรมข้อมูลแล้ว การโจรกรรมข้อมูลส่วนบุคคล ส่งผลกระทบต่อสถาบันการเงิน ภาคธุรกิจอื่นในสหรัฐอเมริกา (Conkey. 2007) ส่งผลกระทบต่อทัศนคติ และความเชื่อมั่นของผู้บริโภคต่อระบบการดำเนินธุรกรรมและการพาณิชย์ โดยเฉพาะอย่างยิ่งการพาณิชย์อิเล็กทรอนิกส์ (e-commerce) ลูกค้าจำนวนหนึ่งเปลี่ยนแปลงพฤติกรรมจากที่เคยใช้จ่ายและชำระเงินออนไลน์ (Jonker. 2007) นักวิชาการบางท่านยังได้ชี้ให้เห็นว่า การรับรู้ถึงความเสี่ยง (Perceived risk) จากการโจรกรรมข้อมูลเป็นปัจจัยสำคัญในการตัดสินใจเลือกช่องทางการชำระเงินของผู้บริโภค (Arango; & Taylor. 2009) ผู้บริโภคจำนวนหนึ่งได้เปลี่ยนแปลงวิธีการไปใช้เงินสดในการชำระเงินแทนการใช้วิธีทางอิเล็กทรอนิกส์ (Arango; Hogg; & Lee. 2011) นอกจากการเปลี่ยนแปลงวิธีการชำระเงินแล้ว ผู้บริโภคส่วนหนึ่งอาจลดการใช้จ่ายซื้อสินค้าหรือบริการออนไลน์ รวมทั้งการใช้บริการธนาคารทางอินเทอร์เน็ตเนื่องจากความกังวลดังกล่าว (Sproule; & Archer. 2010) ความกังวลต่อการถูกโจรกรรมข้อมูลเชิงเอกลักษณ์ส่งผลกระทบต่อการขยายตัวของการบริโภคและเป็นผลลบต่อการเจริญเติบโตทางเศรษฐกิจโดยรวมของประเทศด้วย ด้วยเหตุนี้ ผู้วิจัยจึงได้ทำการศึกษามาตรการทางกฎหมายสำหรับการกระทำดังกล่าว โดยศึกษากฎหมายต่างประเทศที่มีการบัญญัติให้การโจรกรรมข้อมูลส่วนบุคคลเป็นความผิดเฉพาะ เพื่อที่จะนำมาวิเคราะห์เปรียบเทียบกับกฎหมายไทยที่มีผลบังคับอยู่ในปัจจุบัน อันจะนำไปสู่ข้อเสนอแนะในการปรับปรุงแก้ไขกฎหมายไทยต่อไป

วัตถุประสงค์

1. ศึกษาการจำแนกรูปแบบพฤติกรรมของการกระทำของการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์
2. ศึกษามาตรการทางกฎหมายของไทยและสหรัฐอเมริกาเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคล ในกรอบกฎหมาย 3 กลุ่ม ตามขอบเขตการวิจัย
3. ศึกษาการตีความและปรับใช้กฎหมายไทยและสหรัฐอเมริกากับการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ โดยจำแนกวิเคราะห์เปรียบเทียบตามกรอบการจำแนกรูปแบบพฤติกรรม

ประโยชน์ที่ได้คาดว่าจะได้รับ

1. ทราบหลักการจำแนกรูปแบบพฤติกรรมของการกระทำของการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์เพื่อนำไปใช้เป็นกรอบการวิเคราะห์และปรับใช้กฎหมาย
2. ทราบหลักการทางกฎหมายของไทยและสหรัฐอเมริกาที่มีผลใช้บังคับเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคล

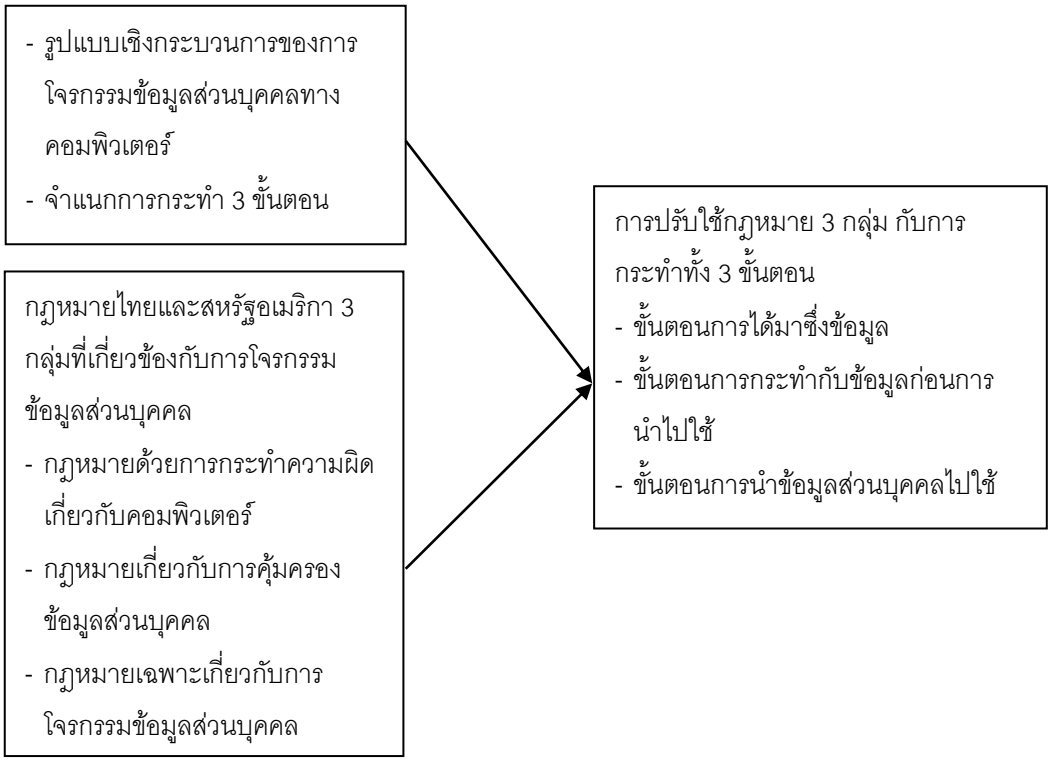
3. ทราบปัญหาการตีความและปรับใช้กฎหมายไทยกับการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์นำไปสู่การจัดทำข้อเสนอแนะปรับปรุงพัฒนากฎหมายไทยโดยอาศัยตัวแบบของกฎหมายสหรัฐอเมริกา

