มาตรการทางกฎหมายเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์: กรณีการเข้าถึงข้อมูลของบุคคลกระทำความผิดเกี่ยวกับธุรกรรมทางการเงินผ่านระบบออนไลน์

Legal Measures for Computer Crimes: In Case of Accessing Information of offenders involving with Online Financial Transactions

พันธรัตน์ ศรีสุวรรณ[1]* | Pantarat Srisuwan
พินิจ ศรีสวัสดิ์[2] | Pinit Srisawat

Abstract

Nowadays, technology is important in human life, especially the use of online media via mobile phones for communication. News awareness including various transactions via computer, making it convenient and fast when the victim receives damages from offenses involving with online financial transactions. It was found that the law on computer crimes still

[1, 2] อาจารย์, สาขาวิชานิติศาสตร์ คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏพระนครศรีอยุธยา; Lecturer, Program in Law, Faculty of Humanities and Social Sciences, Phranakhon Si Ayutthaya Rajabhat University

*Corresponding author email: Pantarat.sr@hotmail.com

รับต้นฉบับ: 22 กุมภาพันธ์ 2566 **ปรับแก้ต้นฉบับ:** 7 เมษายน 2566 **รับลงตีพิมพ์:** 18 เมษายน 2566
DOI: 10.14456/husoaru.2023.7

could not enforce the offenders. Although the state has measures to protect individual rights as provided in the Constitution of the Kingdom of Thailand, the state should update the law and speed up the implementation. Also, a special court should be established to hear computer-related cases.

Keywords: Computer Crimes, Information Access, Electronic Transactions

บทคัดย่อ

ปัจจุบันเทคโนโลยีมีความสำคัญในการดำรงชีวิตของมนุษย์ โดยเฉพาะการใช้สื่อออนไลน์ผ่านทางโทรศัพท์มือถือในการติดต่อสื่อสาร การรับรู้ข่าวสาร รวมถึงการทำธุรกรรมต่าง ๆ ทางคอมพิวเตอร์ทำให้ได้รับความสะดวกรวดเร็ว เมื่อผู้เสียหายได้รับความเสียหายจากการกระทำความผิดทางด้านธุรกรรมทางการเงินผ่านระบบออนไลน์ พบว่ากฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ยังไม่สามารถบังคับเอาผิดกับผู้กระทำความผิดได้ แม้รัฐจะมีมาตรการในเรื่องของการคุ้มครองสิทธิส่วนบุคคลตามที่บัญญัติไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทยไว้ ดังนั้น รัฐควรปรับปรุงกฎหมายให้มีความทันสมัยและส่งผลให้ทางปฏิบัติเป็นไปด้วยความรวดเร็ว และควรมีการจัดตั้งศาลพิเศษเพื่อพิจารณาคดีที่เกี่ยวกับคอมพิวเตอร์โดยเฉพาะ

คำสำคัญ: ความผิดทางคอมพิวเตอร์, การเข้าถึงข้อมูล, ธุรกรรมทางอิเล็กทรอนิกส์

บทนำ

ปัจจุบันเทคโนโลยีมีความสำคัญในการดำรงชีวิตของมนุษย์ โดยเฉพาะการใช้สื่อออนไลน์ผ่านทางโทรศัพท์มือถือในการติดต่อสื่อสาร การรับรู้ข่าวสาร รวมถึงการทำธุรกรรมต่าง ๆ ทางคอมพิวเตอร์ทำให้ได้รับความสะดวกรวดเร็วและประหยัดเวลามากขึ้น ในขณะเดียวกันการใช้สื่อออนไลน์ก็อาจมีอันตรายแฝงอยู่ เมื่อมีการใช้สื่อออนไลน์มากขึ้นก็เป็นการเปิดโอกาสให้มิจฉาชีพได้กระทำความผิดทางออนไลน์เพิ่มมากขึ้น

จากข้อมูลสำนักงานตำรวจแห่งชาติได้พัฒนาระบบการรับแจ้งความออนไลน์ www.ThaiPoliceOnline.com ซึ่งช่วยให้ประชาชนเข้าถึงกระบวนการสืบสวนสอบสวนอย่างทั่วถึง นับตั้งแต่วันที่ระบบเริ่มใช้งาน 1 มีนาคม 2565 ถึง 31 ธันวาคม 2565 รวม 10 เดือน มีผู้เข้ามาแจ้งความจำนวน 163,091 คดี ได้แก่ คดีที่ผู้กระทำความผิดอยู่ในประเทศไทย เช่น การซื้อขายสินค้าหรือบริการผ่านทางออนไลน์แต่ไม่ได้รับสินค้า การปล่อยกู้ผ่านแอปพลิเคชันนอกระบบ การลงทุนแบบแชร์ลูกโซ่ เป็นต้น มีสถิติการรับแจ้งประมาณร้อยละ 40.5 คดีที่ผู้กระทำความผิดอยู่ต่างประเทศ และมีคนไทยร่วมขบวนการ โดยเดินทางไปทำงานผ่านช่องทางธรรมชาติ เพื่อไปทำหน้าที่เป็นแก๊งคอลเซ็นเตอร์หลอกลวงคนไทยผ่านทางออนไลน์ด้วยวิธีการต่าง ๆ ซึ่งเป็นกลุ่มคดีที่มีมูลค่าความเสียหายมากที่สุด ประมาณร้อยละ 51 และคดีอื่น ๆ ร้อยละ 8.5 เช่น แฮ็กระบบคอมพิวเตอร์ การเรียกค่าไถ่ทางคอมพิวเตอร์ การคุกคามทางเพศ หลอกให้ไปทำงานต่างประเทศ เป็นต้น (เร่งแก้ปัญหา ‘อาชญากรรมออนไลน์’ อายัดบัญชีม้าแล้ว 5.8 หมื่นบัญชี, 2566)

การกระทำความผิดทางคอมพิวเตอร์มีการกระทำความผิดในรูปแบบที่แตกต่างกันและมีแนวโน้มเพิ่มสูงขึ้น โดยเฉพาะการกระทำความผิดทางด้านธุรกรรมทางการเงินผ่านระบบออนไลน์ ซึ่งปัจจุบันมีผู้เสียหายหลายรายถูกแฮ็กข้อมูลทางการเงินและถูกคนร้ายขโมยเงินผ่านแอปพลิเคชันของธนาคารจนหมดบัญชี โดยเกิดจากการที่ผู้เสียหายถูกมิจฉาชีพสร้างกลอุบายหลอกลวงให้กดลิงก์ดาวน์โหลด หรือติดตั้งแอปพลิเคชันปลอม โดยเฉพาะอย่างยิ่งแอปพลิเคชันที่มีไว้สำหรับการหาคู่ แอปพลิเคชันดูไลฟ์สด ดูภาพลามกอนาจาร และแอปพลิเคชันพูดคุยยอดนิยม เช่น Viber, Sweet meet, Bumble, Snapchat, Kakao Talk และ Flower Dating เป็นต้น (ตำรวจไซเบอร์ เผยเหยื่อถูกมิจฉาชีพลวง กดลิงก์โหลดแอปฯปลอมดูดเงินเกลี้ยงบัญชี, 2566)

ดังนั้น เมื่อผู้เสียหายได้รับความเสียหายจากการกระทำความผิดทางด้านธุรกรรมทางการเงินผ่านระบบออนไลน์ จึงจำเป็นที่จะต้องนำกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มาบังคับใช้เอาผิดกับผู้กระทำความผิด โดยเจตนารมณ์ของกฎหมายเพื่อป้องกันปราบปรามอาชญากรรมที่เกิดจากการใช้วิธีการใด ๆ เข้าไปล่วงรู้

ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ ก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคมและความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน ในทางปฏิบัติเมื่อผู้เสียหายได้รับความเสียหายจากการกระทำความผิดทางด้านธุรกรรมทางการเงินผ่านระบบออนไลน์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์สามารถบังคับเอาผิดกับผู้กระทำความผิดได้มากน้อยเพียงใด มีปัจจัยใดบ้างที่ส่งผลกระทบต่อการนำกฎหมายไปปฏิบัติ และประชาชนผู้ได้รับความเสียหายมีกฎหมายให้หลักประกันเกี่ยวกับสิทธิและเสรีภาพในเรื่องของการใช้บริการการทำธุรกรรมทางการเงินผ่านระบบออนไลน์ได้เพียงพอหรือไม่

บทความนี้กล่าวถึงประเด็นสำคัญเกี่ยวกับแนวคิดทางกฎหมายเกี่ยวกับหลักประกันสิทธิเสรีภาพในเรื่องของการทำธุรกรรมทางการเงินผ่านระบบออนไลน์ ประเด็นทางกฎหมายเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ ขั้นตอนการดำเนินคดีและหน่วยงานผู้รับผิดชอบ ข้อเสนอแนะทางกฎหมายถึงแนวทางในการป้องกันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์กรณีการทำธุรกรรมทางการเงินผ่านระบบออนไลน์ ซึ่งจะได้พิจารณาเป็นลำดับ ดังนี้

1. แนวคิดทางกฎหมายเกี่ยวกับหลักประกันสิทธิเสรีภาพเกี่ยวกับสิทธิความเป็นส่วนตัว

“สิทธิความเป็นส่วนตัว” (Right of privacy) คือ การดำเนินชีวิตของบุคคลในสังคมโดยปราศจากการถูกรบกวน หรือการนำข้อมูลไปเปิดเผยต่อสาธารณชน ก่อให้เกิดความเสียหายและส่งผลกระทบต่อการดำเนินชีวิต หรือสูญเสียศักดิ์ศรีในความเป็นตัวเองในการดำเนินชีวิต โดยคำนึงถึงสภาพการปกครองในสังคม เศรษฐกิจ วัฒนธรรม และเทคโนโลยีมาเป็นองค์ประกอบ (ทิพาพร นะมาตร์, 2550: 10)

สิทธิความเป็นอยู่ส่วนตัวเป็นสิทธิที่ติดตัวมาตั้งแต่เกิด เป็นหนึ่งในสิทธิมนุษยชนและเป็นสิทธิขั้นพื้นฐานของมนุษย์ที่ได้รับการรับรองไว้ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 (Universal Declaration of Human Right 1948) ในมาตรา 12 บัญญัติว่า *“บุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นส่วนตัว ในครอบครัวในเคหสถาน หรือในการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่*

จะได้รับความคุ้มครองตามกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น” โดยสิทธิมนุษยชนในปฏิญญาสากลฉบับนี้มีความหมายกว้างขวางครอบคลุมถึงสิทธิอื่น ๆ ไม่ว่าจะเป็น สิทธิความเป็นส่วนตัวในข้อมูลส่วนบุคคล (Information privacy) สิทธิความเป็นส่วนตัวในชีวิตร่างกาย (Bodily privacy) สิทธิความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication privacy) สิทธิความเป็นส่วนตัวในอาณาเขตหรือสถานที่ของตนเอง (Territorial privacy) ซึ่งความเป็นส่วนตัวเหล่านี้กลายเป็นหลักการพื้นฐานที่ได้รับการยอมรับกันทั่วไป (ภาระวี ปุณเสรีพิพัฒน, 2557) ซึ่งสิทธิส่วนบุคคลดังกล่าวจะต้องได้รับการคุ้มครองตามกฎหมาย ดังนี้ (บรรเจิด สิงคะเนติ, นนทวัชร์ นวตระกูลพิสุทธิ์ และเรวดี ขวัญทองยิ้ม, 2554)

1) สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล เป็นสิทธิส่วนบุคคลที่เกี่ยวข้องกับบุคคลธรรมดาอาจเป็นทางตรงหรือโดยอ้อม อาทิ การระบุหมายเลขประชาชน หรือองค์ประกอบที่เป็นเอกลักษณ์ของบุคคล เช่น ชื่อ นามสกุล วันเดือนปีเกิด ลายพิมพ์นิ้วมือ ดีเอ็นเอ เป็นต้น ซึ่งประชาชนจะได้รับความคุ้มครองจากการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคล

2) สิทธิความเป็นส่วนตัวในชีวิตร่างกาย เป็นการให้ความคุ้มครองในชีวิตร่างกายของบุคคลในทางกายภาพที่จะไม่ถูกดำเนินการใด ๆ อันละเมิดความเป็นส่วนตัว เช่น การทดลองยา การทดลองทางพันธุกรรม เป็นต้น

3) สิทธิความเป็นส่วนตัวในการติดต่อสื่อสาร เป็นการให้ความคุ้มครองในความปลอดภัย และความเป็นส่วนตัวในการติดต่อสื่อสารทางจดหมาย โทรศัพท์ หรือวิธีการสื่อสารอื่นใดที่ผู้อื่นจะล่วงรู้มิได้

4) สิทธิความเป็นส่วนตัวในอาณาเขตหรือสถานที่ของตนเอง เป็นการกำหนดขอบเขตหรือข้อจำกัดที่บุคคลอื่นจะรุกล้ำเข้าไปในอาณาเขตแห่งสถานที่ส่วนตัวมิได้

หลักการคุ้มครองข้อมูลส่วนบุคคลนอกจากจะได้รับการคุ้มครองตามปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 (Universal Declaration of Human Right 1948) แล้ว ยังมีการยอมรับหลักการคุ้มครองข้อมูลส่วนบุคคลในกติการะหว่างประเทศและกฎหมายระหว่างประเทศ ได้แก่ หลักการคุ้มครองข้อมูลส่วนบุคคลตามแนวทางของ

องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) โดยมีการจัดทำข้อมูลในการคุ้มครองข้อมูลส่วนบุคคลที่เรียกว่า Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (นคร เสรีรักษ์, 2562) หรือ หลักการคุ้มครองข้อมูลส่วนบุคคลตามแนวทางของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation: GDPR) (ปัทมา มัญชุนากร, 2565) หรือ หลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษ คือ กฎหมายคุ้มครองข้อมูลส่วนบุคคล Data Protection Act 1998 (บุญญรัตน์ โชคบันดาลชัย, 2561) หรือ หลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศส คือ รัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ. 1978 ว่าด้วยข้อมูล สารสนเทศ แฟ้มข้อมูล และเสรีภาพ (The Act on Data Processing Data Files and Individual Liberties) เป็นต้น (นพดล นิ่มหนู, 2565)

สำหรับประเทศไทย รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ได้สร้างหลักประกันการคุ้มครองสิทธิและเสรีภาพของบุคคลในเรื่องสิทธิส่วนบุคคลหรือสิทธิส่วนตัวในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 32 ซึ่งบัญญัติไว้ว่า

“บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ”

จากบทบัญญัติมาตรา 32 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 เห็นได้ชัดว่ากฎหมายได้ให้ประกันถึงสิทธิและเสรีภาพของบุคคลซึ่งข้อมูลส่วนบุคคลเป็นสิทธิส่วนบุคคล โดยเฉพาะกฎหมายให้หลักประกันของบุคคลในเรื่องของการนำข้อมูลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ ไม่สามารถทำได้ ซึ่งแนวคิดเรื่องความเป็นส่วนตัวเป็นหลักสากลที่ให้หลักประกันการคุ้มครองสิทธิและเสรีภาพของประชาชนไว้

จะเห็นได้ว่า ปัจจุบันความเจริญก้าวหน้าทางเทคโนโลยีสารสนเทศเป็นไปอย่างรวดเร็ว และการเข้าถึงข้อมูลออนไลน์ในการทำธุรกรรมต่าง ๆ เป็นไปอย่างง่ายดายและ

