NCTiM 2023

March 9, 2023

Rajabhat Maha Sarakham University

Phetchaburi Rajabhat University

Nakhon Ratchasima Rajabhat University

Buriram Rajabhat University

Phranakhon Rajabhat University

Sisaket Rajabhat University

Sakon Nakhon Rajabhat University

Nakhon Pathom Rajabhat University

Rajamangala University of Technology Suvarnabhumi

Thepsatri Rajabhat University

Surindra Rajabhat University

The 9th National Conference on Technology and Innovation Management

การปรับปรุงพัฒนาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ตามแนวทางองค์การสหประชาชาติ ในกรณีความผิดฐานโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์

The Development of Computer related-crime Act by using model offence of the United Nations in case of online identity theft.

คณาธิป ทองรวีวงศ์[1*]

Kanathip Thongrawewong[1*]

คณะนิติศาสตร์ และ สถาบันกฎหมายสื่อดิจิทัล มหาวิทยาลัยเกษมบัณฑิต[1]

kanathip.tho@kbu.ac.th[*]

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ 1) ศึกษากรอบแนวคิดการจำแนกกระบวนการของการโจรกรรมข้อมูลทางคอมพิวเตอร์ 2) เพื่อวิเคราะห์กฎหมายไทยที่เกี่ยวข้องกับการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ และ 3) เพื่อวิเคราะห์องค์ประกอบต้นแบบฐานความผิดการโจรกรรมข้อมูลส่วนบุคคลตามร่างสนธิสัญญาสหประชาชาติ โดยจำแนกตามกรอบกระบวนการการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ และเปรียบเทียบกับฐานความผิดตามพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่แก้ไขเพิ่มเติม พ.ศ. 2560

ผลการวิจัยพบว่า 1) การโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์สามารถจำแนกรูปแบบเชิงกระบวนการได้3 ขั้นตอน คือ การได้มาซึ่งข้อมูล การกระทำกับข้อมูลก่อนการนำไปใช้ และ การนำข้อมูลไปใช้ 2) ในภาพรวมกฎหมายไทยไม่ความผิดฐานโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์โดยเฉพาะ และ 3) ผลการวิเคราะห์องค์ประกอบฐานความผิดต้นแบบตามร่างสนธิสัญญาสหประชาชาติ พบว่ามีฐานความผิด 3 แนวทาง ซึ่งสามารถครอบคลุมการโจรกรรมข้อมูลส่วนบุคคล 3 ขั้นตอนแต่พระราชบัญญัติความผิดเกี่ยวกับคอมพิวเตอร์ไม่มีฐานความผิดเฉพาะและฐานความผิดที่มีอยู่ไม่ครอบคลุมการกระทำทั้ง 3 ขั้นตอน ผู้วิจัยจึงมีข้อเสนอเชิงนโยบายให้ปรับปรุงแก้ไขโดยเพิ่มเติมฐานความผิด 3 รูปแบบตามแนวทางสหประชาชาติ

คำสำคัญ: ความผิดเกี่ยวกับคอมพิวเตอร์,การโจรกรรมข้อมูลส่วนบุคคล, ข้อมูลส่วนบุคคล, กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ABSTRACT

The purposes of the research were to study the framework for classifying the process of online identity theft, to analyze Thai laws relating to online identity theft, and to analyze the elements of model law of the United Nations draft treaty on cybercrime by using the framework and comparing content with The Computer-related crime Act B.E. 2550 as amended B.E. 2560.

The research findings showed that 1) online identity theft could be classified into three processes; data acquisition, alteration, and use of data, 2) Thai law does not stipulate an offence of online identity theft, and 3) the draft treaty of the United Nations provided three proposals of model offenses of online identity theft which covers three processes of the crime. However, the Computer-related crime Act does

not stipulate such offence, and the existing offence does not cover all three processes of the crime. Therefore, the researcher suggests improving the Computer-related crime Act by adding three new offences relating to online identity theft using the United Nations model law.

Keyword: Computer crime, Identity theft, personal data, personal data protection law.

