

ปัญหาพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี¹

ณัฐนรินทร์ ชานนท์²

จากการศึกษาเกี่ยวกับปัญหาทางกฎหมายตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 โดยมีวัตถุประสงค์เพื่อศึกษาลักษณะและความหมายของการกระทำความผิดอาชญากรรมทางเทคโนโลยี และมาตรการกฎหมายตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ด้วยรัฐบาลได้ออกพระราชกำหนดดังกล่าว เนื่องจากปัจจุบันมีการใช้วิธีการทางเทคโนโลยีในการหลอกลวงประชาชนเป็นจำนวนมาก รัฐบาลจึงเห็นว่าเป็นกรณีฉุกเฉินที่มีความจำเป็นรีบด่วนอันมิอาจจะหลีกเลี่ยงได้ ซึ่งมีกระทบต่อเศรษฐกิจประเทศไทย เช่น แก๊งคอลเซ็นเตอร์ที่หลอกลวงผู้เสียหายหลายรายเพื่อให้ได้มาซึ่งทรัพย์สิน เป็นต้น ดังนั้นจึงออกมาตรการต่าง ๆ ผ่านพระราชกำหนดดังกล่าว โดยมีผลบังคับใช้เมื่อวันที่ 17 มีนาคม 2566

อย่างไรก็ตามเมื่อได้ทำการศึกษาปัญหาพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีพบว่ายังมีปัญหาอยู่หลายประการสามารถสรุปได้ดังนี้

ประการแรก ปัญหาการนิยามตามมาตรา 3 คำว่า “อาชญากรรมทางเทคโนโลยี” ตามมาตรา 3 ได้ให้คำนิยาม “อาชญากรรมทางเทคโนโลยี” หมายความว่า การกระทำความผิดหรือพยายามกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง ทุจริต หรือรีดเอาทรัพย์สินบุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกง ทุจริต หรือรีดเอาทรัพย์สิน โดยใช้ระบบคอมพิวเตอร์ จากคำนิยามดังกล่าว องค์ประกอบส่วนหนึ่งของอาชญากรรมทางเทคโนโลยีคือผู้กระทำความผิดต้องกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีวัตถุประสงค์การกระทำ 2 ประเภทคือ การกระทำความผิดต่อระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ หรืออาจไม่ต้องกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แต่หากใช้ระบบคอมพิวเตอร์ในการกระทำความผิดฐานฉ้อโกง ทุจริต หรือรีดเอาทรัพย์สิน ก็เป็นอาชญากรรมทางเทคโนโลยีได้ ในขณะที่การคัดลอกข้อมูลจากแถบแม่เหล็กของบัตรอิเล็กทรอนิกส์โดยเครื่องสกินเมอร์ (skimmer) ที่ติดตั้งไว้ที่ตู้เอทีเอ็ม. หรือเป็นเครื่องสกินเมอร์ขนาดพกพาหรือเครื่องแฮนด์เฮลด์สกินเมอร์ (handheld skimmer) เมื่อคนร้ายได้ข้อมูลบัตรอิเล็กทรอนิกส์ดังกล่าวก็จะนำไปทำบัตรใหม่เพื่อนำไปใช้ประโยชน์โดยมิ

¹บทความนี้เรียบเรียงจากการค้นคว้าอิสระ เรื่อง ปัญหาพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยมีอาจารย์ที่ปรึกษา คือ รองศาสตราจารย์จุฑาพร วงศ์ทองสรรค์ และคณะกรรมการสอบ คือ รองศาสตราจารย์จรัส เล็งวิทยา และรองศาสตราจารย์ประเทือง ธนียผล

²นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต (ส่วนกลาง) คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง

ชอบ ซึ่งการกระทำความผิดดังกล่าวเป็นการปลอมบัตรอิเล็กทรอนิกส์ตามมาตรา 269/1³ ประกอบกับมาตรา 1 (14) (ก) แห่งประมวลกฎหมายอาญา⁴ แต่จากคำนิยาม “อาชญากรรมทางเทคโนโลยี” แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ดังกล่าวยังไม่ครอบคลุมฐานความผิดปลอมบัตรอิเล็กทรอนิกส์ตามมาตรา 269/1 ประกอบกับมาตรา 1(14) (ก)

ทั้งนี้ นายโปลิต สุขสว่าง ได้ให้ความเห็นว่า คำนิยาม “บัตรอิเล็กทรอนิกส์” ของประมวลกฎหมายอาญา ไม่ใช่ “ระบบคอมพิวเตอร์” แม้บัตรอิเล็กทรอนิกส์ได้มีการบันทึกข้อมูลหรือรหัสไว้ด้วยวิธีการทางอิเล็กทรอนิกส์ก็ตาม ก็มีได้เป็นคอมพิวเตอร์ตั้งแต่แรก ทั้งแถบแม่เหล็ก (Magnetic Stripe) หรือชิป (Chip) ในเอกสารนั้นก็เพียงหน่วยความจำสำรองอันเป็นองค์ประกอบหนึ่งของคอมพิวเตอร์เท่านั้นจึงไม่ใช่เครื่องคอมพิวเตอร์ ส่วนบัตรอิเล็กทรอนิกส์ที่เป็นวัตถุอื่นใดที่พบเห็นได้ทั่วไป ย่อมไม่มีองค์ประกอบของคอมพิวเตอร์ครบถ้วน ทั้งแหล่งบันทึกข้อมูลในวัตถุอื่นใดนั้นก็เพียงหน่วยความจำสำรองอันเป็นองค์ประกอบหนึ่งของคอมพิวเตอร์เท่านั้นจึงไม่ใช่เครื่องคอมพิวเตอร์ นอกจากนี้คำนิยาม “บัตรอิเล็กทรอนิกส์” ของประมวลกฎหมายอาญา ไม่ใช่ “ข้อมูลอิเล็กทรอนิกส์” แม้ว่าจะได้มีข้อมูลในรูปแบบดิจิทัล (Digital) บันทึกไว้ในแหล่งบันทึกความจำสำรองในเอกสารดังกล่าว เช่น ข้อมูลที่บันทึกอยู่ในแถบแม่เหล็ก (Magnetic Stripe) หรือชิป (Chip) และเนื่องจากการเป็นเอกสารนั้นขาดองค์ประกอบของการเป็นคอมพิวเตอร์ตั้งแต่แรก ดังนั้นหากมีการดึงข้อมูลออกจากเอกสารที่เป็นบัตรอิเล็กทรอนิกส์ดังกล่าวโดยตรง จะไม่สามารถปรับใช้ฐานความผิดอันเกี่ยวกับข้อมูลคอมพิวเตอร์ตามพระราชบัญญัตินี้ได้ ส่วนบัตรอิเล็กทรอนิกส์ที่เป็นวัตถุอื่นใด แม้ว่าจะได้มีข้อมูลในรูปแบบดิจิทัล (Digital) บันทึกไว้ในแหล่งบันทึกความจำสำรองในวัตถุอื่นใดนั้นก็ตาม แต่เนื่องจากบัตรประเภทดังกล่าวที่พบเห็นได้ทั่วไปโดยปกติแล้วย่อมไม่มีองค์ประกอบของคอมพิวเตอร์ครบถ้วนจึงไม่ใช่คอมพิวเตอร์ตั้งแต่แรก ข้อมูลดังกล่าวจึงไม่ใช่ข้อมูลคอมพิวเตอร์ด้วย⁵