สะดวก เมื่อการทำธุรกรรมต่าง ๆ สามารถทำได้ง่ายและรวดเร็ว ส่งผลทำให้มิจฉาชีพแฝงตัวเข้าไปกระทำละเมิดต่อประชาชนในการล่วงล้ำข้อมูลส่วนบุคคลได้ง่ายเช่นเดียวกัน ดังนั้น แนวคิดเรื่องการให้หลักประกันการคุ้มครองสิทธิเสรีภาพในการคุ้มครองสิทธิส่วนบุคคลจึงเป็นสิ่งที่มีความสำคัญที่ทุกประเทศให้หลักประกันแก่ประชาชนไว้ และเป็นสิ่งที่ทุกประเทศต้องตระหนัก โดยเฉพาะการเตรียมความพร้อมในการรับมือกับการพัฒนาทางด้านเทคโนโลยีในปัจจุบันมีการขับเคลื่อนเป็นไปอย่างรวดเร็วและก้าวกระโดด หากไม่มีมาตรการที่เพียงพอในการคุ้มครองสิทธิส่วนบุคคลก็จะทำให้ประชาชนถูกละเมิดและก่อให้เกิดความเสียหายต่อประชาชน สังคม โดยเฉพาะความมั่นคงทางด้านเศรษฐกิจและสังคมของประเทศ

2. ประเด็นทางกฎหมายเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์

สำหรับการกระทำความผิดทางด้านธุรกรรมทางการเงินผ่านระบบออนไลน์เมื่อมีการกระทำความผิดเกิดขึ้น จึงจำเป็นที่จะต้องนำกฎหมายที่เกี่ยวข้องกับการกระทำความผิดทางคอมพิวเตอร์มาบังคับใช้ โดยกฎหมายที่เกี่ยวข้อง ดังนี้

2.1 ที่มาและความสำคัญของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์จึงมีวัตถุประสงค์เพื่อสร้างความตระหนักถึงความปลอดภัยด้านสารสนเทศเพื่อป้องกันควบคุมการกระทำผิดที่จะเกิดขึ้นได้จากการใช้คอมพิวเตอร์ จึงกำหนดกฎหมายเกี่ยวกับมาตรการเพื่อป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ขึ้น โดย

บัญญัติไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550

ต่อมา รูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้นตามพัฒนาการทางเทคโนโลยีซึ่งเปลี่ยนแปลงอย่างรวดเร็ว และโดยที่มีการจัดตั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมซึ่งมีภารกิจในการกำหนดมาตรฐานและมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของประเทศ จึงมีการแก้ไขปรับปรุงบทบัญญัติเพิ่มเติมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

2.2 นิยามความหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550, 2550: มาตรา 3)

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550, 2550: มาตรา 3)

ดังนั้น ข้อมูลคอมพิวเตอร์ คือ ข้อมูลทุกอย่างที่อยู่ในระบบคอมพิวเตอร์ รวมทั้งชุดคำสั่งด้วย หากอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลได้ นอกจากนั้นยังให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ด้วย โดยข้อมูลอิเล็กทรอนิกส์อยู่ในความหมายของข้อมูลคอมพิวเตอร์ แต่เพื่อให้ครอบคลุมถึงข้อมูลประเภทอื่น ๆ ที่อาจสร้างด้วยวิธีการทางอิเล็กทรอนิกส์ในอนาคตที่ไม่ใช่คอมพิวเตอร์ โดย **“ข้อมูลอิเล็กทรอนิกส์”**

หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร (พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พุทธศักราช 2544, 2544: มาตรา 4) อย่างไรก็ตาม องค์ประกอบความผิดตามพระราชบัญญัติส่วนใหญ่จะเชื่อมโยงองค์ประกอบความผิด “ข้อมูลคอมพิวเตอร์” กับ “ระบบคอมพิวเตอร์” เข้าด้วยกัน ซึ่งจะได้กล่าวต่อไป

2.3 ฐานความผิด องค์ประกอบความผิดและบทกำหนดโทษ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 บัญญัติให้การกระทำที่เป็นความผิดและกำหนดบทลงโทษไว้ในหมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์ ตั้งแต่มาตรา 5 ถึงมาตรา 16 โดยกำหนดองค์ประกอบความผิดและบทลงโทษไว้ ซึ่งการกระทำความผิดที่เกี่ยวกับความผิดทางด้านธุรกรรมทางการเงินผ่านระบบออนไลน์ ดังนี้

2.3.1 ความผิดฐานการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ

มาตรา 5 บัญญัติว่า *“ผู้ใด**เข้าถึง**โดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้น มิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ”* (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550, 2550: มาตรา 5) โดยมีองค์ประกอบความผิด ดังนี้

องค์ประกอบความผิดประการแรก คือ “การเข้าถึง”

การเข้าถึง (Access) หมายถึง การเข้าถึงทั้งในระดับกายภาพ เช่น กรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์ และผู้กระทำความผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมา รวมถึงการเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์ แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์ แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการได้ (พรเพชร วิชิตชลชัย, ม.ป.ป.)

ดังนั้น เมื่อบุคคลใดได้เข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ อาจจะเข้าเพียงบางส่วนหรือทั้งหมดก็มีความผิดตามความหมายนี้ โดยในการเข้าถึงนั้นอาจเป็นการเข้าถึงฮาร์ดแวร์ หรือส่วนประกอบต่าง ๆ ของคอมพิวเตอร์ หรือข้อมูลที่บันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงบุคคลอื่น โดยวิธีการเข้าถึงนั้นรวมทุกวิธีการ ไม่ว่าจะเข้าถึงโดยผ่านทางเครือข่ายอินเทอร์เน็ต หรือการเข้าถึงโดยผ่านระบบเครือข่ายด้วยกัน เช่น ระบบ LAN อันเป็นเครือข่ายที่มีการเชื่อมต่อในพื้นที่ใกล้ ๆ เข้าด้วยกัน และรวมถึงการเข้าถึงโดยการติดต่อสื่อสารแบบไร้สาย เป็นต้น

องค์ประกอบความผิดประการที่สอง คือ “โดยมิชอบ”

การกระทำจะผิดความผิดฐานเข้าถึงระบบคอมพิวเตอร์ตามมาตรานี้ต้องเป็นการเข้าถึงโดยมิชอบ กล่าวคือ เป็นการเข้าถึงโดยปราศจากสิทธิโดยชอบธรรม หากผู้กระทำการเข้าถึงข้อมูลได้รับอนุญาตให้ทำการเข้าถึงนั้นได้เข้าถึงระบบหรือข้อมูลคอมพิวเตอร์เกินกว่าที่ตนได้รับอนุญาต ก็จะมีความผิดมาตรานี้เช่นกัน เช่น การเข้าถึงเพื่อดูแลระบบของผู้ดูแลเว็บ เป็นต้น (พรเพชร วิชิตชลชัย, ม.ป.ป.)

