



ปัญหาทางกฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์ ศึกษากรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่

Legal Issues in Cybercrime A Case Study of Mobile Data Theft

ทศพร วงษา^{1*} และศิวพร เสาวคนธ์²

Tossaphon Wongs^{1*} and Siwaporn Saowakon²

^{1*}นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม

²อาจารย์ ประจำหลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม

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

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

*Corresponding author e-mail: tossaphonwongsa@outlook.com

Received: 8 May 2025

Revised: 25 May 2025

Accepted: 29 May 2025

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์ 1. เพื่อศึกษาแนวคิด ทฤษฎีและหลักการที่เกี่ยวกับปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ 2. เพื่อศึกษามาตรการทางกฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ของต่างประเทศและประเทศไทย 3. เพื่อวิเคราะห์ปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ และ 4. เพื่อศึกษาแนวทางแก้ไขปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ เป็นการวิจัยเชิงคุณภาพ โดยการศึกษาวิจัยจากเอกสาร อาทิ หนังสือ ตำรา เอกสารวิชาการ งานวิจัย และสื่ออิเล็กทรอนิกส์ที่เกี่ยวข้อง แล้วนำข้อมูลที่รวบรวมได้จากเอกสารต่าง ๆ ที่เกี่ยวข้องมาวิเคราะห์ในเชิงเนื้อหา ผลการวิจัยพบว่า 1) แนวคิด ทฤษฎีและหลักการเกี่ยวกับอาชญากรรมไซเบอร์ ได้แก่ แนวคิดเกี่ยวกับโทรศัพท์เคลื่อนที่ แนวคิดเกี่ยวกับการโจรกรรมข้อมูล แนวคิดเกี่ยวกับกระบวนการยุติธรรมทางอาญา ทฤษฎีอาชญาวิทยาและอาชญากรรมทางไซเบอร์ หลักการที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ รวมทั้งมีหลักการที่สำคัญที่เกี่ยวข้องคือ หลักสิทธิมนุษยชน หลักการคุ้มครองข้อมูลส่วนบุคคล หลักการตรวจสอบค้นหาความจริง หลักความโปร่งใส หลักความรับผิดชอบและหลักความชอบธรรม 2) การควบคุมปัญหาความรับผิดและการพิสูจน์เจตนาของผู้เปิดบัญชีม้า กรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่มีประสิทธิภาพมากขึ้น และสร้างบรรทัดฐานในการตรวจสอบคุณสมบัติของบุคคลที่ประสงค์จะขอเปิดบัญชีกับธนาคาร และสร้างความเกรงกลัวต่อกฎหมายแก่บุคคลเหล่านั้นได้อย่างเป็นรูปธรรม ควรมีความสอดคล้องกับมาตรฐานทางกฎหมายของกฎหมายของสหรัฐอเมริกา สหราชอาณาจักรและสหพันธ์สาธารณรัฐเยอรมนี 3) ปัญหาความรับผิดของผู้เปิดบัญชีม้ากรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ กฎหมายยังขาดความชัดเจนว่าการกระทำลักษณะใดที่จะถือเป็นเจตนาเปิดบัญชีเพื่อสนับสนุนการกระทำความผิด ส่งผลให้การดำเนินคดีมีความคลุมเครือรวมถึงบทลงโทษของผู้เปิดบัญชีม้าและผู้กระทำการโจรกรรมข้อมูลโทรศัพท์เคลื่อนที่ซึ่งมีอัตราโทษในทางกฎหมายต่ำเมื่อเทียบกับระดับความเสียหายที่เกิดขึ้น นอกจากนั้นยังมีปัญหาเกี่ยวกับการกำหนดความรับผิดของบุคคลที่ร่วมขบวนการโจรกรรมข้อมูล ซึ่ง



ไม่ได้ระบุความรับผิดชอบของผู้ที่มีส่วนร่วมในการกระทำความผิดไว้ชัดเจน ทำให้ผู้ร่วมกระทำความผิดอาจใช้ช่องว่างของกฎหมายในการหลีกเลี่ยงความผิด และ 4) เสนอให้แก้ไขบทบัญญัติกฎหมายที่เกี่ยวข้องกับปัญหาอาชญากรรมทางไซเบอร์กรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ ได้แก่ 4.1) กำหนดลักษณะการกระทำและบทสันนิษฐานเบื้องต้นว่าการกระทำลักษณะใดที่ถือว่าบุคคลมีเจตนาเปิดบัญชีม้า 4.2) เพิ่มเติมบทลงโทษสำหรับบุคคลผู้เปิดบัญชีม้า 4.3) เพิ่มเติมบทบัญญัติความรับผิดชอบของผู้ที่มีส่วนร่วมในการกระทำความผิด และ 4.4) เพิ่มเติมคำนิยามและโทษทางอาญาสำหรับการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่

คำสำคัญ: อาชญากรรมทางไซเบอร์, โจรกรรมข้อมูล, โทรศัพท์เคลื่อนที่

Abstract

This research consists purposes were 1. to study the concepts, theories, and principles related to cybercrime issues in the case of mobile phone data theft 2. to examine the legal measures concerning cybercrime in cases of mobile phone data theft in both foreign countries and Thailand 3. to analyze the issues of cybercrime in cases of mobile phone data theft and 4. to explore possible solutions to address cybercrime in cases of mobile phone data theft. This is a qualitative research study conducted through document analysis, including books, textbooks, academic papers, research articles, and relevant electronic media. The collected information from these various sources is then analyzed using content analysis. The results of the study found that 1) Concepts, theories and principles of cybercrime include concepts about mobile phones, concepts about data theft, concepts about the criminal justice process, criminology and cybercrime theories, principles related to cybercrime, including important principles such as human rights, personal data protection, truth-finding principles, transparency, responsibility and legitimacy 2) Controlling the problem of liability and proving the intention of the person opening the mule account in the case of mobile phone data theft is more effective and establishing a standard for checking the qualifications of people who wish to open an account with the bank and creating a fear of the law for those people in a tangible way. It should be consistent with the legal standards of the United States, the United Kingdom and the Federal Republic of Germany 3) Problems of liability of the person opening the mule account in the case of mobile phone data theft the law still lacks clarity on what kind of action will be considered as intention to open an account to support the offense, resulting in unclear prosecution, including the punishment of the person opening the mule account and the perpetrator of the mobile phone data theft, which has a low penalty rate in law compared to the level of damages incurred. In addition, there is a problem of determining the liability of the person involved in the data theft, which does not clearly specify the liability of those involved in the offense. This causes the accomplices to use loopholes in the law to avoid the crime and 4) Propose amending the legal provisions related to the



cybercrime problem in the case of mobile phone data theft as follows 4.1) Define the nature of the act and the initial assumption that what kind of act is considered a person's intention to open a mule account 4.2) Add penalties for the person who opens a mule account 4.3) Add provisions on the liability of those involved in the crime and 4.4) Add the definition and criminal penalties for mobile phone data theft.

