ปัญหาการบังคับใช้กฎหมายเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

นายโปลิต สุขสว่าง

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์ ไม่สังกัดภาควิชา/เทียบเท่า
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2563

THE PROBLEM OF LAW ENFORCEMENT RELATED TO OBTAINING ELECTRONIC CARD INFORMATION

Mr. Polit Suksawang

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Laws in Laws

Common Course

FACULTY OF LAW

Chulalongkorn University

Academic Year 2020

หัวข้อวิทยานิพนธ์	ปัญหาการบังคับใช้กฎหมายเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์
โดย	นายโปลิต สุขสว่าง
สาขาวิชา	นิติศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	อาจารย์ ดร.ปราโมทย์ เสริมศีลธรรม

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต

..... คณบดีคณะนิติศาสตร์
(ผู้ช่วยศาสตราจารย์ ดร.ปารีณา ศรีวนิชย์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์มัทยา จิตติรัตน์)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(อาจารย์ ดร.ปราโมทย์ เสริมศีลธรรม)

..... กรรมการภายนอกมหาวิทยาลัย
(พันตำรวจเอก ดร.วิวัฒน์ สิทธิสรเดช)

..... กรรมการภายนอกมหาวิทยาลัย
(พันตำรวจโทพงศ์พจน์ ธรรมากุลวิชช์)

โปลิต สุขสว่าง : ปัญหาการบังคับใช้กฎหมายเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์. (THE PROBLEM OF LAW ENFORCEMENT RELATED TO OBTAINING ELECTRONIC CARD INFORMATION) อ.ที่ปรึกษาหลัก : อ. ดร.ปราโมทย์ เสริมศีลธรรม

วิทยานิพนธ์ฉบับนี้มีวัตถุประสงค์เพื่อศึกษาปัญหาการบังคับใช้กฎหมายที่เกี่ยวข้องกับการกระทำความผิดในลักษณะการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ อุปสรรคที่เกิดขึ้นจากการนำกฎหมายไทยมาปรับใช้กับการกระทำความผิดในรูปแบบต่างๆ ตลอดจนศึกษาแนวคิด ความคุ้มครอง และบทบัญญัติกฎหมายต่างประเทศที่เกี่ยวข้อง เพื่อนำมาวิเคราะห์เปรียบเทียบและเสนอแนวทางที่เหมาะสมในการกำหนดบทบัญญัติกฎหมายในประเทศไทย

จากการศึกษาพบว่า การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ยังคงเป็นการกระทำความผิดที่เกิดขึ้นในประเทศไทยเป็นอย่างมาก และจากการพิเคราะห์บทบัญญัติกฎหมายอาญาในประเทศไทยพบว่า ไม่มีบทบัญญัติเฉพาะที่เหมาะสมในการบังคับใช้กับลักษณะการกระทำความผิดในรูปแบบนี้ได้โดยตรง และบทบัญญัติกฎหมายที่มีอยู่แล้วก็ไม่สามารถคุ้มครองข้อมูลที่เกิดจากการดึงได้อย่างครบถ้วน อันทำให้เกิดปัญหาการบังคับใช้กฎหมาย เมื่อได้พิจารณาถึงบทบัญญัติกฎหมายของต่างประเทศพบว่า สหรัฐอเมริกา สหราชอาณาจักร สาธารณรัฐฟิลิปปินส์และเครือรัฐออสเตรเลีย ก็ต่างมีบทบัญญัติที่ใช้บังคับกับการกระทำความผิดในลักษณะนี้อันเป็นการเฉพาะและมีความครอบคลุมไม่แตกต่างกัน

ด้วยเหตุที่กล่าวมาข้างต้น ผู้เขียนวิทยานิพนธ์จึงเสนอให้มีการกำหนดบทบัญญัติอันเป็นการเฉพาะอันเป็นความผิดตามกฎหมายอาญา เพื่อบังคับใช้กับการกระทำความผิดในลักษณะการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ โดยนำประเด็นต่างๆ ที่กฎหมายของต่างประเทศได้กำหนดไว้มาเป็นแนวทางในการปรับใช้ให้เหมาะสมกับบริบทในสังคมไทย อันก่อให้เกิดประโยชน์สูงสุดในการคุ้มครองข้อมูลจากบัตรอิเล็กทรอนิกส์ ทั้งป้องกันและปราบปรามการกระทำความผิดที่เกิดขึ้นต่อไป

สาขาวิชา นิติศาสตร์ ลายมือชื่อนิสิต .....
ปีการศึกษา 2563 ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

5985990534 : MAJOR LAWS
KEYWORD: Electronic Card, Obtaining data, Electronic Card Information

Polit Suksawang : THE PROBLEM OF LAW ENFORCEMENT RELATED TO OBTAINING ELECTRONIC CARD INFORMATION. Advisor: Pramote Sermsilatham, Ph.D.

This thesis focuses on studying the problem of law enforcement related to illegally obtaining electronic card information, the various obstacles to dealing with the offence as well as the relevant concepts, protections and foreign legislations in order to analyze, compare and suggest the appropriate provision for Thailand.

According to researches, obtaining electronic card information is one of the frequently committed offences in Thailand nowadays. Meanwhile, it can be seen that there is no specific provision tackling this offence directly. The existing provisions cannot entirely protect the information from illegal obtaining. On the contrary, many countries such as the United States, the United Kingdom, the Republic of Philippines and Australia have distinct and comprehensive provision handling this offence.

Consequently, the author of this thesis suggests that Thailand should enact a specific provision of criminal offence of obtaining electronic card information by properly applying the concept of the relevant foreign legislations in order to protect the information as well as to prevent and control this crime effectively.

Field of Study: Laws Student's Signature .....

Academic Year: 2020 Advisor's Signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี เนื่องจากได้รับความเมตตาและอนุเคราะห์เป็นอย่างสูงจากท่านอาจารย์ ดร.ปราโมทย์ เสริมศีลธรรม ที่ได้กรุณาสละเวลาอันมีค่ายิ่งของท่านรับเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ ทั้งยังให้ความรู้ คำแนะนำ คำปรึกษา ตรวจทานและแก้ไขในการเขียนวิทยานิพนธ์ฉบับนี้ ตลอดจนให้กำลังใจ ให้ความช่วยเหลือและเชื่อมั่นในตัวผู้วิจัยเสมอมา จนสามารถทำวิทยานิพนธ์ออกมาได้อย่างสมบูรณ์ ผู้วิจัยจึงขอกราบขอบพระคุณท่านอาจารย์เป็นอย่างสูง

ผู้วิจัยขอกราบขอบพระคุณท่านรองศาสตราจารย์มัทยา จิตติรัตน์ ที่ได้กรุณารับเป็นประธานกรรมการสอบวิทยานิพนธ์ และขอกราบขอบพระคุณท่านพันตำรวจเอก ดร.วิวัฒน์ สิทธิสรเดช และท่านพันตำรวจโทพงศ์พจน์ ธรรมากุลวิชช์ ที่ได้กรุณารับเป็นกรรมการสอบวิทยานิพนธ์ ตลอดจนให้ความรู้ความเห็นและคำแนะนำที่เป็นประโยชน์อันช่วยให้วิทยานิพนธ์ฉบับนี้มีความสมบูรณ์มากยิ่งขึ้น

ผู้วิจัยขอกราบขอบพระคุณ คุณมนูญ สุขสว่าง และคุณสุจิตร สุขสว่าง ผู้เป็นบิดามารดาของผู้วิจัย ซึ่งได้ให้กำเนิด เลี้ยงดู อบรมสั่งสอน ให้โอกาสทางการศึกษา และยังให้ความรัก ความเข้าใจ ตลอดจนให้กำลังใจและสนับสนุนผู้วิจัยในทุกเรื่อง และขอบคุณนางสาวยลรดี สุขสว่าง ผู้เป็นน้องสาว ที่คอยให้กำลังใจแก่ผู้วิจัยเสมอมา ซึ่งบุคคลทั้งหมดเหล่านี้ต่างเป็นแรงผลักดันให้ผู้วิจัยสามารถผ่านพ้นอุปสรรคและสามารถทำวิทยานิพนธ์จนสำเร็จลุล่วงไปได้ด้วยดี

ผู้วิจัยขอขอบคุณเพื่อนๆ รหัส 59 หลักสูตรนิติศาสตรมหาบัณฑิต สาขากฎหมายอาญาและกระบวนการยุติธรรมทางอาญาทุกท่านที่คอยช่วยเหลือผู้ทำวิจัยเสมอมา โดยเฉพาะนายชินวัตร บุญส่ง สุวรรณ์ และนายชลัฎ ฟองกษีร ที่คอยช่วยเหลือ รับฟังปัญหาและให้กำลังใจแก่ผู้วิจัยในช่วงสุดท้ายของการทำวิทยานิพนธ์ฉบับนี้ ทำให้ผู้วิจัยสามารถดำเนินการทุกอย่างให้สำเร็จไปได้ด้วยดี

ในท้ายที่สุด ผู้วิจัยอยากจะขอกราบขอบพระคุณท่านศาสตราจารย์วีระพงษ์ บุญโญภาส ที่ได้ให้ความรู้ ความเมตตาและได้มอบโอกาสให้ผู้วิจัยได้ทำงานวิจัยฉบับนี้ ถึงแม้ท่านจะถึงแก่อนิจกรรมไปก่อนที่วิทยานิพนธ์ฉบับนี้ได้เสร็จสมบูรณ์ แต่ผู้วิจัยยังพึงระลึกเสมอถึงความตั้งใจอันดีของท่าน ที่ต้องการให้เกิดการศึกษาวิจัยในหัวข้อวิทยานิพนธ์ฉบับนี้ อันเป็นการก่อให้เกิดประกายความคิดในการพัฒนากฎหมายที่จะเป็นประโยชน์แก่สังคมไทยในอนาคตต่อไป ผู้วิจัยจึงได้ตั้งใจทำวิทยานิพนธ์ฉบับนี้ให้ออกมาอย่างสมบูรณ์ ครบถ้วนที่สุดและขอสำนึกในพระคุณของท่านตลอดไป

โปลิต สุขสว่าง

สารบัญ

หน้า

สารบัญตาราง

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

นับตั้งแต่วิทยาการและเทคโนโลยีในการดำเนินธุรกรรมทางการเงินได้พัฒนาไปอย่างมาก การทำธุรกรรมทางการเงินจากเดิมโดยทั่วไปซึ่งจะต้องชำระกันด้วยเงินสด และการฝากถอนเงินจากธนาคารซึ่งจะต้องดำเนินการผ่านบุคลากรของธนาคารอันใช้เวลาในการดำเนินการมาก จึงถูกแทนที่ด้วยเทคโนโลยีรูปแบบใหม่คือการชำระเงินหรือการถอนเงินผ่านเครื่องมืออิเล็กทรอนิกส์โดยอาศัยบัตรอิเล็กทรอนิกส์ประเภทต่างๆ เช่น บัตรเอทีเอ็ม (ATM Card) บัตรเดบิต (Debit Card) บัตรเครดิต (Credit Card) หรือผ่านอุปกรณ์อิเล็กทรอนิกส์อื่น เช่น โทรศัพท์มือถือ เทคโนโลยีเหล่านี้ได้ถูกนำมาใช้เพื่อเอื้ออำนวยความสะดวกในการทำธุรกรรมทางการเงินแก่ผู้ใช้บริการของธนาคารนั้นๆ ทั้งยังเป็นการประหยัดเวลาและลดภาระงานของบุคลากรในธุรกิจทางการเงินได้อย่างมาก อันเป็นวิธีที่ทั่วโลกต่างนำมาใช้ปฏิบัติอย่างเป็นสากล สนองต่อการทำธุรกรรมทางเงินในปัจจุบันที่ต้องการความรวดเร็วในภาวะที่แนวโน้มทางเศรษฐกิจมีอัตราการขยายตัวเพิ่มสูงขึ้น การประกอบธุรกิจของธนาคารซึ่งเป็นผู้ให้บริการด้วยกันจึงต้องแข่งขันช่วงชิงความได้เปรียบจากเทคโนโลยีดังกล่าวเพื่อดึงดูดให้มีผู้ใช้บริการของตนมากขึ้น โดยการทำให้ผู้ใช้บริการสามารถเข้าถึงสิ่งอำนวยความสะดวกในการทำธุรกรรมทางการเงินให้ได้มากที่สุด อาทิ การเพิ่มจุดบริการของเครื่องจ่ายเงินอัตโนมัติ (Automated teller machine : ATM) ให้ครอบคลุมพื้นที่ต่างๆ หรือการรับชำระเงินที่จุดบริการขาย (Point of sale) ที่ผู้ใช้บริการได้ทำการซื้อสินค้าและบริการนั้นๆ ซึ่งการดำเนินการดังกล่าวต้องใช้ควบคู่ไปกับบัตรอิเล็กทรอนิกส์ประเภทต่างๆ ที่ทางธนาคารได้ออกให้แก่ผู้ใช้บริการ[1] และการทำธุรกรรมด้วยบัตรอิเล็กทรอนิกส์ของธนาคารดังกล่าว ผู้ใช้บริการอาจได้รับสิทธิประโยชน์อย่างอื่นนอกจากความสะดวกอีกด้วย เช่น ผู้ใช้บริการไม่ต้องเสียค่าธรรมเนียมในโอนหรือถอนเงิน การสะสมแต้มคะแนนแลกสิทธิพิเศษ การลดค่าธรรมเนียมบัตร อันเป็นทางเลือกให้แก่ผู้ใช้บริการในการตัดสินใจสมัครเข้ามาใช้บริการของธนาคารนั้นๆ เพื่อประโยชน์ทางธุรกิจของตน ประกอบกับการทำธุรกรรมด้วยบัตรอิเล็กทรอนิกส์นั้นหาได้จำกัดอยู่แต่เพียงภายในประเทศไม่ แต่ยังสามารถนำบัตร

[1] ในปัจจุบัน การถอนเงินจากเครื่องจ่ายเงินอัตโนมัติสามารถทำได้โดยไม่จำต้องมีตัวบัตรอิเล็กทรอนิกส์ร่วมด้วย เรียกว่า การถอนเงินโดยไม่ใช้บัตร อันเป็นการถอนเงินจากบัญชีเงินฝาก บัตรเครดิต หรือสินเชื่อหมุนเวียน ภายใต้เงื่อนไขที่ธนาคารได้กำหนดไว้ ดู ธนาคารไทยพาณิชย์, "กดเงินไม่ใช้บัตร" [ออนไลน์], เข้าถึงเมื่อ 2 กุมภาพันธ์ 2563. แหล่งที่มา: https://www.scb.co.th/th/personal-banking/digital-banking/scb-easy/how-to/cardless.html.

อิเล็กทรอนิกส์ของผู้ให้บริการด้านการชำระเงินข้ามประเทศ (Multinational Financial Corporation) อันเป็นที่ยอมรับกันในต่างประเทศ เช่น บัตรวีซ่า (VISA) บัตรมาสเตอร์การ์ด (MasterCard) ไปใช้ทำธุรกรรมผ่านระบบเครือข่ายอิเล็กทรอนิกส์แก่ธนาคารต่างๆ ได้ทั่วโลก เนื่องด้วยเหตุดังกล่าว บัตรอิเล็กทรอนิกส์จึงนับว่าเป็นสิ่งที่มีความสำคัญต่อการดำรงชีพในด้านการทำธุรกรรมทางการเงินในปัจจุบัน อันมีผลต่อการไหลเวียนของเงินในระบบเศรษฐกิจ ไม่ว่าจะในด้านจุลภาคโดยผ่านปัจเจกบุคคล หรือในด้านมหภาคโดยผ่านการทำธุรกรรมภายในประเทศและในต่างประเทศ

อย่างไรก็ดี แม้ว่าการใช้บัตรอิเล็กทรอนิกส์นั้นจะเป็นสิ่งอำนวยความสะดวกและสร้างผลประโยชน์นานัปการในทางเศรษฐกิจก็ตาม แต่เนื่องด้วยประโยชน์อันเป็นจำนวนเงินมหาศาลและลักษณะเฉพาะตัวของบัตรอิเล็กทรอนิกส์ที่ประกอบด้วยข้อมูลส่วนบุคคลและข้อมูลทางธนาคารของผู้มีสิทธิใช้บัตรนั้น จึงเป็นสิ่งล่อใจให้อาชญากรพัฒนาเทคนิคและวิธีการให้ได้มาซึ่งเงินหรือข้อมูลในบัตรอิเล็กทรอนิกส์ อันเปรียบเสมือนดาบสองคมอันเกิดแก่การใช้เทคโนโลยีอันหลีกเลี่ยงไม่ได้ โดยการใช้อุปกรณ์ต่างๆ ที่พัฒนาขึ้นมาโดยเฉพาะ ในการดึงเอาข้อมูลออกจากบัตรอิเล็กทรอนิกส์นั้น เช่น การสกิมมิ่ง (Skimming) โดยการใช้เครื่องสกิมเมอร์ (Skimmer) แบบติดตั้งเข้ากับเครื่องจ่ายเงินอัตโนมัติ (ATM Skimmer) เครื่องจ่ายน้ำมันของปั้ม (Gas Pump Skimmer)[2] หรือแบบพกพา (Handheld Skimmer) หรือการดึงข้อมูลบัตรอิเล็กทรอนิกส์ที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ โดยการติดตั้งโปรแกรมมัลแวร์ (Malware) หรือไวรัส (Virus) เข้าไปในเครื่องคอมพิวเตอร์ผ่านทางการใช้งานระบบอินเตอร์เน็ต (Web skimmer)[3] หรือติดตั้งเข้าไปในเครื่องจ่ายเงินอัตโนมัติ (ATM Malware)[4] เพื่อที่จะนำข้อมูลในบัตรอิเล็กทรอนิกส์ดังกล่าวนั้น ไปใช้ในการกระทำความผิดอื่นๆ ต่อไป เช่น การปลอมบัตรอิเล็กทรอนิกส์และนำบัตรที่ได้ทำปลอมขึ้นไปกดเงิน การนำข้อมูลในบัตรอิเล็กทรอนิกส์ไปดัดแปลง แก้ไข ส่งต่อหรือขายต่อให้แก่ผู้กระทำความผิดคนอื่นๆ

---

[2] Krebsonsecurity, "Gas Theft Gangs Fuel Pump Skimming Scams" [Online], Accessed: 2 February 2020. Available from: https://krebsonsecurity.com/tag/gas-pump-skimmers/.