บทนำ

การโจรกรรมข้อมูลระบุตัวบุคคลหรือข้อมูลส่วนบุคคล (Identity theft) โดยทั่วไปหมายถึง การที่บุคคลหนึ่งนำข้อมูลส่วนบุคคลของเหยื่อ เช่น ชื่อ หมายเลขประจำตัวประชาชน ชื่อ ภาพ ฯลฯ ไปแสดงตัวตนว่าเป็นเหยื่อ (Mitchison, Wilikens, Breitenbach, Urry, & Portesi, 2004) โดยอาจนำไปสู่การกระทำความผิดอาญาอื่นๆ เช่น การฉ้อโกงหลอกลวงทางคอมพิวเตอร์ (Yvonne, 2010) ในทางวิชาการและกรอบความร่วมมือระหว่างประเทศมีการให้ความหมายของอาชญากรรมประเภทนี้แตกต่างกันไป เช่น องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา นิยามไว้ว่าหมายถึง “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 ผู้กระทำการโจรกรรมข้อมูลส่วนบุคคล อาจนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้ในการประกอบอาชญากรรมอื่นได้หลายรูปแบบ และส่งผลกระทบต่อเจ้าของข้อมูลในหลายมิติ เช่น ผลกระทบในด้านการเงิน โดยเฉพาะการนำไปใช้เกี่ยวกับบัญชีธนาคาร เช่น ใช้ข้อมูลของผู้อื่นเพื่อเปิดบัญชีใหม่ หรือ การเข้าไปสวมรอยในบัญชีการเงินของผู้อื่น เช่น การเจาะเข้าระบบบัญชีธนาคารออนไลน์ของผู้อื่นและใช้บัญชีของบุคคลนั้นทำธุรกรรม (Hoofnagle, 2007) การกระทำทั้งสองกรณีอาจทำขึ้นโดยที่ผู้เป็นเจ้าของข้อมูลอาจไม่รับรู้หรือรับทราบการกระทำดังกล่าวเลย นอกจากผลโดยตรงด้านการเงินที่เสียไปจากการโจรกรรมแล้ว ยังมีผลกระทบด้านอื่นเช่น เวลาที่เสียไปในการจัดการกับปัญหาที่เกิดขึ้น เวลาและค่าใช้จ่ายเกี่ยวกับการดำเนินคดีอันเป็นผลจากการถูกโจรกรรมข้อมูล (Listerman and Romesberg,2009) ผลกระทบที่ไม่เกี่ยวกับการเงินโดยตรง เช่น นำไปใช้สวมรอยประกอบอาชญากรรมภายใต้เอกลักษณ์ของผู้ที่ถูกโจรกรรม รวมทั้งอาจนำไปใช้ในการก่อการร้าย เช่น ในการวางแผนก่อการร้ายมีการใช้ข้อมูลของบุคคลอื่นเช่าห้องพัก เช่าสำนักงาน เช่ายานพาหนะ เปิดใช้โทรศัพท์ ใช้หนังสือเดินทางปลอม เปิดบัญชีทางการเงินโดยใช้ชื่อบุคคลอื่น (Biegelman, 2009)

จึงกล่าวได้ว่า การโจรกรรมข้อมูลส่วนบุคคล ส่งผลกระทบต่อเจ้าของข้อมูลหลายด้าน นอกจากผลกระทบทางการเงิน ยังรวมถึงผลกระทบต่อสิทธิเสรีภาพ เช่น ต้องตกเป็นผู้ต้องหาในคดีอาญาจากความผิดที่ตนไม่ได้ก่อขึ้นเพราะอาชญากรรมใช้ข้อมูลส่วนบุคคลของเหยื่อในการปกปิดการระบุตัวตนของผู้กระทำ เสียโอกาสในการประกอบอาชีพหรือการจ้างงานจากประวัติข้อมูลดังกล่าว รวมทั้งผลกระทบในมิติความรู้สึก สภาพอารมณ์และจิตใจ ซึ่งไม่อาจคำนวณเป็นเงินได้ นอกจากในระดับของบุคคลผู้ได้รับผลกระทบโดยตรงจากการโจรกรรมข้อมูลแล้ว การโจรกรรมข้อมูลส่วนบุคคล ส่งผลกระทบต่อสถาบันการเงิน ภาคธุรกิจอื่นในสหรัฐอเมริกา (Conkey 2007) ส่งผลกระทบต่อทัศนคติ และความเชื่อมั่นของผู้บริโภคต่อการพาณิชย์อิเล็กทรอนิกส์ (e-commerce) ลูกค้าจำนวนหนึ่งเปลี่ยนแปลงพฤติกรรมโดยลดการใช้จ่ายและชำระเงินออนไลน์ (Jonker, 2007) นอกจากการเปลี่ยนแปลงวิธีการชำระเงินแล้ว ผู้บริโภคส่วนหนึ่งอาจลดการใช้จ่ายซื้อสินค้าหรือบริการออนไลน์ รวมทั้งการใช้บริการธนาคารทางอินเทอร์เน็ตเนื่องจากความกังวลดังกล่าว (Sproule & Archer, 2010)

