ความรับผิดทางกฎหมายเกี่ยวกับการหลอกลวงให้ทำธุรกรรมทางออนไลน์

Legal liability involved to cheating to have people in general perform transaction through online

วชิราภรณ์ ปราชญ์อักษร[1] , จิตรดารมย์ รัตนวุฒิ[2]

Wachiraporn Prachaksorn[1],Chitdarom Rattanawut [2]

[1] นิติศาสตรมหาบัณฑิต คณะนิติศาสตรมหาวิทยาลัยราชภัฏสุราษฎร์ธานี จังหวัดสุราษฎร์ธานี

โทร .0-7791-3333 โทรสาร 0-7791-3348 อีเมล์ 61052538209@student.sru.ac.th

[2] รองศาสตราจารย์ ประจำหลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยราชภัฏสุราษฎร์ธานี

โทร .0-7791-3333 โทรสาร 0-7791-3348 อีเมล์ lawman077355623@gmail.com

บทคัดย่อ

การศึกษาครั้งนี้มีวัตถุประสงค์เพื่อศึกษา 1) รูปแบบการหลอกลวงให้ทำธุรกรรมทางออนไลน์ 2) ความรับผิดทางกฎหมายเกี่ยวกับการหลอกลวงให้ทำธุรกรรมทางออนไลน์ 3) ข้อเสนอแนะในการจัดการปัญหาการหลอกลวงให้ทำธุรกรรมทางออนไลน์ เป็นการวิจัยเชิงคุณภาพ ด้วยการศึกษาเอกสารค้นคว้าข้อมูลจากหนังสือ ตำรา บทความวิชาการ งานวิจัยและเอกสาร โดยนำข้อมูลมาวิเคราะห์สังเคราะห์ และใช้วิธีเรียบเรียงแบบพรรณนาความเพื่อให้ทราบถึง ความรับผิดทางกฎหมายเกี่ยวกับการหลอกลวงให้ทำธุรกรรมทางออนไลน์

ผลการศึกษาพบว่า 1) การหลอกลวงให้ทำธุรกรรมทางออนไลน์แบ่งได้เป็น 2 กรณี คือ (1) ผู้ถูกหลอกลวงเป็นผู้กระทำการทางธุรกรรมทางการเงินด้วยตนเอง (2) ผู้ถูกหลอกลวงโหลดแอปพลิเคชั่นและถูกเข้าควบคุมโทรศัพท์ ซึ่งก่อให้เกิดผลความรับผิดในทางกฎหมายที่แตกต่างกัน 2) กฎหมายเกี่ยวกับความรับผิดของบุคคลจากการหลอกลวงให้ทำธุรกรรมทางออนไลน์ ในทางอาญาผู้กระทำผิดมีความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญา การนำเข้าข้อมูลอันเป็นเท็จตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ส่วนผู้สนับสนุนย่อมมีความผิดตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ส่วนความรับผิดทางแพ่งหากเป็นในกรณีที่ผู้เสียหายเป็นผู้ทำธุรกรรมทางการเงินด้วยตนเองแล้วถือว่าผู้เสียหายได้มีส่วนก่อให้เกิดความเสียหายด้วย แต่หากโทรศัพท์ถูกควบคุมจากบุคคลภายนอกแล้วผู้เสียหายไม่ได้มีส่วนก่อให้เกิดความเสียหาย สถาบันการเงินเจ้าของบัญชีเงินฝากจึงต้องชดใช้เงินเต็มจำนวน 3) ข้อเสนอแนะในเชิงนโยบายให้สถาบันการเงินผู้เป็นเจ้าของบัญชีเงินฝากสร้างระบบป้องกันการทำธุรกรรมทางการเงินให้จำกัดเฉพาะเจ้าของบัญชีเงินฝาก ส่วนข้อเสนอแนะ ในเชิงกฎหมายควรมีกฎหมายเฉพาะเกี่ยวกับการหลอกลวงให้ทำธุรกรรมทางออนไลน์โดยมีขอบเขตความรับผิด ทั้งในทางแพ่งและทางอาญา

คำสำคัญ : ความรับผิดทางกฎหมาย การหลอกลวง ธุรกรรมออนไลน์

ABSTRACT

The objectives of this study were 1) to examine various models pertaining to fraudulent online transactions, 2) to investigate the legal ramifications associated with fraudulent online transactions; and 3) to propose recommendations for effectively addressing issues related to fraudulent online transactions. The present investigation was conducted using a qualitative research design. The author conducted a comprehensive investigation by consulting various sources, such as books, textbooks, academic papers, research studies, and documents. Through the process of analysis and synthesis, the author examined the

gathered information and subsequently presented a detailed explanation regarding the legal liability associated with fraudulent activities in online transactions.

The findings indicated that fraudulent online transactions could be categorized into two scenarios: (1) cases where the individuals who were defrauded conducted the transactions themselves, and (2) cases where the defrauded individuals had downloaded applications that allowed their phones to be remotely controlled. These two cases resulted in contrasting legal liabilities. The legal ramifications of fraudulent online transactions involved criminal liability, specifically for the offenses of Cheating and Fraud as outlined in the Criminal Code. Additionally, the act of disseminating false information in relation to computer-related crimes was also punishable under the Computer-Related Crime Act. The accomplices were found to be culpable in accordance with the provisions of the Royal Act on the Prevention and Suppression of Technological Crimes, B.E. 2566. In the context of civil liability, it was important to note that if the injured party personally engaged in the transaction, they might be deemed partially responsible for the resulting harm. However, in the event that external entities gained control over individuals' mobile devices and the affected party was not responsible for any resulting damages, financial institutions holding the deposit accounts would provide full compensation for the incurred losses. Additionally, policy recommendations are proposed for financial institutions to establish protective measures exclusively for account owners. In relation to legal recommendations, it is imperative to include precise legislations pertaining to fraudulent online transactions, encompassing both criminal and civil legal provisions.

Keywords: Legal Liability, Fraud, Online Transaction

ความสำคัญของปัญหา

อาชญากรรมไซเบอร์นั้นคือ อาชญากรรมที่เกิดจากการกระทำความผิดทางเทคโนโลยีเป็นอาชญากรรมไซเบอร์ หรือ Cyber Crime ที่เกิดการทุจริต หลอกลวง หรือทำให้หลงเชื่อบนโลกอินเตอร์เน็ต และได้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ในช่องทางออนไลน์ประเภทต่างๆ เช่นบนเว็บไซต์ แพลตฟอร์มโซเชียลมีเดีย หรือ แอปพลิเคชั่นบนมือถือ ได้ง่ายนับตั้งแต่อินเตอร์เน็ตเข้ามามีบทบาทในชีวิตของผู้คนในปัจจุบัน ทำให้อาชญากรรมทางไซเบอร์ได้พัฒนาตามวิวัฒนาการของเทคโนโลยีเช่นกัน

โดยอาชญากรรมไซเบอร์คือ อาชญากรรมที่กระทำความผิดในระบบคอมพิวเตอร์หรือการใช้คอมพิวเตอร์เพื่อกระทำความผิด รวมถึงกระทำความผิดในเครือข่ายคอมพิวเตอร์และอุปกรณ์ที่เชื่อมต่อกับเครือข่ายคอมพิวเตอร์ โดยอาชญากรรมไซเบอร์สามารถแบ่งได้เป็น .1 ลักษณะคือ 2การก่ออาชญากรรมที่มีผลต่อวัตถุ)Matter) เช่น การทำลายข้อมูลมัลแวร์)Malware),การเรียกค่าไถ่ทางคอมพิวเตอร์)Ransomware) เป็นต้น .2การก่ออาชญากรรมที่มีผลต่อจิตใจ)Mind) เช่น การข่มขู่ให้หวาดกลัว)Call Center), การหลอกให้รัก)Romance scams), การฉ้อโกงผ่านอินเทอร์เน็ต เช่น หลอกขายสินค้าออนไลน์ หลอกให้ทำงานเสริม การฟิชชิง)Phishing),เงินกู้ออนไลน์, หลอกลวงให้ลงทุนในรูปแบบต่าง ๆ)Hybrid Scam), หลอกให้ดาวน์โหลดโปรแกรม หลอกลวงผ่านอีเมล์)email scam) แชร์ลูกโซ่การพนันออนไลน์ เป็นต้น