สมมติฐานในการวิจัย

ในระบบกฎหมายไทยปัจจุบัน ไม่มีกฎหมายเฉพาะกำหนดความผิดสำหรับการโจรกรรมข้อมูลส่วนบุคคล สำหรับกฎหมายที่เกี่ยวข้องที่อยู่ในขอบเขตการศึกษานี้ คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มีข้อจำกัดไม่สามารถปรับใช้กับการโจรกรรมข้อมูลส่วนบุคคลอย่างเป็นกระบวนการที่ครอบคลุมการกระทำ 3 ขั้นตอน คือ การได้มาซึ่งข้อมูล การกระทำต่อข้อมูลก่อนการใช้และการใช้ข้อมูล ซึ่งต่างจากกฎหมายสหรัฐอเมริกาที่มีการกำหนดความผิดเฉพาะครอบคลุมการกระทำทั้ง 3 ขั้นตอน การศึกษานี้จึงวิเคราะห์เปรียบเทียบกฎหมายเพื่อเสนอแนะแนวทางแก้ไขพัฒนากฎหมายไทยต่อไปสถานะการบริหารสถานศึกษามีอิทธิพลต่อการจัดการความรู้ของสถานศึกษาด้านอาชีวศึกษาในเขตกรุงเทพมหานคร

กรอบแนวคิดในการวิจัย

การศึกษา เรื่อง “มาตรการทางกฎหมายเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์: ศึกษาเปรียบเทียบกฎหมายไทยกับกฎหมายสหรัฐอเมริกา” ผู้วิจัย กำหนดกรอบแนวคิดในการศึกษาไว้ ดังนี้



ภาพประกอบ 1 กรอบแนวคิดในการวิจัย

วิธีดำเนินการวิจัย

ขอบเขตการศึกษา

1. ขอบเขตด้านตัวบทกฎหมาย ประกอบด้วยกฎหมาย 3 กลุ่ม คือ กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎหมายเฉพาะเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคล โดยขอบเขตกฎหมายต่างประเทศที่เลือกศึกษาคือระดับรัฐบาลกลางของสหรัฐอเมริกา

2. ขอบเขตระยะเวลาที่ใช้ในการเก็บรวบรวมข้อมูลและวิเคราะห์ข้อมูล ระหว่างเดือนสิงหาคม-ธันวาคม 2565

3. ขอบเขตด้านเนื้อหาเชิงพฤติกรรมที่จะนำมาวิเคราะห์การปรับใช้กฎหมาย ประกอบด้วย การกระทำโจรกรรมข้อมูลส่วนบุคคล 3 ขั้นตอน คือ การได้มาซึ่งข้อมูล การกระทำต่อข้อมูลก่อนนำไปใช้ และการนำข้อมูลส่วนบุคคลไปใช้

วิธีการและขั้นตอนการวิจัย

งานวิจัยนี้เป็นการวิจัยเอกสาร (Documentary Research) ตามกระบวนการดังนี้

1. ข้อมูลที่นำมาวิเคราะห์ ประกอบด้วย ตัวบทกฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายสหรัฐอเมริการเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคล แนวปฏิบัติของหน่วยงานกำกับหรือบังคับใช้กฎหมาย วรรณกรรมเกี่ยวกับแนวคิดทฤษฎีทางกฎหมายที่เกี่ยวข้อง กรอบแนวคิดทฤษฎีการจำแนกพฤติกรรมการโจรกรรมข้อมูลส่วนบุคคล รวมทั้งการตีความฐานทางกฎหมาย จากงานวิชาการ งานวิจัย บทความวิชาการ

2. การวิเคราะห์ข้อมูล ใช้วิธีการวิเคราะห์เชิงเนื้อหา (Content Analysis) โดยนำรูปแบบพฤติกรรมตามขั้นตอนการโจรกรรมข้อมูลส่วนบุคคลตามกรอบแนวคิด มาวิเคราะห์การตีความปรับใช้กฎหมาย โดยวิเคราะห์เนื้อหากฎหมายทั้งสองประเทศในเชิงเปรียบเทียบ (Comparative Analysis) เพื่อการตีความและการปรับใช้กฎหมาย

ผลการศึกษา

1. การโจรกรรมข้อมูลส่วนบุคคล (Identity theft) มีลักษณะเชิงพฤติกรรมที่หลากหลาย โดยในทางวิชาการไม่ปรากฏว่ามีการกำหนดนิยามที่ครอบคลุมอันยอมรับกันทั่วไป แต่พบว่าแนวทางศึกษาและปรับใช้กฎหมายกับอาชญากรรมประเภทนี้พิจารณาจากรูปแบบพฤติกรรม ซึ่งมีการนำเสนอกรอบแนวคิดจำแนกรูปแบบหลายแนวทางแตกต่างกัน แต่การจำแนกรูปแบบมีขั้นตอนการกระทำสำคัญคล้ายคลึงกัน 3 ขั้นตอน คือ 1) การได้มาซึ่งข้อมูล 2) การกระทำกับข้อมูลก่อนการนำไปใช้ และ 3) การนำข้อมูลไปใช้