Keywords: Cybercrime, Identity Theft, Mobile Phone

บทนำ

การทำธุรกรรมที่เกี่ยวกับด้านการเงินต่าง ๆ ของประเทศไทย ได้มีการพัฒนาระบบการให้บริการแก่ผู้ใช้บริการอย่างต่อเนื่อง โดยธนาคารซึ่งถือเป็นสถาบันการเงินหลักของประเทศไทยได้มีการพัฒนาระบบการทำธุรกรรมทางการเงินเพื่อความสะดวกแก่ผู้ใช้บริการ เรียกว่า “การทำธุรกรรมทางออนไลน์ (E-Banking)” หรืออาจเรียกชื่ออย่างอื่น ได้แก่ Internet Banking (ธนาคารอินเทอร์เน็ต) ซึ่งเป็นการให้บริการด้านการเงินของธนาคารผ่านทางระบบอิเล็กทรอนิกส์ หรือผ่านเครือข่ายอินเทอร์เน็ต เช่น การฝากเงิน ถอนเงิน โอนเงิน หรือ สอบถามยอดเงิน เป็นต้น (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2566) แม้ว่าการทำธุรกรรมทางออนไลน์ (E-Banking) จะสร้างความสะดวกและความพึงพอใจแก่ผู้ใช้บริการ แต่ก็ยังคงส่งผลเสียต่อผู้ใช้บริการอยู่ คือ เป็นการเปิดโอกาสให้มิจฉาชีพนำมากำใช้เป็นช่องทางในการโจรกรรมหรือดูดเงินจากบัญชีธนาคารของเจ้าของบัญชีซึ่งเป็นผู้ใช้บริการ (สำนักงานกิจการยุติธรรม, 2567) ซึ่งส่วนใหญ่ มิจฉาชีพจะมีวิธีการดำเนินการโดยการใช้อุบายหลอกลวงให้ผู้เสียหายติดตั้งโปรแกรม ขอข้อมูล และให้ทำตามขั้นตอนเพื่อติดตั้งแอปพลิเคชันปลอม (ไฟล์ติดตั้งนามสกุล .apk) หรือการกระทำด้วยการหลอกลวง (Phishing) เพื่อให้ได้มาซึ่งข้อมูลสำคัญของผู้เสียหาย เช่น รหัสผ่าน หมายเลขบัตรเครดิต หมายเลขพิน (Pin Number) ของบุคคลนั้น ๆ เพื่อนำรหัสหรือข้อมูลที่ได้ดังกล่าวไปใช้ในการเข้าถึงและควบคุมโทรศัพท์มือถือที่ตกอ้อมผู้เสียหายได้ (สาวตรี สุขศรี, 2563)

ปัญหาการดูดเงินจากบัญชีของธนาคารผ่านโทรศัพท์มือถือ ยังคงเป็นปัญหาที่แก้ไขไม่ได้ และมีแนวโน้มที่อัตราการเกิดของคดีจะเพิ่มสูงขึ้นอยู่ (สภาองค์กรของผู้บริโภค, 2566) โดยขบวนการมิจฉาชีพที่โจรกรรมหรือดูดเงินจากบัญชีธนาคาร มักจะมีผู้ร่วมกระทำความผิดหลายคน ไม่ว่าจะเป็นตัวมิจฉาชีพที่เป็นผู้ลงมือหลอกลวงเพื่อเข้าถึงบัญชีธนาคารของเหยื่อ นายทุนซึ่งเป็นผู้อยู่เบื้องหลังของกลุ่มมิจฉาชีพที่คอยช่วยเหลือในการให้เครื่องมือหรืออำนวยความสะดวก รวมถึง บัญชีม้าซึ่งใช้เป็นเครื่องมือที่ใช้ในการกระทำความผิดเช่นกัน (สรวิศ บุญมี, 2566) จึงแสดงให้เห็นได้ว่า หากกล่าวถึงกรณีปัญหาอาชญากรรมทางไซเบอร์ หรือการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ พบว่ามีบทบัญญัติกฎหมายที่มีโทษทางอาญาซึ่งใช้บังคับเพื่อควบคุมกรณีปัญหาดังกล่าวหลายฉบับ ได้แก่ ประมวลกฎหมายอาญา พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 นอกจากนั้น กระบวนการการกระทำความผิดดังกล่าวยังมีบุคคลที่เกี่ยวข้องในการกระทำความผิดหลายกลุ่ม และจากการศึกษากฎหมายที่เกี่ยวข้องพบว่ายังมีข้อจำกัดหลายประการ ส่งผลให้การควบคุมปัญหาอาชญากรรมทางไซเบอร์



กรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ยังคงขาดประสิทธิภาพ โดยเฉพาะการนำบุคคลที่เกี่ยวข้องในการกระทำความผิดมาลงโทษในความผิดดังกล่าวได้อย่างเหมาะสม