การฟิชชิง)Phishing) พบเป็นอันดับที่ 2 โดยมีผู้มาแจ้งความร้องทุกข์จำนวน 597 ราย มีความเสียหายรวมประมาณ 67 ล้านบาท และข้อมูลจาก Nation Business Intelligence หน่วยงานวิเคราะห์ข้อมูลทางธุรกิจด้วยเทคโนโลยีของ Nation Group ตรวจสอบพบการหลอกลวงรูปแบบ ใหม่บนสื่อสังคมออนไลน์อย่างFacebook โดยทำทีเป็น แจ้งเตือนเพจเฟซบุ๊ก

แล้วหลอกให้กดลิงค์ โดยอ้างว่า เนื้อหาของเราทำผิดกฎของแพลตฟอร์ม วิธีการของคนร้าย หลอกแจ้งเตือนเพจเฟซบุ๊ก ปลอม ใช้วิธีการที่เรียกว่า ฟิชชิง)Phishing) คือการสร้างหน้าเว็บปลอมที่เหมือนกับของจริงแล้ว หลอกให้ผู้ใช้กรอก ชื่อผู้ใช้)User) และ รหัสผ่าน)Password) ด้วยตัวเอง แต่ที่อยู่เว็บไซต์หรือ URLs เป็นชื่ออื่น วิธีการหลอกลวงออนไลน์แบบนี้ จะทำให้คนร้ายได้รับ User และ Password ของเราไปโดยที่ไม่ต้องอาศัยวิธีการแฮก หรือ ช่องทางที่ซับซ้อนเลย

ในการสืบสวนสอบสวนคดีอาชญากรรมไซเบอร์นั้น พยานหลักฐานนั้น จะได้ข้อมูลจากผู้เสียหาย จากผู้ให้บริการอินเทอร์เน็ต)Internet Service Providers : ISP) และการรวบรวมข้อมูล จากตัวผู้กระทำความผิด ซึ่งตำรวจฝ่ายสืบสวนจะติดต่อประสานงานกับพนักงานสอบสวนเพื่อร้อง ขอข้อมูลจากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอสจะออกหมายเรียกข้อมูล .ตร.ซึ่ ง ศปอส(.ตร.คอมพิวเตอร์ ข้อมูลระบบคอมพิวเตอร์ ข้อมูลจราจรโดยอาศัยอำนาจของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550

อย่างไรก็ดีกฎหมายซึ่งให้อำนาจหน่วยงานที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ในการ ป้องกันปราบปรามอาชญากรรมไซเบอร์ คือ ประมวลกฎหมายวิธีพิจารณาความอาญา พุทธศักราช 2477 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พุทธศักราช 2550 และ พระราชกำหนดมาตรการป้องกัน และปราบปรามอาชญากรรมทางเทคโนโลยี พุทธศักราช 2566 กลับ ไม่สามารถป้องกันปราบปรามอาชญากรรมไซเบอร์ได้อย่างมีประสิทธิภาพ เนื่องด้วยเกิดปัญหาในทางปฏิบัติเกิดปัญหาในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาชญากรรมไซเบอร์

ปัญหาในค้นเพื่อให้ได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาชญากรรมไซเบอร์ ในทางปฏิบัติ มักจะกระทำ ได้โดยยาก ถึงแม้เจ้าพนักงานจะกระทำ โดยไม่เกินขอบเขตอำนาจของที่ กฎหมายที่ให้ในแต่เจ้าพนักงานตำรวจฝ่ายสืบสวน และพนักงานสอบสวนหากแต่อำนาจดังกล่าว นั้นกลับไม่สมเหตุสมผลในการได้มาซึ่งพยานหลักฐานพยานหลักฐานอิเล็กทรอนิกส์เนื่องด้วยลักษณะของพยานหลักฐานดังกล่าวนั้นมีลักษณะเฉพาะคือ สามารถแก้ไขเปลี่ยนแปลงได้ง่ายและการแก้ไขนั้นอาจไม่เหลือร่องรอยให้ตรวจสอบในภายหลัง กล่าวคือ ในกรณีที่พนักงานสอบสวน สืบสวนสอบสวนจากพยานหลักฐานทั่วไปและพยานหลักฐานอิเล็กทรอนิกส์จนทราบถึงแหล่ง สถานที่ที่อาชญากรใช้ในการกระทำความผิด ในการค้นก่อนการค้นจ้าพนักงานตำรวจต้องแสดง ความบริสุทธิ์เสียก่อน ซึ่งในระหว่างนี้การแจ้งเตือนนี้พยานหลักฐานอิเล็กทรอนิกส์อาจถูกทำลาย ต่อมาเมื่อเจ้าหน้าที่เข้าไปในสถานที่ที่ทำการค้นแล้ว

ในการค้นตามประมวลกฎหมายวิธีพิจารณาความอาญา พุทธศักราช 2477 ซึ่งเป็น เครื่องมือในการแสวงหาพยานหลักฐานของพนักงานสอบสวนพบว่า การค้นเพื่อพบและยึดสิ่งของ ซึ่งจะเป็นพยานหลักฐานในการดำเนินคดี เพื่อพบและยึดสิ่งของซึ่งมีไว้เป็นความผิดหรือได้มาโดย ผิดกฎหมาย หรือมีเหตุอันควรสงสัยว่า ได้ใช้หรือตั้งใจจะใช้ในการกระทำความผิดเพื่อจับกุมบุคคล ซึ่งมีหมายจับให้จับ เพื่อพบและยึดสิ่งของตามคา พิพากษาหรือตามคำสั่งศาล ในกรณีที่จะพบหรือจะยึดโดยวิธีอื่นไม่ได้แล้ว โดย คำว่า ”สิ่งของ“ ประมวลกฎหมายวิธีพิจารณาความอาญา พุทธศักราช 2477 มาตรา 2 อนุมาตรา 18 หมายความถึง สังหาริมทรัพย์ใด ซึ่งอาจใช้เป็น พยานหลักฐานคดีอาญาได้ ให้รวมทั้งจดหมาย โทรเลขและเอกสารอย่างอื่น ๆ และหมายค้นต้องทำเป็นหนังสือและมีข้อความดังต่อไปนี้)1) สถานที่ที่ออกหมาย)2) วันเดือนปีที่ออกหมาย)3) เหตุที่ต้องออกหมาย)4) สถานที่ที่จะค้น และชื่อ หรือรูปพรรณบุคคล หรือลักษณะสิ่งของที่ต้องการค้นกำหนดวันเวลาที่จะทำการค้นและชื่อกับตำแหน่งของเจ้าพนักงานผู้จะทำการค้นนั้น)5) ระบุความผิด)6) ลายมือชื่อและประทับตราของศาล (7) ทำให้เกิดปัญหาในการตีความว่าเจ้าหน้าที่ตำรวจ สามารถขอหมายค้นข้อมูลคอมพิวเตอร์โดยอาศัยอำนาจดังที่กล่าวมาแล้วข้างต้นได้หรือไม่

แต่อย่างไรก็ตามด้วยเหตุผลอาชญากรเหล่านี้มีการแบ่งหน้าที่กันทำ ทำงานเป็นทีม มีการติดต่อสื่อสารกันตลอดเวลา เมื่อมีบุคคลหนึ่งบุคคลใดในทีมอาชญากร ที่ขาดการติดต่อสื่อสาร ต้องสงสัยว่าบุคคลนั้นอาจถูกเจ้าหน้าที่ตำรวจจับกุม อาชญากรที่มีหน้าที่ในการทำลายพยาน หลักฐานก็จะเข้ามาควบคุมคอมพิวเตอร์หรือโทรศัพท์มือถือจากระยะไกล เพื่อทำลายลบล้าง