[3] Jérôme Segura, "Web Skimmer Phishes Credit Card Data Via Rogue Payment Service Platform" [Online], Accessed: 2 February 2020. Available from: https://blog.malwarebytes.com/web-threats/2019/11/web-skimmer-phishes-credit-card-data-via-rogue-payment-service-platform/.

[4] David Sancho, "Atm Malware on the Rise" [Online], Accessed: 2 February 2020. Available from: https://blog.trendmicro.com/trendlabs-security-intelligence/atm-malware-on-the-rise/?_ga=2.110755589.1613302766.1580972794-179933209.1580972794.

การนำข้อมูลดังกล่าวไปกรรโชกหรือรีดเอาทรัพย์จากเจ้าของข้อมูล ตลอดจนถึงการนำข้อมูลในบัตรอันเป็นความลับไปเปิดเผยแก่สาธารณชน

ในปัจจุบันแม้ว่าธนาคารแห่งประเทศไทยได้ผลักดันให้ธนาคารพาณิชย์เปลี่ยนการออกบัตรเอทีเอ็มและบัตรเดบิตแบบแถบแม่เหล็ก (Magnetic Card) ให้เป็นบัตรแบบชิปการ์ด (Chip Card) โดยใช้เทคโนโลยีไมโครชิปอีเอ็มวี (EMV Chip Card)[5] ให้แก่ลูกค้า[6] เพื่อยกระดับความปลอดภัยในการใช้บัตรอิเล็กทรอนิกส์ อาทิ การป้องกันการปลอมแปลงบัตร (Counterfeit Card Fraud) และการโจรกรรมข้อมูล (Skimming) อันมีผลทำให้บัตรอิเล็กทรอนิกส์ของธนาคารพาณิชย์นั้นประกอบไปด้วยชิปการ์ดด้านหน้าและแถบแม่เหล็กด้านหลังของบัตรควบคู่กันในการใช้งาน แต่จากการศึกษากรณีตัวอย่างในต่างประเทศที่ได้มีการเปลี่ยนรูปแบบของบัตรอิเล็กทรอนิกส์ดังกล่าวมานานก่อนประเทศไทยแล้วนั้นพบว่า ยังไม่สามารถป้องกันการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้อย่างสมบูรณ์ เพียงแต่ทำให้การดึงเอาข้อมูลออกจากบัตรประเภทดังกล่าวทำได้ยากขึ้นกว่าเดิม[7] และจากการทำงานอันซับซ้อนของเทคโนโลยีนี้เอง เมื่อเกิดการพยายามดึงข้อมูลออกจากชิปการ์ด จะทำให้เกิดกรณีที่อุปกรณ์อิเล็กทรอนิกส์ เช่น เครื่องจ่ายเงินอัตโนมัติ กลับไปอ่านค่าแถบแม่เหล็กหลังบัตร

[5] EMV มีที่มาจากคำว่า Europay, Mastercard and Visa ซึ่งเป็นสามบริษัทแรกที่สร้างมาตรฐานของการใช้บัตรชำระเงินอัจฉริยะ (Smart payment cards) การชำระเงินปลายทาง (Payment terminals หรือ Point of Sale : POS) และเครื่องจ่ายเงินอัตโนมัติ

[6] โดยธนาคารแห่งประเทศไทยได้เริ่มผลักดันให้ธนาคารพาณิชย์ทุกแห่ง ออกบัตรเอทีเอ็มและบัตรเดบิตประเภทชิปการ์ดแทนการออกบัตรเอทีเอ็มและบัตรเดบิตประเภทแถบแม่เหล็ก เริ่มมีผลใช้บังคับเมื่อวันที่ 16 พฤษภาคม 2559 เป็นต้นมา ซึ่งบัตรประเภทแถบแม่เหล็กที่มีอยู่เดิม ยังคงสามารถใช้ทำธุรกรรมทางการเงินกับตู้เอทีเอ็มทุกตู้ได้ตามปกติจนถึงวันที่ 31 ธันวาคม 2562 และขยายระยะเวลาเป็นวันที่ 15 มกราคม 2563 ที่ผ่านมา ดู ธนาคารแห่งประเทศไทย, ข่าวธนาคารแห่งประเทศไทย ฉบับที่ 25/2559 เรื่อง ข้อเท็จจริงเกี่ยวกับบัตรเอทีเอ็มและบัตรเดบิตแบบชิป (Chip Card) [ออนไลน์], 2 กุมภาพันธ์ 2563. แหล่งที่มา https://www.bot.or.th/Thai/PressandSpeeches/Press/News2559/n2559t.pdf. และ ธนาคารแห่งประเทศไทย, ข่าวธนาคารแห่งประเทศไทย ฉบับที่ 49/2562 เรื่องการเปลี่ยนบัตรเดบิตและบัตรเอทีเอ็มเป็นบัตรแบบชิปการ์ด [ออนไลน์], 2 กุมภาพันธ์ 2563. แหล่งที่มา https://www.bot.or.th/Thai/PressandSpeeches/Press/News2562/n4962t.pdf.

[7] Megan Geuss, "An Atm Hack and a Pin-Pad Hack Show Chip Cards Aren't Impervious to Fraud" [Online], Accessed: 3 February 2020. Available from: https://arstechnica.com/information-technology/2016/08/an-atm-hack-and-a-pin-pad-hack-show-chip-cards-arent-impervious-to-fraud/.

อันนำไปสู่การดึงข้อมูลออกจากแถบแม่เหล็กด้านหลังบัตรได้ง่ายดังเดิม[8] และยังคงพบการกระทำความผิดดังกล่าวได้อยู่ในต่างประเทศ[9]

จากการศึกษาพบว่า การกระทำความผิดในลักษณะของการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ยังคงเกิดขึ้นในประเทศไทยเสมอมา[10] อันเป็นปัญหาสำคัญซึ่งกระทบต่อการคุ้มครองข้อมูลส่วนบุคคลและข้อมูลของธนาคารพาณิชย์ซึ่งก่อให้เกิดความเสียหายในเชิงทรัพย์สิน ทั้งยังกระทบต่อความเชื่อมั่นในการใช้บัตรอิเล็กทรอนิกส์ในการทำธุรกรรมทางการเงิน สร้างความเสียหายต่อระบบเศรษฐกิจของประเทศ เป็นปัญหาสังคมที่จำต้องแก้ไขโดยบทบัญญัติของกฎหมาย เพื่อป้องปราบไม่ให้เกิดการกระทำความผิดและเพื่อนำผู้กระทำความผิดดังกล่าวมาลงโทษ แต่จากการพิเคราะห์บทบัญญัติของกฎหมายในประเทศไทยที่มีใช้อยู่แล้วพบว่า เมื่อนำลักษณะของการกระทำความผิดดังกล่าวที่เกิดขึ้นมาปรับกับบทบัญญัติของกฎหมายแล้วจะทำให้เกิดปัญหาของการบังคับใช้กฎหมายหลายประการดังนี้

1.1.1 ไม่มีบทบัญญัติของกฎหมายที่ใช้บังคับกับลักษณะการกระทำความผิดในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้โดยตรง

การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ไม่สามารถลงโทษผู้กระทำความผิดฐานลักทรัพย์ได้ เพราะข้อมูลอิเล็กทรอนิกส์ ไม่ใช่ทรัพย์ตามคำจำกัดความในประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 137 การเข้าถึงและเอาไปซึ่งข้อมูลดังกล่าวจึงไม่มีความผิดฐานลักทรัพย์[11] อันเป็นที่มาของการแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547 และการบังคับใช้พระราชบัญญัติว่า

[8] Danny Bradbury, "Has Chip-and-Pin Failed to Foil Fraudsters?" [Online], Accessed: 3 February 2020. Available from: https://www.theguardian.com/technology/2008/jan/03/hitechcrime.news.

[9] จำนวนสถิติในประเทศอังกฤษปี 2018 ดู Megan Geuss, Why aren't chip credit cards stopping "card present" fraud in the US? [Online], 3 February 2020. Available from: https://arstechnica.com/information-technology/2018/11/why-arent-chip-credit-cards-stopping-card-present-fraud-in-the-us/. และจำนวนสถิติในประเทศออสเตรเลียปี 2018 ดู Australian Payment Network, AUSTRALIAN PAYMENT CARD FRAUD 2018 [Online], 3 February 2020. Available from: https://www.auspaynet.com.au/sites/default/files/2018-08/AustralianPaymentCardFraud-2018-Report.pdf.

[10] ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน (ศคง.), "รายงานผลการดำเนินงานของศูนย์คุ้มครองผู้ใช้บริการทางการเงิน (ศคง.) ในการให้ข้อมูล/คำปรึกษา และรับเรื่องร้องเรียน ปี 2561," (3 มกราคม 2562).

[11] เทียบคำพิพากษาศาลฎีกาที่ 5161/2547

ด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เนื่องจากในขณะนั้นยังไม่มีบทบัญญัติของกฎหมายที่เป็นการคุ้มครองข้อมูลอิเล็กทรอนิกส์ดังกล่าว

พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547 มาตรา 3 ได้เพิ่มความเป็น (14) ของมาตรา 1 แห่งประมวลกฎหมายอาญา โดยการกำหนดคำว่า “บัตรอิเล็กทรอนิกส์” แล้วนั้น แต่จากความหมายของคำว่า “บัตรอิเล็กทรอนิกส์” ตามมาตรา 1(14) ทั้ง (ก) และ (ข) พบว่า มาตรา 1(14)(ก) นั้นระบุให้ “เอกสารหรือวัตถุอื่นใด” เป็น “บัตรอิเล็กทรอนิกส์” โดยมุ่งถึงตัวบัตรที่เป็นกายภาพหรือรูปธรรมเป็นสำคัญ และมาตรา 1(14)(ข) นั้นระบุให้ “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” เป็น “บัตรอิเล็กทรอนิกส์” ด้วย โดยมุ่งถึงข้อมูลเกี่ยวกับบัตรนั้นที่เป็นนามธรรมเป็นสำคัญ แต่เนื่องจากมาตรา 1(14)(ข) ได้ระบุเพิ่มเติมต่อไปด้วยว่าข้อมูลที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิจะใช้นั้นต้อง “มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้” ด้วยจึงจะเข้าความหมายของคำว่า “บัตรอิเล็กทรอนิกส์”

การกำหนดความหมายดังกล่าว จึงส่งผลให้ “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” ที่ “มีการออกเอกสารหรือวัตถุอื่นใดให้” ด้วยนั้น ไม่เป็น “บัตรอิเล็กทรอนิกส์” ตามมาตรา 1(14) ซึ่งส่งผลให้ “เอกสารหรือวัตถุอื่นใด” ตามมาตรา 1(14)(ก) ที่เป็น “บัตรอิเล็กทรอนิกส์” ที่มี “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” อยู่ในตัวบัตรที่มีการ “ออกเอกสารหรือวัตถุอื่นใดให้” ด้วยนั้น ถูกตีความโดยนักกฎหมายไทยหลายท่าน[12] ว่า “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” ที่อยู่ในบัตรที่มีการออกให้นั้นไม่เป็น “บัตรอิเล็กทรอนิกส์” ในความหมายตามม่าตรา 1(14) ด้วย นั่นหมายความว่า หากมีการกระทำความผิดแก่ “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” ที่อยู่ในบัตรอิเล็กทรอนิกส์นั้น เช่น การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ที่มีการ “ออกเอกสารหรือวัตถุอื่นใดให้” จะไม่เป็นการกระทำต่อ “บัตรอิเล็กทรอนิกส์” ตามประมวลกฎหมายอาญา อันส่งผลให้บทบัญญัติที่มีวัตถุแห่งการกระทำเป็น “บัตรอิเล็กทรอนิกส์” ในภาค 2 ลักษณะ 7 หมวด 4 “ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์” ที่แก้ไขเพิ่มเติมใน พ.ศ.2547 แล้วนั้น ไม่สามารถใช้ในการลงโทษโดยตรงได้ เนื่องจากลักษณะการกำหนดความหมายในมาตรา 1(14) นั้นเอง ซึ่งไม่รวมถึง “ข้อมูล” ในบัตร “ที่มีการออกเอกสารหรือวัตถุอื่นใดให้” ด้วย การบัญญัติกฎหมายกล่าวจึงไม่ครอบคลุมการกระทำความผิดทั้งหมดที่เกิดขึ้นในสภาพความเป็นจริง

[12] เช่น เกียรขจร วัจนะสวัสดิ์, วีระวัฒน์ ปวาราจารย์ และ สมศักดิ์ เธียรจรูญกุล

จากการพิจารณาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 8 แล้วพบว่าได้บัญญัติให้ การกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ “เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์” เป็นความผิดแล้วนั้น แต่การจะผิดตามมาตรานี้ เบื้องต้นต้องวินิจฉัยเสียก่อนว่าอุปกรณ์นั้นๆ เป็น “คอมพิวเตอร์” หรือไม่เสียก่อน โดยไม่ใช่การพิจารณาแต่เพียงรูปลักษณ์ภายนอกของอุปกรณ์ แต่ต้องได้ความว่าอุปกรณ์นั้นๆ ต้องประกอบไปด้วยซอฟแวร์ (Software) และฮาร์ดแวร์ (Hardware) ซึ่งต้องมี ซีพียู (CPU) รอม (ROM) และ ไบออส (BIOS) ครบถ้วนจึงจะเป็นเครื่องคอมพิวเตอร์ที่สมบูรณ์ได้ เมื่อวินิจฉัยได้ว่าอุปกรณ์นั้นๆ เป็นเครื่องคอมพิวเตอร์แล้วจึงจะทำการวินิจฉัยต่อไปว่า กรณีเป็นการดักรับในระหว่างการส่งในระบบคอมพิวเตอร์หรือไม่ การดักรับที่ไม่ได้ส่งในระบบคอมพิวเตอร์ย่อมไม่เป็นความผิดตามมาตราดังกล่าว[13] แต่การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์บางประเภท[14] โดยตรง โดยการใช้อุปกรณ์ที่ผู้กระทำความผิดได้พัฒนาขึ้นมาเฉพาะ เช่น เครื่องสกิมเมอร์ หรือเครื่องมือใดๆ ซึ่งไม่เข้าลักษณะของการเป็นเครื่องคอมพิวเตอร์ เพราะขาดองค์ประกอบใดองค์ประกอบหนึ่ง ตามองค์ประกอบของคอมพิวเตอร์ที่ต้องพิจารณาในเบื้องต้นแล้ว แม้จะเป็นการกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ก็ตาม แต่ก็ไม่ใช่การส่งผ่านข้อมูลคอมพิวเตอร์ในระบบคอมพิวเตอร์ จึงไม่อาจปรับบทความผิดตามมาตรา 8 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ดังกล่าว แก่การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์โดยตรงได้[15]

1.1.2 บทบัญญัติของกฎหมายที่มีใช้บังคับอยู่แล้วไม่ครบถ้วนตามวัตถุประสงค์ของกฎหมาย

พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547 มาตรา 5 ได้เพิ่มหมวด 4 ของลักษณะ 7 ให้มี “ความผิดเกี่ยวกับการบัตรอิเล็กทรอนิกส์” โดยเพิ่มมาตรา 269/1 ถึงมาตรา 269/7 ซึ่งเมื่อพิจารณาแล้ว ไม่อาจนำมาปรับบทกับการกระทำความผิดในลักษณะการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้โดยตรง เพราะการกระทำดังกล่าวไม่เข้าองค์ประกอบความผิดของมาตราเหล่านั้น

---

[13] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, พิมพ์ครั้งที่ 1 (กรุงเทพฯ: กรุงสยาม พับลิชชิ่ง, 2559), หน้า 117-118.

[14] หมายถึง “บัตรอิเล็กทรอนิกส์” ที่ได้กำหนดไว้ในมาตรา 1(14)(ก)

[15] สมศักดิ์ เธียรจรูญกุล, "รายงานการวิจัย เรื่อง ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา," (รายงานการวิจัย สาขานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2558), หน้า 70.