2. ในระบบกฎหมายไทยปัจจุบันไม่มีความผิดฐานโจรกรรมข้อมูลส่วนบุคคลเป็นการเฉพาะ แต่มีกฎหมายที่เกี่ยวข้องสองฉบับที่มีข้อจำกัดแตกต่างกัน กล่าวคือ 1) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อันเป็นกฎหมายเฉพาะเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ แต่ไม่ได้กำหนดฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์ การปรับใช้กฎหมายจึงขึ้นอยู่กับสภาพข้อเท็จจริงเป็นกรณีไป และ 2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดนิยามข้อมูลส่วนบุคคลโดยเฉพาะ แต่เป็นกฎหมายที่กำหนดหน้าที่แก่ผู้ควบคุมข้อมูลในการจัดมาตรการรักษาความปลอดภัยข้อมูล ไม่ใช่กฎหมายอาญาที่กำหนดฐานความผิดสำหรับผู้ประกอบอาชญากรรมเกี่ยวกับการโจรกรรมข้อมูล ผลการวิเคราะห์เปรียบเทียบกับสหรัฐอเมริกา

พบว่า กฎหมายมีกฎหมายเฉพาะที่กำหนดฐานความผิดสำหรับการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ แยกออกมาจากกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ (CFAA) โดยเฉพาะ

3. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ นำมาปรับใช้กับขั้นตอนการได้มาซึ่งข้อมูล แต่มีข้อจำกัดในแง่องค์ประกอบการกระทำไม่ครอบคลุมการกระทำต่าง ๆ ในขั้นตอนการกระทำต่อข้อมูลก่อนนำไปใช้ และขั้นตอนการนำข้อมูลไปใช้ ในขณะที่ผลการเปรียบเทียบกับสหรัฐอเมริกาพบว่ากฎหมายโจรกรรมข้อมูลส่วนบุคคลกำหนดความผิดดังกล่าวเป็นการเฉพาะครอบคลุมการโจรกรรมข้อมูลส่วนบุคคลทั้ง 3 ขั้นตอน โดยเฉพาะองค์ประกอบความผิดฐานโอนข้อมูลที่ครอบคลุมการนำข้อมูลส่วนบุคคลผู้อื่นไปแสดงหรือสร้างร่องรอยการกระทำผิดทางออนไลน์

การอภิปรายผล

1. จากวัตถุประสงค์ของการวิจัยข้อ 1 ผลศึกษาการจำแนกรูปแบบพฤติกรรมของการกระทำของการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ พบว่า การโจรกรรมข้อมูลส่วนบุคคล (Identity theft) อาจเกิดขึ้นได้โดยไม่จำกัดสภาพแวดล้อมและเทคโนโลยี ในบางกรณีอาจไม่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ เช่น การโจรกรรมข้อมูลสำเนาบัตรประชาชนไปใช้ทำธุรกรรมทางเอกสาร แต่ในบทความนี้จะศึกษาเฉพาะการโจรกรรมข้อมูลส่วนบุคคลในฐานะที่เป็นวิธีการหนึ่งของอาชญากรรมคอมพิวเตอร์ อย่างไรก็ตามอาชญากรรมนี้มีลักษณะ และวิธีการที่หลากหลาย อีกทั้งไม่มีคำนิยามในลักษณะครอบคลุมทั่วไป ในการพิจารณากฎหมายที่เกี่ยวข้องจึงขึ้นอยู่กับพฤติกรรมในแต่ละกรณีที่มีรายละเอียดแตกต่างกันจากการศึกษา พบว่า ในทางวิชาการได้มีการศึกษาวิเคราะห์พฤติกรรมเชิงกระบวนการของอาชญากรรมประเภทนี้ ซึ่งแบ่งการกระทำเป็นขั้นตอนย่อย แต่นักวิชาการจำแนกขั้นตอนการกระทำไว้แตกต่างกัน เช่น

การจำแนกรูปแบบพฤติกรรมการโจรกรรมข้อมูลส่วนบุคคลในรูปแบบวงจร (Identity theft Cycle) (Steve; Chad; Conan; & Mark. 2011) ซึ่งจำแนกเป็นขั้นตอนย่อย คือ 1) ขั้นตอนการค้นหา (Discovery stage) กล่าวคือ อาชญากรได้มาซึ่งข้อมูลส่วนบุคคล โดยใช้วิธีการต่าง ๆ เช่น การเข้าถึงคอมพิวเตอร์เพื่อไปบันทึกข้อมูล 2) ขั้นตอนการดำเนินการ หมายถึง การนำข้อมูลระบุตัวของเหยื่อที่ได้มา ไปเตรียมสำหรับการลงมือกระทำเพื่อแสวงประโยชน์ในขั้นต่อไป เช่น เปิดบัญชี สมัครบัตรเครดิต สมัครใช้งานการซื้อขายออนไลน์ และ 3) ขั้นตอนการลงมือ กระทำการเพื่อให้ได้มาซึ่งทรัพย์สินหรือประโยชน์ เช่น การใช้บัตรเครดิตที่เปิดขึ้นในนามของเหยื่อไปซื้อสินค้าหรือบริการ

การจำแนกรูปแบบการโจรกรรมข้อมูลส่วนบุคคลแบบ 2 ขั้นตอน (Nazura; Anita; & Hossein. 2015) คือ ขั้นตอนการได้มาซึ่งข้อมูลส่วนบุคคลโดยมิชอบ และ ขั้นตอนการนำข้อมูลระบุตัวผู้อื่นไปใช้ในทางมิชอบ (Fraudulent use) เช่นนำไปใช้ทำธุรกรรมต่าง ๆ หรือหลอกลวงผู้อื่นอีกทอดหนึ่ง

การจำแนกรูปแบบการโจรกรรมข้อมูลส่วนบุคคลแบบ 3 ระยะ (Marco. 2007) ได้แก่ ระยะที่หนึ่ง การได้มาซึ่งข้อมูลส่วนบุคคล (Obtaining information) ระยะที่สอง การกระทำเกี่ยวข้องกับข้อมูล ก่อนที่จะนำไปใช้กระทำผิด (Interaction with information prior to the use) เช่น การขายข้อมูล ระยะที่สาม การใช้ข้อมูลส่วนบุคคลในการกระทำผิดต่าง ๆ เช่น การนำไปหลอกลวงฉ้อโกงบุคคลอื่น

นอกจากนี้ ยังมีขั้นตอนที่สำคัญอีกประการคือ การค้นพบอาชญากรรม (Discovery of the theft) กล่าวคือ การตรวจสอบพบข้อเท็จจริงว่าเจ้าของข้อมูลที่อ้างอิงหรือถูกนำข้อมูลไปใช้นั้นไม่เกี่ยวข้องกับการกระทำผิด