ความกังวลต่อการถูกโจรกรรมข้อมูลส่วนบุคคลส่งผลกระทบต่อการขยายตัวของการบริโภคและเป็นผลลบต่อการเจริญเติบโตทางเศรษฐกิจโดยรวมของประเทศด้วย

ด้วยเหตุนี้ ผู้วิจัยจึงได้ทำการศึกษามาตรการทางกฎหมายสำหรับอาชญากรรมดังกล่าว เมื่อพิจารณาภาพรวมทางกฎหมายของประเทศไทยแล้วพบว่ามีกฎหมายที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์โดยตรงคือ คือ พระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่แก้ไขเพิ่มเติม พ.ศ. 2560 แต่ไม่ได้ระบุโดยตรงถึงการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ ในขณะที่สหประชาชาติมีการร่างสนธิสัญญาอาชญากรรมอิเล็กทรอนิกส์ โดยประเทศต่างๆที่เข้าร่วมเป็นผู้แทนและคณะทำงานเฉพาะกิจ (Ad hoc committee) ได้เสนอร่างต้นแบบฐานความผิดสำหรับการโจรกรรมทางคอมพิวเตอร์เพื่อให้ประเทศต่างๆ นำไปใช้เป็นแนวทางปรับปรุงกฎหมายภายในเพื่อกำหนดความผิดสำหรับอาชญากรรมประเภทนี้ ซึ่งมีความซับซ้อนและยังไม่สามารถมีคำนิยามสากลอันครอบคลุมพฤติกรรมทั้งหมดได้ ในทางกฎหมายจึงมีแนวคิดการกำหนดความผิดโดยจำแนกขั้นตอนของการกระทำ แต่ยังคงมีความเห็นทางวิชาการในการจำแนกขั้นตอนที่แตกต่างกันไป จึงนำไปสู่การวิจัยนี้ อันเป็นการศึกษาเพื่อให้ทราบกรอบแนวคิดการจำแนกกระบวนการของพฤติกรรมการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ จากนั้นจะวิเคราะห์กฎหมายไทยในปัจจุบันที่เกี่ยวข้องกับการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ วิเคราะห์ฐานความผิดต้นแบบของสหประชาชาติโดยใช้กรอบแนวคิดการจำแนกกระบวนการโจรกรรมข้อมูลส่วนบุคคล และวิเคราะห์เปรียบเทียบกับกฎหมายไทยเพื่อชี้ให้เห็นข้อจำกัดขององค์ประกอบและขอบเขตกฎหมายไทยอันนำไปสู่ข้อเสนอแนะการปรับปรุงพัฒนากฎหมายให้สอดคล้องกับแนวทางสากลต่อไป

1. วัตถุประสงค์การวิจัย

1.1 เพื่อศึกษากรอบแนวคิดการจำแนกกระบวนการของการโจรกรรมข้อมูลทางคอมพิวเตอร์

1.2 เพื่อวิเคราะห์กฎหมายไทยที่เกี่ยวข้องกับการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์

1.3 เพื่อวิเคราะห์องค์ประกอบต้นแบบฐานความผิดการโจรกรรมข้อมูลส่วนบุคคลตามร่างสนธิสัญญาสหประชาชาติโดยจำแนกตามกรอบกระบวนการการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ และเปรียบเทียบกับฐานความผิดตามกฎหมายไทย

2. เอกสารและงานวิจัยที่เกี่ยวข้อง

การศึกษาเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลในทางเศรษฐกิจจะเน้นถึงการชี้ให้เห็นผลกระทบด้านต่างๆของอาชญากรรมประเภทนี้ เช่น ความเสียหายด้านการเงิน (Arango & Taylor, 2009) ผลกระทบต่อผู้บริโภค การค้าและการพาณิชย์ (Arango, Hogg & Lee, 2011)

การศึกษาเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลในแง่ผลกระทบต่อสิทธิเสรีภาพ ชี้ให้เห็นถึงความเสี่ยงของเหยื่อที่ถูกโจรกรรมอาจเป็นผู้ต้องหากระทำผิด ดังจะเห็นได้จากงานวิจัยที่ชี้ให้เห็นว่า การค้นพบอาชญากรรม (Discovery of the theft) อาจใช้เวลานานหรืออาจไม่สามารถตรวจพบได้เลย (Graeme & Megan,2005)

การศึกษาเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลในทางกฎหมาย จะไม่มุ่งเน้นการกำหนดนิยามกลางที่ครอบคลุมอาชญากรรมประเภททั้งหมดเพราะมีความหลากหลายในแง่พฤติกรรมและวิธีการกระทำ โดยนักวิชาการจะพิจารณาเชิงกระบวนการหรือวงจร (Steve, Chad, Conan, & Mark, 2011) ซึ่งยังมีความแตกต่างกันในมุมมองและกรอบการจำแนกประเภท (Nazura, Anita, & Hossein, 2015) (Marco,2007)

วิธีดำเนินการวิจัย

งานวิจัยนี้ใช้วิธีการวิจัยเชิงคุณภาพ (Qualitative Research) ศึกษาข้อมูลเอกสาร (Documentary Research) โดยมีขั้นตอนดังนี้

1. ข้อมูลที่นำมาวิเคราะห์ ประกอบด้วยเอกสาร 3 กลุ่มคือ (1) วรรณกรรมเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ (2) ฐานความผิดต้นแบบตามร่างสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมอิเล็กทรอนิกส์ ตัวบทกฎหมายของไทยที่เกี่ยวข้องได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล รวมถึงศึกษาเนื้อหาของแนวปฏิบัติของหน่วยงานกำกับหรือบังคับใช้กฎหมาย (3) วรรณกรรมทางกฎหมายที่เกี่ยวข้องจากงานวิจัย บทความวิชาการ

2.การเก็บรวบรวมข้อมูลมาจากแหล่งเอกสาร ห้องสมุด ในส่วนของแหล่งข้อมูลอิเล็กทรอนิกส์ เก็บรวบรวมจากเว็บไซต์ของหน่วยงานที่เกี่ยวข้องกับการบัญญัติและตีความกฎหมาย เช่น เว็บไซต์องค์การสหประชาชาติ เว็บไซต์ของสถาบันการศึกษา ฐานข้อมูลวิจัยออนไลน์ต่างประเทศ เช่น SpingerLink , EBSCO, ProQuest เป็นต้น

3. การวิเคราะห์ข้อมูล ใช้วิธีการวิเคราะห์เชิงเนื้อหา (Content analysis) นำฐานความผิดต้นแบบตามร่างของสหประชาชาติมาวิเคราะห์เนื้อหาเชิงเปรียบเทียบกับกฎหมายไทยที่มีอยู่ในปัจจุบัน (Comparative analysis) ประกอบกับศึกษาวิเคราะห์เนื้อหาวรรณกรรมทางกฎหมายเกี่ยวกับประเด็นการกำหนดความผิดสำหรับการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์

การศึกษาวิจัยนี้มุ่งเน้นการวิเคราะห์ตีความเนื้อหาตัวบทกฎหมายโดยเปรียบเทียบองค์ประกอบความผิด (element of offence) ตามต้นแบบของสหประชาชาติกับกฎหมายไทย เพื่อทราบข้อจำกัดของกฎหมายไทย ซึ่งจะนำไปสู่การจัดทำข้อเสนอปรับปรุงพัฒนาแก้ไขต่อไป โดยไม่ได้ใช้วิธีเชิงปริมาณและสถิติ

ผลการวิจัย

1. ผลการศึกษาการจำแนกรูปแบบพฤติกรรมของการกระทำของการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์

การโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ประกอบด้วยพฤติกรรมที่หลากหลาย ในทางวิชาการได้มีการศึกษาอาชญากรรมประเภทนี้โดยใช้วิธีวิเคราะห์พฤติกรรมเชิงกระบวนการ ซึ่งแบ่งการกระทำเป็นขั้นตอนย่อยแตกต่างกัน ซึ่งสามารถสรุปเป็น 3 ขั้นตอน คือ 1.การได้มาซึ่งข้อมูล 2.การกระทำกับข้อมูลก่อนการนำไปใช้ และ 3.การนำข้อมูลไปใช้