นอกจากนี้ ยังมีปัญหาที่เกี่ยวข้องปัญหาทางกฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์ที่สำคัญ ได้แก่ ปัญหาความรับผิดชอบของผู้เปิดบัญชีมีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ ซึ่งในประเด็นนี้เห็นว่า บทบัญญัติกฎหมายที่ใช้ในการควบคุมการกระทำความผิดเกี่ยวกับบัญชีม้า ได้แก่ ประมวลกฎหมายอาญา มาตรา 334 ประกอบมาตรา 86 ซึ่งเป็นความผิดฐานเป็นผู้สนับสนุนในความผิดฐานลักทรัพย์ และพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 5 ประกอบมาตรา 60 ซึ่งเป็นความผิดฐานฟอกเงิน และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาตรา 9 ซึ่งเป็นความผิดฐานเป็นผู้ใช้บัญชีม้า แต่อย่างไรก็ตาม การใช้บังคับกฎหมายดังกล่าวยังคงมีข้อจำกัดเกี่ยวกับการพิสูจน์เจตนาของผู้เปิดบัญชีว่ากรณีใดบ้างที่จะถือว่าผู้กระทำความผิดมีเจตนาเปิดบัญชีเพื่อใช้ในการกระทำความผิดจริง (ทิพาพร แคล้วคล่อง, 2567) ปัญหาบทลงโทษสำหรับผู้เปิดบัญชีมีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ ซึ่งในประเด็นนี้เห็นว่า บทลงโทษทางอาญาตามกฎหมายสำหรับบุคคลผู้เปิดบัญชีม้านั้น ได้แก่ ประมวลกฎหมายอาญา มาตรา 334 ประกอบมาตรา 86 ซึ่งเป็นความผิดฐานเป็นผู้สนับสนุนในความผิดฐานลักทรัพย์ กำหนดให้ผู้กระทำความผิดต้องระวางโทษ 2 ใน 3 จากโทษจำคุกไม่เกิน 3 ปี และปรับไม่เกิน 60,000 บาท ซึ่งเป็นโทษที่กฎหมายกำหนดไว้สำหรับความผิดฐานลักทรัพย์ และพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 5 ประกอบมาตรา 60 ซึ่งเป็นความผิดฐานฟอกเงิน กำหนดให้ผู้กระทำความผิดต้องระวางโทษจำคุกตั้งแต่ 1 - 10 ปี หรือปรับตั้งแต่ 20,000 บาทถึง 200,000 บาท หรือทั้งจำทั้งปรับ และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ซึ่งเป็นความผิดฐานเป็นผู้ใช้บัญชีม้า ตามมาตรา 9 กำหนดให้ผู้กระทำความผิดต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 200,000 บาท หรือทั้งจำทั้งปรับ แต่อย่างไรก็ตามกฎหมายแต่ละฉบับยังกำหนดโทษทางอาญาที่ไม่เป็นมาตรฐานเดียวกัน ปัญหาการกำหนดความรับผิดชอบของผู้ที่มีส่วนร่วมกระทำความผิดในขบวนการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ ซึ่งในประเด็นนี้เห็นว่า ปัจจุบันยังไม่มีบทบัญญัติกฎหมายเฉพาะที่จะกำหนดว่าให้กลุ่มบุคคลเหล่านี้มีความรับผิดชอบและบทลงโทษที่เท่ากัน หรือแตกต่างกันหรือไม่ เพียงใด ทำให้การบังคับใช้กฎหมายยังมีความไม่ชัดเจนเพียงพอ (กฤษณ์ท เหล่ากอ, 2567) ปัญหาการกำหนดบทลงโทษทางอาญาให้ต้องรับโทษหนักขึ้นกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ ซึ่งในประเด็นนี้เห็นว่า การกระทำการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่นั้น ผู้กระทำความผิดจะมีความผิดเพียงฐานลักทรัพย์ธรรมดา ตามประมวลกฎหมายอาญา มาตรา 334 ซึ่งมีระวางโทษจำคุกไม่เกิน 3 ปี และปรับไม่เกิน 60,000 บาท เท่านั้น แต่อย่างไรก็ตาม ประมวลกฎหมายอาญา มาตรา 335 เป็นบทบัญญัติสำหรับความผิดฐานลักทรัพย์โดยมีเหตุฉกรรจ์ซึ่งเป็นเหตุที่ทำให้ผู้กระทำความผิดต้องรับโทษหนักขึ้น โดยได้กำหนดลักษณะของเหตุดังกล่าวไว้ ตั้งแต่ (1) ถึง (12) ซึ่งมีระวางโทษตั้งแต่ 1 - 5 ปี และปรับตั้งแต่ 20,000 - 100,000 บาท แต่ไม่มีอนุมาตราใดที่กำหนดลักษณะของการกระทำสำหรับกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ไว้ (กิตติศักดิ์ ครุพันธ์, 2566)

ดังนั้น จากสภาพปัญหาที่กล่าวมาข้างต้น ผู้วิจัยจึงมีความสนใจที่จะศึกษาปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ เนื่องจากเป็นปัญหาที่มีความซับซ้อน รวมถึงมีการใช้เทคโนโลยีที่มีความทันสมัย ทำให้อาชญากรสามารถใช้วิธีการในรูปแบบใหม่ ๆ เพื่อเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งานผ่านโทรศัพท์เคลื่อนที่ อันนำไปสู่ปัญหาการ



ก่อให้เกิดความเสียหายเป็นจำนวนมาก ภายใต้การวิจัยเรื่องปัญหาทางกฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์ ศึกษากรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษา แนวคิด ทฤษฎี หลักการที่เกี่ยวกับปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่
2. เพื่อศึกษามาตรการทางกฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ของต่างประเทศและประเทศไทย
3. เพื่อศึกษาวิเคราะห์ปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่
4. เพื่อให้ศึกษาแนวทางแก้ไขปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่

การทบทวนวรรณกรรม

การวิจัยนี้ เป็นการศึกษาปัญหาทางกฎหมายปัญหาทางกฎหมาย แนวคิด ทฤษฎี หลักการเกี่ยวกับกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ ได้แก่ แนวคิดเกี่ยวกับโทรศัพท์เคลื่อนที่ แนวคิดเกี่ยวกับการโจรกรรมข้อมูล แนวคิดเกี่ยวกับกระบวนการยุติธรรมทางอาญา ทฤษฎีอาชญาวิทยาและอาชญากรรมทางไซเบอร์ หลักการที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ รวมทั้งมีหลักการที่สำคัญที่เกี่ยวข้องคือ หลักสิทธิมนุษยชน หลักการคุ้มครองข้อมูลส่วนบุคคล หลักการตรวจสอบค้นหาความจริง หลักความโปร่งใส หลักความรับผิดชอบและหลักความชอบธรรม รวมทั้งกฎหมายที่เกี่ยวข้องคือ ประมวลกฎหมายแพ่งและพาณิชย์ ประมวลกฎหมายอาญา พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 อีกทั้งกฎหมายมหาชนระหว่างประเทศและกฎหมายต่างประเทศ โดยนำไปใช้ในการวิเคราะห์และเสนอแนวทางในการแก้ปัญหา