แต่ขั้นตอนนี้อาจใช้เวลานานหรืออาจไม่ปรากฏหรือตรวจสอบพบเลยก็ได้ (Graeme; & Megan. 2005) อย่างไรก็ตาม ขั้นตอนนี้เป็นการดำเนินการของเจ้าหน้าที่บังคับใช้กฎหมาย มิใช่การดำเนินการประกอบอาชญากรรมของผู้โจรกรรมข้อมูล งานวิจัยนี้จึงไม่ได้นำขั้นตอนการค้นพบอาชญากรรมมาใช้วิเคราะห์ความผิดของการประกอบอาชญากรรมนี้ อย่างไรก็ตาม ขั้นตอนนี้แสดงให้เห็นความสำคัญและผลกระทบต่อเหยื่อผู้ถูกโจรกรรมข้อมูลส่วนบุคคลเพราะอาจตกเป็นจำเลยและต้องรับโทษหากไม่มีการตรวจสอบพบว่าความผิดนั้นเกิดจากการโจรกรรมข้อมูลส่วนบุคคล

จะเห็นได้ว่า ในทางวิชาการมีการนำเสนอรูปแบบการโจรกรรมข้อมูลส่วนบุคคลไว้หลายแนวทาง แต่พบว่าแนวทางต่าง ๆ มีขั้นตอนการกระทำสำคัญคล้ายคลึงกันโดยแบ่งได้ 3 ขั้นตอน คือ 1) การได้มาซึ่งข้อมูล 2) การกระทำกับข้อมูลก่อนการนำไปใช้ และ 3) การนำข้อมูลไปใช้ ซึ่งงานวิจัยนี้จะนำแต่ละขั้นตอนมาวิเคราะห์การปรับใช้กฎหมายต่อไป

2. จากวัตถุประสงค์ของการวิจัยข้อ 2 ผลการศึกษามาตรการทางกฎหมายของไทยและสหรัฐอเมริกาเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคล พบว่า

2.1 กฎหมายไทย จำแนกกฎหมายที่เกี่ยวข้องกับพฤติกรรมการโจรกรรมข้อมูลส่วนบุคคล ดังนี้

2.1.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม พ.ศ. 2560 เป็นกฎหมายเฉพาะเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ แต่ไม่ได้กำหนดฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์หรือออนไลน์ (Online Identity theft) การปรับใช้กฎหมายจึงขึ้นอยู่กับสภาพข้อเท็จจริงของพฤติกรรม และพิจารณาฐานความผิดที่มีอยู่ เช่น ฐานความผิดที่อาจเกี่ยวข้องกับการโจรกรรมข้อมูลส่วนบุคคล เช่น การเข้าถึงระบบโดยมิชอบ (มาตรา 5) การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7)

2.1.2 กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลบังคับในเดือนมิถุนายน พ.ศ. 2565 แม้ว่าพระราชบัญญัตินี้มีความเกี่ยวข้องโดยตรงกับข้อมูลส่วนบุคคลและมีการกำหนดนิยามของข้อมูลส่วนบุคคลในมาตรา 6 ว่า ข้อมูลระบุตัวบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่ใช่เป็นกฎหมายที่กำหนดฐานความผิดทางอาญาสำหรับการโจรกรรมข้อมูลส่วนบุคคล ทั้งนี้เมื่อพิจารณาตัวบทมาตราของพระราชบัญญัตินี้จะสามารถจำแนกเป็นหลักการสำคัญสองส่วนที่อยู่บนแนวคิดแตกต่างกัน (คณาธิป ทองรวีวงศ์. 2564) คือ 1) กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความปลอดภัย ซึ่งอยู่บนแนวคิดความมั่นคงปลอดภัยของข้อมูลหรือความมั่นคงปลอดภัยสารสนเทศ (Information security) ซึ่งไม่เกี่ยวข้องกับประเด็นการศึกษาในที่นี้ และ 2) กำหนดให้ผู้ควบคุมข้อมูลต้องอ้างอิง “ฐานทางกฎหมาย” (Legal or lawful basis of processing personal data) เช่น การขอความยินยอมจากเจ้าของข้อมูล จะเห็นได้ว่ากฎหมายนี้มีหลักการกำหนดหน้าที่แก่ผู้ควบคุมข้อมูล (Data controller) เช่น ผู้ประกอบการต่าง ๆ ที่เก็บรวบรวมใช้เปิดเผยข้อมูลส่วนบุคคลของผู้ใช้บริการ ต้องมีหน้าที่ต่าง ๆ เช่น การขอความยินยอมก่อนการเก็บรวบรวม (มาตรา 24 มาตรา 26) การรักษาความปลอดภัยข้อมูล (มาตรา 37) ในกรณีที่มีการการโจรกรรมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลอาจต้องเป็นผู้รับผิดหากปรากฏว่าไม่จัดให้มีมาตรการป้องกันรักษาความปลอดภัยที่เหมาะสม (มาตรา 37) ซึ่งอาจนำไปสู่โทษปรับทางปกครอง อย่างไรก็ตาม พระราชบัญญัตินี้ไม่ได้กำหนดฐานความผิดอาญาสำหรับอาชญากรที่เป็นผู้ก่อให้เกิดภัยคุกคามหรือกระทำการโจรกรรมข้อมูลส่วนบุคคล หลักการนี้เป็นไปในแนวทางเดียวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป (GDPR) ซึ่งไม่ใช่กฎหมายที่กำหนดความผิดอาญาสำหรับอาชญากรที่ใช้วิธีการต่าง ๆ ในการโจรกรรมข้อมูลส่วนบุคคล แต่การควบคุมอาชญากรรมประเภทนี้จะต้องพิจารณากฎหมายอื่น