องค์ประกอบความผิดประการที่สาม คือ “ระบบคอมพิวเตอร์”

ในคำนิยามของคำว่า “ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ ดังนั้น การจะกระทำความผิดตามมาตรานี้จะต้องเป็นการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบด้วยกฎหมายจึงจะมีความผิดตามมาตรานี้

องค์ประกอบความผิดประการที่สี่ คือ “ระบบคอมพิวเตอร์ที่มีวิธีการป้องกันการเข้าถึงโดยเฉพาะ”

การกระทำจะผิดความผิดฐานการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบนั้น ต้องเป็นการเข้าถึงระบบคอมพิวเตอร์ที่มีวิธีการป้องกันการเข้าถึงโดยเฉพาะ เช่น มีการกำหนดรหัสการเข้าถึงข้อมูล แต่หากเจ้าของไม่ได้หวงแหนการเข้าถึงนั้นก็จะไม่มีความผิดฐานนี้

องค์ประกอบความผิดประการที่ห้า คือ “เจตนา”

นอกจากองค์ประกอบภายนอกทั้งสี่ประการที่เป็นองค์ประกอบภายนอกแล้ว การกระทำความผิดที่จะมีความผิดฐานการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบนั้น ต้องคำนึงถึงองค์ประกอบภายในในเรื่อง “เจตนา” ตามประมวลกฎหมายอาญามาตรา 59 ด้วย โดยมีเจตนาที่จะกระทำความผิดโดยการเข้าถึงข้อมูลคอมพิวเตอร์ของบุคคลที่มีวิธีการเข้าถึงโดยเฉพาะ เมื่อบุคคลได้กระทำการเข้าไปล่วงล้ำสิทธิส่วนบุคคลและทำให้เกิดความเสียหาย บุคคลดังกล่าวจะมีความผิดฐานนี้ โดยในการกระทำความผิดมีหลายกรณี เช่น การเข้าเจาะระบบ (Hacking or cracking) หรือการบุกรุกทางคอมพิวเตอร์ (Computer trespass) การกระทำการเป็นการขัดขวางการใช้ระบบคอมพิวเตอร์โดยชอบของบุคคลอื่นอันอาจทำให้เกิดการเปลี่ยนแปลงแก้ไข หรือทำงานระบบคอมพิวเตอร์ได้โดยปกติ

จะเห็นได้ว่า จากการกระทำของมิจฉาชีพที่มีการล่วงล้ำข้อมูลของบุคคลโดยได้ทำธุรกรรมทางการเงินถอนเงินออกจากแอปพลิเคชันธนาคาร การกระทำดังกล่าวเป็นการกระทำที่ครบองค์ประกอบความผิดและมีความผิดฐานการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ กล่าวคือ การกระทำของมิจฉาชีพเป็นการเข้าถึงโดยมิชอบ ซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะจึงต้องรับโทษตามความผิดฐานนี้

2.3.2 ความผิดฐานการเข้าถึงข้อมูลคอมพิวเตอร์

มาตรา 7 บัญญัติว่า *“ผู้ใด**เข้าถึง**โดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้น มิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ”*

สำหรับองค์ประกอบในความผิดฐานนี้มีลักษณะเช่นเดียวกันกับความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ โดยในการเข้าถึงข้อมูลคอมพิวเตอร์นี้ เป็นการเข้าถึงข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย การกระทำความผิดฐานนี้ไม่รวมถึงการเข้าถึงข้อมูลที่เป็นการบรรจุไว้ในแผ่นซีดี หรือแผ่นดิสก์ (พรเพชร วิชิตชลชัย, ม.ป.ป.)

2.3.3 ความผิดฐานทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ

มาตรา 9 บัญญัติว่า *"ผู้ใดทำให้เสียหาย ทำลาย แก้ไขเปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ"* โดยมีองค์ประกอบความผิด ดังนี้

องค์ประกอบความผิดประการแรก คือ "กระทำการอันเป็นการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลงเพิ่มเติมโดยมิชอบข้อมูลคอมพิวเตอร์ของผู้อื่น"

การกระทำความผิดฐานนี้ได้ต้องเป็นการกระทำที่มีการเข้าไปในข้อมูลคอมพิวเตอร์ของผู้อื่น และการเข้าไปนั้นเป็นการเข้าไปโดยมิชอบ โดยทำให้เกิดความเสียหายแก่เจ้าของข้อมูล นอกจากทำให้เจ้าของข้อมูลได้รับความเสียหายแล้ว หากเป็นการแก้ไขหรือทำลาย หรือเปลี่ยนแปลง หรือเพิ่มเติมข้อมูลก็มีความผิดฐานนี้

องค์ประกอบความผิดประการที่สอง คือ "เจตนา"

นอกจากองค์ประกอบภายนอกแล้ว การกระทำความผิดที่จะมีความผิดฐานทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบนั้น ต้องคำนึงถึงองค์ประกอบภายในในเรื่อง "เจตนา" ตามประมวลกฎหมายอาญามาตรา 59 ด้วย โดยการกระทำความผิดตามมาตรานี้ เช่น การป้อนข้อมูลที่มีไวรัสทำลายข้อมูลหรือโปรแกรมคอมพิวเตอร์ หรือการป้อน Trojan Horse เข้าไปในระบบเพื่อขโมยรหัสผ่านของผู้ใช้คอมพิวเตอร์สำหรับเพื่อเข้าไปลบ เปลี่ยนแปลงข้อมูล แก้ไขข้อมูลหรือกระทำการใด ๆ อันเป็นการรบกวนข้อมูล

จะเห็นได้ว่า มิจฉาชีพผู้แฮ็กข้อมูลจะมีการกระทำเป็นการที่ทำให้เกิดความเสียหายแก่เจ้าของข้อมูล โดยการที่ผู้เป็นเจ้าของข้อมูลทำการโหลดแอปพลิเคชันที่มีปัญหาเข้าไปในระบบคอมพิวเตอร์ โดยบุคคลดังกล่าวเข้าไปในระบบคอมพิวเตอร์เพื่อที่จะขโมยรหัสผ่านของเจ้าของข้อมูล กระทำการแก้ไข หรือการกระทำการถอนเงินอันเป็นการกระทำที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลจึงมีความผิดฐานนี้

2.3.4 ความผิดฐานกระทำการเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานตามปกติได้

มาตรา 10 บัญญัติว่า *"ผู้ใดกระทำด้วยประการใดโดยมิชอบเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวน จนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท"* โดยมีองค์ประกอบความผิดดังนี้

องค์ประกอบความผิดประการแรก คือ "กระทำด้วยประการใดโดยมิชอบ"

การกระทำใดโดยมิชอบ หมายถึง การกระทำใด ๆ ที่มีความหมายกว้าง และการกระทำนั้นเป็นการกระทำอาชญากรรมทางคอมพิวเตอร์ การกระทำนี้เป็นการกระทำที่เข้าไปทำกับระบบคอมพิวเตอร์และรวมถึงการเข้าไปกระทำทางกายภาพด้วย

องค์ประกอบความผิดประการที่สอง คือ "มีเจตนาเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวน จนไม่สามารถทำงานตามปกติได้"

กล่าวคือ ผู้กระทำต้องมีเจตนาที่จะทำให้เกิดความเสียหายและเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานได้ตามปกติ อันเป็นการกระทำที่ทำให้การทำงานของระบบคอมพิวเตอร์ไม่สมบูรณ์หรือผิดปกติไป เช่น การป้อนโปรแกรมที่ทำให้ระบบคอมพิวเตอร์ปฏิเสธการทำงาน หรือทำให้ระบบคอมพิวเตอร์ทำงานได้ช้าลง อันเกิดผลกับระบบ

จะเห็นได้ว่า ในการกระทำความผิดทางคอมพิวเตอร์ของมิจฉาชีพที่ทำการแฮกข้อมูลของเจ้าของ ได้ทำการเข้าถึงระบบคอมพิวเตอร์และทำให้ระบบการทำงานของระบบคอมพิวเตอร์ระงับ หรือทำให้เจ้าของไม่สามารถใช้งานระบบคอมพิวเตอร์ได้ แสดงให้เห็นว่ามิจฉาชีพมีความผิดฐานนี้ด้วย เนื่องจากเป็นการกระทำโดยมิชอบ และมีเจตนาทำให้ระบบคอมพิวเตอร์ของบุคคลอื่นถูกระงับ หรือมีการรบกวนจนไม่สามารถใช้งานได้อย่างเป็นปกติ

เมื่อพิจารณาการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ว่าด้วยการเข้าถึงข้อมูลของบุคคลกระทำความผิดเกี่ยวกับธุรกรรมทางการเงินผ่านระบบออนไลน์ สามารถพิจารณาความรับผิดได้ 2 ลักษณะ ดังนี้