ตลอดจน การโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่เป็นหนึ่งในรูปแบบของอาชญากรรมทางไซเบอร์ที่มีแนวโน้มเพิ่มสูงขึ้นตามการพัฒนาเทคโนโลยีสารสนเทศและการใช้งานอุปกรณ์สื่อสารเคลื่อนที่อย่างแพร่หลาย งานวิจัยและวรรณกรรมที่เกี่ยวข้องชี้ให้เห็นว่าอาชญากรรมรูปแบบนี้มักเกิดจากการเจาะระบบหรือใช้กลวิธีทางจิตวิทยา เช่น การหลอกลวงผ่านแอปพลิเคชันปลอม ลิงก์อันตราย หรือการแอบอ้างตัวตนเพื่อเข้าถึงข้อมูลสำคัญของผู้ใช้งาน ซึ่งก่อให้เกิดผลกระทบร้ายแรงทั้งในระดับบุคคลและองค์กร แม้ว่าประเทศไทยจะมีกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่ยังพบข้อจำกัดในด้านการบังคับใช้กฎหมาย การตามจับผู้กระทำความผิดข้ามเขตแดน และการตระหนักรู้ของประชาชนเกี่ยวกับภัยคุกคามไซเบอร์ งานศึกษาส่วนใหญ่จึงเสนอให้มีการพัฒนากฎหมายให้ทันต่อเทคโนโลยี รวมถึงส่งเสริมการให้ความรู้แก่ประชาชนเกี่ยวกับการป้องกันตนเองจากการถูกโจรกรรมข้อมูลผ่านโทรศัพท์เคลื่อนที่



วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีวิธีการดำเนินการวิจัย ดังนี้

1. แหล่งข้อมูลการวิจัย ได้แก่ การวิจัยเอกสาร (Documentary Research) อันประกอบด้วย การค้นคว้าและเก็บรวบรวมข้อมูลจากเอกสารวิชาการทั้งภาษาไทยและภาษาต่างประเทศจากแหล่งข้อมูลที่มีความน่าเชื่อถือมาประกอบกรวิจัย อาทิ หนังสือ บทความ รายงานการการศึกษาจากสถาบันต่าง ๆ ที่เกี่ยวข้องกับปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่

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

3. การวิเคราะห์ข้อมูล ได้แก่ การวิเคราะห์ข้อมูลเชิงคุณภาพ โดยการนำข้อมูลที่ได้จากการรวบรวมข้อมูลเอกสารต่าง ๆ มาวิเคราะห์ในเชิงเนื้อหา (Content Analysis)

ผลการวิจัย

การวิจัยนี้ ผู้วิจัยสามารถจำแนกผลได้ ดังนี้

1. การศึกษา แนวคิด ทฤษฎี หลักการที่เกี่ยวกับปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่

ผลการวิจัยพบว่า แนวคิด ทฤษฎี หลักการที่เกี่ยวกับปัญหาอาชญากรรมทางไซเบอร์ในกรณี การโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ มีแนวคิด ทฤษฎีและหลักการเกี่ยวกับอาชญากรรมไซเบอร์ที่สำคัญ ได้แก่ แนวคิดเกี่ยวกับโทรศัพท์เคลื่อนที่ แนวคิดเกี่ยวกับการโจรกรรมข้อมูล แนวคิดเกี่ยวกับกระบวนการยุติธรรมทางอาญา ทฤษฎีอาชญาวิทยาและอาชญากรรมทางไซเบอร์ หลักการที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ รวมทั้งมีหลักการที่สำคัญที่เกี่ยวข้องคือ หลักสิทธิมนุษยชน หลักการคุ้มครองข้อมูลส่วนบุคคล หลักการตรวจสอบค้นหาความจริง หลักความโปร่งใส หลักความรับผิดชอบและหลักความชอบธรรม ถือเป็นส่วนสำคัญที่ทำให้กฎหมายถือเป็นส่วนสำคัญในการกำหนดบริบทของสังคมหรือรัฐนั้น ๆ ก่อให้เกิดหลักเกณฑ์ที่จะนำมาใช้บังคับกฎหมายเกี่ยวกับอาชญากรรมไซเบอร์ซึ่งเป็นกฎหมายที่มีโทษทางอาญา ซึ่งการจะบังคับใช้กฎหมายใด ต้องปรากฏว่าประชาชนในรัฐนั้นได้รับรู้แล้วว่ามีกฎหมายนั้นใช้บังคับอยู่ในขณะกระทำความผิด และกฎหมายต้องมีลักษณะเป็นการทั่วไปใช้ได้กับบุคคลทุกคนทุกกรณี และจะไม่มีผลย้อนหลังเป็นโทษแก่บุคคลใด รวมถึงการให้สิทธิผู้ถูกกล่าวหาว่ากระทำความผิดในการต่อสู้คดีอย่างเต็มที่ อีกทั้ง หากมีการกระทำ หรือกฎหมายใดที่ฝ่าฝืนต่อแนวคิด ทฤษฎี หลักการที่เกี่ยวข้องข้างต้นย่อมไม่มีผลใช้บังคับทางกฎหมาย

2. การศึกษามาตรการทางกฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ของต่างประเทศและประเทศไทย

ผลการวิจัยพบว่า กฎหมายที่เกี่ยวข้องกับความผิดรับของบุคคลผู้เปิดบัญชีม้ากรณี การโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ของประเทศไทย ได้แก่ พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 5 (1) พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาตรา 9 และประมวลกฎหมายอาญา มาตรา 334 ประกอบ