2.1.3 ในระบบกฎหมายไทยไม่มีกฎหมายเฉพาะสำหรับอาชญากรรมประเภทโจรกรรมข้อมูลส่วนบุคคล

2.2 กฎหมายสหรัฐอเมริกา ผลการศึกษากฎหมายสหรัฐอเมริกา ที่เกี่ยวข้องกับการโจรกรรมข้อมูลส่วนบุคคล ตามขอบเขตการศึกษากฎหมาย 3 กลุ่มดังนี้

2.2.1 กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์สหรัฐอเมริกา (The Computer Fraud and Abuse Act ,18 U.S.C., Section 1030 ซึ่งต่อไปจะใช้คำย่อว่า “CFAA”) ไม่ได้กำหนดความผิดฐานโจรกรรมข้อมูลส่วนบุคคลไว้เป็นการเฉพาะ แต่มีฐานความผิดที่สามารถนำมาปรับใช้ได้กับการโจรกรรมข้อมูลส่วนบุคคลขึ้นอยู่กับรายละเอียดข้อเท็จจริง พฤติกรรม และ องค์ประกอบของตัวบทฐานความผิดที่เกี่ยวข้อง เช่น (คณาธิป ทองรวีวงศ์. 2560) เข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบอำนาจ และได้มาซึ่งข้อมูลที่อาจถูกนำไปใช้ในทางเสียหายต่อรัฐ หรืออาจถูกนำไปใช้ประโยชน์โดยรัฐบาลต่างชาติ เข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบอำนาจ และได้มาซึ่งข้อมูลเกี่ยวกับสถาบันการเงิน หรือข้อมูลสถานะการเงินของผู้บริโภค หรือข้อมูลจากหน่วยงานของรัฐตามที่กฎหมายกำหนด หลอกลวงเพื่อให้ได้มาซึ่งรหัสผ่านหรือข้อมูลอื่นที่คล้ายคลึงกันซึ่งอาจนำไปสู่การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ

จะเห็นได้ว่ากฎหมาย CFAA ไม่ได้กำหนดความผิดฐานโจรกรรมข้อมูลคอมพิวเตอร์ (Identity theft) เป็นการเฉพาะ คล้ายคลึงกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของไทย แต่มีความผิดฐานโจรกรรมข้อมูลทั่วไปที่ไม่ระบุเจาะจงถึงข้อมูลส่วนบุคคล ซึ่งอาจนำมาปรับใช้กับการโจรกรรมข้อมูลส่วนบุคคลได้ตามสภาพข้อเท็จจริงแต่ละกรณี

2.2.2 สหรัฐไม่มีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะที่ใช้บังคับทั่วไป (General law) ในระดับรัฐบาลกลาง ซึ่งต่างจากสหภาพยุโรปและกฎหมายไทย

2.2.3 กฎหมายเฉพาะสำหรับการโจรกรรมข้อมูล ในช่วงระยะก่อนที่ประเทศสหรัฐอเมริกาจะมีกฎหมายเฉพาะความผิดฐานโจรกรรมข้อมูลส่วนบุคคล มีการเรียกชื่อความผิดดังกล่าวหลากหลาย เช่น การฉ้อโกงบัตรเครดิต (Credit card fraud) การฉ้อโกงชื่อ (True name fraud) การฉ้อโกงเอกลักษณ์ (Identity fraud) (Biegelman. 2009) ต่อมา ค.ศ. 1998 มีการตรากฎหมายเฉพาะสำหรับการโจรกรรมข้อมูลส่วนบุคคลในระดับรัฐบาลกลาง (Federal law) คือ “The Identity Theft and Assumption Deterrence Act” (ต่อไปจะเรียกกว่า รัฐบัญญัติ ITADA) ซึ่งแก้ไขประมวลกฎหมายสหรัฐโดยเพิ่มเติมฐานความผิดการโจรกรรมข้อมูลส่วนบุคคล (Title 18 United States Code-Section. 1028) ใน ค.ศ. 2004 ฐานความผิดดังกล่าวมีการแก้ไขโดย รัฐบัญญัติ “The Identity Theft Penalty Enhancement Act” ซึ่งเพิ่มเติมมาตรา 1028 A เกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลชนิดร้ายแรง (Aggregated identity theft)สำหรับการโจรกรรมข้อมูลส่วนบุคคลเกี่ยวข้องกับฐานความผิดบางประการ เช่น ความผิดเกี่ยวกับกฎหมายคนเข้าเมือง ความผิดเกี่ยวกับการรับเงินสวัสดิการสังคมของรัฐบาลกลาง เป็นต้น ความผิดฐานโจรกรรมข้อมูลส่วนบุคคล (Identity theft) ตามมาตรา 1028 ครอบคลุมการกระทำต่อ “เอกสารข้อมูลส่วนบุคคล” (Identification document) ซึ่งหมายถึง“เอกสารซึ่งทำขึ้นหรือออกโดยอำนาจของรัฐบาลกลาง มลรัฐ หน่วยการปกครองของรัฐ รัฐบาลต่างประเทศ หรือองค์กรระหว่างประเทศ ซึ่งเมื่อประกอบกับข้อมูลที่เกี่ยวกับบุคคลนั้นแล้วจะเป็นเอกสารที่มีวัตถุประสงค์อันเป็นการยอมรับกันทั่วไปสำหรับการระบุตัวบุคคล” โดยการกระทำที่เข้าข่ายความผิด เช่น ผลิต หรือ โอน (Transfer) เอกสารแสดงข้อมูลส่วนบุคคลปลอมโดยรู้ว่าเอกสารนั้นถูกขโมยหรือถูกทำ

ขึ้นโดยปราศจากอำนาจตามกฎหมาย ครอบครองเอกสารแสดงข้อมูลส่วนบุคคลปลอมด้วยเจตนาจะใช้หรือโอนเอกสารดังกล่าวโดยมิชอบด้วยกฎหมาย โอนหรือใช้เอกสารแสดงข้อมูลส่วนบุคคลของบุคคลอื่นโดยมีเจตนากระทำความผิดหรือสนับสนุนการกระทำความผิดตามกฎหมายรัฐบาลกลางหรือกฎหมายมลรัฐหรือกฎหมายท้องถิ่น จากการเปรียบเทียบกับกฎหมายไทย พบว่า ไม่มีกฎหมายเฉพาะที่กำหนดความผิดฐานโจรกรรมข้อมูลส่วนบุคคลดังเช่นกฎหมาย ITADA