อย่างไรก็ตาม จากการศึกษาย้อนไปในชั้นยกร่างกฎหมาย พบว่าในชั้นรับหลักการแห่งร่างพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่...) พ.ศ. ... (บัตรและข้อมูลอิเล็กทรอนิกส์) ที่ได้เสนอแก่ที่ประชุมสภาผู้แทนราษฎร ในสมัยสามัญทั่วไปครั้งที่ 20 ในวันที่ 23 เมษายน 2546 จำนวน 2 ร่าง ของคณะรัฐมนตรีและของสมาชิกสภาผู้แทนราษฎรนั้น ต่างก็มีบทบัญญัติที่กล่าวถึงการกระทำความผิดเกี่ยวกับการใช้หรือมีไว้เพื่อนำออกใช้ซึ่งข้อมูลอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ[16] อันกำหนดให้เป็นความผิดตามประมวลกฎหมายอาญานอกจากการกระทำความผิดในลักษณะอื่นๆ ตามมาตรา 269/1 ถึงมาตรา 269/7 ดังเช่นปัจจุบัน แต่ในชั้นการแปรญัตติของร่างนี้เอง คณะกรรมการแปรญัตติกลับตัดบทบัญญัติที่เกี่ยวข้องดังกล่าวออกไป จึงส่งผลให้บทบัญญัติของกฎหมายที่ออกมาบังคับใช้นั้นไม่ครบถ้วน ทำให้เกิดกรณีของ “ข้อมูล” ที่ไม่เป็น “บัตรอิเล็กทรอนิกส์” เพราะ “มีการออกเอกสารหรือวัตถุอื่นใดให้” ตามคำนิยามในมาตรา 1(14)(ข) เช่น การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้น ไม่สามารถนำไปปรับบทลงโทษกับมาตรา 269/1 ถึงมาตรา 269/7 ได้เลย ทั้งที่เจตนารมณ์ของการแก้ไขเพิ่มเติมบทบัญญัติในหมวดดังกล่าวมีวัตถุประสงค์เพื่อ “กำหนดความผิดอาญาสำหรับการกระทำความผิดเกี่ยวกับบัตรและข้อมูลอิเล็กทรอนิกส์” อันเป็น “การกระทำความผิดเกี่ยวกับบัตรและลักลอบนำข้อมูลอิเล็กทรอนิกส์ของผู้อื่นมาใช้”[17] ซึ่งได้ระบุเป็นหมายเหตุท้าย พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547 โดยให้มีการกำหนดฐานความผิดเกี่ยวกับ “บัตร” และ “ข้อมูลอิเล็กทรอนิกส์” ในบัตรนั้นด้วย

จากการศึกษาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พบว่าพระราชบัญญัติดังกล่าวได้บัญญัติความผิดฐาน “เข้าถึง” (Accesses) ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบไว้ในมาตรา 5 และมาตรา 7 และความผิดฐาน “ดักรับ” (Intercepts)

---

[16] ร่างที่คณะรัฐมนตรีเสนอ มาตรา 269/6 “ผู้ใดใช้ข้อมูลบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ” และมาตรา 269/6/1 “ผู้ใดมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/5 หรือซึ่งข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/6 ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

และร่างของสมาชิกสภาผู้แทนราษฎรเสนอ มาตรา 269/6 “ผู้ใดใช้หรือมีไว้เพื่อใช้ข้อมูล หรือรหัสบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

[17] หมายเหตุท้ายพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547

ข้อมูลคอมพิวเตอร์ที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์โดยมิชอบในมาตรา 8[18] ดังที่ได้กล่าวมาแล้วว่า การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์บางประเภท[19] โดยตรงนั้นไม่อาจปรับบทมาตรา 5 หรือ มาตรา 7 หรือ มาตรา 8 เพื่อลงโทษได้เพราะไม่ครบองค์ประกอบความผิดของการเป็นคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ ในขณะที่การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์บางประเภทนั้น[20] อาจสามารถปรับบทลงโทษฐานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ตามมาตรา 5 หรือฐานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ตามมาตรา 7 ได้ เพราะการดึงข้อมูลบัตรในประเภทนั้นจะต้องมีการ “เข้าถึง” ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์เสียก่อน โดยที่กฎหมายบัญญัติให้ข้อมูลบัตรอิเล็กทรอนิกส์ประเภทดังกล่าวนั้นเป็นข้อมูลคอมพิวเตอร์ประการหนึ่งด้วย และเมื่อเป็นข้อมูลคอมพิวเตอร์จึงสามารถปรับความผิดฐานกระทำด้วยประการใดโดยมิชอบเพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ ตามมาตรา 8 ได้เช่นกัน แต่การ “เข้าถึง” ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบ ตามมาตรา 5 และมาตรา 7 นั้นเปรียบได้กับความผิดฐานบุกรุก ตามประมวลกฎหมายอาญามาตรา 362 มาตรา 364[21] อันเข้าไปเพื่อถือการครอบครองข้อมูลคอมพิวเตอร์ หรือเข้าไปกระทำการใดๆ อันเป็นการรบกวนการครอบครองข้อมูลคอมพิวเตอร์ หรือโดยไม่มีเหตุอันสมควร เข้าไปในข้อมูลคอมพิวเตอร์ของผู้อื่น โดยมิได้กระทำความผิดอื่นเพิ่มขึ้นนอกเหนือไปจากการเข้าถึงนั้น แท้จริงแล้วหากพิจารณาเฉพาะองค์ประกอบของการกระทำความผิดของมาตรา 5 และมาตรา 7 นั้นจะพบว่า มาตราดังกล่าวมิได้บัญญัติเพิ่มเติมหรือให้คำนิยาม “การเข้าถึง” นั้นให้รวมถึงการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ด้วย อันต่างกับการ “ดักรับ” ข้อมูลคอมพิวเตอร์ที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ ตามมาตรา 8 ที่ต้องมีการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์นั้นก่อนแล้วได้ทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ไป อันปรียบได้กับการกระทำความผิดฐานบุกรุกแล้วผู้กระทำได้กระทำความผิดอื่นเพิ่มเติมขึ้นด้วย เช่น รื้อข้าวของ สลับที่ หรือลักเอาข้าวของออกมา[22] ซึ่งผู้กระทำต้องรับโทษในความผิดฐานอื่นเพิ่มขึ้น

---

[18] ในกฎหมาย Computer Fraud and Abuse Act มาตรา 1030 ของประเทศสหรัฐอเมริกา ได้บัญญัติอย่างชัดเจนให้การเข้าถึง (Accessed) ใน (a)(1) แยกจากการเข้าถึงและได้รับข้อมูล (Accessed and Obtain Information) ใน (a)(2) ซึ่งมีบทลงโทษต่างกัน

[19] หมายถึง “บัตรอิเล็กทรอนิกส์” ที่ได้กำหนดไว้ในมาตรา 1(14)(ก)

[20] หมายถึง “บัตรอิเล็กทรอนิกส์” ที่ได้กำหนดไว้ในมาตรา 1(14)(ข)

[21] สราวุธ ปิติยาศักดิ์, คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ (ฉบับที่ 2) พ.ศ. 2560, พิมพ์ครั้งที่ 2 (กรุงเทพฯ: นิติธรรม, 2561), หน้า 57.

[22] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, หน้า 133-136.

นอกเหนือจากฐานบุกรุกนั้นด้วย การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์บางประเภท[23] นั้นจึงควรลงโทษตามมาตรา 8 นี้เพียงประการเดียวเท่านั้น

การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์บางประเภท[24] ที่ไม่สามารถปรับบทบัญญัติตามมาตรา 5 มาตรา 7 หรือ มาตรา 8 เพื่อลงโทษได้นั้น นอกจากจะไม่เป็นความผิดตามพระราชบัญญัตินี้แล้ว การที่ผู้กระทำได้รับข้อมูลในบัตรอิเล็กทรอนิกส์ไป ซึ่งผู้กระทำความผิดสามารถนำข้อมูลเหล่านั้นไปทำสำเนา (Copy) เสมือนต้นฉบับ อันเป็นลักษณะพิเศษเฉพาะตัวของข้อมูลอิเล็กทรอนิกส์และนำไปใช้ในการกระทำความผิดอื่นๆ ได้นับไม่ถ้วนและอาจส่งผลเสียอย่างร้ายแรงต่อไป การที่ไม่อาจปรับบทลงโทษใดๆ แก่การดึงข้อมูลบัตรประเภทดังกล่าวได้เพราะบทบัญญัติของกฎหมายตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่ไม่ครอบคลุมเช่นนี้ จึงไม่ตรงตามเป้าประสงค์ของกฎหมายที่ต้องการให้มีการป้องกันและปราบปรามการกระทำความผิดดังกล่าวด้วย[25]

1.1.3 อาจเกิดการตีความบทบัญญัติที่มีอยู่เพื่อลงโทษผู้กระทำความผิด ซึ่งขัดกับหลักกฎหมาย

เมื่อได้พิจารณาความผิดทุกมาตราในหมวด “ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์” จะพบว่าหากวัตถุแห่งการกระทำความผิดเป็น “บัตรอิเล็กทรอนิกส์” ตามคำจำกัดความใน มาตรา 1(14) ไม่ว่าจะใน (ก) (ข) หรือ (ค) แล้วก็ตาม ผู้กระทำความผิดนั้นอาจถูกลงโทษตามมาตราต่างๆ ที่ได้บัญญัติไว้ในหมวดดังกล่าวได้ทุกมาตรา เช่น ความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/1 ฐานทำหรือมีเครื่องมือในการปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/2 หรือฐานใช้หรือมีไว้เพื่อใช้บัตรอิเล็กทรอนิกส์ปลอม ตามมาตรา 269/4

---

[23] หมายถึง “บัตรอิเล็กทรอนิกส์” ที่ได้กำหนดไว้ในมาตรา 1(14)(ข)

[24] หมายถึง “บัตรอิเล็กทรอนิกส์” ที่ได้กำหนดไว้ในมาตรา 1(14)(ก)

[25] หมายเหตุท้ายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 “เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใดๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือ ใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์ อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้”

อย่างไรก็ตาม เนื่องจาก “ข้อมูล” ที่อยู่ในบัตรอิเล็กทรอนิกส์ประเภทที่ผู้ออกได้มีการ “ออกเอกสารหรือวัตถุอื่นใดให้” ด้วย ซึ่งไม่เป็น “บัตรอิเล็กทรอนิกส์” ตามคำจำกัดความในมาตรา 1(14) จึงมีปัญหาว่า หากมีการกระทำความผิดต่อ “ข้อมูล” ในบัตรอิเล็กทรอนิกส์ดังกล่าวนั้น จะสามารถปรับบทบัญญัติกฎหมายเพื่อลงโทษ ตามมาตราใดได้บ้างในหมวดนี้

เมื่อพิจารณาถึงลักษณะของ “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” ที่อยู่ในบัตร “ที่มีการออกให้” แล้วพบว่า โดยลักษณะทั่วไปของข้อมูลอิเล็กทรอนิกส์ที่อยู่ในบัตรอิเล็กทรอนิกส์นั้น “ข้อมูล” ต้องอาศัยแหล่งบันทึกใดๆก็ตาม ไม่ว่าจะเป็นบันทึกลงในแถบแม่เหล็ก (Magnetic Stripe) ด้านหลังบัตรหรือในชิป (Chip) ของบัตร หรือหากมีการโอนถ่ายหรือคัดลอกไปยังเครื่องมืออิเล็กทรอนิกส์อื่นๆ “ข้อมูล” ก็จะต้องไปบันทึกอยู่ในหน่วยความจำในเครื่องมืออิเล็กทรอนิกส์นั้นๆ เช่น ในฮาร์ดดิสก์ (Harddisk) ของเครื่องคอมพิวเตอร์ เพราะข้อมูลเหล่านี้เป็นเพียงสัญญาณไฟฟ้าที่มีอยู่ชั่วขณะเท่านั้น หากไม่มีแหล่งบันทึก ข้อมูลที่เป็นสัญญาณไฟฟ้าเหล่านี้จะหายไปเปลี่ยนเป็นพลังงานรูปแบบอื่น[26] จึงสรุปได้ในเบื้องต้นว่า โดยลักษณะทั่วไปของ “ข้อมูล” นั้นต้องมีแหล่งบันทึกไม่ว่าที่ใดที่หนึ่ง[27] จะอยู่ลอยๆ ในอากาศไม่ได้[28]

เมื่อพิเคราะห์ประมวลกฎหมายอาญา มาตรา 269/2 ที่ระบุว่า ผู้ใด “มี” เครื่องมือหรือวัตถุเพื่อใช้หรือให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์แล้วพบว่า เครื่องมือประเภทนี้ได้ถูกบัญญัติไว้กว้างๆ อาจจะเป็น เครื่องคอมพิวเตอร์ โทรศัพท์ หรือเครื่องสกิมเมอร์ เป็นต้น ซึ่งผู้ที่มีเครื่องมือพวกนี้อาจมีความผิดตามมาตรา 269/2 นี้ได้ และด้วยการที่เครื่องมือพวกนี้มักจะมีแหล่งบันทึกความจำอยู่ในเครื่องมือนั้นด้วย ซึ่งหากพบว่าเครื่องมือที่เป็นวัตถุแห่งการกระทำความผิดดังกล่าวมี “ข้อมูล” บัตรอิเล็กทรอนิกส์ได้บันทึกอยู่ในเครื่องด้วยแล้ว ก็อาจตีความได้ว่า ผู้นั้น “มี” เครื่องมือหรือวัตถุเพื่อใช้หรือให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/2 อันอาจตีความบทบัญญัติของกฎหมายเพื่อลงโทษผู้กระทำความผิดในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้

---

[26] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, หน้า 119.

[27] สัมภาษณ์ พ.ต.อ.ดร.วิวัฒน์ สิทธิสรเดช, นักวิทยาศาสตร์ สัญญาบัตร 4 กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง สำนักงานตำรวจแห่งชาติ, 2558.

[28] ผู้วิจัยเห็นว่า การใช้ความจำก็เป็นแหล่งบันทึกข้อมูลเช่นกัน โดยใช้สมอง แต่การกระทำความผิดแก่ข้อมูลในสมองในปัจจุบันเทคโนโลยียังไม่สามารถขโมยหรือดึงข้อมูลออกมาจากสมองมนุษย์ได้ จึงต้องใช้การเค้นเอาข้อมูลนั้น อันอาจเป็นความผิด ฐานข่มขืนใจผู้อื่น ตามมาตรา 309

การตีความดังกล่าวนั้น ขัดกับหลักกฎหมายอาญาซึ่งจะต้องตีความโดยเคร่งครัด จักนำกฎหมายใกล้เคียงไปบังคับใช้ให้เป็นผลร้ายแก่ผู้กระทำความผิดมิได้ และขัดกับหลักไม่มีกฎหมายไม่มีโทษ ซึ่งการจะลงโทษผู้กระทำความผิดใดก็ต่อเมื่อได้มีกฎหมายบัญญัติไว้โดยชัดแจ้ง อันเป็นหลักการที่ได้บัญญัติไว้ในประมวลกฎหมายอาญามาตรา 2[29] ด้วย ทั้งการลงโทษผู้กระทำความผิดโดยอาศัยมาตรา 269/2 ยังทำให้เกิดปัญหาที่ตามมาหลายประการ ทั้งองค์ประกอบภายนอกในด้านวัตถุแห่งการกระทำ ฐานความผิดของการกระทำ การกระทำความผิดหลายกรรม อัตราโทษ และเจตนารมณ์ในการยกร่างกฎหมาย ดังจะได้ทำการวิเคราะห์ในงานวิจัยต่อไป

จากปัญหาของการบังคับใช้กฎหมายอันเกี่ยวกับการกระทำความผิดดังที่ได้กล่าวมาแล้วหลายประการ ผู้วิจัยจึงเล็งเห็นว่าเป็นปัญหาสำคัญ ที่ควรจะต้องศึกษาวิจัยปัญหาเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ อันนำไปสู่การกำหนดบทบัญญัติของกฎหมายอาญาที่เป็นการเฉพาะเพื่อลงโทษผู้กระทำความผิดดังกล่าวให้เหมาะสม ซึ่งเป็นการป้องกันและปราบปรามการกระทำความผิด และให้มีบทบัญญัติของกฎหมายเป็นการครอบคลุมการกระทำความผิดต่างๆ ที่เกี่ยวข้องต้องตามวัตถุประสงค์และเจตนารมณ์ของกฎหมายที่มีใช้บังคับแล้วต่อไป

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อให้ทราบถึงลักษณะ รูปแบบและองค์ประกอบในการกระทำความผิดอันเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ที่เกิดขึ้นทั้งในประเทศไทยและในต่างประเทศ

1.2.2 เพื่อให้ทราบถึงปัญหาและอุปสรรคในการบังคับใช้กฎหมายเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในประเทศไทย

1.2.3 เพื่อวิเคราะห์ปัญหาและอุปสรรคในการบังคับใช้กฎหมายเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในประเทศไทย

1.2.4 เพื่อศึกษาบทบัญญัติของกฎหมายและการบังคับใช้กฎหมายของต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์และนำมาวิเคราะห์เปรียบเทียบกับบทบัญญัติของกฎหมายในประเทศไทย

---

[29] ประมวลกฎหมายอาญา มาตรา 2 วรรคแรก “บุคคลจักต้องรับโทษในทางอาญาต่อเมื่อได้กระทำการอันกฎหมายที่ใช้ในขณะกระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแก่ผู้กระทำความผิดนั้น ต้องเป็นโทษที่บัญญัติไว้ในกฎหมาย”

1.2.5 เพื่อเสนอแนะแนวทางในการแก้ไขปรับปรุงบทบัญญัติของกฎหมายให้มีความครอบคลุม อันนำไปสู่การป้องกันและปราบปรามการกระทำความผิดที่เกี่ยวกับดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ต่อไป

1.3 สมมติฐานของการวิจัย

การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ เป็นปัญหาที่สำคัญซึ่งส่งผลกระทบต่อ การคุ้มครองข้อมูลส่วนบุคคลและข้อมูลในการทำธุรกรรมทางการเงิน และเป็นการกระทำที่มีลักษณะพิเศษเฉพาะตัว จากการพิเคราะห์บทบัญญัติของกฎหมายอาญาในประเทศไทยพบว่า ไม่มีบทบัญญัติเฉพาะที่เหมาะสมในการบังคับใช้กับลักษณะการกระทำความผิดในรูปแบบนี้ได้โดยตรง และบทบัญญัติกฎหมายที่มีอยู่แล้วก็ไม่สามารถคุ้มครองข้อมูลที่เกิดจากการดึงได้อย่างครบถ้วน จึงเห็นสมควร ศึกษาหลักเกณฑ์และบทบัญญัติที่เกี่ยวข้องกับการดึงข้อมูลบัตรอิเล็กทรอนิกส์ในกฎหมายต่างประเทศ เพื่อเป็นแนวทางในการกำหนดให้มีบทบัญญัติที่เป็นการเฉพาะในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ให้ครอบคลุมลักษณะของการกระทำความผิดอย่างครบถ้วนตามเจตนารมณ์ของกฎหมาย ทัดเทียมกับสากล เพื่อป้องปราบไม่ให้เกิดการกระทำความผิด และเพื่อนำผู้กระทำความผิดดังกล่าวมาลงโทษ