³ มาตรา 269/1 บัญญัติว่า ผู้ใดทำบัตรอิเล็กทรอนิกส์ปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด เดิมหรือดัดทอนข้อความ หรือแก้ไขด้วยประการใด ๆ ในบัตรอิเล็กทรอนิกส์ที่แท้จริง โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ถ้าได้กระทำให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นบัตรอิเล็กทรอนิกส์ที่แท้จริงหรือเพื่อใช้ประโยชน์อย่างหนึ่งอย่างใด ผู้นั้นกระทำความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงห้าปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนบาท

⁴ มาตรา 1 (14) (ก) เอกสารหรือวัตถุอื่นใด ไม่ว่าจะมิใช่ลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า...

⁵ โปลิต สุขสว่าง, “ปัญหาการบังคับใช้กฎหมายเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์,” (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย, 2563), หน้า 113.

ดังนั้นเมื่อการกระทำความผิดต่อบัตรอิเล็กทรอนิกส์มาตรา 1 (14) ก แห่งประมวลกฎหมายอาญาไม่ถือว่าเป็นการกระทำต่อ “ระบบคอมพิวเตอร์” หรือ “ข้อมูลคอมพิวเตอร์” จึงไม่อาจเป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้ และไม่เป็นอาชญากรรมทางเทคโนโลยี ตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 อีกทั้งการคัดลอกข้อมูลจากแถบแม่เหล็กของบัตรอิเล็กทรอนิกส์โดยเครื่องสกินเมอร์ (skimmer) หรือเป็นเครื่องสกินเมอร์ขนาดพกพาหรือเครื่องแฮนด์เฮลด์สกินเมอร์ (handheld skimmer) มิใช่เป็นการกระทำความผิดฐานฉ้อโกง กรรโชก หรือรีดเอาทรัพย์สิน โดยใช้ระบบคอมพิวเตอร์ ตามคำนิยามของ “อาชญากรรมทางเทคโนโลยี” อีกด้วย อย่างไรก็ตาม หากพิจารณาลักษณะการกระทำดังกล่าวว่าเป็นการใช้อุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือในการก่อให้เกิดความเสียหายและยังนำข้อมูลบัตรอิเล็กทรอนิกส์ที่ได้ไปใช้ประโยชน์ส่วนตัวโดยมิชอบด้วยกฎหมาย พิจารณาได้ว่าเป็นอาชญากรรมทางเทคโนโลยีตามความหมายทั่วไป ประกอบกับกองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีของประเทศไทยที่มีอำนาจการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยีโดยการใช้เทคโนโลยีสารสนเทศและเครื่องมือพิเศษ ก็ได้ออกมาเตือนภัยกับประชาชนถึงการกระทำความผิดเกี่ยวกับ Skimmer⁶ และในสำนักงานสอบสวนกลางหรือเอฟบีไอกับหน่วยงาน United States Secret Service ของประเทศสหรัฐอเมริกาที่มีอำนาจสอบสวนด้านไซเบอร์ ก็ยังต้องดำเนินการสอบสวนการคัดลอกข้อมูลจากแถบแม่เหล็กของบัตรอิเล็กทรอนิกส์โดยเครื่องสกินเมอร์ (skimmer) อยู่

ประการสอง ปัญหาตามมาตรา 7 ของพระราชกำหนดดังกล่าว พิจารณาถึงขั้นตอนและระยะเวลาการระงับธุรกรรมชั่วคราวของบัญชีเงินฝากที่ไม่ใช่บัญชีที่ใช้ในการรับเงินจากการทำความผิด โดยตามมาตรา 7 ไม่มีขั้นตอนให้เจ้าของบัญชีผู้รับโอนได้คัดค้านการระงับธุรกรรมชั่วคราวเพื่อเป็นพยานหลักฐานประกอบการใช้ดุลพินิจของพนักงานสอบสวนในการพิจารณาว่าจะระงับธุรกรรมชั่วคราวต่อไปหรือไม่ และยังขาดความชัดเจนในการกำหนดระยะเวลาการยกเลิกการระงับธุรกรรมว่าต้องใช้เวลานาน โดยตามมาตรา 7 กำหนดขั้นตอนว่ากรณีที่สถาบันการเงินหรือผู้ประกอบการธุรกิจ⁷ ได้รับแจ้งจากผู้เสียหายซึ่งเป็นผู้ถือบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ว่า ได้มีการทำธุรกรรมโดยบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ดังกล่าวและเข้าข่ายเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี ให้สถาบันการเงินหรือผู้ประกอบการธุรกิจดังกล่าวมีหน้าที่ระงับการทำธุรกรรมนั้นไว้ชั่วคราว พร้อมทั้งนำข้อมูลเข้าสู่ระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามมาตรา 4 เพื่อให้สถาบันการเงินและผู้ประกอบการธุรกิจผู้รับโอนทุกทอดทราบและระงับการทำธุรกรรมดังกล่าวไว้ทันที จากนั้นสถาบันการเงินหรือผู้ประกอบการธุรกิจจะแจ้งให้ผู้เสียหายไปร้องทุกข์ต่อพนักงานสอบสวนภายใน 72 ชั่วโมง เมื่อมีการร้องทุกข์แล้ว ให้พนักงานสอบสวนแจ้งให้สถาบันการเงินหรือผู้ประกอบการธุรกิจที่ได้รับการทำธุรกรรมไว้ทราบ และให้พนักงานสอบสวนพิจารณาดำเนินการ