มาตรา 86 ซึ่งไม่มีกฎหมายฉบับใดที่ได้มีการกำหนดถึงลักษณะการกระทำอันจะถือว่าบุคคลผู้เปิดบัญชีมีเจตนาที่จะใช้บัญชีของตนในการยกย่ำหรือปิดบังแหล่งที่มาของเงินหรือทรัพย์สินที่ได้มาจากการกระทำความผิดไว้อย่างชัดเจนเพียงพอ แต่หากวิเคราะห์เปรียบเทียบกับกฎหมายที่เกี่ยวข้องกับปัญหาความรับผิดชอบของผู้เปิดบัญชีมีการจัดการข้อมูลทางโทรศัพท์เคลื่อนที่ของสหราชอาณาจักรหรือประเทศอังกฤษ ได้แก่ พระราชบัญญัติรายได้จากอาชญากรรม ค.ศ. 2002 (The Proceeds of Crime Act : POCA) ตามมาตรา 327 (1) และกฎหมายที่เกี่ยวข้องกับปัญหาความรับผิดชอบของผู้เปิดบัญชีมีการจัดการข้อมูลทางโทรศัพท์เคลื่อนที่ของสหพันธ์สาธารณรัฐเยอรมนี ได้แก่ ประมวลกฎหมายอาญาเยอรมัน (German Criminal Code) ตามมาตรา 261 (1) พบว่า กฎหมายได้มีการบัญญัติลักษณะการกระทำความผิดว่ากรณีใดที่จะเข้าลักษณะการยกย่ำหรือปิดบังแหล่งที่มาของทรัพย์สินที่ได้มาจากการกระทำความผิดไว้หลายกรณีและมีความชัดเจนยิ่งกว่า ดังนั้น ประเทศไทยจึงควรบัญญัติกฎหมายให้มีความชัดเจนและแน่นอนว่ากรณีลักษณะการกระทำของบุคคลผู้เปิดบัญชีมีรูปแบบใดที่จะถือว่าเป็นความผิดฐานเป็นผู้เปิดบัญชีมาตามกฎหมายอันถือว่าการกระทำโดยเจตนากระทำความผิดโดยกำหนดรูปแบบการกระทำความผิดให้ครอบคลุมถึงลักษณะของการกระทำให้มีหลายกรณียิ่งขึ้น หรือควรบัญญัติเป็นบทสันนิษฐานตามกฎหมายว่ากรณีการกระทำลักษณะใดที่กฎหมายจะให้ถือว่าเป็นการกระทำโดยมีเจตนากระทำความผิด เพื่อไม่ให้เกิดช่องว่างทางกฎหมาย และแก้ไขปัญหาการพิสูจน์ความผิดในลักษณะที่มีความซับซ้อน และปัญหาการรวบรวมพยานหลักฐานของเจ้าหน้าที่รัฐ เพื่อให้การควบคุมปัญหาความรับผิดชอบและการพิสูจน์เจตนาของผู้เปิดบัญชีมีการจัดการข้อมูลทางโทรศัพท์เคลื่อนที่มีประสิทธิภาพมากขึ้น และสร้างบรรทัดฐานในการตรวจสอบคุณสมบัติของบุคคลที่ประสงค์จะขอเปิดบัญชีกับธนาคารและสร้างความเกรงกลัวต่อกฎหมายแก่บุคคลเหล่านั้นได้อย่างเป็นรูปธรรมต่อไป สอดคล้องกับมาตรฐานทางกฎหมายของสหราชอาณาจักร และมาตรฐานทางกฎหมายของสหพันธ์สาธารณรัฐเยอรมนี

และปัญหาการกำหนดความรับผิดชอบของผู้ที่มีส่วนร่วมกระทำความผิดในขบวนการจัดการข้อมูลทางโทรศัพท์เคลื่อนที่ ผลการศึกษาพบว่า กฎหมายที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์กรณีการจัดการข้อมูลทางโทรศัพท์เคลื่อนที่ของประเทศไทยตามประมวลกฎหมายอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 หรือพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาตรา 3 ซึ่งไม่ปรากฏว่ามีบทบัญญัติกฎหมายฉบับใดที่ได้กำหนดให้การกระทำความผิดที่ได้กระทำระหว่างบุคคลหลายคนต้องมีความรับผิดชอบและบทลงโทษทางอาญาอย่างไรเป็นการเฉพาะ แต่หากวิเคราะห์เปรียบเทียบกับกฎหมายเกี่ยวกับการกำหนดความรับผิดชอบของผู้ที่มีส่วนร่วมกระทำความผิดในขบวนการจัดการข้อมูลทางโทรศัพท์เคลื่อนที่ ควรมีการกำหนดให้บุคคลทุกคนที่มีส่วนเกี่ยวข้องกับการกระทำความผิด ต้องรับโทษในฐานะตัวการทุกกรณี ซึ่งถือเป็นการใช้บังคับกฎหมายที่เหมาะสมยิ่งกว่า เพื่อให้เกิดความยุติธรรมเมื่อเปรียบเทียบกับสภาพความร้ายแรงและมูลค่าความเสียหายอันสืบเนื่องมาจากการกระทำความผิดดังกล่าว ดังนั้น ประเทศไทยจึงควรกำหนดความรับผิดชอบและกำหนดบทลงโทษทางอาญาของผู้ร่วมกระทำความผิดในขบวนการจัดการข้อมูลทางโทรศัพท์เคลื่อนที่ให้มีความแน่นอนและชัดเจนเพียงพอ เพื่อสร้างบรรทัดฐานและแนวปฏิบัติในการใช้บังคับกฎหมายให้มีความชัดเจนยิ่งขึ้น และมีบทลงโทษทางอาญาที่มีอัตราโทษร้ายแรงซึ่งเหมาะสมและได้สัดส่วนกับความร้ายแรงของการกระทำความผิดมากกว่า ดังนั้น ประเทศไทยจึงควรกำหนดความรับผิดชอบและกำหนดบทลงโทษทางอาญาสำหรับกรณีการจัดการข้อมูลทางโทรศัพท์เคลื่อนที่ให้มีอัตราโทษที่เหมาะสมและได้สัดส่วนกับความร้ายแรงของการกระทำความผิดและมูลค่าความเสียหายที่



กระทบต่อผู้เสียหายหรือระบบเศรษฐกิจของประเทศ เพื่อพัฒนากฎหมายให้มีความก้าวหน้าเท่าทันกับสภาพปัญหาของสังคมในปัจจุบันต่อไป