ข้อมูล ต่างๆในคอมพิวเตอร์หรือโทรศัพท์มือถือ ทำให้เจ้าหน้าที่ตำรวจไม่สามารถเก็บรวบรวมพยาน หลักฐานเพื่อใช้ข้อมูลเหล่านั้น ได้ในขยายผลเพื่อสืบสวนสอบสวนไปถึงตัวอาชญากรคนอื่นๆ ด้วย ต้องส่งคอมพิวเตอร์หรือโทรศัพท์มือถือที่ถูกยึดไว้เป็นพยานหลักฐานไปทำ การเรียกคืนข้อมูล หรือเรียกว่าการกู้ข้อมูล ทำให้เกิดปัญหาในการเข้าถึงเพื่อให้ได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์ ปัญหาการถอดรหัสลับเพื่อให้ได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์ ถึงแม้ตำรวจฝ่าย สืบสวนพนักงานสอบสวนจะค้นโดยมีหมายค้น หรือค้นโดยชอบด้วยกฎหมาย ปัญหาในการ รวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาชญากรรมไซเบอร์นั้นยังมีปัญหาการถอดรหัสลับ เพื่อให้ได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์กล่าวคือ พยานหลักฐานอิเล็กทรอนิกส์ทุกชนิดที่ จัดเก็บอยู่ในคอมพิวเตอร์หรือโทรศัพท์มือถืออาชญากรอาจทา การเข้ารหัสรักษาความปลอดภัยเอาไว้ ในการเข้าถึงเพื่อให้ได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์ดังกล่าวนี้ พนักงานสอบสวน ประสานกับศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอสอาศัยอำนา .ตร.ซึ่ง ศปอส (.ตร.จของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการ กระทา ความผิดเกี่ยวกับคอมพิวเตอร์พุทธศักราช 2550 ในการถอดรหัสลับของข้อมูลคอมพิวเตอร์ ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว และด้วยเหตุผลอาชญากรเหล่านี้มีการแบ่งหน้าที่กันทำ ทำงานเป็นทีม มีการติดต่อ สื่อสารกันตลอดเวลา เมื่อมีบุคคลหนึ่งบุคคลใดในทีมอาชญากร ที่ขาดการติดต่อสื่อสารต้องสงสัย ว่าบุคคลนั้นอาจถูกเจ้าหน้าที่ตำรวจจับกุม อาชญากรที่มีหน้าที่ในการทำ ลายพยานหลักฐานก็จะเข้า มาควบคุมคอมพิวเตอร์หรือโทรศัพท์มือถือจากระยะไกล เพื่อทา ลาย ลบล้างข้อมูลต่างๆใน คอมพิวเตอร์หรือโทรศัพท์มือถือ ทำให้เจ้าหน้าที่ตำรวจไม่สามารถเก็บรวบรวมพยานหลักฐานเพื่อ ใช้ข้อมูลเหล่านั้นได้ในขยายผลเพื่อสืบสวนสอบสวนไปถึงตัวอาชญากรคนอื่นๆ ด้วย ต้องส่ง คอมพิวเตอร์หรือโทรศัพท์มือถือที่ถูกยึดไว้เป็นพยานหลักฐานไปทำการเรียกคืนขอมูล หรือเรียกว่า การกู้ข้อมูล และที่สำคัญผู้ต้องสงสัยจะเข้ารหัสรักษาความปลอดภัยโทรศัพท์มือถือไว้ ทำให้ เจ้าหน้าที่ตำรวจฝ่ายสืบสวนไม่สามารถเข้าถึงข้อมูลที่ถูกจัดเก็บไว้ในโทรศัพท์มือถือ ปัญหาการ ถอดรหัสลับเพื่อให้ได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์ คดีอาชญากรรมไซเบอร์นั้น มีโอกาสให้การคดีเกิดขึ้นได้ตลอดเวลา เพียงแค่ประชาชน สามารถเขาถึงอินเทอร์เน็ต ก็สามารถตกเป็นเหยื่อของอาชญากรซึ่งชักจูงด้วยความโลภของมนุษย์ ทา ให้คดีอาชญากรรมไซเบอร์มีแนวโน้มเพิ่มสูงขึ้น และอาชญากรมก็จะพัฒนารูปแบบในการ กระทำความผิดเพื่อให้สามารถบรรลุวัตถุประสงค์ในการกระทำความผิดอยู่ตลอดเวลา หากแต่ การป้องกันปราบปรามอาชญากรรมดังกล่าวนั้นกลับไม่สามารถแก้ไขปัญหาอาชญากรรมไซเบอร์ ด้วยเหตุผลของกฎหมายที่ให้อำนาจพนักงานสอบสวน ขั้นตอนในการดำเนินการคดีอาชญากรรม ไซเบอร์ทำให้เกิดปัญหาคดีคงค้างชำระคดีผู้เสียหายไม่ได้รับความเป็นธรรม แต่มาตรการใน การป้องกันปราบปรามอาชญากรรมดังกล่าวนั้น กลับไม่สามารถบังคับใช้ได้อย่างมีประสิทธิภาพ ด้วยเหตุผลที่ว่า พนักงานสอบสวนไม่มีอำนาจในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ได้อย่างสมเหตุสมผล

ด้วยเหตุดังกล่าวนี้ ผู้ศึกษาจึงเกิดประเด็นขึ้นว่าผู้กระทำความผิดหรือธนาคารผู้ใดต้องรับผิดชอบให้แก่โจทก์ กรณีศึกษาจากสภาพปัญหาของคำพิพากษาฎีกาที่ 2564/6233

จำเลยประกอบกิจการธนาคารพาณิชย์ และให้บริการอื่นที่เกี่ยวกับการเงิน รับฝากเงิน และให้บริการการใช้หรือโอนเงินทาง xxx application online ผ่านโทรศัพท์เคลื่อนที่และคอมพิวเตอร์ จึงเป็นผู้รับฝาก ซึ่งเป็นผู้มีวิชาชีพเฉพาะกิจการค้าขายหรืออาชีวะ จำต้องใช้ความระมัดระวังและใช้ฝีมือเท่าที่เป็นธรรมดาจะต้องใช้และสมควรจะต้องใช้ ในกิจการค้าขายหรืออาชีวะอย่างนั้น ตาม ป.พ.พ. มาตรา 659 วรรคสาม ปรากฏว่าระหว่าง เวลา 23.41 นาฬิกา ของวันที่ 7 กรกฎาคม 2560 ถึงเวลา 2.01 นาฬิกา ของวันที่ 8 กรกฎาคม 2560 เงินในบัญชีเงินฝากของโจทก์ ถูกโอนไปยังบัญชีเงินฝากของผู้อื่นจำนวน 3 บัญชี รวม 12 ครั้ง รวมเป็นเงิน 1,099,999 บาท การโอนเงินที่เป็นการโอนจำนวนย่อยหลายครั้งติดต่อกันในช่วงเวลาเดียวกันในเวลากลางคืน จากบัญชีเงินฝากของโจทก์ ไปยังบัญชีเงินฝากของบุคคลอื่น โดยเป็นบัญชีเดียวกันหรือชื่อบัญชีเดียวกัน ย่อมเป็นพฤติกรรมในการทำธุรกรรมทางการเงินที่ผิดปกติ จำเลยซึ่งเป็นผู้มีวิชาชีพเฉพาะกิจการค้าขายหรืออาชีวะ ต้องทราบถึง

วิธีการดังกล่าว และย่อมสังเกตได้ว่าเป็นเรื่องผิดปกติ และอาจเป็นการกระทำของมิจฉาชีพผู้ประกอบอาชญากรรมทางอิเล็กทรอนิกส์ จำเลยจึงควรมีมาตรการที่เหมาะสมในการป้องกันการกระทำธุรกรรมทางการเงินโดยไม่ชอบดังกล่าวด้วย