1) ความรับผิดทางอาญา โดยพิจารณาความรับผิดทางอาญาระหว่างผู้กระทำกระทำความผิดกับผู้เสียหาย กล่าวคือ เมื่อผู้กระทำความผิดได้เข้าไปในข้อมูลของบุคคลอื่นโดยมิชอบ ซึ่งมีมาตรการในการป้องกันคือการเข้าโดยใช้รหัสผ่านส่วนบุคคล โดยการเข้าไปถอนเงินในบัญชีแอปพลิเคชันธนาคาร ทำให้ผู้เสียหายไม่สามารถใช้งานดังกล่าวได้ปกติและก่อให้เกิดความเสียหายทำให้ไม่มีเงินในบัญชีเหลืออยู่ การกระทำดังกล่าวเป็นความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญามาตรา 334 และการกระทำดังกล่าวต้องรับโทษหนักขึ้นเนื่องจากการลักทรัพย์นั้นเป็นการแปลงตัวหรือปลอมตัวเป็นบุคคลอื่นตามมาตรา 335 (5) และยังมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ในฐานความผิดฐานการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบตามมาตรา 5 ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ตามมาตรา 7 ความผิดฐานทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบตามมาตรา 9 และความผิดฐานการกระทำการเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ปกติ ตามมาตรา 10

นอกจากนี้ศาลได้มีคำพิพากษาในคดีอาญา คดีหมายเลขดำที่ อ.912/55 คดีปรากฏว่าจำเลยบังอาจใช้ข้อมูลหมายเลข 16 หลัก ที่ปรากฏบนหน้าบัตรเอทีเอ็ม พร้อมรหัสลับที่ใช้ถอนเงินของธนาคารไทยพาณิชย์ จำกัด (มหาชน) ที่ออกให้แก่ลูกค้าซึ่งเป็นผู้เสียหายอีก 4 ราย แล้วจำเลยนำไปสมัครขอใช้บริการ SCB EASY NET โดยกำหนดชื่อประจำตัว และรหัสผ่านด้วยตนเองตามขั้นตอนและวิธีการที่ธนาคารฯ กำหนด เป็นเหตุให้ธนาคารฯ หลงเชื่อว่าจำเลยเป็นผู้เสียหาย 4 ราย จึงออกชื่อประจำตัวผู้ใช้ให้ จากนั้นจำเลยได้นำชื่อประจำตัวของผู้เสียหาย และรหัสผ่านไปโอนเงินจากบัญชีผู้เสียหายเพื่อใช้ชำระค่าสินค้า หรือบริการทางอินเทอร์เน็ตหลายครั้ง ซึ่งเป็นร้านค้าต่างประเทศรวม 4 ครั้ง เป็นเงินจำนวน 368,800 บาท ต่อมาเจ้าหน้าที่ตำรวจกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรรมทางเทคโนโลยี (ปอท.) ติดตามจับกุมได้ พร้อมให้

การรับสารภาพ เหตุเกิดที่แขวงและเขตจตุจักร กทม. และที่อื่นเกี่ยวพันกัน จำเลยให้การรับสารภาพ

ศาลพิเคราะห์แล้วเห็นว่า จำเลยกระทำผิดตามประมวลกฎหมายอาญา มาตรา 269/5 ประกอบมาตรา 269/7, 334,335 พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 5, 7, 9 เป็นความผิดหลายกรรมให้ลงโทษทุกกรรม ฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ 5 กระทง จำคุกกระทงละ 9 เดือน เป็นจำคุก 3 ปี 9 เดือน ฐานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกัน ทำลาย แก้ไข เปลี่ยนแปลงเพิ่มเติม ทำให้เกิดความเสียหายฯ 4 กระทง จำคุกกระทงละ 2 ปี เป็นจำคุก 8 ปี และฐานลักทรัพย์ฯ จำคุกกระทงละ 2 ปี จำนวน 5 กระทง เป็นจำคุก 10 ปี รวมจำคุกจำเลย 21 ปี 9 เดือน คำรับสารภาพเป็นประโยชน์ลดโทษให้กึ่งหนึ่ง คงจำคุกจำเลยไว้ 10 ปี 10 เดือน 15 วัน และให้จำเลยชดใช้เงินคืนจำนวน 368,800 บาทแก่ผู้เสียหายด้วย

2) ความรับผิดทางแพ่ง โดยพิจารณาความรับผิดทางแพ่งระหว่างผู้เสียหาย (ผู้ฝากเงิน) กับธนาคาร (ผู้รับฝาก) กล่าวคือ เมื่อผู้เสียหายได้มีการนำเงินไปฝากเงินกับธนาคาร ซึ่งตามสัญญาดังกล่าวเป็นสัญญารับฝากเงินตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 672 บัญญัติว่า *“ถ้าฝากเงิน ท่านให้สันนิษฐานไว้ก่อนว่าผู้รับฝากไม่พึงต้องส่งคืนเป็นเงินทองตราอันเดียวกับที่ฝากนั้นออกใช้ก็ได้ แต่หากจำต้องคืนเงินให้ครบจำนวนเท่านั้น แม้ว่าเงินซึ่งฝากนั้นจะได้สูญหายไปด้วยเหตุสุดวิสัยก็ตาม ผู้รับฝากก็จำต้องคืนเงินเป็นจำนวนดังว่านั้น”* กล่าวคือ กรรมสิทธิ์ในการเงินที่รับฝากนั้นตกเป็นของผู้ที่รับฝากก็ตาม แต่เมื่อพิจารณาจากหลักกฎหมายเรื่องฝากทรัพย์ วิธีเฉพาะการฝากเงิน และหลักกฎหมายทั่วไป ให้ผู้เป็นเจ้าของต้องรับบาปเคราะห์ที่เกิดแก่ตัวทรัพย์ เท่ากับว่าเมื่อผู้รับฝากต้องรับผิดชอบต่อเงินฝากที่สูญหายโดยไม่อาจอ้างเหตุสุดวิสัยมาเป็นข้อยกเว้นความรับผิดได้ ตามหลัก Res Perit Domino จึงเท่ากับว่าผู้รับฝากเงินตกอยู่ในฐานะเจ้าของกรรมสิทธิ์นั่นเอง (ปองปรัชญ์ เกศาสุวรรณ, จักรพงศ์ ลิ้มสุวรรณ และสุธิดา ผิวขาว, 2562) จะเห็นได้ว่าเมื่อธนาคารเป็นผู้รับฝากเงินตามสัญญาการฝากเงิน เมื่อผู้เสียหายได้รับความเสียหายจากการกระทำความผิด โดยมีผู้เข้าถึงระบบ

คอมพิวเตอร์เข้าไปในบัญชีของผู้เสียหายทำการถอนเงิน ตามประมวลกฎหมายแพ่งและพาณิชย์มาตรา 672 ธนาคารผู้รับฝากจึงต้องรับผิดในความเสียหายดังกล่าว