3. การศึกษาวิเคราะห์ปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่

ผลการวิจัยพบว่า ในปัจจุบันกฎหมายที่เกี่ยวข้องกับความผิดรับของบุคคลผู้เปิดบัญชีม้ากรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ของประเทศไทย ได้แก่ พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 5 (1) พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาตรา 9 และประมวลกฎหมายอาญา มาตรา 334 ประกอบมาตรา 86 ซึ่งไม่มีกฎหมายฉบับใดที่ได้มีการกำหนดถึงลักษณะการกระทำความผิดอันจะถือว่าบุคคลผู้เปิดบัญชีมีเจตนาที่จะใช้บัญชีของตนในการยกย่ายหรือปิดบังแหล่งที่มาของเงินหรือทรัพย์สินที่ได้มาจากการกระทำความผิดไว้อย่างชัดเจนเพียงพอ และบทลงโทษสำหรับผู้เปิดบัญชีม้ากรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ พบว่า ประมวลกฎหมายอาญา มาตรา 334 ประกอบมาตรา 86 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 5 (1) และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาตรา 9 ซึ่งอัตราโทษตามกฎหมายดังกล่าวยังไม่เป็นมาตรฐานเดียวกัน และอัตราโทษทางอาญายังไม่เหมาะสมเพียงพอต่อสภาพความร้ายแรงของความเสียหายที่เกิดขึ้นในปัจจุบัน อีกประการคือ การกำหนดความรับผิดของผู้ที่มีส่วนร่วมกระทำความผิดในขบวนการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ พบว่า ประมวลกฎหมายอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 หรือพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาตรา 3 ไม่ปรากฏว่ามีบทบัญญัติกฎหมายฉบับใดที่ได้กำหนดให้กรณีความผิดที่ได้กระทำความผิดระหว่างบุคคลหลายคนต้องมีความรับผิดและบทลงโทษทางอาญาอย่างไรเป็นการเฉพาะ รวมทั้งปัญหาการกำหนดบทลงโทษทางอาญาให้ต้องรับโทษหนักขึ้นกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ พบว่า พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ประมวลกฎหมายอาญา มาตรา 334 ซึ่งบทบัญญัติดังกล่าวยังคงมีการกำหนดอัตราโทษทางอาญาที่ไม่ได้สัดส่วนกับสภาพความร้ายแรงของการกระทำความผิดแสดงให้เห็นว่า ปัญหาความรับผิดของผู้เปิดบัญชีม้ากรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ กฎหมายยังขาดความชัดเจนว่าการกระทำลักษณะใดที่จะถือเป็นเจตนาเปิดบัญชีเพื่อสนับสนุนการกระทำความผิด ส่งผลให้การดำเนินคดีมีความคลุมเครือ รวมถึงบทลงโทษของผู้เปิดบัญชีม้าและผู้กระทำการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ซึ่งมีอัตราโทษในทางกฎหมายต่ำเมื่อเทียบกับระดับความเสียหายที่เกิดขึ้น นอกจากนี้ยังมีปัญหาเกี่ยวกับการกำหนดความรับผิดของบุคคลที่ร่วมขบวนการโจรกรรมข้อมูล ซึ่งไม่ได้ระบุความรับผิดของผู้ที่มีส่วนร่วมในการกระทำความผิดไว้อย่างชัดเจน ทำให้ผู้ร่วมกระทำความผิดอาจใช้ช่องว่างของกฎหมายในการหลีกเลี่ยงความผิด

4. การศึกษาแนวทางแก้ไขปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่

ผลการวิจัยพบว่า จากศึกษาปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ เนื่องจากปัญหาการโจรกรรมข้อมูลจากโทรศัพท์เคลื่อนที่ถือเป็นการกระทำความผิดทางไซเบอร์ที่มีความซับซ้อน รวมถึงมีการใช้เทคโนโลยีที่มีความทันสมัย จึงทำให้อาชญากรรมสามารถใช้วิธีการในรูปแบบใหม่ ๆ เพื่อเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งานผ่านโทรศัพท์เคลื่อนที่ อันนำไปสู่ปัญหาการก่อให้เกิดความเสียหายเป็นจำนวนมาก ดังนั้น จึงมุ่งเน้นศึกษากฎหมายทั้งของประเทศไทยและต่างประเทศที่เกี่ยวข้องกับการป้องกันและการควบคุมการกระทำความผิดในรูปแบบการโจรกรรมข้อมูล เพื่อกำหนดความรับผิดที่เกี่ยวข้องกับ



อาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ ควรมีการเสนอให้แก่ไซเบอร์นิติกฎหมายที่เกี่ยวข้องกับปัญหาอาชญากรรมทางไซเบอร์กรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ คือ (1) กำหนดลักษณะการกระทำและบทสันนิษฐานเบื้องต้นว่าการกระทำลักษณะใดที่ถือว่าบุคคลมีเจตนาเปิดบัญชีม้า (2) เพิ่มเติมนโยบายสำหรับบุคคลผู้เปิดบัญชีม้า (3) เพิ่มเติมนโยบายนิติความรับผิดชอบของผู้ที่มีส่วนร่วมในการกระทำความผิด (4) เพิ่มเติมนโยบายและโทษทางอาญาสำหรับการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่

สรุปผลการวิจัย

การวิจัยนี้ ผู้วิจัยสามารถสรุปผลการวิจัยตามวัตถุประสงค์ได้ ดังนี้

1. เพื่อศึกษา แนวคิด ทฤษฎี หลักการที่เกี่ยวข้องกับปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ พบว่า การศึกษา แนวคิด ทฤษฎี หลักการที่เกี่ยวข้องกับปัญหาอาชญากรรมทางไซเบอร์ในกรณี การโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ มีแนวคิด ทฤษฎีและหลักการเกี่ยวกับอาชญากรรมไซเบอร์ที่สำคัญ ได้แก่ แนวคิดเกี่ยวกับโทรศัพท์เคลื่อนที่ แนวคิดเกี่ยวกับการโจรกรรมข้อมูล แนวคิดเกี่ยวกับกระบวนการยุติธรรมทางอาญา ทฤษฎีอาชญาวิทยาและอาชญากรรมทางไซเบอร์ หลักการที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ รวมทั้งมีหลักการที่สำคัญที่เกี่ยวข้องคือ หลักสิทธิมนุษยชน หลักการคุ้มครองข้อมูลส่วนบุคคล หลักการตรวจสอบค้นหาความจริง หลักความโปร่งใส หลักความรับผิดชอบและหลักความชอบธรรม

2. เพื่อศึกษามาตรการทางกฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ของต่างประเทศและประเทศไทย พบว่า ในการศึกษามาตรการทางกฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ของต่างประเทศและประเทศไทย ในกรณีการควบคุมปัญหาความรับผิดชอบและการพิสูจน์เจตนาของผู้เปิดบัญชีม้า กรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่มีประสิทธิภาพมากขึ้น และสร้างบรรทัดฐานในการตรวจสอบคุณสมบัติของบุคคลที่ประสงค์จะขอเปิดบัญชีกับธนาคาร และสร้างความเกรงกลัวต่อกฎหมายแก่บุคคลเหล่านั้นได้อย่างเป็นรูปธรรม ควรมีความสอดคล้องกับมาตรฐานทางกฎหมายของสหรัฐอเมริกา สหราชอาณาจักรและสหพันธ์สาธารณรัฐเยอรมนี

3. เพื่อศึกษาวิเคราะห์ปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ พบว่า วิเคราะห์ปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ แสดงให้เห็นถึงปัญหาความรับผิดชอบของผู้เปิดบัญชีม้ากรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ ซึ่งกฎหมายยังขาดความชัดเจนว่าการกระทำลักษณะใดที่จะถือเป็นเจตนาเปิดบัญชีเพื่อสนับสนุนการกระทำความผิด ส่งผลให้การดำเนินคดีมีความคลุมเครือ รวมถึงบทลงโทษของผู้เปิดบัญชีและผู้กระทำการโจรกรรมข้อมูลโทรศัพท์เคลื่อนที่ซึ่งมีอัตราโทษในทางกฎหมายต่ำเมื่อเทียบกับระดับความเสียหายที่เกิดขึ้น นอกจากนั้นยังมีปัญหาเกี่ยวกับการกำหนดความรับผิดชอบของบุคคลที่ร่วมขบวนการโจรกรรมข้อมูล ซึ่งไม่ได้ระบุความรับผิดชอบของผู้ที่มีส่วนร่วมในการกระทำความผิดไว้ชัดเจน ทำให้ผู้ร่วมกระทำความผิดอาจใช้ช่องว่างของกฎหมายในการหลีกเลี่ยงความผิด