⁶ สถานีประชาชน ไทยพีบีเอส, กลโกงบัตรอิเล็กทรอนิกส์ [Online], Available URL:

https://www.facebook.com/photo.php?fbid=710034917837605&set=a.360386166135817&type=3&locale=th_TH&_rdr

⁷ มาตรา 3 “ผู้ประกอบการธุรกิจ” หมายความว่า ผู้ประกอบการตามกฎหมายว่าด้วยระบบการชำระเงิน

เกี่ยวกับบัญชีเงินฝากและบัญชีเงินอิเล็กทรอนิกส์ดังกล่าวภายใน 7 วันนับแต่วันที่ได้รับความร้องทุกข์ หากไม่มีคำสั่งให้ระงับการทำธุรกรรมไว้ต่อไปภายในเวลาดังกล่าว ให้สถาบันการเงินหรือผู้ประกอบการธุรกิจ “ยกเลิก” การระงับการทำธุรกรรมนั้น

ทั้งนี้การใช้มาตรการนี้ย่อมกระทบสิทธิต่อเจ้าของบัญชีผู้รับโอนที่ถูกระงับธุรกรรมไว้ชั่วคราว ไม่สามารถใช้จ่ายเงินได้จะก่อให้เกิดความเสียหาย เพราะเป็นการกำหนดให้สถาบันการเงินหรือผู้ประกอบการธุรกิจ ดำเนินการซึ่งไม่ใช่หน่วยงานทางด้านกระบวนการยุติธรรมโดยตรงเช่น ตำรวจ พนักงานอัยการ เป็นต้น มีอำนาจระงับการใช้บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ของด้านผู้รับโอนได้ โดยอาศัยเหตุตามที่ผู้เสียหายแจ้งว่าบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์เป็นบัญชีเข้าข่ายเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีเพียงอย่างเดียว อีกทั้งมาตรา 7 ไม่ได้กำหนดให้มีการสอบถามไปยังเจ้าของบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ผู้รับโอนเพื่อเปิดโอกาสให้เจ้าของบัญชีได้ชี้แจงและให้ข้อมูลว่าตนอาจไม่ได้กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ดังนั้นย่อมขัดหลักฟังความทุกฝ่ายอันเป็นหลักในการดำเนินกระบวนการพิจารณาความอาญา กล่าวคือ ต้องเปิดโอกาสให้เจ้าของบัญชีที่จะแก้ข้อกล่าวหาได้ หรือมีสิทธิที่จะโต้แย้งคัดค้าน

สำหรับกฎหมายของประเทศสหรัฐอเมริกา กำหนดให้การค้นเพื่อตรวจยึดสิ่งของในคดีอาญา ต้องมีหมายค้นที่ออกโดยผู้พิพากษามาจิสเตรทส์ (Magistrate Court) ต้องมีเหตุผลสมควร และรายละเอียดสถานที่ที่จะค้น หรือตัวบุคคลหรือสิ่งของที่จะยึด โดยตามกฎหมายของรัฐบาลกลาง ผู้ถูกค้นมีเหตุคัดค้านคำขออนุญาตหมายนั้นหลายประการ เช่น การอ้างว่าข้อความเป็นเท็จหรือหลักฐานไม่น่าเชื่อถือ หรือไม่มีเหตุอันควรเชื่อของข้อเท็จจริงนั้น (probable cause) เป็นต้น ส่วนกฎหมายของประเทศญี่ปุ่น กำหนดว่าหากสถาบันการเงินพบบัญชีธนาคารที่ต้องสงสัยว่าใช้ในอาชญากรรม เช่น ล้อโกง เป็นต้น สถาบันการเงินจะใช้มาตรการระงับการทำธุรกรรมเกี่ยวกับบัญชีธนาคารที่ต้องสงสัยว่ากระทำความผิดล่อโกง และสถาบันการเงินจะร้องขอให้สถาบันประกันเงินฝากของญี่ปุ่น (Deposit Insurance Corporation of Japan หรือ DICJ) จัดทำคำประกาศสาธารณะ (Public Notices) เพื่อแจ้งให้เจ้าของบัญชีทราบว่ามีการรับเงินฝากในบัญชีธนาคารในฐานะผู้ต้องสงสัย ซึ่งทำให้เจ้าของบัญชีมีโอกาสใช้สิทธิคัดค้านตามกฎหมายได้ ดังนี้ เห็นได้ว่ากฎหมายทั้งสองประเทศเปิดโอกาสให้เจ้าของบัญชีมีโอกาสได้โต้แย้งคัดค้านการยึดหรืออายัดบัญชีเงินฝาก นอกจากนี้ กฎหมายของประเทศไทยตามมาตรา 298 ประกอบมาตรา 299 ประมวลกฎหมายวิธีพิจารณาความแพ่ง กำหนดให้ในกรณีที่เจ้าพนักงานบังคับคดีสงสัยว่าทรัพย์สินหรือสิทธิเรียกร้องนั้นไม่ใช่เป็นของลูกหนี้ตามคำพิพากษาและไม่ยอมทำการยึดหรืออายัด ถ้าเจ้าหนี้ตามคำพิพากษายืนยันให้ยึดหรืออายัด ตามมาตรา 298 เจ้าพนักงานบังคับคดีอาจจะสั่งการยึดหรือการอายัดก็ได้ ในกรณีที่สั่งคดีให้เจ้าพนักงานบังคับคดีมีคำสั่งห้ามการโอน ขาย ยักยอก จำหน่าย ทำลาย ทำให้เสื่อมค่า หรือเปลี่ยนแปลงซึ่งสิทธิในทรัพย์สินหรือสิทธิเรียกร้องนั้นไว้ก่อน วรรคแรก และมาตรา 299 วรรคแรก บุคคลผู้มีชื่อเป็นเจ้าของทรัพย์สินหรือสิทธิเรียกร้องตามที่ปรากฏในทะเบียนหรือหลักฐานอย่างอื่น หรือผู้มีส่วนได้เสียในทรัพย์สินหรือสิทธิเรียกร้องนั้น จะร้องขอต่อเจ้าพนักงานบังคับคดีให้เพิกถอนคำสั่งห้ามดังกล่าวโดยวางเงินหรือหา