1.4 ขอบเขตของการวิจัย

วิทยานิพนธ์ฉบับนี้มุ่งศึกษาลักษณะ รูปแบบและองค์ประกอบของการกระทำความผิดเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ อันเป็นการดึงเอาข้อมูลโดยตรงจากบัตรอิเล็กทรอนิกส์ซึ่งมิใช่การส่งในระบบคอมพิวเตอร์ โดยบทบัญญัติของกฎหมายไทยที่เกี่ยวข้อง อันได้แก่ ประมวลกฎหมายอาญา ร่างพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญาเกี่ยวกับบัตรและข้อมูลอิเล็กทรอนิกส์ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แนวคำพิพากษาของศาลทั้งในประเทศไทยและในต่างประเทศ บทบัญญัติของกฎหมายต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ เช่น การโจรกรรมข้อมูลส่วนบุคคล การฉ้อโกงบัตรเครดิตหรือบัตรชำระเงิน และอาชญากรรมทางคอมพิวเตอร์ เพื่อนำมาวิเคราะห์ปัญหาและอุปสรรคในการบังคับใช้กฎหมายในประเทศไทย และเสนอแนวทางที่เหมาะสมในการแก้ไขปรับปรุงบทบัญญัติของกฎหมายในส่วนที่เกี่ยวข้องกับการกระทำความผิดอันเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ต่อไป

1.5 วิธีดำเนินการวิจัย

การศึกษาวิจัยนี้มุ่งศึกษาวิจัยทางเอกสาร (Documentary Research) โดยการค้นคว้าและรวบรวมข้อมูลจากประมวลกฎหมาย พระราชบัญญัติ เอกสารทางกฎหมายต่างๆ เช่น หนังสือกฎหมาย บทความ วารสารจุลสาร รายงานวิจัย วิทยานิพนธ์ บทวิเคราะห์ของนักกฎหมาย สื่อสิ่งพิมพ์ คำพิพากษาของศาล แหล่งข้อมูลจากเครือข่ายอินเตอร์เน็ตทั้งในประเทศและต่างประเทศ นอกจากนี้ยังได้รวบรวมข้อมูลจากการศึกษาวิจัยจากภาคสนาม (Field Source) โดยอาศัยการสัมภาษณ์จากเจ้าพนักงานของรัฐ เช่น เจ้าพนักงานสอบสวนประจำกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ เจ้าพนักงานพิสูจน์หลักฐานประจำกองพิสูจน์หลักฐานกลาง สำนักงานตำรวจแห่งชาติ ตลอดจนพนักงานและเจ้าหน้าที่อื่นของภาครัฐและภาคเอกชนที่เกี่ยวข้อง โดยการนำข้อมูลที่ได้มาทำการวิเคราะห์และเสนอแนวทางที่เหมาะสมในการแก้ไขปรับปรุงบทบัญญัติของกฎหมายในส่วนที่เกี่ยวข้องกับการกระทำความผิดอันเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ให้มีความครอบคลุมต่อไป

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 ทำให้ทราบถึงลักษณะ รูปแบบและองค์ประกอบในการกระทำความผิดอันเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ที่เกิดขึ้นทั้งในประเทศไทยและในต่างประเทศ

1.6.2 ทำให้ทราบถึงปัญหาและอุปสรรคในการบังคับใช้กฎหมายเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในประเทศไทย

1.6.3 ทำให้สามารถวิเคราะห์ปัญหาและอุปสรรคในการบังคับใช้กฎหมายเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในประเทศไทย

1.6.4 ทำให้ทราบบทบัญญัติของกฎหมายและการบังคับใช้กฎหมายของต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ และนำมาวิเคราะห์เปรียบเทียบกับบทบัญญัติของกฎหมายในประเทศไทย

1.6.5 สามารถเสนอแนะแนวทางในการแก้ไขปรับปรุงบทบัญญัติของกฎหมายให้มีความครอบคลุม อันนำไปสู่การป้องกันและปราบปรามการกระทำความผิดที่เกี่ยวกับดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ต่อไป

1.7 เอกสารและงานวิจัยที่เกี่ยวข้อง

1.7.1 งานวิจัยที่เกี่ยวกับการกระทำความผิดกับทรัพย์ไม่มีรูปร่าง

ศิริภัทร ธรรมเขต ได้จัดทำวิทยานิพนธ์เรื่อง “ความผิดฐานลักทรัพย์ : ศึกษากรณีการลักทรัพย์ไม่มีรูปร่าง”[30] ซึ่งได้ทำการศึกษาความผิดฐานลักทรัพย์ในกฎหมายไทยเทียบกับกฎหมายอังกฤษ เยอรมันและแคนาดา จากงานวิจัยพบว่า กฎหมายในต่างประเทศได้ให้คำนิยามว่าทรัพย์ไว้อย่างกว้างครอบคลุมถึงทรัพย์ทุกประเภท จึงเสนอแนะให้เพิ่มเติมคำนิยามของคำว่า ทรัพย์ไว้ในวรรคสอง ของมาตรา 334 แห่งประมวลกฎหมายอาญาให้หมายรวมถึง กระแสไฟฟ้า ก๊าซ และคลื่นสัญญาณต่างๆ ให้วัตถุแห่งการกระทำในความผิดฐานลักทรัพย์ได้ โดยไม่จำต้องบัญญัติกฎหมายให้มากเกินความจำเป็น แต่จากงานวิจัยดังกล่าวนั้นแสดงให้เห็นได้ว่า หากกฎหมายในต่างประเทศต่างๆ จะกำหนดให้ทรัพย์ไม่มีรูปร่างใดสามารถลักกันได้ กฎหมายในต่างประเทศนั้นจะกำหนดให้มีบทบัญญัติหรือมีกฎหมายเฉพาะระบุประเภทของทรัพย์ที่ไม่มีรูปร่างเป็นกรณีๆ ไป ข้อมูลในบัตรอิเล็กทรอนิกส์ก็นับว่าเป็นทรัพย์ที่ไม่มีรูปร่างประเภทหนึ่งซึ่งเป็นสัญญาณไฟฟ้า จึงเห็นสมควรนำมาวิเคราะห์ว่า หากกำหนดให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นความผิดแล้วนั้น ควรบัญญัติไว้เป็นบทบัญญัติในมาตราใดหรือในกฎหมายใดเป็นการเฉพาะต่อไป

1.7.2 งานวิจัยที่เกี่ยวกับการกระทำความผิดกับบัตรอิเล็กทรอนิกส์

ธวัชชัย สมบุญเจริญ ได้จัดทำวิทยานิพนธ์เรื่อง “ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์”[31] ซึ่งได้ทำการศึกษาบทบัญญัติในประมวลกฎหมายอาญา (ใน พ.ศ. 2549) กับการกระทำความผิดในรูปแบบต่างๆ ที่เกี่ยวกับบัตรอิเล็กทรอนิกส์ ในฐานะที่บัตรอิเล็กทรอนิกส์นั้นเป็นเครื่องหมายเพื่อใช้ระบุตัวบุคคลประเภทหนึ่ง จากงานวิจัยพบว่า บทบัญญัติในประมวลกฎหมายอาญาสามารถนำมาใช้บังคับกับอาชญากรรมบัตรเครดิตได้เฉพาะความผิดกับการกระทำต่อตัวบัตรในลักษณะที่เป็นวัตถุ (Object) แต่ยังไม่ครอบคลุมทุกกรณี จึงเสนอให้มีการแก้ไขบทบัญญัติในประมวลกฎหมายอาญา ในลักษณะ 7 หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ให้ครอบคลุมมากยิ่งขึ้น โดยงานวิจัยดังกล่าวไม่ได้วิเคราะห์ไว้ว่าการแก้ไขดังกล่าวนั้นเหมาะสมแล้วหรือไม่ กระทบบทบัญญัติ

---

[30] ศิริภัทร ธรรมเขต, "ความผิดฐานลักทรัพย์ : ศึกษากรณีการลักทรัพย์ไม่มีรูปร่าง," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ มหาวิทยาลัยรามคำแหง, 2550), หน้า 1-165.

[31] ธวัชชัย สมบุญเจริญ, "ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2549), หน้า 1-154.

ในมาตราอื่นๆ อย่างไร อาจมีปัญหาในการตีความต่อไปได้หรือไม่ และนำบทบัญญัติในกฎหมายต่างประเทศใดมาเป็นแนวทางในการแก้ไข และเนื่องจากเป็นงานวิจัยก่อนที่ได้มีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 บังคับใช้ งานวิจัยดังกล่าวจึงไม่ได้ทำการวิเคราะห์ไว้ด้วยว่าหากมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์บังคับใช้แล้วจะเป็นการแก้ปัญหา อันทำให้ปัญหาทางกฎหมายของงานวิจัยจะยังคงมีอยู่หรือไม่

จรัสศรี จริยากูล ได้จัดทำวิทยานิพนธ์เรื่อง “มาตรการทางกฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมบัตรเครดิต”[32] ซึ่งได้ทำการศึกษามาตรการทางกฎหมายต่างๆ ในประมวลกฎหมายอาญา (ใน พ.ศ. 2533) กับอาชญากรรมบัตรเครดิตในรูปแบบต่างๆ ซึ่งมีเนื้อหาคล้ายกับวิทยานิพนธ์ของ ธวัชชัย สมบุญเจริญ เรื่อง “ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์”[33] จากงานวิจัยพบว่า บทบัญญัติในประมวลกฎหมายอาญาสามารถนำมาใช้บังคับกับอาชญากรรมบัตรเครดิตได้เฉพาะความผิดกับการกระทำต่อตัวบัตรในลักษณะที่เป็นวัตถุ (Object) เช่น ฐานลักทรัพย์ ฐานยักยอกทรัพย์ ฐานปลอมเอกสารสิทธิ แต่ยังไม่ครอบคลุมทุกกรณี อาทิ ไม่ได้กำหนดความผิดเกี่ยวกับการมีเครื่องมือสำหรับทำปลอมบัตรเครดิต จึงควรมีการออกกฎหมายเฉพาะเพื่อใช้กับอาชญากรรมบัตรเครดิต ซึ่งในปัจจุบันได้มีพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547 ออกมาใช้บังคับกับปัญหาดังกล่าวแล้ว และ จรัสศรี จริยากูล ได้เสนอแนะเพิ่มเติมอีกด้วยว่าควรกำหนดให้การใช้เฉพาะหมายเลขบัตรเครดิตที่ได้มาโดยทุจริตเป็นความผิดด้วยในอนาคต แต่ตามประมวลกฎหมายอาญาในปัจจุบันนั้นลักษณะดังกล่าวจะเป็นความผิดอันเกี่ยวกับบัตรอิเล็กทรอนิกส์ได้ต่อเมื่อ หมายเลขบัตรเครดิตนั้น เป็นข้อมูลที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิจะใช้โดย “มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้” ตามมาตรา 1(14)(ข) ซึ่งมีปัญหาที่ผู้วิจัยจะต้องศึกษาต่อไป

จนิษฐ คันธสมบูรณ์ ได้จัดทำวิทยานิพนธ์เรื่อง “การทุจริตโดยใช้บัตรเครดิต”[34] ซึ่งได้ทำการศึกษารูปแบบการทุจริตโดยใช้บัตรเครดิตกับบทบัญญัติของประมวลกฎหมายอาญา (ใน พ.ศ. 2538) ซึ่งมีเนื้อหาและข้อเสนอแนะคล้ายกับวิทยานิพนธ์ของ จรัสศรี จริยากูล เรื่อง “มาตรการทางกฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมบัตรเครดิต”[35] ใน พ.ศ. 2533 โดยได้เพิ่มหลักกฎหมายของประเทศอังกฤษเข้ามาในการวิเคราะห์ ถึงอย่างไรก็ตาม วิทยานิพนธ์ดังกล่าวก็ไม่ได้

---

[32] จรัสศรี จริยากูล, "มาตรการทางกฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมบัตรเครดิต," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2533), หน้า 1-173.

[33] ธวัชชัย สมบุญเจริญ, “ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์,”, หน้า 1-154.

[34] จนิษฐ คันธสมบูรณ์, "การทุจริตโดยใช้บัตรเครดิต,," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2538), หน้า 1-152.

[35] จรัสศรี จริยากูล, “มาตรการทางกฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมบัตรเครดิต,”, หน้า 1-173.

กล่าวถึงกรณีเกี่ยวกับการทุจริตข้อมูลในบัตรอิเล็กทรอนิกส์ ที่มีการออกเอกสารหรือวัตถุอื่นใดให้ด้วย อันเป็นปัญหาซึ่งผู้วิจัยจะทำการศึกษาต่อไป

พีรพันธุ์ เปรมภูติ ได้จัดทำวิทยานิพนธ์เรื่อง “มาตรการทางกฎหมายในการป้องกันปราบปรามการปลอมบัตรเครดิต”[36] ซึ่งได้ทำการศึกษามาตรการทางกฎหมายอาญา (ใน พ.ศ. 2539) ที่ใช้บังคับกับการปลอมบัตรเครดิต ซึ่งมีเนื้อหาและข้อเสนอแนะคล้ายกับวิทยานิพนธ์ของ จรัสศรี จริยากูล เรื่อง “มาตรการทางกฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมบัตรเครดิต”[37] ใน พ.ศ. 2533 และ จนิษฐ คันธสมบูรณ์ เรื่อง “การทุจริตโดยใช้บัตรเครดิต”[38] ใน พ.ศ. 2538 โดยได้เพิ่มหลักกฎหมายของประเทศฮ่องกงที่พัฒนามาจากประเทศอังกฤษและเพิ่มเนื้อหาอันเกี่ยวกับมาตรการของพนักงานเจ้าหน้าที่และศาล ซึ่งงานวิจัยดังกล่าวสนับสนุนให้มีการกำหนดความผิดเฉพาะเกี่ยวกับการเอาไปเสีย ซึ่งข้อมูลหรือรหัสบัตรเครดิตของผู้อื่น อันผู้วิจัยจะทำการศึกษาต่อไป

1.7.3 งานวิจัยที่เกี่ยวกับการกระทำความผิดกับข้อมูลส่วนบุคคล

ฐาปณีย์ รติจารุภัทร ได้จัดทำวิทยานิพนธ์เรื่อง “การกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล”[39] ซึ่งได้ทำการศึกษาการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลกับกฎหมายไทยที่มีโทษทางอาญา (ใน พ.ศ. 2555) เปรียบเทียบกับกฎหมายของสหรัฐอเมริกา สหราชอาณาจักร และประเทศแคนาดา ซึ่งมีปัญหาของงานวิจัยเหมือนกับวิทยานิพนธ์ของ ธวัชชัย สมบุญเจริญ เรื่อง “ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์”[40] แต่ศึกษาเฉพาะกฎหมายเกี่ยวกับข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) อันเป็นส่วนหนึ่งของวิทยานิพนธ์ของ ธวัชชัย สมบุญเจริญ จากงานวิจัยพบว่า การกระทำความผิดต่อข้อมูลที่เชื่อมโยงกับบุคคลในบางกรณีเท่านั้นที่สามารถปรับใช้บทบัญญัติของกฎหมายอาญาได้ แต่ยังไม่ครอบคลุมกับการกระทำความผิดที่เกี่ยวกับ

---

[36] พีรพันธุ์ เปรมภูติ, "มาตรการทางกฎหมายในการป้องกันปราบปรามการปลอมบัตรเครดิต," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2539), หน้า 1-211.

[37] จรัสศรี จริยากูล, “มาตรการทางกฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมบัตรเครดิต,”, หน้า 1-173.

[38] จนิษฐ คันธสมบูรณ์, “การทุจริตโดยใช้บัตรเครดิต,”, หน้า 1-152.

[39] ฐาปณีย์ รติจารุภัทร, "การกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2555), หน้า 1-165.

[40] ธวัชชัย สมบุญเจริญ, “ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์,”, หน้า 1-154.