2. ผลการวิเคราะห์กฎหมายไทยที่เกี่ยวข้องกับการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ และการวิเคราะห์องค์ประกอบและขอบเขตของฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ในภาพรวม ไทยไม่มีกฎหมายกำหนดความผิดฐานโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์โดยเฉพาะ สำหรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ไม่ใช่กฎหมายที่กำหนดฐานความผิดอาญาสำหรับอาชญากรผู้ทำการโจรกรรมข้อมูล กฎหมายที่เกี่ยวข้องในการกำหนดความผิดสำหรับอาชญากรรมประเภทนี้ คือพระราชบัญญัติความผิดเกี่ยวกับคอมพิวเตอร์ แต่ไม่มีฐานความผิดเฉพาะ

3. ผลการวิเคราะห์องค์ประกอบและขอบเขตของต้นแบบฐานความผิดการโจรกรรมข้อมูลส่วนบุคคลตามร่างสนธิสัญญาสหประชาชาติ โดยจำแนกตามกรอบกระบวนการการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ และเปรียบเทียบกับฐานความผิดตามกฎหมายไทย

ตามร่างสนธิสัญญาสหประชาชาติ กำหนดฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลไว้ 3 แนวทาง ซึ่งเมื่อนำมาวิเคราะห์ตามกรอบการจำแนกกระบวนการโจรกรรมข้อมูลส่วนบุคคลพบว่า ฐานความผิดแต่ละแนวทางไม่ครอบคลุม

การกระทำทั้ง 3 ขั้นตอน แต่หากกำหนดความผิดทั้ง 3 แนวทางจะสามารถครอบคลุมการการโจรกรรมข้อมูลส่วนบุคคลได้อย่างเป็นกระบวนการ แต่เมื่อวิเคราะห์เปรียบเทียบกับฐานความผิดตามกฎหมายไทยพบว่า พระราชบัญญัติความผิดเกี่ยวกับคอมพิวเตอร์ ไม่มีความผิดเฉพาะที่ครอบคลุมการกระทำทั้ง 3 ขั้นตอนดังเช่นแนวทางทั้ง 3 ของสหประชาชาติ

อภิปรายผลการวิจัย

1. ผลการศึกษา พบว่า การโจรกรรมข้อมูลส่วนบุคคล (Identity theft) เกิดขึ้นได้โดยไม่จำกัดสภาพแวดล้อมและเทคโนโลยี ในบางกรณีอาจไม่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ เช่น การโจรกรรมข้อมูลสำเนาบัตรประชาชนไปใช้ทำธุรกรรมทางเอกสาร แต่ในที่นี้จะศึกษาเฉพาะการโจรกรรมข้อมูลส่วนบุคคลในฐานะที่เป็นวิธีการหนึ่งของอาชญากรรมคอมพิวเตอร์ อย่างไรก็ตามอาชญากรรมนี้มีลักษณะ และวิธีการที่หลากหลาย อีกทั้งไม่มีคำนิยามในลักษณะครอบคลุมทั่วไปในการพิจารณากฎหมายที่เกี่ยวข้องจึงขึ้นอยู่กับพฤติกรรมในแต่ละกรณีที่มีรายละเอียดแตกต่างกัน จากการศึกษาเอกสารและวรรณกรรมทางวิชาการพบว่ามีการศึกษาวิเคราะห์พฤติกรรมเชิงกระบวนการของอาชญากรรมประเภทนี้ ซึ่งแบ่งการกระทำเป็นขั้นตอนย่อย แต่นักวิชาการจำแนกขั้นตอนการกระทำไว้แตกต่างกัน เช่น

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

การจำแนกรูปแบบการโจรกรรมข้อมูลส่วนบุคคลแบบ 2 ขั้นตอน (Nazura, Anita, & Hossein, 2015) คือ ขั้นตอนการได้มาซึ่งข้อมูลส่วนบุคคลโดยมิชอบ และ ขั้นตอนการนำข้อมูลระบุตัวผู้อื่นไปใช้ในทางมิชอบ (Fraudulent use) เช่นนำไปใช้ทำธุรกรรมต่างๆ หรือหลอกลวงผู้อื่นอีกทอดหนึ่ง