4. เพื่อให้ศึกษาแนวทางแก้ไขปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ พบว่า แนวทางแก้ไขปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ จากการศึกษาวิจัยควรมีการเสนอให้แก้ไขบทบัญญัติกฎหมายที่เกี่ยวข้องกับปัญหาอาชญากรรมทางไซเบอร์กรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ คือ (1) กำหนดลักษณะการกระทำและบทสันนิษฐานเบื้องต้นว่าการกระทำลักษณะใดที่ถือว่าบุคคลมีเจตนาเปิดบัญชีม้า (2) เพิ่มเติม



บทลงโทษสำหรับบุคคลผู้เปิดบัญชีม้า (3) เพิ่มเติมบทบัญญัติความรับผิดของผู้ที่มีส่วนร่วมในการกระทำความผิด (4) เพิ่มเติมค่านิยามและโทษทางอาญาสำหรับการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่

การอภิปรายผล

การวิจัยนี้ ผู้วิจัยสามารถอภิปรายผลได้ ดังนี้

1. ในปัจจุบันการที่ยังไม่มีบทบัญญัติกฎหมายปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ การบังคับใช้กฎหมายเพื่อกำหนดความรับผิดและบทลงโทษของผู้ที่เกี่ยวข้องกับขบวนการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ที่มีความไม่ชัดเจนเพียงพอว่า ผู้ร่วมกระทำความผิดแต่ละบุคคลควรได้รับโทษเท่ากันทุกคน หรือแตกต่างกันตามลักษณะและบริบทของการกระทำของบุคคลนั้นหรือไม่ ดังนั้น หากมีการกำหนดความรับผิดและกำหนดบทลงโทษทางอาญาของผู้ร่วมกระทำความผิดในขบวนการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ที่มีความแน่นอนและชัดเจนเพียงพอ ย่อมส่งผลให้การพิจารณากำหนดความรับผิดและบทลงโทษของผู้กระทำความผิดแต่ละบุคคลไม่ต้องมีปัญหาพิพาท เรื่องการตีความหรือเกิดความคลุมเครือว่าบุคคลใดควรมีความรับผิดตามกฎหมายฐานใด ฐานใดและต้องรับโทษเพียงใด เพื่อสร้างบรรทัดฐานและแนวปฏิบัติในการใช้บังคับกฎหมายสำหรับคดีอาญากรณีขบวนการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ที่มีความชัดเจนยิ่งขึ้นต่อไป

2. จากบทลงโทษตามบทบัญญัติกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ แม้ว่าในปัจจุบันจะมีกฎหมายหลายฉบับที่ได้บัญญัติกำหนดบทลงโทษสำหรับการกระทำความผิดฐานแก่บุคคลผู้เปิดบัญชีม้าไว้ก็ตาม แต่พบว่าการพิจารณาว่าผู้เปิดบัญชีม้าจะต้องรับโทษตามกฎหมายอาญามากน้อยเพียงใดนั้น มักจะขึ้นอยู่กับลักษณะของการกระทำความผิดว่าการกระทำดังกล่าวเป็นการเปิดบัญชีม้าเพื่อใช้ในการกระทำความผิดในรูปแบบใด จึงแสดงให้เห็นว่า ความผิดฐานเปิดบัญชีม้าเป็นความผิดที่ต้องยึดโยงกับความผิดหลักกว่ามีความร้ายแรงหรือไม่ เพียงใด จึงจะสามารถกำหนดบทลงโทษของผู้เปิดบัญชีม้าในกรณีนั้น ๆ ได้

ข้อค้นพบ หรือองค์ความรู้ใหม่

แนวทางการแก้ปัญหาอาชญากรรมทางไซเบอร์ในกรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่ เนื่องจากปัญหาการโจรกรรมข้อมูลจากโทรศัพท์เคลื่อนที่ถือเป็นการกระทำความผิดทางไซเบอร์ที่มีความซับซ้อน รวมถึงมีการใช้เทคโนโลยีที่มีความทันสมัย จึงทำให้อาญากรรมสามารถใช้วิธีการในรูปแบบใหม่ ๆ เพื่อเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งานผ่านโทรศัพท์เคลื่อนที่ อันนำไปสู่ปัญหาการก่อให้เกิดความเสียหายเป็นจำนวนมาก การกำหนดกฎหมายให้สอดคล้องกับสถานการณ์ปัจจุบันก็จะเป็นผลดีต่อการบังคับใช้กฎหมายให้มีประสิทธิภาพมากยิ่งขึ้น ซึ่งการศึกษานี้ได้เสนอแนวทางคือ 1) กำหนดลักษณะการกระทำและบทสันนิษฐานเบื้องต้นว่าการกระทำลักษณะใดที่ถือว่าบุคคลมีเจตนาเปิดบัญชีม้า 2) เพิ่มเติมบทลงโทษสำหรับบุคคลผู้เปิดบัญชีม้า 3) เพิ่มเติมบทบัญญัติความรับผิดของผู้ที่มีส่วนร่วมในการกระทำความผิด และ 4) เพิ่มเติมค่านิยามและโทษทางอาญาสำหรับการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่



ข้อเสนอแนะการวิจัย

1. ข้อเสนอแนะในการนำไปใช้ประโยชน์

1.1 แก้ไขเพิ่มเติมพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ดังนี้

(1) เพิ่มเติมความต่อไปนี้เป็น “วรรคสอง” ของมาตรา 5

“มาตรา 5 วรรคสอง กรณีการกระทำตามวรรคก่อน หากเป็นการเปิดบัญชีเพื่อรับโอนและจำหน่ายทรัพย์สินที่ได้มาจากการกระทำความผิด โดยผู้รับได้รับค่าตอบแทน หรือมีการเปิดบัญชีเป็นจำนวนมากโดยไม่มีเหตุอันสมควร หรือยอมให้ผู้อื่นใช้บัญชีของตนโดยไม่มีเหตุอันสมควร หรือบัญชีมีพฤติกรรมทางการเงินผิดวิสัยของวิญญูชนทั่วไป หรือมีลักษณะการกระทำเป็นอาชญากรรม ให้สันนิษฐานไว้ก่อนว่าผู้รับมีเจตนากระทำความผิด”