คำพิพากษาฎีกาที่ 6233/2564 จำเลยประกอบกิจการธนาคารพาณิชย์ และให้บริการอื่นที่เกี่ยวกับการเงิน รับฝากเงิน และให้บริการการใช้หรือโอนเงินทาง Application online ผ่านโทรศัพท์เคลื่อนที่และคอมพิวเตอร์ จึงเป็นการรับฝากซึ่งเป็นผู้มีวิชาชีพเฉพาะกิจการค้าขายหรืออาชีวะ จำต้องใช้ความระมัดระวังและใช้ฝีมือเท่าที่เป็นธรรมดาจะต้องใช้และสมควรจะต้องใช้ในกิจการค้าขายหรืออาชีวะอย่างนั้น ตามประมวลกฎหมายแพ่งและพาณิชย์มาตรา 659 วรรคสาม ปรากฏว่าเงินในบัญชีเงินฝากของโจทก์ถูกโอนไปยังบัญชีเงินฝากของผู้อื่นจำนวน 3 บัญชี รวม 12 ครั้ง รวมเป็นเงิน 1,099,999 บาท การโอนเงินที่เป็นการโอนจำนวนย่อยหลายครั้งติดต่อกันในช่วงเวลาเดียวกันในเวลากลางคืน ย่อมเป็นพฤติกรรมในการทำธุรกรรมทางการเงินที่ผิดปกติ การที่จำเลยแจ้งเตือนให้แก่ลูกค้าผู้ใช้บริการต่าง ๆ ระมัดระวังอีเมล์หลอกลวงจากมิจฉาชีพหรือที่เรียกว่า Phishing email มาตลอด โดยโจทก์เป็นผู้ใช้บริการก็ได้ทำธุรกรรมทางการเงินอิเล็กทรอนิกส์ผ่านทางอินเทอร์เน็ตหลายครั้ง โจทก์ย่อมมีความเข้าใจในการทำธุรกรรมทางการเงินผ่านช่องทางดังกล่าว และย่อมทราบถึงคำเตือนของจำเลยตามที่ปรากฏในคดีนี้ จึงถือว่าโจทก์มีส่วนทำให้เกิดความเสียหายด้วย พฤติกรรมของโจทก์และจำเลยจึงถือว่ามีส่วนทำให้เกิดความเสียหายในคดีนี้ไม่ยิ่งหย่อนกว่ากัน และเห็นสมควรกำหนดให้จำต้องรับผิดชดใช้เงินให้แก่โจทก์เป็นเงิน 550,000 บาท เมื่อค่าเสียหายที่จำเลยต้องรับผิดเป็นหนี้เงิน หากชำระล่าช้าย่อมก่อให้เกิดความเสียหายแก่โจทก์ซึ่งค่าเสียหายของหนี้เงินตามปกติย่อมคิดกันในรูปแบบดอกเบี้ย จึงเห็นควรกำหนดให้จำเลยรับผิดดอกเบี้ยดังกล่าวนับแต่วันที่อ่านคำพิพากษาฎีกาเป็นต้นไป ทั้งนี้ตามป.พ.พ. มาตรา 222 วรรคหนึ่ง โดยควรให้ในอัตราเดียวกับดอกเบี้ยในระหว่างผิดนัดตามมาตรา 224 วรรคหนึ่ง ซึ่งปัจจุบันอยู่ที่อัตราร้อยละ 5 ต่อปี

จากคำพิพากษาฎีกาแสดงให้เห็นว่าการที่ผู้เสียหายได้รับความเสียหายจากการใช้ Application online โดนถูกถอนเงินออกจากบัญชีธนาคาร ธนาคารต้องรับผิด แม้ธนาคารจะเคยประกาศเตือนลูกค้าแล้ว แต่เนื่องจากการเตือนดังกล่าวเกิดจากการที่

ลูกค้าได้กดลิงค์ที่ไม่ใช่ธนาคาร ได้มีการใส่ usename password และ OTP เอง ดังนั้น ลูกค้าและธนาคารมีส่วนทำให้ความเสียหายจากเงิน 1,099,999 บาทโดยให้ธนาคารใช้เงิน 550,000 บาทโดยให้ผู้เสียหายรับผิดร่วมด้วยในความประมาทดังกล่าว อย่างไรก็ตาม คำพิพากษาฎีกาดังกล่าวเป็นกรณีที่ใช้เทคนิคทางคอมพิวเตอร์โดยผู้กระทำความผิดทางคอมพิวเตอร์หรือสมาร์ทโฟนของผู้เสียหายโดยมิชอบ หรือการ Hacking เพื่อให้มีการโอนเงินให้ผู้กระทำความผิด โดยมีการกระทำตั้งแต่ขโมยชื่อบัญชี รหัสผ่าน และข้อมูลที่ใช้ในการโอนเงิน โดยผู้เสียหายไม่ได้ทำธุรกรรมเองแต่เป็นคนร้ายที่ทำธุรกรรม เมื่อพิจารณาความผิดอาญาไม่ถือว่าผู้เสียหายมีส่วนร่วมในการกระทำความผิด ผู้เสียหายจึงสามารถดำเนินคดีทางอาญากับผู้กระทำความผิดได้ เพราะฉะนั้นธนาคารควรมีหน้าที่ในการวางกลไกไม่ให้บุคคลได้เข้าล่วงล้ำข้อมูลเพื่อนำเงินไปใช้โดยไม่มีสิทธิ และธนาคารควรที่ติดตามเงินดังกล่าวคืนจากผู้กระทำความผิดไม่ใช่ผู้เสียหาย เนื่องจากธนาคารมีศักยภาพ ทรัพยากร และอำนาจต่อรองที่ทำได้มากกว่าผู้เสียหายและเป็นสถาบันทางการเงินที่ควรสร้างความน่าเชื่อถือให้กับประชาชน

3. ขั้นตอนการดำเนินคดีและหน่วยงานผู้รับผิดชอบ

เนื่องจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550 เป็นกฎหมายอาญากล่าวคือ มีลักษณะการกำหนดความผิดและบทลงโทษทางอาญาไว้ ดังนั้น กระบวนการในการดำเนินคดีกับผู้กระทำความผิดจึงจำเป็นที่ต้องนำประมวลกฎหมายวิธีพิจารณาความอาญามาใช้ แต่เนื่องจากเพื่อให้การดำเนินคดีมีประสิทธิภาพจึงจะมีกระบวนการในการสอบสืบสวนและสอบสวน และเป็นการเพิ่มให้พนักงานเจ้าหน้าที่เข้ามามีอำนาจในการสอบสวนความผิดตามพระราชบัญญัตินี้ โดยพนักงานสอบสวนตามพระราชบัญญัติมีอำนาจหน้าที่ ดังนี้ (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550, 2550: มาตรา 18)

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดมาเพื่อให้ถ้อยคำส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือ ที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน

(4) ทำสำเนาข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

จากอำนาจหน้าที่ของพนักงานสอบสวนที่มีอำนาจเพิ่มมากขึ้น การกระทำของพนักงานเจ้าหน้าที่เพื่อให้เป็นไปอย่างรวดเร็วจึงไม่จำเป็นต้องขออนุญาตศาลตาม (1) (2) (3) ส่วนการใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7)และ (8) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำ

หรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิด เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ประกอบคำร้องด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550, 2550: มาตรา 19) โดยเจ้าพนักงานเจ้าหน้าที่ต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจ โดยคำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ และศาลจะดำเนินการพิจารณาเป็นไปด้วยความรวดเร็ว เมื่อศาลอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาลให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา 18(4) (5) (6) (7) และ (8) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์ไว้เป็นหลักฐาน หลังจากได้รับอนุญาตจากศาลให้ดำเนินการตามคำร้องแล้วให้สำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการเพื่อเป็นหลักฐาน

นอกจากเจ้าพนักงานเจ้าหน้าที่จะมีอำนาจหน้าที่ในการสอบสวนแล้ว ตามพระราชบัญญัติกำหนดให้รัฐมนตรีกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมมีอำนาจแต่งตั้งเจ้าหน้าที่กับออกกฎกระทรวงและประกาศเพื่อปฏิบัติการตามพระราชบัญญัตินี้ และยังมีหน่วยงานอื่นที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ได้แก่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) ซึ่งมีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อย ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวนสอบสวนปฏิบัติงานตามกฎหมายวิธีพิจารณาความอาญา และกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์ซึ่งผู้ได้รับความเสียหายหรือพบเห็นการกระทำที่ถือเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550 โดยสามารถแจ้งเหตุหรือแจ้งเบาะแสต่อหน่วยงานดังกล่าวได้โดยตรง

4. บทสรุปและข้อเสนอแนะทางกฎหมายถึงแนวทางในการป้องกันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กรณีการทำธุรกรรมทางการเงินผ่านระบบออนไลน์