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

จากแนวทางการจำแนกรูปแบบต่างๆ เมื่อนำมาเปรียบเทียบเนื้อหาของการกระทำพบว่ามีขั้นตอนการกระทำสำคัญคล้ายคลึงกันโดยแบ่งได้ 3 ขั้นตอนคือ 1.การได้มาซึ่งข้อมูล 2.การกระทำกับข้อมูลก่อนการนำไปใช้ และ 3.การนำข้อมูลไปใช้ ซึ่งงานวิจัยนี้จะนำแต่ละขั้นตอนมาวิเคราะห์องค์ประกอบและขอบเขตของกฎหมายไทยและเปรียบเทียบกับฐานความผิดตามร่างสนธิสัญญาสหประชาชาติต่อไป

2. ผลการศึกษามาตรการทางกฎหมายของไทย พบว่า ในภาพรวมไม่มีกฎหมายกำหนดความผิดฐานโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์โดยเฉพาะ แต่มีกฎหมายที่เกี่ยวข้อง 2 ฉบับดังนี้

(1) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลบังคับในเดือนมิถุนายน พ.ศ. 2565 แม้ว่ามีความเกี่ยวข้องโดยตรงกับข้อมูลส่วนบุคคลและกำหนดนิยามของข้อมูลส่วนบุคคลในมาตรา 6 ว่า ข้อมูลระบุตัวบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่ใช่เป็นกฎหมายที่กำหนดฐานความผิดทางอาญาสำหรับการโจรกรรมข้อมูลส่วนบุคคล ทั้งนี้เมื่อพิจารณาตัวบทมาตราของพระราชบัญญัตินี้จะสามารถจำแนกเป็นหลักการสำคัญสองส่วนที่อยู่บนแนวคิดแตกต่างกัน (คณาธิป ทองรวีวงศ์, 2564) คือ 1. กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความปลอดภัย ซึ่งอยู่บนแนวคิดความมั่นคงปลอดภัยของข้อมูลหรือความมั่นคงปลอดภัยสารสนเทศ (Information security) 2. กำหนดให้ผู้ควบคุมข้อมูลต้อง

อ้างอิง “ฐานทางกฎหมาย” (Legal or lawful basis) เช่น การขอความยินยอมจากเจ้าของข้อมูล จะเห็นได้ว่ากฎหมายนี้มีหลักการกำหนดหน้าที่แก่ผู้ควบคุมข้อมูล (Data controller) เช่น ผู้ประกอบการที่เก็บรวบรวมใช้เปิดเผยข้อมูลส่วนบุคคลของผู้ใช้บริการ ต้องมีหน้าที่ต่างๆ เช่น การขอความยินยอมก่อนการเก็บรวบรวม (มาตรา 24 มาตรา 26) การรักษาความปลอดภัยข้อมูล (มาตรา 37) ในกรณีที่มีการการโจรกรรมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลอาจต้องเป็นผู้รับผิดหากปรากฏว่าไม่จัดให้มีมาตรการป้องกันรักษาความปลอดภัยที่เหมาะสม (มาตรา 37) ซึ่งอาจนำไปสู่โทษปรับทางปกครอง อย่างไรก็ตาม พระราชบัญญัตินี้ไม่ได้กำหนดฐานความผิดอาญาสำหรับอาชญากรที่เป็นผู้ก่อให้เกิดภัยคุกคามหรือกระทำการโจรกรรมข้อมูลส่วนบุคคล หลักการนี้เป็นไปในแนวทางเดียวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป (GDPR) ซึ่งไม่ใช่กฎหมายที่กำหนดความผิดอาญาสำหรับอาชญากรที่ใช้วิธีการต่างๆ ในการโจรกรรมข้อมูลส่วนบุคคล แต่การควบคุมอาชญากรรมประเภทนี้จะต้องพิจารณากฎหมายอื่น

(2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม พ.ศ. 2560 เป็นกฎหมายเฉพาะเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ แต่ไม่ได้กำหนดฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์หรือออนไลน์ (Online Identity theft) การปรับใช้กฎหมายจึงขึ้นอยู่กับสภาพข้อเท็จจริงของพฤติกรรม

3.ผลการวิเคราะห์องค์ประกอบต้นแบบฐานความผิดการโจรกรรมข้อมูลส่วนบุคคลตามร่างสนธิสัญญาสหประชาชาติ พบว่ามีการกำหนดฐานความผิดไว้ 3 แนวทางตามข้อเสนอของผู้แทนประเทศต่างๆในคณะทำงาน ดังนี้