จากการศึกษาหลักการในภาพรวมของกฎหมายทั้ง 3 กลุ่ม พบว่า กฎหมายที่เกี่ยวข้องและสามารถนำมาปรับใช้กับการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ ได้แก่ กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายเฉพาะ ซึ่งจะนำไปวิเคราะห์การปรับใช้แยกตามขั้นตอนการโจรกรรมข้อมูลส่วนบุคคลต่อไป สำหรับกฎหมายคุ้มครองข้อมูลส่วนบุคคลไม่ใช่กฎหมายที่กำหนดความผิดสำหรับอาชญากรผู้โจรกรรมข้อมูล จึงไม่นำไปวิเคราะห์ในลำดับต่อไป

3. จากวัตถุประสงค์ของการวิจัยข้อ 3 ผลการศึกษาการปรับใช้กฎหมายไทยและสหรัฐอเมริกากับการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ จำแนกอภิปรายตามรูปแบบพฤติกรรมจำแนกได้ดังนี้

3.1 ขั้นตอนการได้มาซึ่งข้อมูลส่วนบุคคล

กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์สหรัฐอเมริกา (CFAA) ไม่ได้กำหนดความผิดเฉพาะสำหรับการโจรกรรมข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์ แต่มีความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจ (มาตรา 1030 (1)) และเข้าถึงระบบคอมพิวเตอร์และได้มาซึ่งข้อมูลการเงิน ข้อมูลบัตรเครดิต (มาตรา 1030 (2)) จึงสามารถนำมาปรับใช้กับการโจรกรรมข้อมูลส่วนบุคคลในขั้นตอนการได้มาซึ่งข้อมูล เปรียบเทียบกับ พรบ. คอมพิวเตอร์ ไม่ได้กำหนดความผิดเฉพาะสำหรับการโจรกรรมข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์ แต่มีความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5) ฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7) จึงสามารถนำมาปรับใช้กับการโจรกรรมข้อมูลส่วนบุคคลในขั้นตอนการได้มาซึ่งข้อมูลได้ในลักษณะคล้ายคลึงกับกฎหมายสหรัฐอเมริกา อย่างไรก็ตาม ฐานความผิดเกี่ยวกับการเข้าถึงโดยมิชอบของไทยตามมาตรา 5 และ มาตรา 7 ต่างจากกฎหมายสหรัฐอเมริกาเนื่องจากมีการกำหนดองค์ประกอบว่าระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์อันเป็นเป้าหมายของการกระทำต้องมี “มาตรการป้องกันการเข้าถึง” ทำให้ไม่สามารถปรับใช้กับการได้มาซึ่งข้อมูลโดยไม่มีการเข้าถึงระบบที่มีมาตรการป้องกัน เช่น การสืบค้นข้อมูลที่ปรากฏทั่วไปจากแหล่งออนไลน์ (คณาธิป ทองรวีวงศ์. 2563) นอกจากนั้น ความผิดฐานเข้าถึงโดยมิชอบตามกฎหมายไทยและสหรัฐอเมริกามีข้อจำกัดในแง่องค์ประกอบการเข้าถึง (Access) ทำให้ไม่สามารถปรับใช้กับกรณีที่อาชญากรใช้วิธีการได้มาซึ่งข้อมูลส่วนบุคคลเหยื่อโดยไม่มีลักษณะการเข้าถึง เช่น การโอนข้อมูลหรือแลกเปลี่ยนข้อมูลส่วนบุคคลของเหยื่อจากแหล่งต่าง ๆ อย่างไรก็ตาม ในประเด็นนี้สหรัฐอเมริกามีกฎหมายโจรกรรมข้อมูลส่วนบุคคลเป็นการเฉพาะที่กำหนดองค์ประกอบความผิดสำหรับการโอนหรือแลกเปลี่ยนข้อมูลส่วนบุคคล

3.2 ขั้นตอนการกระทำต่อข้อมูลก่อนการนำไปใช้

กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์สหรัฐอเมริกา (CFAA) ไม่ได้กำหนดความผิดเฉพาะสำหรับการโจรกรรมข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์ แม้ว่ามีความผิดฐานเข้าถึงโดยมิชอบที่อาจนำมาปรับใช้กับการโจรกรรมข้อมูลส่วนบุคคลในขั้นตอนการได้มา แต่ไม่ได้กำหนดความผิดสำหรับการกระทำต่อข้อมูลที่ได้มาดังกล่าวก่อนนำไปใช้