ประกันมาให้แทนทรัพย์สินหรือสิทธิเรียกร้องนั้นก็ได้ ถ้าเจ้าพนักงานบังคับคดีพอใจในเงินหรือประกันก็ให้เพิกถอนคำสั่งห้ามดังกล่าวและรับเงินหรือประกันนั้นไว้ จะเห็นได้ว่าการอายัดสิทธิเรียกร้องในชั้นบังคับคดีแพ่งเองก็ยิ่งเปิดโอกาสให้อีกฝ่ายได้แย้งคำสั่งห้ามของเจ้าพนักงานบังคับคดีได้ ด้วยเหตุนี้ผู้เขียนเห็นว่ามาตรา 7 ควรมีขั้นตอนการคัดค้านการระงับธุรกรรมชั่วคราวได้เพื่อให้เจ้าของบัญชีได้มีโอกาสในการแสดงพยานหลักฐานคัดค้านไปยังพนักงานสอบสวน

นอกจากนี้ตามมาตรา 7 ได้วางหลักว่าให้พนักงานสอบสวนแจ้งให้สถาบันการเงินหรือผู้ประกอบการธุรกิจที่ได้รับการทำธุรกรรมทราบ และให้พนักงานสอบสวนพิจารณาดำเนินการเกี่ยวกับบัญชีเงินฝากและบัญชีเงินอิเล็กทรอนิกส์ดังกล่าวภายใน 7 วันนับแต่วันที่ได้รับความร้องทุกข์ หากไม่มีคำสั่งให้ระงับการทำธุรกรรมไว้ต่อไปภายในเวลาดังกล่าว ให้สถาบันการเงินหรือผู้ประกอบการธุรกิจยกเลิกการระงับการทำธุรกรรมนั้น จึงมีข้อพิจารณาว่าหากผู้เสียหายไม่ดำเนินการร้องทุกข์ การเริ่มต้นระยะเวลา 7 วันดังกล่าวย่อมไม่อาจเริ่มนับได้เพราะไม่มีการร้องทุกข์ ดังนี้ สถาบันการเงินหรือผู้ประกอบการธุรกิจอาจยกเลิกการระงับการทำธุรกรรมไม่ได้ มาตรา 7 จึงมีความไม่ชัดเจนว่าในกรณีที่ผู้เสียหายไม่ร้องทุกข์นั้น สถาบันการเงินหรือผู้ประกอบการธุรกิจจะยกเลิกการระงับการทำธุรกรรมได้ภายในกำหนดเวลาใด โดยความไม่ชัดเจนนี้ก่อให้เกิดความเสียหายแก่เจ้าของบัญชีเงินฝากหรือบัตรอิเล็กทรอนิกส์ ทั้งนี้สาเหตุที่ผู้เสียหายไม่ร้องทุกข์อาจเนื่องจากว่าตนไม่ใช่ผู้เสียหายทางอาชญากรรมทางเทคโนโลยี นอกจากนี้การแจ้งข้อความอันเป็นเท็จต่อสถาบันการเงินเพื่อใช้ประโยชน์ในการระงับธุรกรรมชั่วคราวยังไม่เป็นความผิดอีกด้วย โดยหากเปรียบเทียบกับมาตรา 6 แห่งพระราชกำหนดเดียวกันที่กำหนดระยะเวลาในการยกเลิกการระงับธุรกรรมไว้อย่างชัดเจน กล่าวคือ ในกรณีสถาบันการเงินหรือผู้ประกอบการธุรกิจเป็นผู้พบเหตุเองว่าบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ใดถูกใช้หรืออาจถูกใช้ทำธุรกรรมที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีหรือการกระทำความผิดมูลฐานหรือความผิดฐานฟอกเงินตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน หลังจากสถาบันการเงินหรือผู้ประกอบการธุรกิจมีระงับการทำธุรกรรมแล้ว และแจ้งให้เจ้าพนักงานผู้มีอำนาจดำเนินคดีอาญาหรือเลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน ดำเนินการตรวจสอบ หากปรากฏพยานหลักฐานอันควรเชื่อได้ว่าบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์นั้นถูกใช้ในการกระทำความผิด ให้ดำเนินการตามกฎหมายภายใน 7 วัน นับแต่วันที่ได้รับความร้องทุกข์การระงับการทำธุรกรรม แต่หากไม่ปรากฏพยานหลักฐานที่เชื่อได้ว่าบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์นั้นถูกใช้ในการกระทำความผิด ให้แจ้งผลการตรวจสอบให้สถาบันการเงินหรือผู้ประกอบการธุรกิจทราบเพื่อยกเลิกการระงับการทำธุรกรรมต่อไป ทั้งนี้ เมื่อพ้นกำหนดเวลาดังกล่าวแล้ว หากเจ้าพนักงานผู้มีอำนาจดำเนินคดีอาญาหรือเลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินไม่แจ้งผลการดำเนินการ ให้สถาบันการเงินหรือผู้ประกอบการธุรกิจยกเลิกการระงับการทำธุรกรรมนั้น