3.1 รูปแบบฐานความผิดต้นแบบแนวทางที่ 1 (Proposal 1) 1 เรียกชื่อความผิดว่า “การได้มาซึ่งรหัสผ่านหรือมาตรการป้องกันของบุคคลอื่น” (Illegal obtaining or receiving of passwords) มีองค์ประกอบร่างฐานความผิดว่า “ประเทศสมาชิกจะดำเนินการที่จำเป็นเพื่อกำหนดฐานความผิดอาญาตามกฎหมายภายในสำหรับการกระทำ โดยเจตนาด้วยประการใดๆ ในการได้มาหรือได้รับซึ่งรหัสผ่านหรือมาตรการป้องกันการเข้าถึงใดๆ ของระบบคอมพิวเตอร์ของผู้อื่น” ร่างมาตรานี้เสนอโดยบราซิลและสิงค์โปร์ (Ad Hoc Committee, 2022) เมื่อนำเนื้อหาฐานความผิดนี้มาวิเคราะห์ตามกรอบการจำแนกกระบวนการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ พบว่า เกี่ยวข้องกับขั้นตอนการกระทำดังนี้ 1. ขั้นตอนการได้มาซึ่งข้อมูลส่วนบุคคล เนื่องจากข้อมูลที่ได้มาอาจเป็นกรณีการได้มาซึ่งรหัสผ่าน ชื่อผู้ใช้งาน ข้อมูลการเข้าถึงระบบ (Credential) ซึ่งจัดเป็นข้อมูลที่สามารถระบุตัวผู้ใช้งานอันเป็นข้อมูลส่วนบุคคลได้ 2. ขั้นตอนการกระทำต่อข้อมูลหลังการได้มา ฐานความผิดต้นแบบแนวทางที่ 1 ไม่มุ่งเน้นการกระทำหลังการได้มาซึ่งข้อมูล เช่น การแก้ไขเปลี่ยนแปลง 3. ขั้นตอนการนำข้อมูลไปใช้ องค์ประกอบของฐานความผิดนี้มุ่งเน้นที่การได้มาหรือได้รับ (Obtain or receive) ซึ่งรหัสผ่านของผู้อื่นซึ่งเมื่อได้มาแล้วอาจนำไปใช้ประกอบอาชญากรรมประเภทใดก็ได้ โดยพฤติกรรมการได้มาซึ่งรหัสผ่านหรือมาตรการป้องกันสามารถเข้าองค์ประกอบเป็นความผิดสำเร็จในตัวเอง แม้ยังไม่ปรากฏว่ามีการใช้รหัสผ่านนั้นเข้าถึงคอมพิวเตอร์หรืออุปกรณ์เพื่อนำไปกระทำความผิดใดก็ตาม

3.2 รูปแบบฐานความผิดต้นแบบแนวทางที่ 2 (Proposal 2) คือความผิดฐานการปลอมตัวเป็นบุคคลอื่น (Impersonation) มีองค์ประกอบตามตัวบทว่า “ประเทศสมาชิกจะดำเนินการที่จำเป็นเพื่อกำหนดฐานความผิดอาญาตามกฎหมายภายในสำหรับการกระทำ โดยทุจริต กระทำการใดๆ ในการใช้ ลายมือชื่ออิเล็กทรอนิกส์ รหัสผ่าน หรือ สิ่งบ่งชี้หรือระบุตัวบุคคลใดๆ ของบุคคลอื่น” เมื่อนำเนื้อหาฐานความผิดนี้มาวิเคราะห์ตามกรอบการจำแนกกระบวนการโจรกรรมข้อมูลส่วนบุคคลทางคอมพิวเตอร์ พบว่า ครอบคลุมขั้นตอนหลังจากได้มาซึ่งข้อมูลส่วนบุคคล โดยเฉพาะขั้นตอนที่ 3 คือการนำไปใช้ -วิเคราะห์เปรียบเทียบกับ พรบ.คอมพิวเตอร์ ไม่ได้กำหนดความผิดรูปแบบนี้โดยเฉพาะแต่อาจเข้าข่ายความผิดบางมาตราของขึ้นอยู่กับข้อเท็จจริงเป็นกรณีไป เช่น การใช้ลายมือชื่ออิเล็กทรอนิกส์ของผู้อื่นเพื่อประกอบการหลอกลวงทางออนไลน์ก็เป็นการนำข้อมูลปลอมหรือเท็จเข้าสู่ระบบตามมาตรา 14 (1) อย่างไรก็ตาม เนื่องจากพระราชบัญญัตินี้ไม่มีฐานความผิดเฉพาะดังเช่นกฎหมายต้นแบบแนวทางที่ จึงอาจไม่สามารถปรับใช้กฎหมายครอบคลุมการโจรกรรมข้อมูลส่วนบุคคลบางกรณี เช่น