การที่จำเลยแจ้งเตือน ให้แก่ลูกค้าผู้ใช้บริการต่าง ๆ ระมัดระวังอีเมล์หลอกลวงจากมิจฉาชีพหรือที่เรียกว่า Phishing Email มาตลอด โดยมีข้อความแจ้งเตือนว่า “แจ้งเตือน กรุณาอย่าหลงเชื่อ อีเมล์ปลอมจากมิจฉาชีพ xxx ไม่มีนโยบายในการส่งอีเมล์ใด ๆ. เพื่อให้ลูกค้ากรอกข้อมูล ชื่อผู้ใช้งาน Password หรือข้อมูลส่วนตัวอื่น ๆ โดยเด็ดขาด” และ “แจ้งเตือนโปรดระวังอีเมล์แอบอ้าง (Phishing Email) ว่าเป็นอีเมล์จากธนาคารหลอกลวงให้คลิกเพื่อไปยังเว็บไซต์ปลอม เพื่อความปลอดภัย กรุณาพิมพ์ www.ttt.com” ตามเว็บไซต์ของจำเลย ในการเข้าระบบ ลูกค้าต้องใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ที่ลูกค้าสมัครไว้กับธนาคารเข้าสู่ระบบ และต้องใส่รหัสโอทีพี (OTP หรือ One Time Password) ที่ระบบธนาคารส่งให้ที่หมายเลขโทรศัพท์ของลูกค้าเพื่อยืนยันการทำธุรกรรม อีกขั้นตอนหนึ่ง จึงจะสามารถทำธุรกรรมต่าง ๆ เกี่ยวกับบัญชีของตนได้ มาตรการดังกล่าว เป็นมาตรการป้องกันความเสียหายแก่การทำธุรกรรมทางการเงิน ทางอิเล็กทรอนิกส์เพื่อไม่ให้ลูกค้าที่ใช้บริการถูกมิจฉาชีพหลอกลวง เพื่อให้ส่งมอบชื่อผู้ใช้ และรหัสผ่านให้เพื่อนำไปใช้ กระทำธุรกรรมทางการเงินโดยไม่ชอบ ซึ่งเป็นข้อควรระวังในด้านของลูกค้า แต่มาตรฐานของจำเลยในการป้องกันการโอนเงิน ที่เป็นการทำธุรกรรมทางการเงินทางอิเล็กทรอนิกส์ที่ไม่ชอบดังกล่าว ควรจะมีอยู่อย่างไร จำเลยควรจะป้องกัน หรือระงับยับยั้งการโอนเงินที่มีความผิดปกติดังกล่าว เมื่อมีการโอนเงินผ่านไปแล้วกี่ครั้ง และเหตุใดพนักงานของจำเลยเพิ่งจะโทรศัพท์แจ้งเตือนไปยังโจทก์หลังจากที่มีการโอนเงินดังกล่าวครั้งที่ 12 และโอนเงินไปรวมเป็นเงิน 1,099,999 บาท แล้ว ซึ่งมาตรการ ในการป้องกันความเสียหาย. ที่เหมาะสม หรือสมควรดังกล่าว อยู่ในความรู้เห็นของจำเลยฝ่ายเดียว จำเลยจึงมีภาระการพิสูจน์ในส่วนนี้ แต่จำเลยกลับแสดงให้เห็นว่า จำเลยไม่ได้มีมาตรการในการป้องกัน หากเกิดการโอนเงิน. หรือการทำธุรกรรมทางอิเล็กทรอนิกส์ที่ไม่ชอบในส่วนนี้เลย และไม่ปรากฏว่าจำเลยมีมาตรการในการป้องกันความเสียหายในส่วนนี้อย่างเพียงพอ แม้ในการโอนเงิน จำเลยได้มีข้อความแจ้งเตือนไปยังโจทก์ทุกครั้งที่ทำการโอนเงินรวม 12 ครั้ง และพนักงานของจำเลยได้โทรศัพท์ไปหาโจทก์หลังจากที่มีการโอนเงิน ครั้งที่ 12 แล้ว มาตรการดังกล่าวถือว่าไม่เพียงพอต่อการป้องกันการโอนเงินหรือการทำรายการ หรือธุรกรรมทางอิเล็กทรอนิกส์ที่ไม่ชอบ นอกจากนี้ ได้ความว่าโจทก์มิใช่รายแรก ที่ถูกหลอกลวงในลักษณะนี้และมีอีกหลายรายที่ถูกหลอกลวงในลักษณะนี้ ย่อมแสดงให้เห็นว่าจำเลยทราบถึงพฤติกรรมการหลอกลวง และวิธีการโอนเงินโดยไม่ชอบดังกล่าวเช่นเดียวกับคดีนี้มาก่อน ทั้งเหตุเกิดซ้ำ ๆ กับลูกค้าจำนวนมาก จำเลยซึ่งเป็นผู้มีวิชาชีพเฉพาะกิจการค้าขาย หรืออาชีวะและในฐานะที่เป็นผู้ควบคุมระบบมีความสามารถในการตรวจสอบหรือทราบถึงความผิดปกติในการทำรายการต่าง ๆ ได้แต่เพียงฝ่ายเดียว ยิ่งต้องเพิ่มความระมัดระวังและหามาตรการในการป้องกันไม่ให้เกิดความเสียหายดังเช่นที่เกิดในคดีนี้อีก หาใช่ว่าหากมีการกรอกชื่อผู้ใช้ และรหัสผ่านที่สามารถยืนยันตัวตนได้แล้วบุคคลดังกล่าวจะสามารถดำเนินการธุรกรรมอย่างใดก็ได้. โดยจำเลยไม่มีหน้าที่ในการป้องกันไม่ให้มีการโอนเงินที่ไม่ถูกต้องแต่อย่างใดไม่

ดังนั้น จึงไม่อาจรับฟังได้ว่าจำเลย ซึ่งเป็นผู้มีวิชาชีพเฉพาะกิจการค้าขายหรืออาชีวะได้ใช้ความระมัดระวังและใช้ฝีมือเท่าที่เป็นธรรมดาจะต้องใช้และสมควรจะต้องใช้ในกิจการ ค้าขาย หรืออาชีวะอย่างนั้นแล้ว

อย่างไรก็ตาม เมื่อโจทก์ได้รับอีเมล์ที่ไม่ได้มาจากจำเลย และมีข้อความเชื่อมโยงหรือลิงค์ ไปยังเว็บไซต์ที่เลียนแบบเว็บไซต์ธนาคารจำเลย และโจทก์กรอกชื่อผู้ใช้ (username) และรหัสผ่าน (Password) ในเว็บไซต์ดังกล่าว ทำให้มีคนร้ายทราบถึงชื่อผู้ใช้ (username) และรหัสผ่าน (Password) ของโจทก์ และนำไปใช้สมัคร xxx App ในโทรศัพท์เคลื่อนที่ และโจทก์ยังได้กรอกหมายเลขโอทีพี (OTP หรือ One Time password) ในเว็บไซต์ดังกล่าวเป็นเหตุให้คนร้ายสามารถสมัครใช้บริการ xxx App ได้สำเร็จ และเกิดการโอนเงินจากบัญชีเงินฝากของโจทก์ไปยังบัญชีอื่น

โจทก์เป็นผู้ใช้ บริการธุรกรรมทางการเงินอิเล็กทรอนิกส์ผ่านทางอินเทอร์เน็ตก่อนเกิดเหตุเป็นเวลากว่า 10 ปี ทั้งตามใบแจ้งรายการบัญชีออมทรัพย์ โจทก์ก็ได้ทำธุรกรรมทางการเงินอิเล็กทรอนิกส์ผ่านทางอินเทอร์เน็ตหลายครั้ง โจทก์ย่อมมี

ความเข้าใจ ในการทำธุรกรรมทางการเงิน ผ่านช่องทางดังกล่าว และย่อมทราบถึงคำเตือนของจำเลยตามที่ปรากฏในเว็บไซต์ของจำเลย โจทก์จึงควรมีความระมัดระวังในการตรวจสอบก่อนทำธุรกรรมดังกล่าวมากกว่าที่ปรากฏในคดีนี้ จึงถือว่าโจทก์มีส่วนทำให้เกิดความเสียหายด้วย

พฤติกรรมของโจทก์ และจำเลย จึงถือว่ามีส่วนทำให้เกิดความเสียหายในคดีนี้ ไม่ยิ่งหย่อนกว่ากัน และเห็นสมควรกำหนดให้จำเลย ต้องรับผิดชดใช้เงินให้แก่โจทก์เป็นเงิน 550,000 บาท เมื่อค่าเสียหาย ที่จำเลยต้องรับผิดเป็นหนี้เงิน หากชำระล่าช้าย่อมก่อให้เกิดความเสียหาย แก่โจทก์ซึ่งค่าเสียหายของหนี้เงินตามปกติย่อมคิดกันในรูปของดอกเบี้ย จึงเห็นควรกำหนดให้จำเลยรับผิดดอกเบี้ยดังกล่าวนับแต่วันที่อ่านคำพิพากษาศาลฎีกาเป็นต้นไป ทั้งนี้ตาม ป.พ.พ. มาตรา 222 วรรคหนึ่ง โดยควรให้ในอัตราเดียวกับอัตราดอกเบี้ย ในระหว่างผิดนัดตาม ป.พ.พ. มาตรา 224

วัตถุประสงค์ของการศึกษา

1. แนวคิด ทฤษฎี เกี่ยวกับความรับผิดทางกฎหมายจากการกระทำทางเทคโนโลยี
2. ผู้ถูกหลอกลวงโหลดแอปพลิเคชั่นและถูกเข้าควบคุมโทรศัพท์
3. ความผิดและผู้เสียหายจากการหลอกลวงให้ทำธุรกรรมทางออนไลน์ โดยดำเนินการศึกษาในลักษณะวิจัยเชิงคุณภาพ

สมมติฐานของการศึกษา

เนื่องจากการกระทำความผิดฐานความผิดในมูลฐานเทคโนโลยีมิได้เกิดจากมนุษย์กระทำเองแต่เกิดจากเทคโนโลยี AI ซึ่งมนุษย์กระทำเองเป็นฐานความผิดจึงควรแก้ไขกฎหมายให้ AI