สำหรับกฎหมายเฉพาะ (ITADA) มีการกำหนดความผิดสำหรับการกระทำต่อข้อมูล เช่น การโอน (Transfer) การแลกเปลี่ยน การนำข้อมูลที่ได้มาประกอบการ “ผลิต” เอกสารข้อมูลส่วนบุคคล รวมทั้งกำหนดความผิดสำหรับการครอบครอง (Possession) ซึ่งจัดเป็นการกำหนดความผิดสำหรับพฤติกรรมในขั้นตอนก่อนการนำข้อมูลไปใช้กระทำความผิดอื่น การกระทำดังกล่าวจะเป็นความผิดเมื่อผู้กระทำมีเจตนาเพื่อกระทำความผิดอื่นด้วยซึ่งจัดเป็นข้อจำกัดประการหนึ่งของกฎหมายนี้ แต่การกระทำนั้นอาจเป็นความผิดสำเร็จในขั้นตอนนี้แม้ว่ายังไม่ได้นำข้อมูลไปใช้กระทำความผิดอื่นก็ตาม ดังนั้น การกำหนดความผิดตามกฎหมายนี้ครอบคลุมพฤติกรรมที่เกี่ยวข้องในขั้นตอนการกระทำต่อข้อมูลในช่วงก่อนที่จะนำไปใช้หลอกลวงฉ้อโกงหรือใช้ในการกระทำผิดอื่น เช่น การครอบครองข้อมูลส่วนบุคคลของผู้อื่นไว้ด้วยเจตนาจะนำไปใช้กระทำผิด สำหรับการขายข้อมูลนั้นอยู่ในความหมายของการ “โอน” ข้อมูล เปรียบเทียบกับกฎหมายไทย พ.ร.บ. คอมพิวเตอร์ กำหนดความผิดในขั้นตอนการได้มาซึ่งข้อมูล อันเกิดจากการเข้าถึงโดยมิชอบ หากมีการกระทำกับข้อมูลที่ได้มาในลักษณะของการ แก้ไข เปลี่ยนแปลง จะเป็นความผิดมาตรา 9 ซึ่งไม่ได้จำกัดว่าการกระทำดังกล่าวต้องมีเจตนาเพื่อกระทำความผิดอื่นด้วย แต่มีข้อจำกัดด้านองค์ประกอบการกระทำไม่รวมถึงการ ครอบครอง โอน ซื้อขายแลกเปลี่ยนข้อมูล ดังเช่นกฎหมายสหรัฐอเมริกา แม้ว่าในการแก้ไขกฎหมายในปี พ.ศ. 2560 มีการเพิ่มเติมความผิดฐาน “ครอบครอง” ตามมาตรา 16/2 แต่เป็นกรณีข้อมูลคอมพิวเตอร์ที่ผิดกฎหมายตามมาตรา 14 เช่น ข้อมูลความผิดเกี่ยวกับความมั่นคง ข้อมูลข่าวสารเท็จ (Fake news) ข้อมูลลามก แต่ไม่ได้กำหนดความผิดฐานครอบครองข้อมูลส่วนบุคคลของผู้อื่นโดยมิชอบ

3.3 ขั้นตอนการนำข้อมูลไปใช้

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ไม่ได้กำหนดความผิดเกี่ยวกับการนำข้อมูลส่วนบุคคลไปใช้กระทำผิดทางคอมพิวเตอร์ต่าง ๆ อย่างไรก็ตาม การกระทำดังกล่าวอาจเกี่ยวข้องกับฐานความผิดที่มีอยู่ขึ้นกับลักษณะการกระทำ เช่น การนำข้อมูลส่วนบุคคลของผู้อื่นไปประกอบการหลอกลวงฉ้อโกงทางคอมพิวเตอร์อาจเป็นความผิดฐานนำข้อมูลปลอมหรือเท็จเข้าสู่ระบบตามมาตรา 14 (1) อย่างไรก็ตาม พระราชบัญญัตินี้ไม่ได้กำหนดฐานความผิด สำหรับการนำข้อมูลส่วนบุคลผู้อื่นไปแสดงระบุตัวตนประกอบการกระทำความผิดต่าง ๆ เพื่อปกปิดตัวตนและทำให้เกิดความเข้าใจผิดว่าการกระทำความผิดนั้นเกิดจากเจ้าของข้อมูล จากเปรียบเทียบกับกฎหมายสหรัฐอเมริกาพบว่า กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ (CFAA) ไม่ได้กำหนดความผิดเกี่ยวกับการนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้โดยมิชอบ แต่กฎหมายเฉพาะ (ITADA) กำหนดความผิดสำหรับการโอนหรือใช้ ซึ่งข้อมูลส่วนบุคคลของบุคคลอื่นโดยมีเจตนากระทำความผิดหรือสนับสนุนการกระทำความผิดซึ่งความผิดที่มุ่งกระทำนี้ไม่จำกัดเฉพาะการหลอกลวงหรือฉ้อโกงเท่านั้น เนื่องจากคำว่า “โอน” (Transfer) หมายถึง การทำให้ข้อมูลส่วนบุคคลปรากฏหรือนำไปใช้ในที่อยู่ข้อมูลออนไลน์ใด ๆ (Online location) ที่ปรากฏต่อบุคคลอื่น (18 U.S. Code § 1028 (10)) จึงรวมถึงการนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้แสดงระบุตัวตนเพื่อให้เจ้าหน้าที่บังคับใช้กฎหมายเข้าใจว่าเป็นการกระทำของเจ้าของข้อมูล เพื่อปกปิดตัวตนของผู้กระทำแท้จริง ส่งผลให้เจ้าของข้อมูลตกเป็นผู้ต้องหาและได้รับผลกระทบต่อเสรีภาพ

ตาราง 1 สรุปผลการวิเคราะห์เปรียบเทียบกฎหมายไทยและสหรัฐอเมริกาตามวัตถุประสงค์ข้อ 3

ขั้นตอนพฤติกรรมการโจรกรรมข้อมูล	กฎหมายสหรัฐอเมริกา	กฎหมายไทย
1. ขั้นตอนการได้มาซึ่งข้อมูล	CFAA ครอบคลุมการได้มาซึ่งข้อมูลในหลายวิธีการ	พ.ร.บ.คอมพิวเตอร์ มีข้อจำกัดเฉพาะการ “เข้าถึง”
2. ขั้นตอนกระทำก่อนนำข้อมูลไปใช้	ITADA ครอบคลุมการผลิต โอน ครอบครองข้อมูล	พ.ร.บ.คอมพิวเตอร์ มีข้อจำกัดไม่รวมถึงการ โอน ครอบครอง
3. ขั้นตอนการนำข้อมูลไปใช้	ITADA ครอบคลุมการ โอน ใช้ ทำให้ปรากฏ ซึ่งข้อมูลระบุตัว	พ.ร.บ.คอมพิวเตอร์ มาตรา 14 (1) มีข้อจำกัดเฉพาะข้อมูลที่เป็นเท็จ