ปัจจุบันการใช้เทคโนโลยีผ่านระบบออนไลน์เป็นสิ่งที่มีความจำเป็นและมีความสำคัญอย่างยิ่งในการดำรงชีวิตของมนุษย์ ดังนั้นข้อมูลของผู้ใช้ระบบสารสนเทศทางเทคโนโลยีอาจถูกโจรกรรม หรือถูกล่วงล้ำโดยเจ้าของไม่รู้ตัว หรือถูกปิดกั้นขัดขวางไม่ให้สามารถเข้าถึงข้อมูลได้ จนทำให้บุคคลได้รับความเสียหายและเกิดความเสียหายต่อความมั่นคงของประเทศ จึงจำเป็นที่ต้องมีกฎหมายที่มีประสิทธิภาพในการป้องกันภัยคุกคามและปราบปรามผู้กระทำความผิด โดยการคำนึงถึงแนวคิดเรื่องการให้หลักประกันการคุ้มครองสิทธิเสรีภาพในการคุ้มครองสิทธิส่วนบุคคล จึงเป็นสิ่งที่มีความสำคัญที่ทุกประเทศให้หลักประกันแก่ประชาชนไว้ และเป็นสิ่งที่ทุกประเทศต้องตระหนัก โดยเฉพาะการเตรียมความพร้อมในการรับมือกับการพัฒนาทางด้านเทคโนโลยีในปัจจุบันที่มีการขับเคลื่อนเป็นไปอย่างรวดเร็วและก้าวกระโดด หากไม่มีมาตรการที่เพียงพอในการคุ้มครองสิทธิส่วนบุคคลก็จะทำให้ประชาชนถูกละเมิดและก่อให้เกิดความเสียหายต่อประชาชน สังคม โดยเฉพาะความมั่นคงทางด้านเศรษฐกิจและสังคมของประเทศ

จากข้อเท็จจริง เมื่อผู้เสียหายได้รับความเสียหายจากการกระทำความผิดทางด้านธุรกรรมทางการเงินผ่านระบบออนไลน์ จึงมีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มาบังคับใช้เอาผิดกับผู้กระทำความผิด โดยเจตนารมณ์ของกฎหมายเพื่อป้องกันปราบปรามอาชญากรรมที่เกิดจากการใช้วิธีการใด ๆ เข้าไปล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน โดยผู้กระทำความผิดจะมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550 ได้แก่ การกระทำความผิดฐานการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ ตามมาตรา 5 การกระทำความผิดฐานการเข้าถึงข้อมูลคอมพิวเตอร์ ตามมาตรา 7 ความผิดฐานทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ ตามมาตรา 9

และการกระทำความผิดฐานกระทำการเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานตามปกติได้ ตามมาตรา 10

ดังนั้น เมื่อผู้เสียหายได้รับความเสียหายจากการกระทำความผิดทางด้านธุรกรรมทางการเงินผ่านระบบออนไลน์ เนื่องจากเข้าไปล่วงล้ำข้อมูลของบุคคลอื่นและทำการถอนเงินออกจากบัญชีในระบบออนไลน์ผ่าน Application online โทรศัพท์เคลื่อนที่ทำให้เจ้าของบัญชีได้รับความเสียหาย โดยผู้กระทำมีความผิดทางอาญาและมีความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ซึ่งกฎหมายได้บัญญัติความผิดไว้และสามารถนำตัวผู้กระทำความผิดมาลงโทษได้ ในทางปฏิบัติ กระบวนการในการดำเนินคดีกับผู้กระทำความผิดมีปัจจัยที่ส่งผลกระทบต่อการปฏิบัติ กล่าวคือ ผู้กระทำความผิดใช้บัญชีบุคคลอื่นในการรับโอนเงินทำให้เกิดอุปสรรคในการนำตัวผู้กระทำความผิดมาลงโทษ เพราะบัญชีที่ใช้ในการกระทำความผิดมีหลายบัญชี (บัญชีม้า) ซึ่งเป็นบัญชีเงินฝากธนาคารของบุคคลอื่นที่ถูกคนร้ายนำมาใช้เป็นช่องทางในการรับเงินและถ่ายโอนเงินที่ได้มาจากการกระทำความผิด เพื่อป้องกันไม่ให้มีพยานหลักฐานเชื่อมโยงมาถึงตัวได้ คนร้ายสามารถทำได้หลายวิธีเพื่อให้ได้มาซึ่งบัญชีม้า ทั้งจากการโจรกรรมข้อมูลส่วนบุคคลเพื่อนำไปใช้เปิดบัญชีในชื่อของคนนั้น ๆ หรือจ้างให้บุคคลอื่นเปิดบัญชี หรือรับซื้อบัญชีเงินฝากธนาคารของบุคคลทั่วไปเพื่อนำไปใช้กระทำความผิด โดยบัญชีม้าเหล่านี้จะถูกรวบรวมเป็นแพ็กเกจพร้อมกับสำเนาบัตรประจำตัวประชาชนและซิมการ์ดโทรศัพท์ที่เจ้าของบัญชีเปิดใช้งานด้วย เพื่อให้คนร้ายที่ซื้อบัญชีม้าไปแล้วสามารถนำข้อมูลส่วนบุคคลของเจ้าของบัญชีไปผูกกับ Mobile banking เพื่อใช้ทำธุรกรรมออนไลน์ได้ทันที ซึ่งผู้กระทำความผิดจะมีบัญชีม้าหลาย ๆ บัญชี เพื่อใช้โอนส่งเงินต่อกันเป็นทอด ๆ เพื่อป้องกันการถูกตำรวจตรวจสอบหรืออายัดเงินในบัญชีม้า เช่น เมื่อผู้เสียหายถูกหลอกให้โอนเงินเข้าบัญชีม้าที่ 1 แล้ว คนร้ายก็จะโอนเงินออกจากบัญชีดังกล่าวต่อไปยังบัญชีม้าที่ 2 จากบัญชีม้าที่ 2 โอนต่อไปยังบัญชีม้าที่ 3 และที่ 4 ซึ่งบางรายมีจำนวนบัญชีม้าถึง 5 บัญชี ท้ายที่สุดคนร้ายก็จะถอนเงินของเหยื่อหรือผู้เสียหายออกไป ซึ่งการโอนเงินจากบัญชีม้าหลายทอดเช่นนี้ตั้งแต่ต้นจนจบใช้เวลาเพียงไม่กี่นาทีเท่านั้น และหากถูกเจ้าหน้าที่ตำรวจอายัดบัญชีม้าบัญชีใด ก็จะเปลี่ยนไปใช้บัญชีม้าอื่น ๆ

ที่ยังสามารถใช้งานแทนได้ ดังนั้น ในการกระทำความผิดเป็นการกระทำอย่างเป็นขบวนการ มีขั้นตอนและการวางแผนเป็นอย่างดี ทำให้ประชาชนไม่ได้รับการปกป้องและคุ้มครองสิทธิเสรีภาพอย่างเป็นธรรมแม้กฎหมายจะบัญญัติความผิดไว้ก็ตาม อย่างไรก็ตาม เมื่อมีการกระทำเกี่ยวกับอาชญากรรมทางเทคโนโลยีเกิดขึ้น รัฐเปิดโอกาสให้ประชาชนผู้ได้รับความเสียหายสามารถแจ้งเหตุต่อกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ได้โดยตรง หรือแจ้งความ ณ สถานีตำรวจท้องที่ที่เกิดเหตุ หรือทางระบบออนไลน์ https://tcsd.go.th/ เพื่อที่จะสามารถนำผู้กระทำความผิดมาลงโทษได้ทันต่อเหตุการณ์และเป็นไปด้วยความรวดเร็ว