อาชญากรรมทางเทคโนโลยีกรณีแอปพลิเคชั่นดูดเงิน จึงควรมีบทบัญญัติกฎหมายในเรื่องเขตอำนาจศาลที่ชัดเจนและควรมีการปรับปรุงแก้ไขเพิ่มเติมการกำหนดเขตอำนาจศาลในการร้องทุกข์ให้สอดคล้องกับสภาพการณ์เพื่อให้บังคับใช้กฎหมายได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

ขอบเขต

งานศึกษานี้มีขอบเขตในการศึกษาเขตอำนาจศาลในการดำเนินคดีอาชญากรรมในกรณีแอปพลิเคชั่นดูดเงินควรมีบทบัญญัติกฎหมายที่ชัดเจนและเพื่อใช้ในการปรับปรุงแก้ไขกฎหมายอาชญากรรมในกรณีแอปพลิเคชั่นดูดเงิน

วิธีดำเนินการศึกษา

งานศึกษานี้ใช้การศึกษาเชิงคุณภาพ (Qualitative research) โดยมุ่งเน้นการวิเคราะห์เอกสาร (Documentary research) โดยศึกษาเอกสารจากตัวบทกฎหมาย ตำราวิชาการ วิทยานิพนธ์บทความจากวารสารหรือนิติยสารทางกฎหมาย เอกสารประกอบการสัมมนา สถิติและข้อมูลจากเว็บไซต์ทางอินเตอร์เน็ตในเขตอำนาจศาลในคดีอาญาเกี่ยวกับปัญหาทางกฎหมายเกี่ยวกับอาชญากรรมกรณีแอปพลิเคชั่นดูดเงิน

ผลการวิจัยและอภิปรายผล

ผลการวิจัยและการอภิปรายผล ปรากฏรายละเอียด ดังนี้

1) ผลการวิจัย

จากการศึกษา ผู้ศึกษาได้ค้นพบข้อมูลด้านกฎหมายเกี่ยวกับปัญหาความรับผิดทางกฎหมายเกี่ยวกับการหลอกลวงให้ทำธุรกรรมทางออนไลน์

อาชญากรรมคอมพิวเตอร์ หมายถึง การกระทำความผิดในระบบคอมพิวเตอร์ หรือการใช้คอมพิวเตอร์เพื่อกระทำความผิด เช่น ทำลายเปลี่ยนแปลง หรือขโมยข้อมูลต่างๆ เป็นต้น รวมถึงการกระทำความผิดในเครือข่ายคอมพิวเตอร์และอุปกรณ์ที่เชื่อมกับระบบดังกล่าว อาชยากรรมในเครือข่ายคอมพิวเตอร์อาจเรียกได้อีกอย่าง อาชญากรรมไซเบอร์ (Cybercrime)

ลักษณะของพยานหลักฐานอิเล็กรอนิกส์ พยานหลักฐานอิเล็กทรอนิกส์คือข้อมูลคอมพิวเตอร์เป็นสิ่งที่ไม่มีรูปร่าง ไม่สามารถจับต้องไม่ได้ อยู่ในรูปแบบเลขฐานสอง)Binary Number Systemจึง 1 และ 0 คือ ตัว 2 มาประกอบด้วยตัวเลข (หรือ รูปภาพ ข้อความ เป็น โทรศัพท์มือถือในการประมวลผลแปลงจากข้อมูลคอมพิวเตอร์ ต้องอาศัยเครื่องคอมพิวเตอร์ลักษณะอื่นใดที่ทำให้สามรถเข้าใจได้ อีกทั้งยังสามารถแก้ไขเปลี่ยนแปลง ทำลายได้โดยไม่ทิ้งร่องรอยในการแก้ไข เปลี่ยนแปลงหรือทำลาย ซึ่งต้องอาศัยเครื่องมือ หรือโปรแกรมในการตรวจสอบ ซึ่งแตกต่างจากพยานหลักฐานโดยทั่วไป

ในการรวบรวมพยานหลักฐานในคดีอาชญากรรมพื้นฐานกับคดีอาชญากรรมไซเบอร์นั้นมีความแตกต่างกันเนื่องจากอาชญากรรมไซเบอร์นั้นการกระทำความผิดเกิดขึ้นบนพื้นที่ไซเบอร์สเปซ)Cyberspaceพยานหลักฐานที่เกิดขึ้นจะถูกจัดเก็บ (โดยในการรวบรวมพยานหลักฐานโดยทั่วไปนั้นจะรวบรวมหลักฐานจากกการ หรือโทรศัพท์มือถือ ไว้ในเครื่องคอมพิวเตอร์ตรวจสถานที่เกิดเหตุ การสืบสวนภาคพื้นดิน การสื่อสาร การเงินและจากกล้องวงจรปิดฉันใดในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์นั้นก็อาศัยการรวบรวมพยานหลักฐานจากแหล่งที่มาดังกล่าวเพียงแต่ข้อมูลนั้นอยู่ในลักษณะของระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์

กระบวนการดำเนินดีอาญาที่เกี่ยวกับอาชญากรรมไซเบอร์หน่วยงานที่เกี่ยวข้องกับคดีอาชญากรรมไซเบอร์สำนักงานตำรวจแห่งชาติโดยพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ พุทธศักราช ได้แบ่งส่วนราชการที่มี 2550 โดยในส่วนที่เกี่ย ฐานะเทียบกองบัญชาการวกับอาชญากรรมไซเบอร์นั้น ประกอบด้วย กองบัญชาการตำรวจนครบาล โดยกองบังคับการตำรวจ นครบาล กองบังคับการ กองบัญชาการตำรวจสอบสวนกลาง กองบังคับการสืบสวนสอบสวน 9-1 9 -ตำรวจภูธร ภาค1 ปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

ขั้นตอนการดำเนินคดีอาชญากรรมไซเบอร์คดีอาชญากรรมไซเบอร์มีรูปแบบที่สลับซับซ้อนซึ่งต้องอาศัยพยานหลักฐานโดยที่หน่วยงานเกี่ยวข้องกับอาชญากรรมไซเบอร์ดังที่กล่าวมานั้น คือกองบัญชาการตำรวจสืบสวนอาชญากรรมทางเทคโนโลยี หรือสถ (.ก.บช) หรือกองบัญชาการตำรวจสอบสวนกลาง (.สอท.บช)านีตำรวจนครบาล หรือ สถานีตำรวจภูธรซึ่งคดีอาชญากรรมไซเบอร์อาจไม่แน่ว่าการกระทำความผิดนั้นกระทำในท้องที่ในระหว่างหลายท้องที่ หรือส่วนหนึ่งกระทำในท้องที่หนึ่ง แต่อีกส่วนหนึ่งกระทำอีกในท้องที่หนึ่ง กลาวคือเป็นการกระทำความผิดที่เกิดขึ้นหลายท้องที่ตามมาตราแห่ง 19 พนักงานสอบสวนท้องที่ใดที่หนึ่งซึ่งเกี่ยวข้องจึงมีอำนาจ 2477 ประมวลกฎหมายวิธีพิจารณาความอาญา พุทธศักราช ก็ถือปฏิบัติเหมือนการรับแจ้งคดีอาญาทั่วไปตามที่ประมวลกฎหมายวิธี สอบสวนได้ซึ่งพนักงานสอบสวนผู้รับผิดชอบคดีนั้นรวมทั้งตามคำสั่งสำน พิจารณาความอาญาักงานตำรวจแห่งชาติที่ คำร้อง เรื่องการรับ 2564 มิถุนายน 18 ลงวันที่ 2564/287 ซึ่งกำหนดให้ หรือคำกล่าวโทษและการสอบสวนคดีอาชญากรรมทางเทคโนโลยี ทุกข์

1) กรณีที่คิดซึ่งเกิด อ้าง หรือเชื่อว่าเกิดภายในเขตท้องที่ใดของพนักงานสอบสวนให้รับคำร้องทุกข์ หรือคำกล่าวโทษตามระเบียบ

2) กรณีคำแจ้งความนั้นมีลักษณะเป็นคำร้องทุกข์ หรือคำกล่าวโทษความผิดอาญา ซึ่งไม่ได้เกิดขึ้นในท้องที่ของพนักงานสอบสวน ให้ลงบันทึกประจำวันเกี่ยวกับคดีอาญา ให้ปรากฏรายละเอียดและที่อยู่ของผู้ร้องทุกข์ หรือผู้กล่าวโทษลักษณะแห่งความผิด พฤติการณ์ต่างๆ ของความผิดที่ ๆ ได้กระทำลง ที่ได้รับความเสียหายและชื่อตำหนิรูปพรรณของผู้กระทำความผิดเท่าที่จะบอได้ให้ครบถ้วนตามมาตรา6(7)(8) และมาตรา 18 และหรือมาตรา 19 แห่งประมวลกฎหมายวิธีพิจารณาความผิดอาญา โดยไม่ต้องออกเลขคดี แต่ให้ออกเลขคดีอาญานอกเขต ทั้งนี้ พนักงานสอบสวนจะทำการบันทึก