ในประเทศญี่ปุ่นมีขั้นตอนที่ชัดเจนในการดำเนินการเกี่ยวกับบัญชีเงินฝาก กล่าวคือพระราชบัญญัติดำเนินการในการชำระหนี้เรียกร้องค่าเสียหายที่ได้รับประโยชน์จากเงินในบัญชีเงินฝากที่ใช้สำหรับการกระทำอาชญากรรม (Act on Payment of Damage Recovery Benefits from Funds in Deposit

Accounts Used for Crime) กำหนดว่าเมื่อสถาบันการเงินได้พบบัญชีเงินฝากที่ต้องสงสัยที่ทำความผิดทางอาญาและสถาบันทางการเงินได้มีการอายัดบัญชีไว้ และได้ร้องขอให้สถาบันประกันเงินฝากของญี่ปุ่น (Deposit Insurance Corporation of Japan หรือ DICJ) จัดทำประกาศสาธารณะเพื่อดำเนินการขั้นตอนการหมดสิทธิเรียกร้องเกี่ยวกับเงินฝาก (The Procedure for Expiry of Claim on Deposits) โดยกำหนดให้เจ้าของบัญชีใช้สิทธิดำเนินการใช้สิทธิตามกฎหมายภายใน 60 วัน ซึ่งหากสถาบันการเงินได้รับข้อโต้แย้งภายในระยะเวลาที่กำหนด สถาบันการเงินจะต้องแจ้งให้สถาบันประกันเงินฝากของญี่ปุ่นทราบ หากปรากฏชัดว่าบัญชีเงินฝากที่ต้องสงสัยไม่ใช่บัญชีเงินฝากที่ใช้เพื่อก่ออาชญากรรม สถาบันการเงินจะต้องแจ้งให้ DICJ ทราบ เมื่อ DICJ ได้รับการแจ้ง DICJ จะต้องแจ้งให้สาธารณชนทราบถึงการยุติขั้นตอนการหมดสิทธิเรียกร้องเกี่ยวกับเงินฝาก (the procedure for expiry of the claim on deposits)

ด้วยเหตุนี้ผู้เขียนเห็นว่ามาตรา 7 ควรปรับปรุงแก้ไขเมื่อมีการระงับธุรกรรมชั่วคราว กฎหมายต้องกำหนดหน้าที่ให้สถาบันการเงินหรือผู้ประกอบการแจ้งข้อมูลเกี่ยวกับสาเหตุที่ผู้เสียหายขอระงับธุรกรรมไปยังพนักงานสอบสวนซึ่งผู้เขียนเห็นว่าควรให้กองบัญชาการตำรวจสืบสวนอาชญากรรมทางเทคโนโลยีเป็นศูนย์กลางรับข้อมูล และเพิ่มช่องทางให้เจ้าของบัญชีที่ถูกระงับธุรกรรมมีโอกาสแสดงพยานหลักฐานว่าบัญชีของตนมิได้มีส่วนร่วมในการกระทำความผิดไปยังพนักงานสอบสวนได้ต่อกองบัญชาการตำรวจสืบสวนอาชญากรรมทางเทคโนโลยีเพื่อให้กองบัญชาการตำรวจสืบสวนอาชญากรรมทางเทคโนโลยีมีหน้าที่รับผิดชอบในการมีคำสั่งว่าจะให้ระงับธุรกรรมต่อไปหรือไม่ และในกรณีที่มิคำสั่งให้ยกเลิกการระงับธุรกรรมนั้นก็ให้สถาบันการเงินหรือผู้ประกอบการยกเลิกการระงับธุรกรรมชั่วคราวทันที และให้อำนาจสถาบันการเงินหรือผู้ประกอบการมีสิทธิยกเลิกการระงับธุรกรรมชั่วคราวได้ หากไม่ได้รับคำสั่งให้ระงับการทำธุรกรรมไว้ต่อไปภายในเวลา 7 วัน นับแต่สถาบันการเงินหรือผู้ประกอบการแจ้งข้อมูลเกี่ยวกับสาเหตุผู้เสียหายขอระงับธุรกรรม

ประการสุดท้าย ปัญหาพนักงานสอบสวนผู้รับผิดชอบตามมาตรา 8 วรรคสอง แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ซึ่งได้วางหลักว่า การร้องทุกข์ในความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีจะกระทำต่อพนักงานสอบสวน ณ สถานีตำรวจหรือต่อกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีก็ได้ และจะร้องทุกข์โดยวิธีการทางอิเล็กทรอนิกส์ก็ได้ และในการสอบสวนหรือดำเนินการเกี่ยวกับการกระทำความผิดดังกล่าว ให้พนักงานสอบสวนที่รับคำร้องทุกข์ไม่ว่าประจำอยู่ที่ใดหรือพนักงานสอบสวนที่ผู้บัญชาการตำรวจแห่งชาติกำหนด เป็นพนักงานสอบสวนผู้รับผิดชอบมีอำนาจสอบสวนและดำเนินการเกี่ยวกับการกระทำความผิดดังกล่าว ไม่ว่าความผิดนั้นจะเกิดขึ้น ณ ที่ใดในราชอาณาจักร หากเกิดกรณีการกระทำความผิดอาชญากรรมทางเทคโนโลยีในท้องที่เดียวโดยไม่คำนึงถึงท้องที่ความผิดที่เกิดขึ้นตามมาตรา 18 วรรคสามแห่งประมวลกฎหมายวิธีพิจารณาความอาญา ดังนั้นหากเป็นพนักงานสอบสวนผู้รับผิดชอบท้องที่ที่มีการสอบสวนซึ่งไม่ใช่ท้องที่ความผิดที่เกิดขึ้นได้สรุปสำนวนส่งไปยังพนักงานอัยการในท้องที่ที่มีการสอบสวน เมื่อพนักงานอัยการได้ยื่นฟ้องไปยังศาลซึ่งไม่ใช่เขตศาลที่ความผิดเกิดขึ้น อ้างหรือเชื่อว่าตามมาตรา 22 แต่อาศัยตามมาตรา 22 (1) โดยอ้างว่าเจ้า