(2) แก้ไขเพิ่มเติมบทลงโทษสำหรับบุคคลผู้เปิดบัญชีมาในความผิดฐานฟอกเงินในมาตรา 60 ดังนี้

จากเดิม

“มาตรา 60 ผู้ใดกระทำความผิดฐานฟอกเงิน ต้องระวางโทษจำคุกตั้งแต่หนึ่งปี ถึงสิบปี หรือปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท หรือทั้งจำทั้งปรับ”

แก้ไขเพิ่มเติมเป็น

“มาตรา 60 ผู้ใดกระทำความผิดฐานฟอกเงิน ต้องระวางโทษจำคุกตั้งแต่หนึ่งปี ถึงสิบปี หรือปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท หรือทั้งจำทั้งปรับ”

1.2 แก้ไขเพิ่มเติมพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาตรา 9 ดังนี้

จากเดิม

“มาตรา 9 ผู้ใดเปิดหรือยินยอมให้บุคคลอื่นใช้บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของตน โดยมีได้มีเจตนาใช้เพื่อตนหรือเพื่อกิจการที่ตนเกี่ยวข้อง หรือยินยอมให้บุคคลอื่นใช้หรือยืมใช้เลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ของตน ทั้งนี้ โดยประการที่รู้หรือควรรู้ว่าจะนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินสามแสนบาท หรือทั้งจำทั้งปรับ”

แก้ไขเพิ่มเติมเป็น

“มาตรา 9 ผู้ใดเปิดหรือยินยอมให้บุคคลอื่นใช้บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของตน โดยมีได้มีเจตนาใช้เพื่อตนหรือเพื่อกิจการที่ตนเกี่ยวข้อง หรือยินยอมให้บุคคลอื่นใช้หรือยืมใช้เลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ของตน ทั้งนี้ โดยประการที่รู้หรือควรรู้ว่าจะนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกินสิบปี หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ความในวรรคก่อนให้ใช้บังคับถึงการเปิดบัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ บัญชีเงินอิเล็กทรอนิกส์ เพื่อรับโอนและจำหน่ายทรัพย์สินที่ได้มาจากการกระทำความผิด โดยผู้รับได้รับค่าตอบแทน หรือมีการเปิดบัญชีเป็นจำนวนมากโดยไม่มีเหตุอันสมควร หรือยอมให้ผู้อื่นใช้บัญชีของตนโดยไม่มีเหตุอันสมควร หรือบัญชีมีพฤติกรรมทางการเงินผิดวิสัยของวิญญูชนทั่วไป หรือมีลักษณะการกระทำเป็นอาชญากรรม ให้สันนิษฐานไว้ก่อนว่าผู้รับมีเจตนากระทำความผิด”



2. ข้อเสนอแนะเชิงนโยบาย

2.1 เพิ่มเติมบทบัญญัติพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ดังนี้

เพิ่มเติมความต่อไปนี้เป็น “มาตรา 7/1 ” แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550

“มาตรา 7/1 ถ้าการกระทำความผิดตามมาตรา 5 หรือมาตรา 7 เป็นการกระทำระหว่างผู้กระทำความผิดหลายคน โดยกระทำการช่วยเหลือ สนับสนุน แนะนำ สั่งการ ชักจูง จัดให้มีการกระทำความผิดนั้น หรือจงใจก่อให้เกิดการกระทำใด ๆ ต้องระวางโทษตามที่กฎหมายกำหนดไว้เช่นเดียวกับตัวการในความผิดนั้น”

2.2 เพิ่มเติมคำนิยามและโทษทางอาญาในประมวลกฎหมายอาญา ดังนี้

(1) เพิ่มเติมความต่อไปนี้ในมาตรา 1 แห่งประมวลกฎหมายอาญา ดังนี้

“มาตรา 1 ในประมวลกฎหมายนี้

ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย”

(2) เพิ่มเติมความต่อไปนี้ในมาตรา 335 (13) แห่งประมวลกฎหมายอาญา ดังนี้

“มาตรา 335 ผู้ใดลักทรัพย์

(13) เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน”

เอกสารอ้างอิง

กฤษณ์ท เหล่ากอ. (2567). การตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในจังหวัดปทุมธานี. *วารสาร มจร อุบล* *ปริทรรศน์*, 9(2). 2321-2323.

กิตติศักดิ์ ครุฑนนท์. (2566). แนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย. *วารสารการบริหารนิติบุคคลและ* *นวัตกรรมท้องถิ่น*, 9(6). 182-183.

ทิพาพร แคล้วคล่อง. (2567). มาตรการในการแก้ปัญหาการรับเปิดบัญชีธนาคารเพื่อให้ผู้อื่นนำไปใช้ในการกระทำความผิด (บัญชีม้า) กรณีศึกษาจังหวัดสกลนคร. *วารสารสังคมศาสตร์เพื่อการพัฒนาท้องถิ่น มหาวิทยาลัยราชภัฏมหาสารคาม*, 8(1), 123-124.

สภาองค์กรของผู้บริโภค. (2566). “หน่วงเงิน” ตั๋ววงจรมิจฉาชีพ. *บุคคล*. สืบค้นเมื่อ 25 ธันวาคม 2567, จาก <https://www.tcc.or.th/scammer-65-67>.

สาวตรี สุขศรี. (2563). *กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์*. (พิมพ์ครั้งที่ 2). กรุงเทพฯ: โรงพิมพ์



เดือนตุลา.

สรวิศ บุญมี. (2566). ภัยแก๊งคอลเซ็นเตอร์ จากอาชญากรรมทางเศรษฐกิจสู่อาชญากรรมทางเทคโนโลยี. *วารสารวิชาการมหาวิทยาลัยอีสเทิร์นเอเซียฉบับวิทยาศาสตร์และเทคโนโลยี*, 17(2), 20-22.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2566). *E-BANKING คือ อะไร*. สืบค้นเมื่อ 15 ธันวาคม 2567, จาก <https://www.etda.or.th/th/Useful-Resource/Knowledge-Sharing/What-Is-e-Banking.aspx>.

สำนักงานกิจการยุติธรรม. (2567). *รู้ทันก่อนโหดแอบๆ ดูดเงิน*. สืบค้นเมื่อ 20 มกราคม 2567, จาก <https://www.justicechannel.org/listen/cybercrime/smartphone-app-fake-scammer>.