บทสรุป

การโจรกรรมข้อมูลส่วนบุคคล มีขั้นตอนการกระทำที่สำคัญ 3 ขั้นตอน คือ การได้มาซึ่งข้อมูล การกระทำต่อข้อมูลก่อนนำไปใช้ และการนำข้อมูลส่วนบุคคลไปใช้ อย่างไรก็ตาม ปัจจุบันไทยไม่มีกฎหมายโดยเฉพาะสำหรับการโจรกรรมข้อมูลส่วนบุคคล แต่มีกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ที่สามารถนำมาปรับใช้กับการโจรกรรมข้อมูลส่วนบุคลทางคอมพิวเตอร์ในขั้นตอนการได้มาซึ่งข้อมูล แต่มีข้อจำกัดในแง่องค์ประกอบการกระทำไม่ครอบคลุมการกระทำต่าง ๆ ในขั้นตอนการกระทำต่อข้อมูลก่อนนำไปใช้ และขั้นตอนการนำข้อมูลไปใช้ ผลการศึกษาเปรียบเทียบกับสหรัฐอเมริกา พบว่ากฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ระดับรัฐบาลกลางไม่ได้กำหนดความผิดฐานโจรกรรมข้อมูลส่วนบุคคล แต่มีกฎหมายเฉพาะสำหรับการโจรกรรมข้อมูลส่วนบุคคลที่กำหนดฐานความผิดครอบคลุมการโจรกรรมข้อมูลส่วนบุคคล 3 ขั้นตอน

ข้อเสนอแนะ

เนื่องจากผลการศึกษาแสดงถึงข้อจำกัดด้านองค์ประกอบของความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่มีผลใช้บังคับในปัจจุบัน ในการปรับใช้กับการโจรกรรมข้อมูลคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งในขั้นตอนการกระทำต่อข้อมูลก่อนนำไปใช้ และการนำข้อมูลไปใช้ ผู้วิจัยจึงมีข้อเสนอแนะเชิงนโยบายต่อฝ่ายนิติบัญญัติในการปรับปรุงแก้ไขกฎหมายโดยเสนอร่างฐานความผิดใหม่ตามแนวทางสหรัฐอเมริกา ดังนี้

1. ฐานความผิดการโจรกรรมข้อมูลส่วนบุคคลในขั้นตอนการกระทำต่อข้อมูลก่อนนำไปใช้ โดยมีร่างองค์ประกอบความผิดว่า “ผู้ใด โดยมิชอบ ครอบครอง ซื้อขายแลกเปลี่ยนข้อมูลส่วนบุคคลที่ได้มาจากการกระทำความผิดตามพระราชบัญญัตินี้ ผู้นั้นมีความผิด.....”

2. ฐานความผิดการโจรกรรมข้อมูลส่วนบุคคลในขั้นตอนการนำข้อมูลส่วนบุคคลผู้อื่นไปใช้ โดยมีร่างองค์ประกอบความผิดว่า “ผู้ใด โดยมิชอบ โอน ทำให้ปรากฏ หรือนำไปใช้ ซึ่งข้อมูลส่วนบุคคลผู้อื่นที่ได้จากการกระทำความผิดตามพระราชบัญญัตินี้ ผู้นั้นมีความผิด.....”

ร่างข้อเสนอฐานความผิดข้างต้น อาจนำไปปรับปรุงเพิ่มเติมกฎหมายได้สองแนวทาง คือ 1) เพิ่มเติมเป็นฐานความผิดใหม่ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และ 2) บัญญัติกฎหมายใหม่ในรูปของพระราชบัญญัติ ซึ่งกำหนดฐานความผิดดังกล่าว

เอกสารอ้างอิง

คณาธิป ทองรวีวงศ์. (2563). **กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 2: ภาคการฉ้อโกงทางคอมพิวเตอร์ สแปม และความผิดอื่น**. กรุงเทพ:สำนักพิมพ์นิติธรรม.

_____. (2564). **หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล**. กรุงเทพฯ: สำนักพิมพ์นิติธรรม.

Arango, C.; & Taylor, V. (2009). **The Role of Convenience and Risk in Consumers' Means of Payment**. Retrieved 8 August, 2022, from https://www.researchgate.net/publication/46475412.

Arango, C.; Hogg, D.; & Lee, A. (2011). **Why is Cash (Still) so Entrenched? Results of the Bank of Canada 2009 Methods of Payment Survey**. Retrieved 8 August, 2022, from http://hdl.handle.net/10419/66961.

Biegelman, T. (2009). **Identity theft Handbook Detection, Prevention and Security**. New Jersey: John Wiley & Sons, Inc.

Chawki, M.; & Abdel, M. (2006). Identity theft in Cyberspace: Issues and Solutions. **Lex Electronica**. 11 (1): 2-40.

Conkey, C. (2007). **Assessing Identity-Theft Costs**. Retrieved 8 August, 2022, from https://www.wsj.com/articles/SB119621922590906207.

Graeme, N.; & Megan, M. (2005). **Identity Theft: A Research Review**. The U.S. National Institute of Justice.

Hoofnagle, J. (2007). Identity theft: Making the Known Unknowns Known. **Harvard Journal of Law & Technology**. 21(1): 98-112.

Jonker, N. (2007). Payment Instruments as Perceived by Consumers-Results from a Household Survey. **De Economist**. 155(3): 271-303.

Listerman, R.; & Romesberg, J. (2009). Are We Safe Yet? Creating a Culture of Security is Key to Stopping a Data Breach. **Strategic Finance**. 91(1): 27-38.

Marco, G. (2007). Internet-related Identity Theft. **Council of Europe**.

Mitchison, N.; Wilikens, M.; Breitenbach, L.; Urry, R.; & Portesi, S. (2004). Identity Theft: A Discussion Paper. **European Commission-Joint Research Center**.

Nazura, A. M.; Anita, A. R.; & Hossein, T. (2015) Cyberspace Identity theft: The Conceptual Framework. **Mediterranean Journals of Social Science**. 6(4): 595-612.

Organization for Economic Cooperation and Development. (2008). **OECD Policy Guidance on Online Identity Theft**. Retrieved August 5, 2022, from http://www.oecd.org/dataoecd/49/40879136.pdf.

Sproule, S.; & Archer, N. (2010) Measuring identity theft and identity fraud. **International Journal of Business Governance and Ethics.** 5 (1):51-63.

Steve, A.; Chad, A.; Conan, A.; & Mark, Z. (2011). Fraud Examination. South Western Cengage Learning.

Yvonne, J. (2010). **Media and Crimes, Second Edition.** London: Sage Publications.