ปากคำผู้แจ้ง ประกอบคำร้องทุกข์ หรือคำกล่าวโทษด้วยหรือไม่ก็ได้และให้พนักงานสอบสวนทำการบันทึกข้อมูลรายละเอียดการร้องทุกข์ในระบบ

ความผิดอันยอมความได้นั้น แม้จะร้องทุกข์นอกเขตอำนาจการสอบสวน เมื่อมีการร้องทุกข์ภายใน 3 เดือน นับแต่วันที่รู้เรื่องความผิดและรู้ตัวผู้กระทำความผิด ย่อมถือเป็นการร้องทุกข์โดยชอบด้วยกฎหมาย ให้พยักงานสอบสวนส่งสำเนารายงานประจำวันดังกล่าวพร้อมรับรองสำเนาถูกต้อง เอกสารประกอบคำร้องทุกข์ ไปยังพนักงานสอบสวนผู้มีอำนาจสอบสวนโดยเร็วภายใน 3 วันนับตั้งแต่วันที่รับคำร้องทุกข์หรือคำกล่าวโทษ ทั้งนี้หากเป็นกรณีเร่งด่วนอาจส่งเรื่องไปทางโทรสารหรือช่องทางอิเล็กทรอนิกส์ไปก่อนแล้วจึงส่งสำเนารายงานประจำวันพร้อมรับรองสำเนาถูกต้องพร้อมเอกสารอื่นที่เป็นต้นฉบับไปยังพนักงานสอบสวนที่มีอำนาจสอบสวน

เนื่องจากคดีอาชญากรรมไซเบอร์เป็นคดีที่คนร้ายใช้เทคโนโลยีทีทันสมัยในการกระทำความผิดเพื่อประโยชน์ในการสืบสวนและสอบสวน และการรวบรวมพยานหลักฐานพิสูจน์ความผิดหรือความบริสุทธิ์ของผู้ต้องหา ให้พนักงานสอบสวนรายงานหัวหน้าพนักงานสอบสวนเพื่อขอให้ฝ่าสืบสวนทำการสืบสวนและออกรายงานการสืบสวนประกอบสำเนาการสอบสวน ในการสืบสวนสอบสวนคดีอาชญากรรมไซเบอร์นั้น พยานหลักฐานจะได้ข้อมูลจากผู้เสียหาย จากผู้ให้บริการอินเทอร์เน็ต และจากตัวผู้กระทำความผิด โดยแบ่งการดำเนินคดีอาชญากรรมไซเบอร์แบ่งออก กา ช่วง คือ 2รสืบสวนของตำรวจฝ่ายสืบสวนและการสอบสวนของพนักงานสอบสวน

ในส่วนของพนักงานสอบสวนนั้นได้รับคำร้องทุกข์แล้วพนักงานสอบสวนรายงานหัวหน้าพนักงานสอบสวน เพื่อขอให้ฝ่ายสืบสวนทำการสืบสวนและออกรายงานการสืบสวนประกอบสำนวนการสอบสวนด้วยในคดีอาชญากรรมไซเบอร์เจ้าหน้าที่ตำรวจจำต้องอาศัยพยานหลักฐานทั่วไป กล่าวคือ พยานวัตถุ พยานเอกสาร พยานวัตถุ และพยานหลักฐานอิเล็กทรอนิกส์ในการหาความเชื่อมโยงไปยังตัวผู้กระทำความผิด

ดังนั้นแล้วพนักงานสอบสวนจึงมีความจำเป็นต้องอาศัยอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญา ในส่วนของการสอบสวน คือตามประมวลกฎหมายวิธีพิจารณา มาตรา 52, มาตรา131 มาตรา132(3)(4) และมาตรา 133 เพื่อขอข้อมูลคำขอเปิดบัญชี รายการเดินบัญชี และขอหมายเลข IP Address (กรณีหลอกเอา OTP) และร้องขอข้อมูลจากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ จะออกหมายเรียกข้อมูลคอมพิวเตอร์ ข้อมูลระบบคอมพิวเตอร์ เพื่อหาตัวผู้กระทำความผิดในคดีอาชญากรรมไซเบอร์

2) อภิปรายผล

จากผลการศึกษาถึงรายละเอียดของกฎหมายเกี่ยวกับความรับผิดทางกฎหมายเกี่ยวกับการหลอกลวงให้ทำธุรกรรมทางออนไลน์ ดังนี้

การบัญญัติความผิดทางอาญาเกี่ยวกับ คอมพิวเตอร์ ให้มีความถูกต้องตามนิติวิธีของระบบประมวลกฎหมาย โดยบัญญัติความผิดทางอาญาเกี่ยวกับ คอมพิวเตอร์ไว้ในประมวลกฎหมายอาญาให้ชัดเจน และบัญญัติเฉพาะการกระทำความผิดที่มีการ เปลี่ยนแปลงในองค์ประกอบความผิดเท่านั้น จะได้ไม่ก่อให้เกิดปัญหาความซ้ำซ้อนกันของฐานความผิด

สำหรับความผิดในส่วนอื่นๆ หรือการดำเนินการต่างๆ อันควรเป็นการใช้อำนาจของฝ่ายบริหาร ให้บัญญัติ ไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ 2550 .ศ.และที่แก้ไขเพิ่มเติมเช่นเดิม

นอกจากนี้ในการกำหนดความผิดอาญาทุกฐานความผิดนั้น นอกเหนือจากการมีวัตถุประสงค์เพื่อ ต้องการป้องปรามไม่ให้เกิดการกระทำความผิดและทำให้เกิดความสงบสุขเรียบร้อยในสังคม สิ่งสำคัญอีก ประการหนึ่งที่ต้องพิจารณาก็คืออันเป็นพื้นฐานทางความคิด ในการบั ”คุณธรรมทางกฎหมาย“ญญัติ ความผิดฐานต่างๆ กล่าวคือ การกระทำใดเป็นการกระทบหรือละเมิดต่อคุณธรรมทางกฎหมาย การกระทำ นั้น ย่อมเป็นความผิดต่อกฎหมายดังนี้ หากการกระทำผิดเกี่ยวกับ 3 คอมพิวเตอร์ในลักษณะที่กระทบสิทธิ และละเมิดต่อคุณธรรมทางกฎหมาย จนก่อให้เกิดเป็นความผิดทางอาญา (Crime) จะต้องบัญญัติความผิด และมาตรการบังคับในลักษณะดังกล่าวไว้ในประมวลกฎหมายอาญาให้ชัดเจนโดยในการวินิจฉัย

ความผิด จะต้องพิจารณาโครงสร้างของความผิดอาญาประกอบด้วย อีกทั้ง หากน าความผิดทางอาญาเกี่ยวกับ คอมพิวเตอร์ โดยตรงมาจัดหมวดหมู่รวมไว้ในประมวลกฎหมายอาญาแล้ว จะไม่เกิดการความซ้ำซ้อนในการ บังคับใช้กฎหมาย