พนักงานทำการสอบสวนในท้องที่หนึ่งนอกเขตของศาลซึ่งเป็นดุลพินิจของศาลว่าจะรับฟ้องหรือไม่ โดยพนักงานอัยการต้องบรรยายฟ้องให้ชัดเจนว่าเหตุใดจึงฟ้องในเขตศาลตามมาตรา 22 (1) ซึ่งศาลอาจมีดุลพินิจไม่รับฟ้องได้ เช่น พิจารณาจากข้อเท็จจริงว่าพยานหลักฐานอยู่ในเขตศาลที่การกระทำความผิดเกิดขึ้นและการดำเนินกระบวนการพิจารณาที่ศาลความผิดเกิดขึ้นจะสะดวกกว่า เป็นต้น หากปรากฏว่าศาลไม่รับคำฟ้องพนักงานอัยการต้องส่งสำนวนกลับไปยังพนักงานสอบสวนผู้รับผิดชอบให้ถูกต้องตามมาตรา 18 วรรคสาม เพื่อให้ดำเนินการสอบสวนและสรุปสำนวนส่งไปยังพนักงานอัยการอีกครั้งเพื่อดำเนินการฟ้องคดีตามมาตรา 22 ดังนี้ ก่อให้เกิดความล่าช้าในการดำเนินคดีแก่ผู้กระทำความผิดอาชญากรรมทางเทคโนโลยี และไม่สอดคล้องกับวัตถุประสงค์ในการดำเนินคดีอาชญากรรมที่จะต้องมีความรวดเร็ว นอกจากนี้ จากการพิจารณากฎหมายของทั้งประเทศสหรัฐอเมริกาและประเทศญี่ปุ่นต่างก็มุ่งสอบสวนในความผิดที่เกิดขึ้นตามท้องที่ความผิดเกิดขึ้น อย่างไรก็ตาม สาเหตุที่มาตรา 8 วรรคสอง วางหลักกฎหมายเช่นนี้ เพื่อแก้ปัญหาที่พนักงานสอบสวนปฏิเสธว่าไม่มีอำนาจสอบสวนเพราะไม่อยู่ในท้องที่ของตนจึงไม่รับคำร้องทุกข์ ดังนั้นจึงวางหลักให้พนักงานสอบสวนทุกท้องที่มีสิทธิรับร้องทุกข์ แต่เขตอำนาจสอบสวนเป็นอย่างไรควรให้ดำเนินการตามประมวลกฎหมายวิธีพิจารณาความอาญาเพื่อลดปัญหาตามมาตรา 22 ตามที่กล่าวมา

นอกจากนี้กรณีเป็นการกระทำความผิดอาชญากรรมทางเทคโนโลยีในราชอาณาจักร เมื่อความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีได้มีการกระทำทั้งในและนอกราชอาณาจักรเกี่ยวพันกัน เมื่อมีผู้เสียหายได้ร้องทุกข์ต่อพนักงานสอบสวนอันมีผลทำให้พนักงานสอบสวนผู้นั้นเป็นพนักงานสอบสวนผู้รับผิดชอบตามมาตรา 8 วรรคสอง แห่งพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 จึงมีปัญหว่าพนักงานสอบสวนต้องส่งสำนวนการสอบสวนไปยังพนักงานอัยการพิจารณาสั่งฟ้องหรือต้องส่งอัยการสูงสุดเป็นผู้สั่งฟ้องตามมาตรา 20 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งตามมาตรา 20 ได้วางหลักว่าให้อัยการสูงสุดเป็นพนักงานสอบสวนผู้รับผิดชอบและมีหน้าที่ในการสั่งสำนวนตามมาตรา 140 ถึง มาตรา 142 โดยมาตรา 20 มีความเห็นที่แตกต่างว่ากรณีใดจะเป็นความผิดซึ่งเกิดนอกราชอาณาจักร แบ่งออกเป็น ดังนี้

ความเห็นแรก ใช้การตีความโดยยึดประมวลกฎหมายอาญาเป็นหลัก โดยความเห็นแรกเห็นว่าความหมายของความผิดที่กระทำนอกราชอาณาจักรตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 20 มีความหมายเฉพาะแต่ความผิดตามประมวลกฎหมายอาญา มาตรา 7 มาตรา 8 และมาตรา 9 เท่านั้น ทั้งนี้ตามคำพิพากษาศาลฎีกาที่ 2679/2559 , 3118/2559 และ 2649/2565

ความเห็นที่สอง การตีความโดยยึดประมวลกฎหมายวิธีพิจารณาความอาญาเป็นหลัก โดยความเห็นที่สองเห็นว่า ให้รวมถึงการกระทำความผิดนอกราชอาณาจักรตามประมวลกฎหมายอาญา มาตรา 4 มาตรา 5 และมาตรา 6 ด้วย เป็นการกระทำความผิดที่ตกอยู่ในบังคับของมาตรา 20 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งมีคำพิพากษาสนับสนุน คือ คำพิพากษาศาลฎีกาที่ 6552/2559 โดยความเห็นนี้เห็นว่า เป็นเรื่องระหว่างประเทศซึ่งกฎหมายที่เกี่ยวข้องกับเรื่องระหว่างประเทศนี้ฝ่ายนิติบัญญัติได้มอบหมายความไว้วางใจให้อัยการสูงสุดเป็นผู้รับผิดชอบตลอดมา ดังนั้น จึงสมควรที่การสอบสวนคดีความผิดซึ่งมี