ข้อมูลซึ่งแสดงเอกลักษณ์บุคคล[41] ทั้งหมด เช่น การนำข้อมูลของบุคคลมาเก็บไว้แต่ยังไม่ได้ทำเอกสารปลอมขึ้น การนำข้อมูลส่วนตัวของเหยื่อไปติดต่อกับธนาคารเพื่อขอทำบัตรใหม่ อันเป็นการใช้ข้อมูลส่วนบุคคลของผู้อื่นเพื่อแสวงหาประโยชน์ในทางที่มิชอบ จึงได้เสนอแนะให้เพิ่มเติมร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ให้นิยามความหมายของคำว่า ข้อมูลส่วนบุคคล มีความชัดเจนและเพิ่มเป็นฐานความผิดกว้างๆ เกี่ยวกับข้อมูลซึ่งแสดงเอกลักษณ์บุคคลให้ครอบคลุมมากยิ่งขึ้น และเนื่องจากข้อมูลในบัตรอิเล็กทรอนิกส์เป็นข้อมูลซึ่งแสดงเอกลักษณ์ของบุคคลประเภทหนึ่งด้วยเพราะสามารถระบุตัวบุคคลผู้เป็นเจ้าของได้ การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ที่ผู้วิจัยมุ่งทำการศึกษา จึงเป็นการวิจัยที่ต่อยอดมาจากวิทยานิพนธ์ฉบับนี้ และต้องการมุ่งศึกษาเฉพาะการกระทำความผิดในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ อันมีลักษณะพิเศษและเป็นการเฉพาะ ซึ่งไม่เพียงแต่นำกฎหมายเกี่ยวกับข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) ในต่างประเทศมาใช้ในการวิเคราะห์เท่านั้น แต่ต้องศึกษากฎหมายอื่นๆ ในต่างประเทศที่เกี่ยวข้องด้วย เพื่อนำมาวิเคราะห์และเสนอแนะให้มีความเหมาะสม สอดคล้องกับบทบัญญัติกฎหมายในประเทศไทยที่มีอยู่แล้วต่อไป

1.7.4 งานวิจัยที่เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

เลิศชาย สุธรรมพร ได้จัดทำวิทยานิพนธ์เรื่อง “อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีความปลอดภัยของข้อมูล”[42] ซึ่งได้ทำการศึกษาว่า การกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์จะสามารถใช้กฎหมายอาญาของไทยในขณะนั้น (พ.ศ. 2541) บังคับได้หรือไม่ จากงานวิจัยพบว่า ยังไม่มีบทบัญญัติที่สามารถนำมาปรับใช้เพื่อลงโทษผู้กระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ได้ จึงเสนอให้มีมาตรการต่างๆ และให้มีการบัญญัติกฎหมายอาชญากรรมคอมพิวเตอร์ขึ้น แต่มิได้เสนอแนะว่ากฎหมายอาชญากรรมคอมพิวเตอร์นั้นควรกำหนดให้มีบทบัญญัติอย่างไร ซึ่งในปัจจุบันประเทศไทยได้มีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้นมาบังคับใช้กับการกระทำความผิดเกี่ยวกับข้อมูลคอมพิวเตอร์แล้ว ดังที่ปรากฏในมาตรา 7 และมาตรา 8 แต่ผู้ศึกษาวิจัยเล็งเห็นว่ายังมีกรณีการกระทำความผิดในบางลักษณะ เช่น

---

[41] ซึ่ง ฐาปณีย์ รติจารุภัทร ได้ให้ความหมายว่า ข้อมูลซึ่งแสดงเอกลักษณ์บุคคล คือ ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคลที่ไม่เหมือนกับบุคคลอื่น โดยข้อมูลหนึ่งๆ อาจอยู่ลำพังแล้วสามารถระบุตัวบุคคลได้ เช่น ลายพิมพ์นิ้วมือ รหัสพันธุกรรม ม่านตา หมายเลขบัตรเครดิต หมายเลขประกันสังคม หรือข้อมูลที่เมื่อรวมกันกับข้อมูลอื่นแล้ว สามารถระบุตัวบุคคลได้ เช่น ชื่อ นามสกุล ที่อยู่ วันเดือนปีเกิด

[42] เลิศชาย สุธรรมพร, "อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีความปลอดภัยของข้อมูล," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2541), หน้า 1-172.

การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ซึ่งมีหลากหลายรูปแบบ ที่ไม่อาจปรับบทตามมาตราดังกล่าวได้ จึงควรทำการศึกษาวิจัยต่อไป

พรทิพย์ ตัณฑวนันท์ ได้จัดทำวิทยานิพนธ์เรื่อง “อาชญากรรมเกี่ยวกับข้อมูลอิเล็กทรอนิกส์”[43] ซึ่งได้ทำการศึกษาการกระทำผิดต่อข้อมูลอิเล็กทรอนิกส์ในภาพรวม ซึ่งนำฐานความผิดต่างๆ ที่กำหนดในร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ... ที่ยังไม่ได้ประกาศใช้มาตั้งเป็นประเด็นปัญหา และเปรียบเทียบกับกฎหมายอาญาของไทยในขณะนั้น (พ.ศ. 2548) จากงานวิจัยพบว่า ยังมีข้อมูลอิเล็กทรอนิกส์อื่นๆ ที่ยังไม่ได้รับความคุ้มครองโดยกฎหมาย อาทิเช่น ข้อมูลที่ไม่ใช่บัตรอิเล็กทรอนิกส์ หรือ ข้อมูลอิเล็กทรอนิกส์ที่ไม่ใช่ข้อมูลคอมพิวเตอร์ ซึ่งในส่วนที่เกี่ยวข้องกับเรื่องการดึงข้อมูลออกจากบัตรอิเล็กทรอนิกส์ที่ผู้วิจัยมุ่งทำการศึกษานั้น พรทิพย์ ตัณฑวนันท์ เห็นว่า “ข้อมูล” ที่ไม่เป็นบัตรอิเล็กทรอนิกส์ ตามคำนิยามในมาตรา 1(14)(ข) ก็สามารถลงโทษผู้กระทำความผิดโดยอาศัยมาตรา 269/2 ได้โดยอาศัยเหตุผลเพียงว่าเมื่อมีเครื่องมือดังกล่าวก็จะต้องมีการคัดลอกบัตรอิเล็กทรอนิกส์เกิดขึ้น โดยไม่ได้วิเคราะห์ว่าการตีความดังกล่าวจะขัดกับหลักกฎหมายอาญาหรือไม่ ทั้งงานวิจัยดังกล่าวเสนอแนะเพียงว่า กฎหมายในขณะนั้นยังไม่เพียงพอในการคุ้มครองข้อมูลอิเล็กทรอนิกส์ โดยไม่ได้เสนอแนะว่าควรแก้ไขบทบัญญัติของกฎหมายอย่างไรด้วย

พรรณสุวัชร รติพงศ์สิทธิ์ ได้จัดทำวิทยานิพนธ์เรื่อง “อาชญากรรมทางคอมพิวเตอร์ : ศึกษาวิเคราะห์หลักเกณฑ์ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ...”[44] ซึ่งได้ทำการศึกษาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ... ฉบับก่อนที่จะได้มีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ว่า กฎหมายที่มีอยู่ในขณะนั้น (พ.ศ. 2550) เพียงพอที่จะใช้จัดการกับปัญหาอาชญากรรมทางคอมพิวเตอร์หรือไม่ โดยศึกษาทุกฐานความผิดที่มีโทษทางอาญาในร่างพระราชบัญญัติดังกล่าว ซึ่งในส่วนของการดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ ตามมาตรา 8 ของร่างฯ พบว่า บทบัญญัติดังกล่าวมีความซ้ำซ้อนกับกฎหมายห้ามดักฟัง ตามพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 มาตรา 74 ซึ่งสามารถปรับใช้กับการลักลอบดักข้อมูลที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ได้อยู่แล้ว จึงไม่

---

[43] พรทิพย์ ตัณฑวนันท์, "อาชญากรรมเกี่ยวกับข้อมูลอิเล็กทรอนิกส์," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548), หน้า 1-98.

[44] พรรณสุวัชร รติพงศ์สิทธิ์, "อาชญากรรมทางคอมพิวเตอร์ : ศึกษาวิเคราะห์หลักเกณฑ์ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ... ," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ มหาวิทยาลัยรามคำแหง, 2550), หน้า 1-123.

จำเป็นต้องกำหนดฐานความผิดดังกล่าวขึ้นมาอีก เว้นเสียแต่ว่า จะได้บัญญัติให้การกระทำบางอย่างที่ไม่อาจใช้มาตรา 74 ดังกล่าวบังคับได้ อาทิเช่น การใช้โปรแกรมจับหน้าจอและดักข้อความที่พิมพ์ลงไป ซึ่งเป็นการดักรับข้อมูลที่ไม่ได้อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ หรือเปลี่ยนให้การจารกรรมข้อมูลเป็นความผิดแทน ในกรณีที่ผู้เข้าถึงข้อมูลโดยมิชอบได้มีการคัดลอกข้อมูลคอมพิวเตอร์ของผู้อื่น ซึ่งต้องรับโทษหนักขึ้นหรือเป็นเหตุฉกรรจ์ของความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ ตามร่างฯ มาตรา 7 ซึ่งแนวความคิดเห็นดังกล่าวสอดคล้องกับเรื่องที่ผู้วิจัยมุ่งทำการศึกษากล่าวคือ ในลักษณะของการกระทำความผิดอันเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์โดยตรงซึ่งไม่ได้อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์นั้น ไม่อาจปรับใช้บทบัญญัติตามมาตรา 8 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ จึงสมควรกำหนดบทบัญญัติที่เฉพาะเพื่อลงโทษแก่ผู้กระทำความผิดดังกล่าว

ชาตรี ส่งสัมพันธ์ ได้จัดทำวิทยานิพนธ์เรื่อง “อาชญากรรมคอมพิวเตอร์ : ศึกษาวิเคราะห์การเข้าโดยมิชอบ”[45] ซึ่งมีเนื้อหาคล้ายกับ พิญดา เลิศกิตติกุล ที่ได้จัดทำวิทยานิพนธ์เรื่อง “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์”[46] ซึ่งได้ทำการศึกษานิยามของคำว่า “เข้าถึง” ซึ่งไม่ได้มีกำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จากงานวิจัยทั้งสองฉบับดังกล่าวพบว่า เมื่อไม่มีการกำหนดนิยามไว้ ศาลจึงควรต้องตีความคำว่า “เข้าถึง” อย่างกว้าง ให้เหมาะสมกับพฤติกรรมการใช้คอมพิวเตอร์ที่หลากหลายและเทคโนโลยีใหม่ๆที่อาจเกิดขึ้น เพื่อนำตัวผู้กระทำความผิดมาลงโทษได้ หากตีความอย่างแคบโดยถือว่าไม่ใช่การเข้าถึงแล้วก็จะทำให้มีปัญหาในการลงโทษได้ สอดรับกับงานวิจัยเรื่อง การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ที่ผู้วิจัยมุ่งทำการศึกษา เพราะในทางหลักกฎหมายที่ผู้วิจัยได้ศึกษานั้น การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เพียงแค่บางกรณีเท่านั้นที่จะต้องรับผิดฐานเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบตามมาตรา 5 และฐานเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ตามมาตรา 7 แต่หากศาลใช้การตีความอย่างกว้าง ย่อมทำให้สามารถนำความผิดดังกล่าวมาปรับใช้ได้กับการเข้าถึงข้อมูลในบัตรอิเล็กทรอนิกส์ทุกกรณีโดยไม่จำต้องคำนึงว่าข้อมูลในบัตรอิเล็กทรอนิกส์นั้นจะอยู่ในระบบคอมพิวเตอร์ก่อนหรือไม่ อันเป็นการตีความรองรับเทคโนโลยีใหม่ๆ ที่อาจเกิดขึ้นและให้เป็นไป

---

[45] ชาตรี ส่งสัมพันธ์, "อาชญากรรมคอมพิวเตอร์ : ศึกษาวิเคราะห์การเข้าโดยมิชอบ," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2552), หน้า 1-118.

[46] พิญดา เลิศกิตติกุล, "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2550), หน้า 1-207.

ในแนวทิศทางเดียวกับกฎหมายในต่างประเทศ และ พิญดา เลิศกิตติกุล เสนอว่าการเข้าถึงเรื่องสำคัญๆ เช่น ข้อมูลทางการเงิน ควรกำหนดให้มีการเพิ่มโทษให้หนักขึ้นกว่าการเข้าถึงข้อมูลทั่วๆ ไป ซึ่งผู้วิจัยเห็นพ้องด้วยว่า การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ซึ่งข้อมูลในบัตรอิเล็กทรอนิกส์นั้นนับเป็นข้อมูลทางการเงินด้วย ผู้กระทำความผิดดังกล่าวสมควรหรือไม่ที่จะต้องรับผิดเพิ่มขึ้น

อัญธิกา ณ พิบูลย์ ได้จัดทำวิทยานิพนธ์เรื่อง “ปัญหาและอุปสรรคในการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550”[47] ซึ่งได้ทำการศึกษาทุกฐานความผิดในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หลังจากที่ได้มีผลใช้บังคับแล้ว และพบว่าการตราบทบัญญัติยังมีข้อบกพร่องอยู่หลายประการ ซึ่งในส่วนที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ที่ผู้วิจัยมุ่งทำการศึกษานั้น อัญธิกา ณ พิบูลย์ พบว่าพระราชบัญญัติดังกล่าวยังไม่ได้กำหนดบทนิยามให้ชัดเจนและครอบคลุม เช่น คำว่า “ข้อมูลคอมพิวเตอร์” “เข้าถึง” “ดักรับข้อมูล” ซึ่งอาจทำให้เกิดปัญหาการตีความ และความผิดฐานดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ ตามมาตรา 8 นั้นกำหนดไว้อย่างกว้างๆและไม่ชัดเจน อีกทั้งยังไม่ได้กำหนดฐานความผิดเกี่ยวกับการลักข้อมูลคอมพิวเตอร์ไว้อีกด้วย โดย อัญธิกา ณ พิบูลย์ ได้เสนอแนะให้มีการบัญญัติคำนิยามศัพท์เพิ่มเติม เช่น คำว่า “ข้อมูลคอมพิวเตอร์” “เข้าถึง” ให้มีความชัดเจน เพิ่มรายละเอียดเกี่ยวกับลักษณะและพฤติการณ์ของการกระทำความผิดในฐานเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตตามมาตรา 5 ฐานดักรับข้อมูลคอมพิวเตอร์ในมาตรา 8 โดยตัดบทบัญญัติฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ ตามมาตรา 7 ออกไปเพราะเห็นว่ามีความซ้ำซ้อนกับมาตรา 5 และเพิ่มความผิดฐานฉ้อโกงที่เกี่ยวกับคอมพิวเตอร์และฐานลักข้อมูลคอมพิวเตอร์ แต่จากการศึกษาของผู้วิจัยบ่งชี้ว่า ความผิดฐานดักรับข้อมูลคอมพิวเตอร์ในมาตรา 8 นั้นสามารถปรับใช้บังคับกับการกระทำความผิดในการลักข้อมูลคอมพิวเตอร์ทั่วๆ ไปที่อยู่ในระบบคอมพิวเตอร์ได้อยู่แล้ว[48] ทั้งอัตราโทษในความผิดฐานลักข้อมูลคอมพิวเตอร์ที่ อัญธิกา ณ พิบูลย์ ได้เสนอนั้น มีอัตราโทษเท่ากับมาตรา 8 อีกด้วย การอ้างว่าไม่มีบทบัญญัติของกฎหมายในความผิดลักษณะนี้ จึงเป็นการตั้งสมมติฐานที่ไม่ถูกต้องเพียงแต่ว่ามีความผิดในบางรูปแบบที่เป็นรูปแบบเฉพาะดังเช่นเรื่อง การดึงข้อมูลจากบัตร

---

[47] อัญธิกา ณ พิบูลย์, "ปัญหาและอุปสรรคในการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2551), หน้า 1-179.

[48] อาทิเช่น ข้อมูลที่ไม่ได้มีการออกเอกสารหรือวัตถุอื่นใดให้ ตามประมวลกฎหมายอาญา มาตรา 1(14)(ข) นั้นสามารถลงโทษผู้กระทำความผิดในลักษณะ 7 หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ หรือ ลงโทษตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 8 หากเป็นการดักรับข้อมูลคอมพิวเตอร์ที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ ได้อยู่แล้ว

อิเล็กทรอนิกส์ที่ผู้วิจัยมุ่งศึกษานั้น ซึ่งไม่อาจนำมาตรา 8 ดังกล่าวมาบังคับใช้ได้ และการเสนอให้มีการกำหนดบทนิยามศัพท์เพิ่มเติมและกำหนดรายละเอียดในบทบัญญัติต่างๆ เพิ่มขึ้น โดยงานวิจัยดังกล่าวมิได้มีบทวิเคราะห์ว่า อย่างไรถึงได้เสนอแนะเช่นนั้น และการเสนอแนะเช่นนั้น จะทำให้กฎหมายที่มีอยู่ชัดเจนและครอบคลุมเพิ่มขึ้นอย่างไร การเพิ่มลักษณะและพฤติการณ์มากๆ เข้าไปในบทบัญญัติของกฎหมายตามที่ได้เสนอ จะเกิดปัญหาการตีความที่ไม่สิ้นสุดและซ้ำซ้อนกับบทบัญญัติอื่นๆ หรือไม่ ตามที่ อัญธิกา ณ พิบูลย์ ได้ตั้งเป็นประเด็นไว้ในตอนต้น ดังนั้นการเสนอแนะในงานวิจัยดังกล่าวจึงยังขาดการวิเคราะห์และอาจสร้างปัญหาแก่การนำข้อเสนอในงานวิจัยไปใช้ต่อไป

บทที่ 2
การกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์

บัตรอิเล็กทรอนิกส์เป็นนวัตกรรมยุคใหม่อันเกิดจากการพัฒนาทางเทคโนโลยีและสารสนเทศอย่างต่อเนื่องและถูกผลิตขึ้นเพื่อให้มีการใช้งานที่หลากหลาย เช่น ใช้ยืนยันหรือระบุตัวบุคคลผู้มีสิทธิใช้บัตรอิเล็กทรอนิกส์ใบนั้น ใช้แลกเปลี่ยนหรือเข้าถึงสิทธิใดๆ ใช้ทำธุรกรรมทางการเงินหลายรูปแบบ เช่น ใช้เบิกถอนเงินจากเครื่องจ่ายเงินอัตโนมัติ ใช้ซื้อสินค้าและบริการในห้างร้านต่างๆ จนไปถึงการซื้อสินค้าหรือบริการทางออนไลน์ ประกอบกับการใช้งานที่ง่าย สะดวกและรวดเร็ว จึงทำให้เกิดการใช้งานบัตรอิเล็กทรอนิกส์อย่างแพร่หลาย จนอาจกล่าวได้ว่าบัตรอิเล็กทรอนิกส์เป็นสิ่งจำเป็นที่บุคคลต้องมีเพื่อใช้งานในชีวิตประจำวันก็ว่าได้ เหตุดังกล่าวจึงเป็นสิ่งล่ออาชญากรให้กระทำการโดยมิชอบเพื่อให้ได้มาซึ่งประโยชน์จากการใช้งานบัตรอิเล็กทรอนิกส์เหล่านั้น จึงทำให้เกิดการกระทำความผิดเกี่ยวบัตรอิเล็กทรอนิกส์ขึ้นอย่างต่อเนื่องนับตั้งแต่มีการเริ่มใช้งานบัตรอิเล็กทรอนิกส์เป็นต้นมา

ในบทที่ 2 นี้จะกล่าวถึงความหมายของบัตรอิเล็กทรอนิกส์โดยทั่วไปและในประมวลกฎหมายอาญาว่าในทางกฎหมายนั้นให้ความหมายครอบคลุมถึงสิ่งใดบ้างที่เป็นบัตรอิเล็กทรอนิกส์และบัตรอิเล็กทรอนิกส์ที่มีใช้อยู่ในปัจจุบันนั้นมีด้วยกันกี่ประเภท ตลอดจนถึงลักษณะของการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามที่ประมวลกฎหมายอาญาได้กำหนดไว้ว่ามีรูปแบบอย่างไรบ้าง

2.1 ความทั่วไปเกี่ยวกับบัตรอิเล็กทรอนิกส์

2.1.1 นิยามของบัตรอิเล็กทรอนิกส์

พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554 ให้ความหมายโดยทั่วไปของคำว่า “บัตร” และคำว่า “บัตรอิเล็กทรอนิกส์” ไว้ดังนี้[1]

บัตร หมายถึง แผ่นเอกสารแสดงสิทธิของผู้ใช้ เป็นต้น มักทำด้วยกระดาษรูปสี่เหลี่ยมผืนผ้า เช่น บัตรประจำตัว บัตรเลือกตั้ง บัตรสมนาคุณ

บัตรอิเล็กทรอนิกส์ หมายถึง บัตรที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้โดยบันทึกข้อมูลหรือรหัสไว้ในบัตรด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้าหรือวิธีอื่นใดในลักษณะ

[1] สำนักงานราชบัณฑิตยสภา, "พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554" [ออนไลน์], เข้าถึงเมื่อ 19 กรกฎาคม 2563. แหล่งที่มา: http://www.royin.go.th/dictionary/index.php.