แนวทางพัฒนากฎหมายกฎหมายเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

ประเทศไทย องค์ประกอบความผิดที่กฎหมายบัญญัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ .ศ.2550 มาตรา 5 คือ การที่บุคคลหนึ่งบุคคลใดผู้ซึ่งไม่มีอำนาจได้เข้าถึง ระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนโดยเจตนา และมาตรา 7 คือ การที่บุคคลหนึ่งบุคคลใดผู้ซึ่งไม่มีอำนาจได้เข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกัน การเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน โดยเจตนานประเทศไทย ยังมีฐานความผิดที่เกี่ยวกับระบบคอมพิวเตอร์หรือข้อมูล คอมพิวเตอร์ โดยตรง ที่นอกเหนือจากที่บัญญัติไว้ในตารางอีกเพียงฐานเดียวคือ การส่งข้อมูลคอมพิวเตอร์รบกวนการใช้ ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ตามมาตรา 11 ส่วนมาตรา 12 นั้น เป็นกรณีการกระทำ ความผิดตามมาตรา 5 ถึงมาตรา 11 ที่ลักษณะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่ถูกการกระทำ หรือผลของการกระทำทำให้ต้องรับโทษหนักขึ้น ซึ่งการที่ประเทศไทยมีบทบัญญัติการกระทำความผิดอาญาเกี่ยวกับคอมพิวเตอร์เยอะไม่ได้ทำ ให้การบังคับใช้กฎหมายได้ครอบคลุมกว่าแต่กลับทำให้เกิดปัญหาต่างๆ ตามมาอีก เนื่องจากพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ .ศ.2550 ถูกตราขึ้นโดยมีวัตถุประสงค์เพื่อเป็นการควบคุม ระงับ และปราบปรามมิให้มีการกระทำความผิดต่อระบบคอมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือการใช้ คอมพิวเตอร์เป็นเครื่องมือในการก่ออาชญากรรมเป็นสำคัญ ทำให้เรื่องของสิทธิเสรีภาพของประชาชนเป็นเรื่องรองลงมาที่จะคำนึงถึง จึงไม่แปลกใจว่าในแต่ละฐานความผิดที่บัญญัติขึ้นมานั้นจะได้กำหนดโทษทาง อาญาไว้ด้วย ด้วยเหตุนี้ หากพิจารณาตามระบบนิติวิธีของประเทศไทยแล้ว ควรกำหนดความผิดในลักษณะ ที่เป็นการกระทำความผิดต่อระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์โดยตรงไว้ในประมวลกฎหมาย อาญาจะมีความเหมาะสมกว่าเฉกเช่นเดียวกับประเทศสหพันธ์สาธารณรัฐเยอรมนีและประเทศสาธารณรัฐ ฝรั่งเศส ซึ่งเป็นประเทศที่ใช้นิติวิธีระบบประมวลกฎหมายเช่นเดียวกับประเทศไทย เนื่องจากจะมีเป็น ความผิดดังกล่าวมีลักษณะกระทบต่อคุณธรรมทางกฎหมายที่สำคัญ และส่งผลกระทบอันก่อให้เกิดความ เสียหายต่อทั้งประชาชน และประเทศในวงกว้าง จึงควรต้องมีการบัญญัติบทบัญญัติดังกล่าวให้มีความ ชัดเจน และให้ตรงตามภารกิจของกฎหมายอาญาอย่างแท้จริง โดยเป็นการใช้กฎหมายอาญาเป็นเครื่องมือใน การคุ้มครองสังคมให้มีความสงบเรียบร้อย ป้องกันและปราบปรามการกระทำความผิด และที่สำคัญคือการ คุ้มครองคุณธรรมทางกฎหมาย อันจะทำให้การอยู่รวมกันเป็นไปด้วยความปกติสุข

สำหรับกรณีของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ 2550 .ศ.และที่ แก้ไขเพิ่มเติม ในปัจจุบันนั้น ผู้เขียนเห็นว่า เพื่อให้เกิดความชัดเจนในการบังคับใช้กฎหมายและเป็นไปตาม ระบบนิติวิธีที่ถูกต้อง ควรนำบทบัญญัติ ดังต่อไปนี้

1. มาตรา 5 การเข้าสู่ระบบคอมพิวเตอร์โดยมิชอบ
2. มาตรา 7 การเข้าสู่ข้อมูลคอมพิวเตอร์โดยมิชอบ
3. มาตรา 8 การดักรับข้อมูลคอมพิวเตอร์โดยมิชอบ
4. มาตรา 9 การแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์โดยมิชอบ
5. มาตรา 10 การกระทำต่อระบบคอมพิวเตอร์โดยไม่ชอบ
6. มาตรา 12 บทบัญญัติที่ทำให้ต้องรับโทษสูงขึ้นจากการกระทำความผิดดังกล่าว
7. มาตรา 13 การเตรียมการ หรือดำเนินการเพื่อให้เกิดการกระทำความผิดต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ โดยมิชอบ

อย่างไรก็ตาม ไม่ว่าจะเป็นผู้เสียหายหรือจำเลย เมื่อมีการกระทำความผิดเกิดขึ้นแล้วต่างก็ได้รับความเสียหายด้วยกันทุกฝ่าย ดังนั้น เพื่อให้การอยู่ร่วมกันในสังคมเป็นไปด้วยความสงบเรียบร้อย ทุกคนในสังคมจึงควรอยู่ร่วมกันอย่างถ้อยทีถ้อยอาศัย ให้อภัยซึ่งกันและกัน ซึ่งจะทำให้ปัญหาอาชญากรรมลดลง และสังคมอยู่ร่วมกันได้อย่างสงบสุข

สำนักงานตำรวจแห่งชาติ ขอประชาสัมพันธ์ แจ้งให้ประชาชนรับทราบ เข้าใจหลักการตาม พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ดังนี้

1. อาชญากรรมทางคอมพิวเตอร์ คดีออนไลน์เพื่อฉ้อโกง กรรโชก และรีดเอาทรัพย์ ถือเป็นคดีที่ต้องอยู่บังคับของกฎหมายฉบับนี้

2. กรณีเพื่อการป้องกันอาชญากรรมทางเทคโนโลยี หรือมีเหตุสงสัยว่าอาจจะมีการทำผิดทางเทคโนโลยี สถาบันการเงินและผู้ประกอบธุรกิจมีอำนาจแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้าผ่านระบบการแลกเปลี่ยนข้อมูลโดยไม่ถือว่าบัญชีม้าเป็นข้อมูลที่ได้รับรองตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ดังนั้น ข้อมูลบัญชีม้าจะถูกธนาคารและเจ้าหน้าที่ส่งต่อให้กันเพื่อระงับช่องทางการทำธุรกรรมและอายัดบัญชีด้วยความรวดเร็วมากยิ่งขึ้น ช่วยระงับความเสียหายของผู้เสียหายได้

3. ผู้ให้บริการโทรคมนาคมมีอำนาจแลกเปลี่ยนข้อมูลให้สำนักงานตำรวจแห่งชาติ สำนักงาน ปปง. และหน่วยงานที่ได้รับอนุญาตเข้าถึงข้อมูลที่มีการแลกเปลี่ยนได้

4. ผู้เสียหายสามารถแจ้งข้อมูลไปยังสถาบันการเงินหรือผู้ประกอบธุรกิจเพื่อแจ้งให้สถาบันการเงินหรือผู้ประกอบธุรกิจที่รับโอนระงับการทำธุรกรรมไว้ทันทีเป็นการชั่วคราว จากนั้นให้ผู้เสียหายร้องทุกข์ต่อพนักงานสอบสวนภายในเวลา 72 ชั่วโมง โดยมีการระบุขั้นตอนในการระงับการทำธุรกรรมไว้ชัดเจนและรวดเร็ว เพื่อป้องกันไม่ให้คนร้ายทำธุรกรรมได้ง่ายเหมือนแต่ก่อน และเมื่อผู้เสียหายไปร้องทุกข์แล้ว พนักงานสอบสวนจะพิจารณาดำเนินการกับบัญชีธนาคารดังกล่าวภายใน 7 วัน

5. มีการเพิ่มช่องทางการแจ้งเหตุ โดยกำหนดให้ผู้เสียหายแจ้งข้อมูลโดยง่ายและเร็ว สามารถแจ้งข้อมูลหรือหลักฐานทางโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์กับสถาบันการเงินหรือผู้ประกอบธุรกิจได้

6. ผู้เสียหายสามารถแจ้งความร้องทุกข์กับพนักงานสอบสวนที่ใดก็ได้ โดยไม่ต้องถามว่าเหตุเกิดที่ใดในประเทศไทย หรือแจ้งผ่านระบบแจ้งความออนไลน์ถือว่าเป็นการร้องทุกข์ และพนักงานสอบสวนนั้นมีอำนาจสอบสวนตาม ป.วิอาญา ซึ่งสำนักงานตำรวจแห่งชาติได้มีวิทยุสั่งการไปยังพนักงานสอบสวนทั่วประเทศให้พนักงานสอบสวนรับคำร้องทุกข์จากพี่น้องประชาชนที่เดินทางมาแจ้งความที่สถานีตำรวจ โดยถือว่าเป็นพนักงานสอบสวนผู้รับผิดชอบ ไม่ว่าเหตุจะเกิดที่ไหน ต้องอำนวยความสะดวกผู้เสียหาย เร่งช่วยเหลือ