โทษตามกฎหมายไทยที่ได้กระทำลงนอกราชอาณาจักรจะดำเนินการโดยอัยการสูงสุดหรือผู้รักษาการแทน โดยความเห็นนี้มีผู้ทรงคุณวุฒิทางกฎหมายวิพิจารณาความอาญาหลายท่านเห็นด้วย เช่น ศาสตราจารย์ คณิง ภาไชยและศาสตราจารย์พิเศษ ธาณิศ เกศวพิทักษ์⁸

หากเกิดความไม่แน่นอนในการตีความมาตรา 20 ของศาล แม้จะมีคำพิพากษาปี 2565 สนับสนุน ความคิดเห็นแรก แต่ผู้เขียนเห็นว่าคำพิพากษาเป็นเพียงตัวอย่างในการตีความกฎหมายเท่านั้น และไม่ผูกพัน คำพิพากษาในคดีอื่นด้วย โดยอาจก่อให้เกิดการยกฟ้องเนื่องจากการสอบสวนไม่ถูกต้อง และต้องฟ้องเป็น คดีใหม่ เกิดความล่าช้าในการดำเนินคดีแก่ผู้กระทำความผิด จากการศึกษากฎหมายของประเทศ สหรัฐอเมริกาและประเทศญี่ปุ่นซึ่งเป็นประเทศที่ให้พนักงานอัยการมีบทบาทในการสอบสวนตั้งแต่เริ่มต้น คดีและมีอำนาจควบคุมการปฏิบัติหน้าที่ของหน่วยงานสอบสวนคดี หากเป็นคดีอาญาที่มีความสำคัญ สลับซับซ้อน มีเครือข่ายโยงใยเชื่อมโยงระหว่างประเทศและอาจกระทบต่อระบบเศรษฐกิจหรือความมั่นคง ระหว่างประเทศ อันเป็นกรณีคาบเกี่ยวกับต่างประเทศ หรือเป็นการกระทำความผิดในหลายประเทศเกินกว่า ประเทศหนึ่งขึ้นไปและประเทศสหรัฐอเมริกาหรือประเทศญี่ปุ่นเป็นประเทศหนึ่งที่ได้รับความสะดวก พนักงานอัยการย่อมมีอำนาจหน้าที่ในการสอบสวนและรับผิดชอบในคดีอาญานั้นได้เอง

จากการศึกษาอาชญากรรมทางเทคโนโลยี ประเภทของอาชญากรรมทางเทคโนโลยี แนวคิดเกี่ยวกับการ สอบสวน มาตรการการปราบปรามอาชญากรรมทางเทคโนโลยีทั้งในประเทศไทยและต่างประเทศ ดังนี้ ผู้เขียนมีข้อเสนอแนะเกี่ยวกับการปรับปรุงแก้ไขพระราชกำหนดมาตรการป้องกันและปราบปราม อาชญากรรมทางเทคโนโลยี ดังนี้

ประการแรก แก้ไขคำนิยาม “อาชญากรรมทางเทคโนโลยี”

เพื่อให้คำนิยามอาชญากรรมทางเทคโนโลยีรวมถึงความผิดเกี่ยวกับฐานปลอมบัตร อิเล็กทรอนิกส์ด้วย ผู้เขียนเสนอแนะแก้ไขคำนิยาม “อาชญากรรมทางเทคโนโลยี” ในมาตรา 3 ดังนี้

“อาชญากรรมทางเทคโนโลยี” หมายความว่า การกระทำหรือพยายามกระทำความผิดตาม กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง ทุจริต หรือฉ้อโกงทรัพย์สินบุคคลหนึ่ง บุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกง ทุจริต หรือฉ้อ โกงทรัพย์สิน โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ หรือกระทำความผิดตามมาตรา 269/1 แห่งประมวล กฎหมายอาญา”

ประการที่สอง แก้ไขวิธีการและระยะเวลาการจับกุมหรือควบคุมตัวมาตรา 7 เพื่อเปิดโอกาสให้เจ้าของ บัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ผู้รับ โอนแสดงพยานหลักฐานว่าไม่มีส่วนเกี่ยวข้องกับ อาชญากรรมทางเทคโนโลยีและกำหนดระยะเวลาการมีคำสั่งเกี่ยวกับการจับกุมหรือควบคุมตัวให้ชัดเจน เพื่อคุ้มครองประโยชน์ของเจ้าของบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ โดยให้กองบัญชาการตำรวจ

⁸อุทัย อาภิเวช, การสอบสวน, พิมพ์ครั้งที่ 1 (กรุงเทพฯ : ห้างหุ้นส่วนจำกัด วิ.เจ พรินติ้ง, 2562), หน้า 305-309

สืบสวนอาชญากรรมทางเทคโนโลยีมีอำนาจในการพิจารณาการระงับธุรกรรมชั่วคราวต่อไปหรือไม่ ผู้เขียนเสนอแนะให้แก้ไข ดังนี้

“มาตรา 7 ในกรณีที่สถาบันการเงินหรือผู้ประกอบการธุรกิจได้รับแจ้งจากผู้เสียหายซึ่งเป็นผู้ถือบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ว่า ได้มีการทำธุรกรรมโดยบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ดังกล่าวและเข้าข่ายเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี ให้สถาบันการเงินหรือผู้ประกอบการธุรกิจดังกล่าวมีหน้าที่ระงับการทำธุรกรรมนั้นไว้ชั่วคราว พร้อมทั้งนำข้อมูลเข้าสู่ระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลตามมาตรา 4 เพื่อให้สถาบันการเงินและผู้ประกอบการธุรกิจได้รับโอนทุกทอดทราบและระงับการทำธุรกรรมดังกล่าวไว้ทันที รวมถึงแจ้งให้เจ้าของบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ และกองบัญชาการตำรวจสืบสวนอาชญากรรมทางเทคโนโลยีทราบในการระงับธุรกรรมดังกล่าว และแจ้งให้ผู้เสียหายไปร้องทุกข์ต่อพนักงานสอบสวน เมื่อมีการร้องทุกข์แล้ว ให้พนักงานสอบสวนแจ้งให้สถาบันการเงินหรือผู้ประกอบการธุรกิจที่ได้รับการทำธุรกรรมไว้ทราบ และให้พนักงานสอบสวนแจ้งให้กองบัญชาการตำรวจสืบสวนอาชญากรรมทางเทคโนโลยีทราบเพื่อดำเนินการสอบสวนเกี่ยวกับอาชญากรรมทางเทคโนโลยี