คล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็ก เช่น บัตรเครดิต บัตรเดบิต บัตรสมาร์ทการ์ด

จากการให้ความหมายของพจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554 ดังกล่าว จึงสรุปได้ว่า ในความหมายโดยทั่วไปนั้น บัตรอิเล็กทรอนิกส์ คือบัตรที่เป็นแผ่นเอกสารอันแสดงสิทธิของผู้ใช้ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยบันทึกข้อมูลหรือรหัสไว้ในบัตรด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้าหรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็ก โดยเป็นการนำข้อความเพียงบางส่วนในประมวลกฎหมายอาญา มาตรา 1(14)(ก) มาให้ความหมาย แต่ในทางกฎหมาย คำว่า “บัตรอิเล็กทรอนิกส์” จะมีความหมายเพียงใดนั้น จำต้องพิเคราะห์จากประมวลกฎหมายอาญา อันเป็นบทหลักที่ได้ให้ความหมายดังกล่าวไว้และกฎหมายอื่นๆ ที่เกี่ยวข้อง อันได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ประกอบกันด้วย

พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547 ได้ให้ความหมายของคำว่า “บัตรอิเล็กทรอนิกส์” โดยการเพิ่มบทนิยามลงในมาตรา 1(14) ของประมวลกฎหมายอาญา ซึ่งบัญญัติไว้ว่า

มาตรา 1(14) “บัตรอิเล็กทรอนิกส์” หมายความว่า

(ก) เอกสารหรือวัตถุอื่นใดไม่ว่าจะมีรูปลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า

(ข) ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ แต่มีวิธีการใช้ในทำนองเดียวกับ (ก) หรือ

(ค) สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ

จากคำนิยามดังกล่าว สิ่งใดจะเป็นบัตรอิเล็กทรอนิกส์ตามกฎหมายอาญาได้นั้น จำต้องเข้าลักษณะใดลักษณะหนึ่งตามมาตรา 1(14)(ก) หรือ มาตรา 1(14)(ข) หรือ มาตรา 1(14)(ค) แห่งประมวลกฎหมายอาญาเท่านั้น หากสิ่งใดเมื่อพิจารณาแล้วไม่มีลักษณะตามที่กฎหมายกำหนดไว้ดังกล่าวก็ไม่เป็นบัตรอิเล็กทรอนิกส์ ซึ่งหากมีการกระทำความผิดเกิดขึ้นแก่สิ่งนั้นซึ่งเป็นวัตถุแห่งการกระทำแล้ว ผู้กระทำความผิดก็ไม่มีความผิดตามประมวลกฎหมายอาญาในลักษณะที่ 7 หมวดที่ 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ แต่อาจจะเป็นความผิดตามลักษณะอื่นหรือผิดกฎหมายอื่นที่มีโทษทางอาญาได้ หากสิ่งนั้นมีลักษณะครบตามที่กฎหมายนั้นๆ ได้กำหนดไว้ ซึ่งผู้วิจัยจะได้กล่าวไว้ในหัวข้ออื่นๆ ต่อไป

ดังนั้นจึงมีความจำเป็นอย่างยิ่งที่จะต้องศึกษาเพื่อระบุให้ชัดเจนว่า สิ่งใดเป็นบัตรอิเล็กทรอนิกส์ โดยพิเคราะห์ความหมายดังที่มาตรา 1(14) ได้ระบุไว้ ซึ่งสามารถจำแนกได้ ดังนี้

2.1.1.1 บัตรอิเล็กทรอนิกส์ในรูปเอกสารหรือวัตถุอื่นใด

สิ่งใดที่จะเป็นบัตรอิเล็กทรอนิกส์ในความหมายแรก ตามมาตรา 1(14)(ก) นั้น ต้องประกอบด้วยลักษณะดังนี้

(ก) เอกสารหรือวัตถุอื่นใด หมายความว่า เป็นเอกสารในความหมายของมาตรา 1(7) ที่บัญญัติว่า “เอกสาร” หมายความว่า กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น หรือเป็นวัตถุอื่นใดที่ไม่ใช่เอกสารเพราะไม่ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น บนวัตถุอื่นใดนั้น และไม่ว่าจะมีรูปลักษณะใด เช่น เป็นเหรียญพลาสติกทรงกลมที่เป็นเหรียญใช้บริการรถไฟฟ้ามหานคร (MRT) ของกรุงเทพมหานคร

(ข) ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยที่ผู้ออกนี้อาจจะเป็นธนาคารพาณิชย์ สถาบันทางการเงิน ซึ่งออกให้ตามสัญญาเปิดบัญชีเงินฝาก หรือตามสัญญาเบิกเงินเกินบัญชีที่ลูกค้าของธนาคารหรือสถาบันดังกล่าวได้ทำไว้ หรือบริษัท โรงเรียน ซึ่งได้ออกบัตรประจำตัวให้แก่บุคคลต่างๆ ในองค์กรเพื่อใช้ระบุตัวตน หรือห้างร้าน ซึ่งได้ออกบัตรเพื่อให้ผู้ใช้บริการเก็บสะสมแต้มหรือคูปองต่างๆ หรือผู้ให้บริการเครือข่ายโทรศัพท์มือถือ เครือข่ายอินเตอร์เน็ต บริการสื่อส่งผ่านสัญญาณต่อเนื่อง (Streaming Media) ซึ่งออกให้แก่ผู้ซื้อบัตรดังกล่าวตามตัวแทนจำหน่ายแลกกับการรับบริการนั้นๆ เป็นต้น

(ค) ซึ่งจะระบุชื่อหรือไม่ก็ตาม เช่นบัตรที่มีชื่อเฉพาะหรือชื่อตามเครื่องหมายการค้า เช่น บัตรประจำตัวประชาชน บัตรวีซ่า (VISA) บัตรมาสเตอร์การ์ด (Mastercard) หรือที่ไม่ระบุชื่อแต่ผู้ออกให้และผู้มีสิทธิใช้เรียกเป็นการทั่วๆไป เช่น บัตรพนักงานบริษัท บัตรประจำตัวนักเรียน

(ง) โดยการบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด อันเป็นวิธีการในการบรรจุข้อมูลหรือรหัสลงในบัตรนั้นเพื่อให้ครอบคลุมถึงวิธีต่างๆ ในกระบวนการสร้างบัตรอิเล็กทรอนิกส์ขึ้น ซึ่งมีด้วยกันหลายรูปแบบในปัจจุบัน ทั้งยังขยายความรองรับอีกว่าวิธีการบรรจุข้อมูลหรือรหัสนั้น ผลลัพธ์สุดท้ายอาจมีทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า เช่น เห็นเป็นตัวเลขหรือหมายเลขบัตร ปรากฏให้เห็นด้วยตาจากด้านนอกบนบัตรหรือจะไม่มีอะไรปรากฏเป็นตัวเลขหรือหมายเลขบัตรให้เห็นด้วยตาเปล่าบนบัตรก็ตาม เอกสารหรือวัตถุอื่นใดนั้นก็ยังเป็นบัตรอิเล็กทรอนิกส์ ในความหมายตามมาตรา 1(14)(ก)

ข้อสังเกต ถ้อยคำตามความหมายแรกของบัตรอิเล็กทรอนิกส์ที่ว่า “การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะที่คล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็ก...” เป็นการคัดลอกมาจากพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ซึ่งให้คำจำกัดความว่า “อิเล็กทรอนิกส์” นั่นเอง[2]

ตัวอย่างบัตรอิเล็กทรอนิกส์ที่อยู่ในรูปเอกสาร เช่น บรรดาบัตรต่างๆ ที่สามารถพบได้ทั่วไป อาทิ บัตรเครดิต บัตรเดบิต บัตรเอทีเอ็ม บัตรซิมการ์ด บัตรเปิดประตูห้องในโรงแรม บัตรสมาร์ทการ์ด[3] บัตรเติมเงินต่างๆ บัตรเติมน้ำมัน[4] บัตรประจำตัวประชาชน บัตรประจำตัวพนักงานในองค์กร บัตรสมาชิกของห้างร้านต่างๆ ซึ่งโดยส่วนใหญ่แล้วมักจะใช้เทคโนโลยีในรูปแบบแถบแม่เหล็ก (Magnetic Card) หรือสมาร์ทการ์ด (Smart Card) ซึ่งเป็นเทคโนโลยีที่พัฒนาขึ้นมาโดยใช้การฝังชิป (Chip) อันเป็นหน่วยบันทึกความจำที่บันทึกข้อมูลเกี่ยวกับผู้ใช้บัตร รหัสผ่าน และวันหมดอายุของบัตรไว้ด้วย ส่วนบัตรอิเล็กทรอนิกส์ที่อยู่ในรูปของวัตถุอื่นใด เช่น เหรียญทรงกลมของรถไฟฟ้าใต้ดินที่

---

[2] สำนักประธานศาลฎีกา สำนักวิชาการ สำนักงานศาลยุติธรรม, "ข้อสังเกตพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547" [ออนไลน์], เข้าถึงเมื่อ 21 พฤศจิกายน 2560. แหล่งที่มา: www.library.coj.go.th/lnfo/44300?c=20348014.

[3] เป็นบัตรที่ใช้แถบแม่เหล็กที่ฝังชิป (Chip) ทำให้บันทึกหน่วยความจำได้มากกว่า เช่น บัตรประจำตัวประชาชน

[4] คำพิพากษาฎีกาที่ 10025/2557

มีการฝังไมโครชิป[5] รีโมตคอนโทรล[6] บัตรเสียบเข้าออกสถานที่ซึ่งไม่มีข้อความใดๆ บนบัตร[7] หีบห่อสินค้าที่มีรหัสแท่ง (Bar Code)[8]

มีข้อสังเกตว่าการจะเป็น บัตรอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ก) ได้นั้น ประการสำคัญนอกจากจะต้องมีการออกเอกสารหรือวัตถุอื่นใดให้แก่ผู้มีสิทธิใช้แล้ว เอกสารหรือวัตถุอื่นใดนั้นต้องมีการใช้งานคงทนพอสมควรด้วย ซึ่งมิใช่การใช้งานเพียงชั่วคราว หากเอกสารนั้นเป็นเพียงกระดาษธรรมดาๆ ที่มีวัตถุประสงค์เพียงแค่เตือนความจำ เช่นจดหมายที่ธนาคารส่งรหัสชั่วคราวให้แก่ลูกค้า เมื่อลูกค้าแกะดูแล้วก็จำไว้แล้วทิ้ง เช่นนี้ ถือว่าเอกสารฉบับนี้ไม่เป็น “บัตรอิเล็กทรอนิกส์” ตามมาตรา 1(14)(ก) เพราะต้องถือว่าทางธนาคาร “มิได้ออกเอกสารหรือวัตถุอื่นใดให้” แต่เฉพาะเลขรหัส ที่อยู่ในจดหมายจะเป็น “บัตรอิเล็กทรอนิกส์” ตามความในมาตรา 1(14)(ข)[9] ซึ่งจะได้กล่าวต่อไป

ดังนั้น จึงอาจกล่าวได้โดยสรุปว่า ความหมายของ บัตรอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ก) นั้นมุ่งถึงตัวบัตรอิเล็กทรอนิกส์ที่เป็นเอกสารหรือวัตถุอื่นใดที่จับต้องได้และเป็นกายภาพ (Physical) เท่านั้น เช่น เป็นกระดาษ แผ่นพลาสติก โลหะ หรือวัสดุใดๆ อันเป็นวัตถุที่สามารถจับต้องได้เท่านั้น หากเป็นวัตถุที่จับต้องไม่ได้ (Nonphysical) ต้องพิจารณาว่า สิ่งใดๆ นั้นเป็น บัตรอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ข) หรือ ตามมาตรา 1(14)(ค) หรือไม่ต่อไป

---

[5] สำนักประธานศาลฎีกา สำนักวิชาการ สำนักงานศาลยุติธรรม, ข้อสังเกตพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ.2547 [ออนไลน์], 21 พฤศจิกายน 2560. แหล่งที่มา www.library.coj.go.th/Info/44300?c=20348014.

[6] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, พิมพ์ครั้งที่ 6 (กรุงเทพฯ: กรุงสยาม พับลิชชิ่ง, 2557), หน้า 305.

[7] เรื่องเดียวกัน.

[8] เรื่องเดียวกัน.

[9] เรื่องเดียวกัน, หน้า 306.

2.1.1.2 บัตรอิเล็กทรอนิกส์ในรูปข้อมูล รหัส หมายเลข หรือตัวเลข

สิ่งใดที่จะเป็นบัตรอิเล็กทรอนิกส์ในความหมายที่สอง ตามมาตรา 1(14)(ข) นั้น ต้องประกอบด้วยลักษณะดังนี้

(ก) ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ

(ข) ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ เหมือนคำนิยาม ตามมาตรา 1(14)(ก)

(ค) โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ ซึ่งนับเป็นข้อสังเกตที่สำคัญที่สุดของการเป็นบัตรอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ข) นี้เพราะ หากข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ได้มีการออกเอกสารหรือวัตถุอื่นใดให้ด้วย ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขนั้น จะไม่เป็นบัตรอิเล็กทรอนิกส์ ไม่ว่า ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขนั้นจะปรากฏบนเอกสารหรือวัตถุอื่นใดนั้น หรือไม่ปรากฏบนเอกสารหรือวัตถุอื่นใดดังกล่าว แต่ได้ถูกบรรจุไว้ในแหล่งบันทึกหน่วยความจำในเอกสารหรือวัตถุอื่นใดนั้นก็ตาม เช่น หมายเลขบนบัตรเครดิตรวมถึงวันหมดอายุของบัตรเครดิตที่ปรากฏบนบัตรเครดิตที่มองเห็นได้ด้วยตาเปล่า รวมทั้งข้อมูลที่บันทึกอยู่ในแถบแม่เหล็ก (Magnetic Stripe) หรือในชิป (Chip) ของบัตรเครดิตใบนั้นที่ไม่สามารถมองเห็นได้ด้วยตาเปล่า เมื่อมีการออกบัตรซึ่งเป็นเอกสารให้ จึงนับว่า หมายเลข วันหมดอายุ ข้อมูลในบัตร ไม่เป็นบัตรอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ข) นี้

ข้อความที่ว่า “มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้” จึงนับว่าเป็นข้อความสำคัญที่จะต้องพิจารณาเสียก่อนว่า ผู้ออกนั้นได้มีการออกเอกสารหรือวัตถุอื่นใดให้หรือไม่ กรณีนี้มีความเห็นทางกฎหมายของนักกฎหมายไทยหลายท่านเห็นว่า หากเอกสารหรือวัตถุอื่นใดที่ผู้ออกได้ออกให้นั้นไม่เป็นสาระสำคัญ หรือเป็นการใช้งานเพียงชั่วคราว ไม่มีการใช้งานคงทนพอสมควรแล้วจะถือว่าผู้ออกมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้[10] อันส่งผลให้ ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ในเอกสารหรือวัตถุอื่นใดดังกล่าว เป็นบัตรอิเล็กทรอนิกส์ตามความหมายของมาตรา 1(14)(ข) นั่นเอง เช่น กระดาษที่ธนาคารส่งมาให้แก่ลูกค้าเพื่อแจ้งรหัสของบัตรเอทีเอ็มที่ทางธนาคารได้ออกให้และมีข้อความว่าให้ทำลายเสีย เมื่อลูกค้าแกะดูแล้วก็จำไว้แล้วทิ้ง หรือ รหัสต่างๆ เพื่อใช้งานอินเตอร์เน็ตที่ปรากฏอยู่บนแผ่นพลาสติกธรรมดาๆ ที่ไม่มีรหัสแท่ง (Bar Code) บนแผ่นพลาสติกนั้น รหัสทั้งสองกรณีดังกล่าวนี้ล้วนเป็นบัตรอิเล็กทรอนิกส์

[10] เรื่องเดียวกัน.