7. มีบทลงโทษเครือข่ายอาจจะทำที่รุนแรงขึ้นทั้งบัญชีม้า คนจัดหาบัญชีม้า

7.1 ห้ามมิให้ผู้ใดเปิดบัญชี บัตรอิเล็กทรอนิกส์ หรือกระเป๋าเงินอิเล็กทรอนิกส์ โดยไม่ได้มีเจตนาใช้เพื่อตน และห้ามไม่ให้ผู้ใดยินยอมให้บุคคลอื่นใช้หรือยืมใช้ซิมโทรศัพท์ของตนทั้งที่รู้หรือควรจะรู้ ซึ่งอาจจะนำไปใช้ในการทุจริตหรือทำผิดกฎหมาย ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ (บัญชีม้า)

7.2 ห้ามไม่ให้ผู้ใดเป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใดๆ เพื่อให้มีการซื้อหรือขายบัญชี บัตรอิเล็กทรอนิกส์ กระเป๋าเงินอิเล็กทรอนิกส์ หรือซิมโทรศัพท์ ซึ่งอาจก่อให้เกิดการกระทำความผิดอาญา ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกตั้งแต่ 2-5 ปี และปรับตั้งแต่ 200,0000-500,000 บาท หรือทั้งจำทั้.งปรับ (คนจัดหาบัญชีม้า)

อย่างไรก็ตาม ผู้เสียหายในคดีอาชญากรรมทางเทคโนโลยีสามารถแจ้งความที่สถานีตำรวจได้ทุกแห่งทั่วประเทศ หรือกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี หรือสามารถแจ้งธนาคารเจ้าของบัญชีตนเองเพื่ออายัดบัญชีคนร้ายได้ตามระบบปกติ

สรุปผลการศึกษาและข้อเสนอแนะ

จากที่ได้ทำการศึกษาเกี่ยวกับปัญหาความรับผิดทางกฎหมายเกี่ยวกับการหลอกลวงให้ทำธุรกรรมทางออนไลน์ ดังต่อไปนี้

1) บทสรุป

อาชญากรรมไซเบอร์นั้นคือ อาชญากรรมที่เกิดจากการกระทำความผิดทางเทคโนโลยีเป็นอาชญากรรมไซเบอร์ หรือ Cyber Crime ที่เกิดการทุจริต หลอกลวง หรือทำให้หลงเชื่อบนโลกอินเตอร์เน็ต และได้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ในช่องทางออนไลน์ประเภทต่างๆ เช่นบนเว็บไซต์ แพลตฟอร์มโซเชียลมีเดีย หรือแอปพลิเคชั่นบนมือถือ ได้ง่ายนับตั้งแต่อินเตอร์เน็ตเข้ามามีบทบาทในชีวิตของผู้คนในปัจจุบัน ทำให้อาชญากรรมทางไซเบอร์ได้พัฒนาตามวิวัฒนาการของเทคโนโลยีเช่นกัน

ซึ่งประเทศไทย มีแนวคิดในทางนิติวิธีเป็นระบบประมวลกฎหมาย (Civil law) โดยการ กระทำใดที่เป็นความผิดทางอาญา (Crime) และกระทบคุณธรรมทางกฎหมาย จะต้องบัญญัติความผิดและ มาตรการบังคับทางอาญาไว้ในประมวลกฎหมายอาญา ด้วยเหตุที่ว่ากฎหมายอาญาต้องการ “หลักความ ชัดเจนแน่นอน” อันเป็นหนึ่งในสี่ของหลักประกันในกฎหมายอาญา เนื่องจากการลงโทษทางอาญาเป็น มาตรการที่รุนแรงที่สุดของรัฐที่ใช้กับประชาชนในรัฐ และเป็นเรื่องที่กระทบต่อชีวิต และสิทธิเสรีภาพของ ประชาชนโดยตรง หากแต่ประเทศไทยกลับแยกบัญญัติความผิดเกี่ยวกับคอมพิวเตอร์ออกเป็น พระราชบัญญัติอีกฉบับหนึ่ง กลายเป็นจุดเริ่มต้นที่ทำให้มีปัญหาตามมา อีกทั้ง ฐานความผิดตามมาเพื่อให้เกิดข้อกฎหมายที่กระทำผิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 บางฐานมีลักษณะของการกระทำ ความผิดที่คล้ายคลึงกับฐานความผิดตามประมวลกฎหมายอาญาที่ได้บัญญัติไว้อยู่แล้ว ที่สามารถนำมาบังคับ ใช้ได้ การที่กฎหมายบัญญัติฐานความผิดที่ซ้ำซ้อนกันมี ความเหลื่อมล้ำของฐานความผิดที่กฎหมายกำหนด ที่สามารถให้การกระทำอย่างหนึ่งเข้าลักษณะความผิดได้หลายประการ ทำให้เกิดปัญหาความไม่แน่นอนใน การบังคับใช้กฎหมาย

ผู้ถูกหลอกลวงโหลดแอปพลิเคชั่นนั้นและถูกเข้าควบคุมโทรศัพท์ ซึ่งก่อให้เกิดผลความรับผิดในทางกฎหมายที่แตกต่างกัน ในทางอาญาผู้กระทำผิดมีความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญา การนำเข้าข้อมูลอันเป็นเท็จตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ส่วนผู้สนับสนุนย่อมมีความผิดตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ 2566.ศ.ส่วนความรับผิดทางแพ่งหากเป็นในกรณีที่ผู้เสียหายเป็นผู้ทำธุรกรรมทางการเงินด้วยตนเองแล้ว ถือว่าผู้เสียหายได้มีส่วนก่อให้เกิดความเสียหายด้วย แต่หากโทรศัพท์ถูกควบคุมจากบุคคลภายนอกแล้ว ผู้เสียหายไม่ได้มีส่วนก่อให้เกิดความเสียหาย สถาบันการเงินเจ้าของบัญชีเงินฝากจึงต้องชดใช้เงินเต็มจำนวน จึงมีข้อเสนอแนะในเชิงนโยบายให้สถาบันการเงินผู้เป็นเจ้าของบัญชีเงินฝากสร้างระบบป้องกันการทำธุรกรรมทางการเงินให้จำกัดเฉพาะเจ้าของบัญชีเงินฝาก ส่วนข้อเสนอแนะในเชิงกฎหมายควรมีกฎหมายเฉพาะเกี่ยวกับการหลอกลวงให้ทำธุรกรรมทางออนไลน์โดยมีขอบเขตความรับผิดทั้งในทางแพ่งและทางอาญา

2) ข้อเสนอแนะ

เพื่อไม่ให้การที่กฎหมายบัญญัติฐานความผิดที่ซ้ำซ้อนกันมี ความเหลื่อมล้ำของฐานความผิดที่กฎหมายกำหนดความรับผิด ที่สามารถให้การกระทำอย่างหนึ่งเข้าลักษณะความผิดได้หลายประการ ทำให้เกิดปัญหาความไม่แน่นอนใน การบังคับใช้กฎหมาย ควรมีบทบัญญัติว่าใครเป็นผู้เสียหายที่แท้จริง เนื่องจากการกระทำของผู้กระทำความผิดทางอาชญากรรมไซเบอร์ จะได้ไม่ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ในช่องทางออนไลน์ประเภทต่างๆ เช่นบนเว็บไซต์ แพลตฟอร์มโซเชียลมีเดีย หรือ แอปพลิเคชั่นบนมือถือบนโลกอินเตอร์เน็ต ในเชิงนโยบายให้สถาบันการเงินผู้เป็นเจ้าของบัญชีเงินฝากสร้างระบบป้องกันการทำธุรกรรมทางการเงินให้จำกัดเฉพาะเจ้าของบัญชีเงินฝาก ส่วนข้อเสนอแนะในเชิงกฎหมายควรมีกฎหมายเฉพาะเกี่ยวกับการหลอกลวงให้ทำธุรกรรมทางออนไลน์โดยมีขอบเขตความรับผิดทั้งในทางแพ่งและทางอาญา

เอกสารอ้างอิง

อัญชลี จวงจันทร์. (2562). อาชญากรรมไซเบอร์. เอกสารข่าวสานงานวิจัยและพัฒนา สำนักวิชาการ สำนัก งานเลขาธิการสภาผู้แทนราษฎร. หน้า 3-4.

ปรเมศวร์ กุมารบุญ. (2565). เริ่มต้นกับ อาชญากรรมไซเบอร์ (Introduction to Cyber crime). (ออนไลน์). เข้าถึงได้จาก: https://www.gotoknow.org/posts/623475. [2566, 2 มีนาคม].

สปริงนิวส์. (2565). เตือนภัย! แจ้งเตือนเพจเฟซบุ๊กปลอม กดกรอกโดนแฮกแน่. (ออนไลน์). เข้าถึงได้จาก: https://www.springnews.co.th/program/834046 [2566 , 4 มีนาคม].