ในกรณีที่สถาบันการเงินหรือผู้ประกอบการธุรกิจระงับการทำธุรกรรมนั้นไว้ชั่วคราวตามวรรคหนึ่ง ให้กองบัญชาการตำรวจสืบสวนอาชญากรรมทางเทคโนโลยีพิจารณาดำเนินการเกี่ยวกับบัญชีเงินฝากและบัญชีอิเล็กทรอนิกส์ดังกล่าวภายใน 7 วันนับแต่วันที่ได้รับแจ้งจากสถาบันการเงินหรือผู้ประกอบการธุรกิจ และแจ้งผลคำสั่งให้สถาบันการเงินหรือผู้ประกอบการธุรกิจทราบโดยพลัน

ทั้งนี้ เจ้าของบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ผู้รับโอนจะร้องขอต่อกองบัญชาการตำรวจสืบสวนอาชญากรรมทางเทคโนโลยี ให้มีคำสั่งยกเลิกการระงับการทำธุรกรรมโดยวงเงินหรือหาประกันมาให้แทนก็ได้ ถ้ากองบัญชาการตำรวจสืบสวนอาชญากรรมทางเทคโนโลยีพอใจในเงินหรือประกันก็ให้เพิกถอนคำสั่งยกเลิกการระงับการทำธุรกรรมดังกล่าวและรับเงินหรือประกันนั้นไว้ และแจ้งคำสั่งยกเลิกการระงับการทำธุรกรรมให้สถาบันการเงินหรือผู้ประกอบการธุรกิจทราบโดยพลัน

หากกองบัญชาการตำรวจสืบสวนอาชญากรรมทางเทคโนโลยีไม่มีคำสั่งให้ระงับการทำธุรกรรมภายในกำหนดระยะเวลาตามวรรคสอง หรือมีคำสั่งยกเลิกการระงับการทำธุรกรรมเพราะเหตุอื่นใดหรือเพราะเหตุตามวรรคสาม ให้สถาบันการเงินหรือผู้ประกอบการธุรกิจยกเลิกการระงับการทำธุรกรรมนั้น”

ประการที่สาม แก้ไขให้การเป็นพนักงานสอบสวนผู้รับผิดชอบให้เป็นไปตามประมวลกฎหมายวิธีพิจารณาความอาญา และแก้ไขกรณีอาชญากรรมทางเทคโนโลยีที่มีการกระทำส่วนหนึ่งเกิดขึ้นนอกราชอาณาจักรกับส่วนใดเกิดในราชอาณาจักรให้พนักงานสอบสวนผู้รับผิดชอบเป็นอัยการสูงสุด ตามมาตรา 20 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา

ทั้งนี้ เพื่อไม่ให้มีปัญหาข้อกฎหมายเกี่ยวกับเขตอำนาจสอบสวนในท้องที่ความผิดทั้งเดียวและความผิดที่เกิดขึ้นทั้งในและนอกราชอาณาจักร รวมถึงปัญหาเรื่องเขตอำนาจศาล ผู้เขียนเสนอแนะให้แก้ไขมาตรา 8 วรรคสอง และเพิ่มเติมมาตรา 8 วรรคสาม ดังนี้

“...การร้องทุกข์ในความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีจะกระทำต่อพนักงานสอบสวน ณ สถานีตำรวจแห่งใดในราชอาณาจักรหรือต่อกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีก็ได้ และจะร้องทุกข์โดยวิธีการทางอิเล็กทรอนิกส์ก็ได้ โดยให้ถือว่าเป็นการร้องทุกข์โดยชอบด้วยประมวลกฎหมายวิธีพิจารณาความอาญา และให้พนักงานสอบสวนที่ได้รับการร้องทุกข์ส่งคำร้องทุกข์ไปยังพนักงานสอบสวนที่มีอำนาจสอบสวนตามมาตรา 18 มาตรา 19 แห่งประมวลกฎหมายวิธีพิจารณาความอาญาแล้วแต่กรณี

ถ้ามีการร้องทุกข์ตามวรรคหนึ่ง และพนักงานสอบสวนดำเนินการสอบสวนความผิดอาชญากรรมทางเทคโนโลยี ปรากฏว่าเป็นการกระทำส่วนหนึ่งส่วนใดเกิดขึ้นในราชอาณาจักรให้พนักงานสอบสวนดำเนินการตามมาตรา 20 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา”

เอกสารอ้างอิง

โปลิต สุขสว่าง, “ปัญหาการบังคับใช้กฎหมายเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์,” วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย, 2563.

อุทัย อาทิวะ. การสอบสวน. พิมพ์ครั้งที่ 1 กรุงเทพฯ : ห้างหุ้นส่วนจำกัด วิ.เจ พรินติ้ง, 2562.

สถานีประชาชน ไทยพีบีเอส, กลโกงบัตรอิเล็กทรอนิกส์ [Online], Available URL:

https://www.facebook.com/photo.php?fbid=710034917837605&set=a.360386166135817&type=3&locale=th_TH&_rdr

EG Eisner Gorin LLP. FEDERAL SEARCH AND SEIZURE (Online) Available

URL:<https://www.egattorneys.com/federal-search-and-seizure>.

United States Secret Service. ATM & POS Skimming (Online), Available URL:

<https://www.secretservice.gov/investigations/skimming>.

กฎหมาย

ประมวลกฎหมายวิธีพิจารณาความแพ่ง

ประมวลกฎหมายวิธีพิจารณาความอาญา

ประมวลกฎหมายอาญา

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

พระราชบัญญัติว่าด้วยการระงับความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

Act on Payment of Damage Recovery Benefits from Funds in Deposit Accounts Used for Crime