นอกจากนี้ ในทางกฎหมายแพ่ง ศาลฎีกาได้มีคำพิพากษาฎีกาที่ 6233/2564 วางหลักว่าการที่ผู้เสียหายได้รับความเสียหายจากการใช้ Application online โดนถูกถอนเงินออกจากบัญชีธนาคาร ธนาคารต้องรับผิดแม้ธนาคารจะเคยประกาศเตือนลูกค้าแล้วก็ตาม เพราะฉะนั้นธนาคารควรมีหน้าที่ในการวางกลไกไม่ให้บุคคลได้เข้าล่วงล้ำข้อมูลเพื่อนำเงินไปใช้โดยไม่มีสิทธิ และธนาคารควรที่ติดตามเงินดังกล่าวคืนจากผู้กระทำความผิดไม่ใช่ผู้เสียหาย เนื่องจากธนาคารมีศักยภาพ ทรัพยากร และอำนาจต่อรองที่ทำได้มากกว่าผู้เสียหายและเป็นสถาบันทางการเงินที่ควรสร้างความน่าเชื่อถือให้กับประชาชน

กล่าวโดยสรุป การกระทำความผิดเกี่ยวกับการแฮ็กข้อมูลของบุคคลเพื่อทำธุรกรรมการเงินและถอนเงินออกจากบัญชีและเกิดความเสียหายแก่บุคคลนั้น การกระทำความผิดของกลุ่มมิจฉาชีพเหล่านี้เป็นการกระทำที่กระทบต่อความมั่นคงของธนาคารผู้รับฝากเงินอันเป็นที่ไว้วางใจของประชาชน และประชาชนได้รับผลกระทบอีกทางหนึ่งด้วย ซึ่งกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ยังไม่สามารถบังคับเอาผิดกับผู้กระทำความผิดได้ทันท่วงที แม้รัฐจะมีมาตรการในเรื่องของการคุ้มครองสิทธิส่วนบุคคลตามที่บัญญัติไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทยไว้อย่างชัดเจนแน่นอนก็ตาม ผู้เขียนเห็นว่ารัฐควรมีแนวทางที่สำคัญ ดังนี้

ประการแรก “รัฐควรมีมาตรการที่ชัดเจนเกี่ยวกับการเข้าถึงข้อมูลในการทำทางธุรกรรมทางระบบออนไลน์” เนื่องจากธนาคารเป็นหน่วยงานทางการเงินที่ได้รับ

ความเชื่อถือจากประชาชนสูงสุด โดยประชาชนมองว่าการนำเงินไปฝากไว้กับธนาคารย่อมได้รับความปลอดภัยเกี่ยวกับทรัพย์สินของตน ดังนั้นการที่ผู้กระทำความผิดได้มีการล่วงล้ำข้อมูลส่วนบุคคลเข้าไปกดถอนเงินผ่านระบบออนไลน์ได้อย่างรวดเร็ว โดยไม่มีมาตรการป้องกันความปลอดภัย ก็จะทำให้ประชาชนเกิดความเสียหายและอาจจะกระทบต่อเศรษฐกิจในอนาคตได้ ดังนั้น รัฐควรมีมาตรการทางกฎหมายเกี่ยวกับการทำธุรกรรมทางการเงินผ่านระบบออนไลน์กำหนดให้ธนาคารวางกลไกที่มีมาตรฐานและความปลอดภัย และรับผิดชอบในการดำเนินคดีกับผู้กระทำความผิด เป็นต้น

ประการที่สอง “ปรับปรุงกฎหมายให้มีความทันสมัย และส่งผลให้ทางปฏิบัติเป็นไปด้วยความรวดเร็ว” ควรมีการแก้ไขปรับปรุงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อให้เกิดการปกป้องคุ้มครองประชาชนได้จริงในทางปฏิบัติ แม้ว่ารัฐจะมีนโยบายเปิดโอกาสให้ประชาชนสามารถร้องเรียนผ่านระบบออนไลน์ได้ก็ตาม แต่เนื่องจากปัจจุบันคดีที่เกี่ยวกับการกระทำความผิดทางออนไลน์มีเป็นจำนวนมาก รัฐควรให้อำนาจพนักงานเจ้าหน้าที่ในการเข้าถึงข้อมูลได้อย่างรวดเร็วและไม่มีกระบวนการที่ซับซ้อน

ประการที่สาม “ควรมีการจัดตั้งศาลพิเศษเพื่อพิจารณาคดีที่เกี่ยวกับคอมพิวเตอร์โดยเฉพาะ” เนื่องจากคดีเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์มีเป็นจำนวนมาก ดังนั้นในการดำเนินคดีเพื่อให้เป็นไปด้วยความรวดเร็วและเกิดความเป็นธรรมแก่ประชาชนผู้ได้รับความเดือดร้อน จึงควรมีศาลพิเศษเกี่ยวกับคดีคอมพิวเตอร์เช่นเดียวกับคดีของศาลล้มละลาย ศาลแรงงาน หรือศาลภาษี เป็นต้น

เอกสารอ้างอิง

ตำรวจไซเบอร์ เผยเหยื่อถูกมิจฉาชีพลวง กดลิงก์โหลดแอปฯปลอมดูดเงินเกลี้ยงบัญชี. (2566). สืบค้น 10 มกราคม 2566, จาก https://www.bangkokbiznews.com/politics/1048618

ทิพาพร นะมาตร์. (2550). **สิทธิความเป็นส่วนตัว: ศึกษากรณีสิทธิความเป็นอยู่ส่วนตัวของบุคคลสาธารณะ.** วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธุรกิจบัณฑิตย์.

นคร เสรีรักษ์. (2562). **ข้อแนะนำเชิงนโยบายด้านข้อมูลส่วนบุคคล (Data privacy guideline) ตอนที่ 2.** สืบค้น 28 มีนาคม 2565, จาก https://www.fpps.or.th/

นพดล นิ่มหนู. (2565). หลักการคุ้มครองข้อมูลส่วนบุคคล: ศึกษาเปรียบเทียบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540. **วารสารมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยมหาสารคาม, 41**(3), 46-67.

บรรเจิด สิงคะเนติ, นนทวัชร์ นวตระกูลพิสุทธิ์ และเรวดี ขวัญทองยิ้ม. (2554). **รายงานการศึกษาวิจัยฉบับสมบูรณ์เรื่องปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นส่วนตัว.** กรุงเทพฯ: สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ.

บุญญรัตน์ โชคบันดาลชัย. (2561). การคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษ. **วารสารนิติศาสตร์ มหาวิทยาลัยนเรศวร, 11**(2), 131-148.

ปองปรัชญ์ เกศาสุวรรณ, จักรพงศ์ ลิ้มสุวรรณ และสุธิดา ผิวขาว. (2562). ธนาคารอิเล็กทรอนิกส์: ความรับผิดทางกฎหมายของธนาคารผู้ให้บริการและผู้ใช้บริการ. **วารสารมหาวิทยาลัยราชภัฏมหาสารคาม, 13**(1), 33-41.

ปัทมา มัญชุนากร. (2565). ปัญหากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในเครือข่ายสังคมออนไลน์: ศึกษากรณีผู้ควบคุมข้อมูลส่วนบุคคลหลายราย. **วารสารรัชต์ภาคย์, 16**(47), 89-107.

พรเพชร วิชิตชลชัย. (ม.ป.ป.). **คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550.** สืบค้น 10 มกราคม 2566, จาก https://www.agri.cmu.ac.th/2017 /files/Download/49080075.pdf

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550. (2550). **ราชกิจจานุเบกษา, 124**(ตอน 27ก), 4-18.

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พุทธศักราช 2544. (2544). **ราชกิจจานุเบกษา, 118** (ตอน 112ก), 26-42.

ภาระวี ปุณเสรีพิพัฒน. (2557). มาตรการทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์: ศึกษากรณีการใช้คุกกี้บนอินเทอร์เน็ต. **วารสารนิติศาสตร์ มหาวิทยาลัยนเรศวร, 7**(1), 166-193.

รัฐยันเร่งแก้ปัญหา 'อาชญากรรมออนไลน์' อายัดบัญชีม้าแล้ว 5.8 หมื่นบัญชี. (2566). สืบค้น 10 มกราคม 2566, จาก https://workpointtoday.com/policeonline/