อาชญากรใช้ลายเซ็นอิเล็กทรอนิกส์ของบุคคลอื่นโดยไม่ได้รับอนุญาตแต่การกระทำนั้นยังไม่เข้าองค์ประกอบมาตรา 14 (1) เนื่องจากไม่มีลักษณะน่าจะทำให้ประชาชนทั่วไปเสียหาย

3.3 รูปแบบฐานความผิดต้นแบบแนวทางที่ 3 (Proposal 3) ความผิดฐาน “การเข้าถึงข้อมูลระบุตัวบุคคลอื่นโดยมิชอบ” (Unauthorized access to personal data) มีองค์ประกอบร่างฐานความผิดว่า ประเทศสมาชิกจะดำเนินการที่จำเป็นเพื่อกำหนดฐานความผิดอาญาตามกฎหมายภายในสำหรับการกระทำ การเข้าถึงโดยมิชอบซึ่งข้อมูลระบุตัวของบุคคลอื่น โดยมีเจตนาทำลาย แก้ไข ทำซ้ำ หรือ แลกเปลี่ยน” ร่างมาตรานี้เสนอโดยรัสเซีย เบลารุส จีน นิคารากัว บุรุนดี ทาจิกิสถาน เมื่อนำตัวบทฐานนี้มาวิเคราะห์ภายใต้กรอบกระบวนการพบว่ามีขอบเขตกว้างสามารถครอบคลุมการกระทำทั้ง 3 ขั้นตอน เพราะการเข้าถึงข้อมูลบุคคลอื่นนอกจากจะเป็นการทำให้ได้มาซึ่งข้อมูลตามขั้นตอนที่ 1 หลังจากนั้นอาจมีการเข้าถึงข้อมูลเพื่อแก้ไขเปลี่ยนแปลงก่อนการนำไปใช้ และในขั้นตอนการนำไปใช้ก็อาจเป็นการใช้เพื่อเข้าถึงข้อมูลส่วนบุคคลอื่น เช่น การเข้าถึงข้อมูลยืนยันตัวตนบุคคลอื่นและนำข้อมูลนั้นไปใช้เข้าถึงข้อมูลธุรกรรมของบุคคลนั้น วิเคราะห์เปรียบเทียบกับ พรบ. คอมพิวเตอร์ พบว่าไม่ได้กำหนดฐานความผิดที่ตรงตามองค์ประกอบของต้นแบบความผิดแนวทางที่ 3 อย่างไรก็ตาม การกระทำในขอบเขตร่างต้นแบบฐานนี้ อาจเข้าข่ายความผิดบางมาตราของพระราชบัญญัตินี้ ขึ้นอยู่กับข้อเท็จจริงเป็นกรณีไป เช่น การเข้าถึงและแก้ไขข้อมูลระบุตัวของเหยื่อเป็นการแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์โดยมิชอบตามมาตรา 9

ข้อเสนอแนะ

งานวิจัยนี้ดำเนินงานโดยมีความร่วมมือจากชุมชน ดังนั้นในการนำผลการวิจัยไปใช้งานจำเป็นต้องศึกษาบริบทของชุมชน รวมทั้งความต้องการให้บริการวิชาการตามที่ชุมชนต้องการ การทำวิจัยครั้งต่อไป ความมีการศึกษาในขอบเขตของรายวิชาอื่นๆ ที่สอดคล้องกับความต้องการของชุมชน และควรศึกษาความต้องการของชุมชนเพื่อนำมาจัดทำแผนการเรียนรู้

เอกสารอ้างอิง

คณาธิป ทองรวีวงศ์ (2564). หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล. กรุงเทพฯ: สำนักพิมพ์นิติธรรม.

คณาธิป ทองรวีวงศ์ (2563).กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 2 : ภาคการฉ้อโกงทางคอมพิวเตอร์ สแปม และความผิดอื่น. กรุงเทพ: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. and 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. SouthWestern Cengage Learning.

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

Rajabhat Maha Sarakham University

The 9th National Conference on Technology and Innovation Management

http://it.rmu.ac.th/nctim