ทั้งสิ้น แต่มีข้อน่าสังเกตว่า หากเป็นหมายเลขรหัสที่ปรากฏเมื่อทำการขูดบัตรเติมเงินโทรศัพท์มือถือ ซึ่งเป็นบัตรเติมเงินพลาสติกที่มีรหัสแท่งบนบัตร หมายเลขรหัสนี้ไม่ใช่บัตรอิเล็กทรอนิกส์เพราะถือว่าได้มีการออกเอกสารหรือวัตถุอื่นใดให้แล้ว แต่หากเป็นหมายเลขรหัสที่ใช้เติมเงินโทรศัพท์มือถือบนกระดาษใบเสร็จรับเงิน (Receipt Slip) ของร้านค้าที่ไม่ปรากฏรหัสแท่งบนกระดาษใบเสร็จรับเงินนั้น หมายเลขรหัสนี้จะเป็นบัตรอิเล็กทรอนิกส์เพราะถือว่ามิได้มีการออกเอกสารหรือวัตถุอื่นใดให้[11] กรณีดังกล่าวผู้วิจัยจึงเห็นว่าการตีความว่า ได้มีการออกเอกสารหรือวัตถุอื่นใดให้หรือไม่นั้นยังขาดหลักเกณฑ์ที่แน่นอน ซึ่งต้องอาศัยการพัฒนาของกฎหมายและความเห็นทางกฎหมายของนักกฎหมายเพราะยังมีเอกสารหรือวัตถุอีกมากที่อาจเข้าลักษณะของบัตรอิเล็กทรอนิกส์ได้ในปัจจุบัน ซึ่งต้องอาศัยการตีความดังกล่าว อันส่งผลต่อความรับผิดทางอาญาของบุคคลได้

(ง) และมีวิธีการใช้ในทำนองเดียวกับ มาตรา 1(14)(ก) หมายความว่า มีการใช้งานเสมือนเป็นบัตรอิเล็กทรอนิกส์ เช่นเดียวกับเอกสารหรือวัตถุอื่นใดในมาตรา 1(14)(ก) เช่น ใช้ข้อมูลรหัส หรือหมายเลขบัญชี นั้นในการทำธุรกรรมออนไลน์ เปิดประตูห้องในโรงแรม ใช้เป็นส่วนลดในห้างร้าน ระบุตัวตนของพนักงานหรือประชาชน

กรณีตามความหมายที่สองของบัตรอิเล็กทรอนิกส์นี้ จะใช้ในทางการติดต่อสื่อสารการค้า การพาณิชย์ผ่านสื่ออิเล็กทรอนิกส์ซึ่งเรียกว่าพาณิชย์อิเล็กทรอนิกส์ ซึ่งในอนาคตจะมีการทำธุรกรรมลักษณะนี้เพิ่มมากขึ้น เช่น การใช้จ่ายผ่านทางเครือข่ายอินเตอร์เน็ต ซึ่งในปัจจุบัน ธนาคารบางแห่งจะออกหมายเลขบัญชีให้โดยไม่ออกตัวบัตรให้แก่ผู้มีสิทธิใช้ อันมีลักษณะคล้ายกับหมายเลขบัตรเครดิตที่ไม่มีการออกบัตรเครดิตให้ หรือการทำธุรกรรมทางอิเล็กทรอนิกส์ซึ่งธนาคารจะให้หมายเลขบัญชีนี้กับบริษัทห้างร้านที่ต้องการทำธุรกรรมผ่านทางธนาคาร หากร้านค้าต้องการทำธุรกรรมก็จะใช้หมายเลขชุดหรือรหัสที่ออกให้เพื่อยืนยันตัวบุคคลเข้าทำธุรกรรม[12]

ตัวอย่างบัตรอิเล็กทรอนิกส์ที่อยู่ในรูปข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลข เช่น รหัสหมายเลขโทรศัพท์ หมายเลขบัญชีและหมายเลขรหัสต่างๆ ที่ธนาคารได้ออกให้แก่ลูกค้าในการทำธุรกรรมทางอินเตอร์เน็ต รหัสพิน (Pin) หกหลักที่ธนาคารส่งไปยังโทรศัพท์มือถือ เสียงที่ธนาคารส่งข้อมูลเข้าไปในระบบโทรศัพท์ให้ลูกค้า ชื่อผู้ใช้ (Username) หรือ รหัสผู้ใช้ (Password) ต่างๆ ที่ใช้ในการเข้าสู่ระบบที่ทางเว็บไซด์เป็นผู้ออกให้

---

[11] เรื่องเดียวกัน, หน้า 306-309.

[12] สำนักประธานศาลฎีกา สำนักวิชาการ สำนักงานศาลยุติธรรม, ข้อสังเกตพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ.2547 [ออนไลน์], 21 พฤศจิกายน 2560. แหล่งที่มา www.library.coj.go.th/Info/44300?c=20348014.

หมายเลขรหัสที่ส่งไปเตือนความจำลูกค้าของธนาคารที่อยู่บนกระดาษธรรมดาๆ รหัสจองตั๋วเครื่องบิน (Booking Number) ที่ได้รับจากสายการบิน หมายเลขรหัสโปรแกรม (Serial Number) สำหรับโปรแกรม (Software) ของเครื่องคอมพิวเตอร์

ดังนั้นจึงอาจกล่าวได้โดยสรุปว่า ความหมายของ บัตรอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ข) นั้นมุ่งถึงสิ่งที่เป็นข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลข ซึ่งไม่มีกายภาพและไม่สามารถจับต้องได้ (Nonphysical) และต้องมีการบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า ในทำนองเดียวกับ มาตรา 1(14)(ก) ด้วย[13] โดยการบันทึกไว้ในหน่วยความจำที่ใดที่หนึ่งหรือหลายที่ อาทิ บันทึกไว้ในฮาร์ดดิส (Harddisk) ของเครื่องคอมพิวเตอร์ ในแผ่นดิสก์ (Diskette) หรือในหน่วยความจำรูปแบบต่างๆ (Storage Device) แต่ถ้าเป็นการบันทึกไว้ในแผ่นแถบแม่เหล็ก (Magnetic Stripe) หรือในชิป (Chip) แล้วต้องมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ด้วย ถ้าผู้ออกได้ออกบัตรซึ่งเป็นเอกสารให้ด้วยแล้ว ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลข ที่ถูกบันทึกไว้ในแผ่นแถบแม่เหล็กหรือในชิปนั้น จะไม่เป็นบัตรอิเล็กทรอนิกส์ตามที่มาตรา 1(14)(ข) ได้กำหนดไว้ ซึ่งส่งผลให้การกระทำแก่วัตถุแห่งการกระทำดังกล่าวไม่เป็นความผิดตามประมวลกฎหมายอาญา เช่น นายแดงใช้เครื่องดูดข้อมูลแถบรหัสแม่เหล็ก (Skimmer) ติดตั้งไว้กับเครื่องจ่ายเงินอัตโนมัติ (ATM Machine) ต่อมานายดำนำบัตรเอทีเอ็มของตนที่มีแผ่นแถบแม่เหล็กด้านหลังบัตรที่บันทึกข้อมูลต่างๆ ไว้ไปรูดผ่านเครื่องดูดข้อมูลแถบรหัสแม่เหล็กนั้น ต่อมานายแดงนำข้อมูลของนายดำที่ได้จากกระบวนการดังกล่าวไปใช้หรือมีไว้เพื่อนำออกใช้ นายแดงก็ไม่มีความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/5 และไม่มีความผิดฐานมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/6 เพราะข้อมูลนั้นของนายดำ ที่ได้มีการออกบัตรซึ่งเป็นเอกสารให้ ไม่เป็นบัตรอิเล็กทรอนิกส์ในความหมายของ มาตรา 1(14)(ข) นั่นเอง

ข้อสังเกตที่ผู้วิจัยได้จากการพิจารณาบทบัญญัติ มาตรา 1(14)(ข) นี้ประกอบกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พบว่า ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ ที่ผู้ออกให้แก่ผู้มีสิทธิใช้ไม่ว่าจะได้มีการออกเอกสารหรือวัตถุอื่นใดให้ อันจะเป็นบัตรอิเล็กทรอนิกส์หรือไม่ก็ตาม ตาม

[13] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 307.

ประมวลกฎหมายอาญา แต่เนื่องจาก ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ นั้นโดยสภาพอาจเข้าลักษณะคำนิยามของคำว่า “ข้อมูลคอมพิวเตอร์” ตามมาตรา 3 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และหมายรวมถึงการเป็น “ข้อมูลอิเล็กทรอนิกส์” ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ด้วย จึงส่งผลให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้นนอกจากจะพิจารณาองค์ประกอบความผิดตามประมวลกฎหมายอาญา มาตรา 269/1 ถึง มาตรา 269/7 แล้ว ก็ต้องพิจารณาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อันมีโทษทางอาญาด้วย ซึ่งผู้กระทำอาจมีความผิดตามพระราชบัญญัตินี้ได้ อันจะกล่าวต่อไป

2.1.1.3 บัตรอิเล็กทรอนิกส์ในรูปสิ่งอื่นใด

สิ่งใดที่จะเป็นบัตรอิเล็กทรอนิกส์ในความหมายสุดท้าย ตามมาตรา 1(14)(ค) ต้องประกอบด้วยลักษณะดังนี้

(ก) สิ่งอื่นใด หมายถึงสิ่งใดก็ตามที่ไม่เข้าลักษณะของบัตรอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ก) และ มาตรา 1(14)(ข)

(ข) ที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ หมายถึง มีข้อมูลอิเล็กทรอนิกส์ที่เป็นสิ่งอื่นใดนั้นได้ทำการจัดเก็บไว้ในแหล่งจัดเก็บข้อมูลหรือระบบคอมพิวเตอร์ใดๆ ไว้ก่อนแล้ว เพียงแต่ต้องใช้สิ่งอื่นใดนั้นอีกครั้งหนึ่ง เพื่อปิดหรือเปิดการทำงาน เพื่อยืนยัน หรือเพื่อระบุตัวบุคคลผู้เป็นเจ้าของสิ่งอื่นใดนั้น อันเป็นการแสดงความสัมพันธ์ระหว่างบุคคลผู้เป็นเจ้าของสิ่งอื่นใดกับข้อมูลอิเล็กทรอนิกส์ที่มีอยู่เดิม ว่าเหมือนกันหรือตรงกัน

ข้อสังเกต นิยามของคำว่า ข้อมูลอิเล็กทรอนิกส์ ในมาตรานี้ จำต้องพิจารณาความหมายที่ได้บัญญัติไว้ใน พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4 ด้วย[14] ซึ่งบัญญัติว่า

“ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

[14] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 310.

ตัวอย่างบัตรอิเล็กทรอนิกส์ในรูปสิ่งอื่นใด เช่น ลายนิ้วมือ ลายมือ ลายเท้า นัยน์ตา คลื่นเสียง เพราะเป็นสิ่งอื่นใดที่ใช้ประกอบข้อมูลอิเล็กทรอนิกส์ที่ได้มีการบันทึกไว้แล้ว เช่น ใช้นิ้วมือไปสัมผัสกับเครื่องเพื่อยืนยันตนผู้เป็นเจ้าของนั้นให้ตรงกับที่ได้บันทึกไว้ในเครื่องนั้นและเพื่อให้ประตูห้องเปิดออกเพราะเป็นชุดข้อมูลที่เหมือนกันกับเจ้าของลายนิ้วมือที่ได้ทำการบันทึกไว้ในระบบก่อนแล้ว[15] เปรียบเสมือนการบัญญัติเพิ่มเติมให้สิ่งที่เกี่ยวข้องกับร่างกายของมนุษย์ที่ใช้งานร่วมกับชุดข้อมูลอิเล็กทรอนิกส์ อันเป็นการใช้เทคโนโลยีทางชีวภาพโดยอาศัยหลักการพื้นฐานของลักษณะเฉพาะทางกายภาพของแต่ละบุคคล[16] ให้ถือว่าเป็นบัตรอิเล็กทรอนิกส์ด้วยเพื่อความครอบคลุมในการคุ้มครองบุคคลในทางอาญาด้วย เช่น หากนายแดงเลียนเสียงของนายดำเพื่อแสดงให้ระบบตู้นิรภัยเข้าใจว่าตนเองเป็นนายดำและใช้เปิดตู้นิรภัยของนายดำ เช่นนี้ นับว่านายดำกระทำการปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/1 และใช้บัตรอิเล็กทรอนิกส์ปลอมนั้น ตาม มาตรา 269/4 หรือถ้านายดำอัดเสียงของนายแดง ซึ่งเสียงของนายแดง ตามคำนิยามนี้คือ บัตรอิเล็กทรอนิกส์ของนายแดง นายดำจะมีความผิดฐานมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/6 ถ้าได้ใช้เสียงที่อัดนั้น นายดำก็จะมีความความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/5 อีกด้วย[17] แต่ถ้าสิ่งใดๆ นั้น มิได้ใช้ประกอบข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์แล้ว สิ่งนั้นก็มิใช่บัตรอิเล็กทรอนิกส์ เช่น คราบเลือด เส้นผม ดีเอ็นเอ (DNA) ของคนร้ายที่ตำรวจพบในที่เกิดเหตุ เว้นแต่ในอนาคตจะได้จัดเก็บลายพิมพ์นิ้วมือ หรือ ดีเอ็นเอ ของบุคคลในฐานข้อมูลทะเบียนราษฎร ก็จะทำให้สิ่งเหล่านี้เป็นบัตรอิเล็กทรอนิกส์เช่นกัน

---

[15] เรื่องเดียวกัน.

[16] สำนักประธานศาลฎีกา สำนักวิชาการ สำนักงานศาลยุติธรรม, ข้อสังเกตพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ.2547 [ออนไลน์], 21 พฤศจิกายน 2560. แหล่งที่มา www.library.coj.go.th/Info/44300?c=20348014.

[17] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 310.

ตารางที่ 1 เปรียบเทียบการเป็นบัตรอิเล็กทรอนิกส์ ตามคำนิยามในมาตรา 1(14) แห่งประมวลกฎหมายอาญา

ลักษณะของสิ่งใดๆ	เป็นบัตรอิเล็กทรอนิกส์	ไม่เป็นบัตรอิเล็กทรอนิกส์	ข้อมูลคอมพิวเตอร์ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	ข้อมูลอิเล็กทรอนิกส์ตาม พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
เอกสาร ซึ่งบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์	เฉพาะตัวเอกสาร ที่ปรากฏความหมายด้วยตัวอักษรเท่านั้นที่เป็นบัตรอิเล็กทรอนิกส์ ตาม มาตรา 1(14)(ก)	ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใด ๆ ที่ปรากฏบนบัตร หรือในหน่วยบันทึกความจำของบัตร	ตัวเอกสารไม่เป็นคอมพิวเตอร์จึงส่งผลให้ ข้อมูลที่ปรากฏบนบัตรไม่เป็นข้อมูลคอมพิวเตอร์เพราะไม่ได้อยู่ในระบบคอมพิวเตอร์	ข้อมูลที่บันทึกในหน่วยบันทึกความจำของบัตรไม่เป็นข้อมูลอิเล็กทรอนิกส์
วัตถุอื่นใด ซึ่งบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์	เฉพาะตัววัตถุอื่นใด ที่ไม่ปรากฏความหมายด้วยตัวอักษรเท่านั้นที่เป็นบัตรอิเล็กทรอนิกส์ ตาม มาตรา 1(14)(ก)	ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใด ๆ ในหน่วยบันทึกความจำของบัตร	ตัววัตถุอื่นใดไม่เป็นคอมพิวเตอร์และไม่ได้อยู่ในระบบคอมพิวเตอร์จึงไม่ใช่ข้อมูลคอมพิวเตอร์	ข้อมูลที่บันทึกในหน่วยบันทึกความจำของบัตรไม่เป็นข้อมูลอิเล็กทรอนิกส์

ลักษณะของสิ่งใดๆ	เป็นบัตรอิเล็กทรอนิกส์	ไม่เป็นบัตรอิเล็กทรอนิกส์	ข้อมูลคอมพิวเตอร์ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	ข้อมูลอิเล็กทรอนิกส์ตาม พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใด ๆ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้	เป็นบัตรอิเล็กทรอนิกส์ตาม มาตรา 1(14)(ข)	-	เป็นข้อมูลคอมพิวเตอร์ เพราะข้อมูลดังกล่าวนั้นจำต้องอยู่ในระบบคอมพิวเตอร์ไว้ก่อนแล้ว	เป็นข้อมูลอิเล็กทรอนิกส์
ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใด ๆ และได้มีการออกเอกสารหรือวัตถุอื่นใดให้	-	ไม่เป็นบัตรอิเล็กทรอนิกส์ตาม มาตรา 1(14)	ข้อมูลที่ปรากฏบนเอกสารหรือวัตถุอื่นใดนั้นไม่เป็นข้อมูลคอมพิวเตอร์ เพราะเอกสารหรือวัตถุอื่นใดไม่ใช่คอมพิวเตอร์จึงทำให้ข้อมูลดังกล่าวไม่ได้อยู่ในระบบคอมพิวเตอร์	ข้อมูลที่บันทึกในหน่วยบันทึกความจำของบัตรไม่เป็นข้อมูลอิเล็กทรอนิกส์

ลักษณะของสิ่งใดๆ	เป็นบัตรอิเล็กทรอนิกส์	ไม่เป็นบัตรอิเล็กทรอนิกส์	ข้อมูลคอมพิวเตอร์ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	ข้อมูลอิเล็กทรอนิกส์ตาม พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ	เป็นบัตรอิเล็กทรอนิกส์ตาม มาตรา 1(14)(ค)	-	ไม่เป็นข้อมูลคอมพิวเตอร์เพราะองค์ประกอบทางชีวภาพของมนุษย์ไม่ใช่ระบบคอมพิวเตอร์	ไม่เป็นข้อมูลอิเล็กทรอนิกส์เพราะองค์ประกอบทางชีวภาพของมนุษย์ไม่ใช่ข้อความที่ได้สร้างขึ้นด้วยวิธีการทางอิเล็กทรอนิกส์

2.1.2 ประเภทของบัตรอิเล็กทรอนิกส์

บัตรอิเล็กทรอนิกส์ในปัจจุบันนั้นมีมากมายหลากหลายรูปแบบ อาจเรียกได้ว่าเอกสารหรือวัตถุใดๆ ที่ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งจะระบุชื่อบัตรนั้นหรือไม่ก็ตาม โดยมีการบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า แสง หรือแม่เหล็กหรือวิธีอื่นใดในลักษณะคล้ายกัน ให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า และในทางกฎหมายอาญาให้รวมบัตรอิเล็กทรอนิกส์ที่เป็นข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ และบัตรอิเล็กทรอนิกส์ที่เป็นสิ่งอื่นใดอันเป็นองค์ประกอบทางชีวภาพของมนุษย์ที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ ยังให้เป็นบัตรอิเล็กทรอนิกส์อีกด้วย จึงกล่าวได้ว่าสิ่งใดที่เข้าลักษณะของการเป็นบัตรอิเล็กทรอนิกส์นั้นมีมากมาย ยากที่จะระบุได้หมดสิ้น

โดยทั่วไปแล้วบัตรอิเล็กทรอนิกส์นั้นจะมีองค์ประกอบด้วยกัน 2 ส่วนคือ ส่วนที่เป็นตัวบัตรที่ทำด้วยวัสดุทั่วๆ ไป เช่น กระดาษ หรือพลาสติก และส่วนที่เก็บข้อมูลต่างๆ ของบัตรใบนั้น ซึ่งข้อมูลต่างๆ อาจมีทั้งที่บันทึกไว้ให้ปรากฏบนบัตรใบนั้นเองหรือบันทึกไว้ในแหล่งบันทึกใดๆ ที่จัดเก็บข้อมูลในรูปแบบข้อมูลอิเล็กทรอนิกส์ ดังนั้นผู้วิจัยจะทำการแบ่งประเภทของบัตรอิเล็กทรอนิกส์ออกตามรูปแบบของการจัดเก็บข้อมูลในบัตรอิเล็กทรอนิกส์ ดังนี้

2.1.2.1 บัตรอิเล็กทรอนิกส์ที่ไม่มีการจัดเก็บข้อมูลในรูปแบบข้อมูลอิเล็กทรอนิกส์

บัตรอิเล็กทรอนิกส์ประเภทนี้เป็นบัตรอิเล็กทรอนิกส์ที่ได้บันทึกข้อมูลต่างๆ ไม่ว่าจะเป็น ข้อความ ตัวอักษร ตัวเลข สัญลักษณ์ต่างๆ ไว้บนพื้นผิวของบัตรใบนั้นทั้งหมดโดยมิได้มีการบันทึกข้อมูลเหล่านั้นไว้ในรูปแบบของข้อมูลอิเล็กทรอนิกส์เลย เพราะข้อมูลอิเล็กทรอนิกส์นั้นจำต้องบันทึกไว้ในแหล่งบันทึกข้อมูลแยกต่างหากจากตัวบัตรอิเล็กทรอนิกส์ ซึ่งอาจถูกติดอยู่ด้านหน้าด้านหลัง หรือถูกฝังอยู่ข้างในบัตรอิเล็กทรอนิกส์นั้นก็ได้ บัตรอิเล็กทรอนิกส์ประเภทนี้จึงเป็นบัตรอิเล็กทรอนิกส์ในรูปแบบเก่าหรือที่เคยใช้กันในอดีตที่เป็นกระดาษธรรมดาหรือเป็นพลาสติกแข็ง ที่มิได้นำเทคโนโลยีอิเล็กทรอนิกส์มาประยุกต์ใช้ในบัตรอิเล็กทรอนิกส์ ตัวอย่างเช่น บัตรคูปองอาหารที่ระบุราคาคูปองตามห้างสรรพสินค้าต่างๆ บัตรกำนัลต่างๆ บัตรประจำตัวประชาชนแบบเก่า บัตรประจำตัวพนักงาน บัตรประจำตัวนักศึกษา บัตรสมาชิกห้างร้านต่างๆ ตั๋วรับชมภาพยนตร์ ตั๋วโดยสารเครื่องบิน ซึ่งอาจกล่าวได้ว่าเป็นบัตรอิเล็กทรอนิกส์ที่มีขึ้นเพื่อใช้ระบุตัวตนผู้ทรงสิทธิในการเข้ารับสิทธิต่างๆ หรือใช้ในการยืนยันตัวตนในฐานะผู้ทรงสิทธิใดๆ นั่นเอง

เนื่องจากลักษณะของบัตรอิเล็กทรอนิกส์ประเภทนี้ทำให้รูปแบบการใช้งานนั้นถูกจำกัด ต่อมาจึงได้มีการนำเอาเทคโนโลยีการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ในรูปแบบการจัดเก็บข้อมูลอิเล็กทรอนิกส์มาใช้ประกอบร่วมด้วย จึงทำให้บัตรอิเล็กทรอนิกส์ประเภทเดิมใช้งานได้หลากหลายขึ้น เช่น ใช้ชำระค่าสินค้าหรือบริการ ใช้เบิกเงินจากตู้จ่ายเงินอัตโนมัติ ใช้เปิดเข้าออกประตูโรงแรม ซึ่งเป็นที่แพร่หลายและพบเห็นได้เป็นปกติในปัจจุบัน

ข้อสังเกตที่ผู้วิจัยได้จากการพิจารณาลักษณะของบัตรอิเล็กทรอนิกส์ประเภทนี้คือ ในเวลายกร่างกฎหมาย ในชั้นรับหลักการแห่งพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547 ซึ่งได้เสนอในวันที่ 20 เมษายน 2546 นั้น แนวความคิดเกี่ยวกับบัตรอิเล็กทรอนิกส์อาจยังคงยึดติดกับบัตรอิเล็กทรอนิกส์ประเภทเดิมนี้ ซึ่งเป็นเพียงกระดาษหรือพลาสติกแข็งธรรมดาที่มุ่งการใช้งานตัวบัตรเป็นสำคัญและการใช้งานข้อมูลอิเล็กทรอนิกส์ที่ติดกับตัวบัตรอาจยังไม่แพร่หลายนัก จึงทำให้เกิดการบัญญัติความหมายของคำว่า “บัตรอิเล็กทรอนิกส์” ในมาตรา

1(14)(ก) ที่ให้หมายถึงตัวเอกสารหรือวัตถุอื่นใดเป็นสำคัญ โดยไม่รวมข้อมูลต่างๆ ที่ได้บันทึกไว้ในแหล่งบันทึกของบัตรให้มีความหมายดังกล่าวด้วย[18] จึงทำให้เกิดปัญหาทางกฎหมายตามมาอันเป็นประเด็นศึกษาในงานวิจัยฉบับนี้

2.1.2.2 บัตรอิเล็กทรอนิกส์ที่มีการจัดเก็บข้อมูลในรูปแบบข้อมูลอิเล็กทรอนิกส์

บัตรอิเล็กทรอนิกส์ประเภทนี้ คือบัตรอิเล็กทรอนิกส์ที่พบได้ทั่วไปและมีใช้แพร่หลายในปัจจุบัน อันเป็นการนำเอาเทคโนโลยีการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ในรูปแบบการจัดเก็บข้อมูลอิเล็กทรอนิกส์มาใช้ประกอบร่วมด้วยกับบัตรอิเล็กทรอนิกส์ประเภทเดิมเพื่อให้มีการใช้งานได้หลากหลายและแม่นยำเที่ยงตรงมากขึ้น อันจำแนกได้ตามแหล่งบันทึกที่ใช้ในการจัดเก็บข้อมูลอิเล็กทรอนิกส์ในบัตรดังกล่าวได้ดังนี้

2.1.2.2.1 บัตรอิเล็กทรอนิกส์ประเภทแถบรหัสแม่เหล็ก

บัตรอิเล็กทรอนิกส์ประเภทแถบรหัสแม่เหล็ก (A Magnetic Stripe Card) เป็นบัตรอิเล็กทรอนิกส์ประเภทหนึ่งซึ่งสามารถเก็บข้อมูลไว้ในแถบแม่เหล็กนั้นได้ ด้วยการดัดแปลงอำนาจแม่เหล็ก (Magnetism) ที่อยู่ในอนุภาคของธาตุเหล็ก (Iron) โดยแถบรหัสแม่เหล็กในบางครั้งจะเรียกว่า สวิฟการ์ด (Swipe Card) หรือ แม็กสตริป (Magstripe) ซึ่งสามารถอ่านค่าได้ด้วยการรูดผ่านอย่างเร็ว (Swiping Past) ผ่านส่วนหัวของแถบแม่เหล็กนั้นๆ ซึ่งบัตรอิเล็กทรอนิกส์ประเภทแถบรหัสแม่เหล็กมักจะนิยมใช้กันในบัตรเครดิต (Credit Card) บัตรระบุตัวตน (Identity Card) หรือบัตรเดินทาง (Transportation Card) ซึ่งอาจมีส่วนประกอบอื่นๆ ด้วย เช่น ป้ายระบุตัวตนแบบใช้คลื่นความถี่วิทยุ (Radio-Frequency Identification Tag ; RFID) หรือ ไมโครชิป (Microchip) ซึ่งบัตรอิเล็กทรอนิกส์ประเภทนี้ มักใช้งานในการผ่านเข้าออกสถานที่ต่างๆ หรือการทำธุรกรรมทางการเงินอิเล็กทรอนิกส์

ตัวอย่างบัตรอิเล็กทรอนิกส์ที่มีส่วนประกอบของแถบรหัสแม่เหล็กที่ใช้กันอย่างแพร่หลายในปัจจุบัน ได้แก่ บัตรประเภทต่างๆ ดังต่อไปนี้

[18] จากการพิจารณา มาตรา 1(14)(ข) ประกอบด้วย

(ก) บัตรเอทีเอ็ม (Automatic Teller Machine Card : ATM)

บัตรเอทีเอ็มเป็นบัตรประเภทแรกที่ธนาคารผลิตออกมาสำหรับใช้ทำธุรกรรมผ่านเครื่องจ่ายเงินอัตโนมัติ เพื่อใช้ฝาก ถอน โอนเงินในบัญชีได้ โดยบัตรเอทีเอ็มมักทำมาจากพลาสติกแข็งและมีขนาดมาตรฐาน คือเป็นรูปสี่เหลี่ยมผืนผ้า ขอบโค้งมน โดยใช้คู่กับแถบแม่เหล็กด้านหลังบัตรหรือชิปในการเก็บข้อมูลของบัตรเอาไว้ เมื่อใส่บัตรลงในตู้เอทีเอ็ม ผู้ใช้จะต้องกดรหัสบัตรให้ตรงกับในบัตรจึงจะสามารถทำธุรกรรมทางการเงินได้ต่อไป ข้อจำกัดของบัตรเอทีเอ็มคือต้องใช้กับเครื่องจ่ายเงินอัตโนมัติเท่านั้น ในปัจจุบันผู้ใช้จึงได้หันมานิยมใช้เป็นบัตรเดบิต ที่สามารถใช้แทนบัตรเอทีเอ็มได้และสามารถใช้รูดผ่านเครื่องรูดบัตรอัตโนมัติ (EDC) เพื่อชำระค่าสินค้าและบริการได้โดยไม่ต้องถอนออกมาเป็นเงินสดก่อน

(ข) บัตรเดบิต (Debit Card)

บัตรเดบิต คือ บัตรที่ผูกไว้กับบัญชีเงินฝากของผู้ถือบัตร เพื่อใช้ทำธุรกรรมที่เครื่องจ่ายเงินอัตโนมัติ เช่น การถอนเงิน โอนเงิน สอบถามยอด ชำระค่าสินค้าและบริการ และสามารถใช้ทำรายการชำระค่าสินค้าและบริการที่ร้านค้าผ่านเครื่องรูดบัตรเครดิต รวมถึงการซื้อสินค้าออนไลน์ได้ โดยจะเป็นการหักเงินออกจากบัญชีเงินฝากทันที ซึ่งเป็นการรวมการใช้งานระหว่างบัตรเครดิตกับบัตรเอทีเอ็มเข้าด้วยกันโดยที่บัตรเดบิตสามารถใช้แทนบัตรเอทีเอ็มได้ทุกประการ แต่บัตรเดบิตจะแตกต่างจากบัตรเครดิตตรงที่ เงินที่ใช้จ่ายผ่านบัตรเดบิตจะผูกกับจำนวนเงินในบัญชีเงินฝากของผู้ใช้บัตร เมื่อชำระค่าสินค้าจะตัดเงินออกจากบัญชีโดยตรง โดยไม่ใช่เงินสินเชื่อที่ธนาคารจัดหาให้อย่างบัตรเครดิต

ในการชำระค่าสินค้าและบริการที่ร้านค้า ร้านค้าที่รับบัตรเดบิตจะติดสัญลักษณ์ของเครือข่ายบัตรเดบิตที่ออกบัตรร่วมกับธนาคารเจ้าของบัตร เช่น เครือข่าย VISA, Master Card, China Union Pay (CUP) ซึ่งผู้ถือบัตรจะชำระโดยการเซ็นชื่อในใบบันทึกการขาย (Sales Slip) หรือกดรหัส (Personal Identification Number: PIN) ทั้งนี้ รูปแบบขึ้นอยู่กับเครือข่ายของผู้ให้บริการบัตรเดบิตเป็นผู้กำหนด ส่วนการซื้อสินค้าออนไลน์ ผู้ถือบัตรจะชำระโดยการระบุหมายเลขบัตรเดบิต 16 หลักและรหัส CVV ซึ่งเป็นหมายเลข 3 หลัก ที่อยู่ด้านหลังบัตร วันหมดอายุของบัตร และรหัสผ่านใช้ครั้งเดียว (One Time Password : OTP) ที่ได้รับทาง SMS ในโทรศัพท์

(ค) บัตรเครดิต (Credit Card)

บัตรเครดิตเป็นบัตรที่สามารถใช้แทนเงินสดได้ เรียกอีกชื่อหนึ่งได้ว่าบัตรสินเชื่อ ซึ่งสามารถใช้รูดผ่านเครื่องรูดบัตรอัตโนมัติ (EDC) เพื่อชำระค่าสินค้าและบริการที่ร้านค้าได้โดยไม่ต้องถอนออกมาเป็นเงินสดก่อน ซึ่งผู้ใช้บริการจะต้องเซ็นลายมือชื่อของตนเองที่เหมือนกับลายมือชื่อที่หลังบัตรลงบนใบเสร็จค่าสินค้าและบริการ (Slip) ที่ร้านค้าพิมพ์ออกมาให้ เพื่อยืนยันความเป็นเจ้าของบัตร โดยธนาคารจะคิดค่าธรรมเนียมการใช้บัตรเป็นเปอร์เซ็นต์ต่อมูลค่าการใช้จ่าย โดยบัตรเครดิตที่นิยมในประเทศไทยนั้นมีหลายประเภท เช่น บัตรวีซ่า (VISA) บัตรมาสเตอร์ (Master) บัตรอเมริกันเอ็กเพรส (American Express) บัตรเจซีบี (JCB) ซึ่งบริษัทเหล่านี้เป็นผู้ให้สิทธิธนาคารพาณิชย์ในการออกบัตร

ในการทำบัตรเครดิต ธนาคารจะขอข้อมูลส่วนตัวและหลักฐานทางการเงินในการพิจารณาอนุมัติสินเชื่อ เพื่อมั่นใจว่าลูกค้ามีความสามารถในการชำระหนี้ได้และจะทำการกำหนดวงเงินสินเชื่อให้ผู้ถือบัตรเพื่อใช้ในการชำระค่าสินค้าและบริการได้เท่าวงเงินสินเชื่อที่ธนาคารอนุมัติให้ หลังจากมีการใช้งานบัตรแล้วธนาคารจะเรียกเก็บเงินเป็นรายเดือนแก่ผู้ถือบัตร ซึ่งหากชำระล่าช้ากว่ากำหนดผู้ถือบัตรจะต้องชำระดอกเบี้ยตามอัตราที่กำหนดไว้

นอกจากนี้บัตรเครดิตยังใช้ชำระค่าสินค้าและบริการผ่านระบบร้านค้าออนไลน์ได้ด้วยโดยผู้ถือบัตรไม่จำเป็นต้องไปรูดบัตรจริง เพียงแต่ระบุหมายเลขบัตรเดบิต 16 หลัก และรหัส CVV ซึ่งเป็นหมายเลข 3 หลัก ที่อยู่ด้านหลังบัตร วันหมดอายุของบัตร และรหัสผ่านใช้ครั้งเดียว (One Time Password : OTP) ที่ได้รับทาง SMS ในโทรศัพท์ให้ตรงกันและภายในระยะเวลาที่กำหนดไว้

(ง) บัตรเงินสด (Cash Card)

บัตรเงินสดเป็นบัตรที่มีการใช้งานเหมือนกับบัตรเครดิตและไม่ใช่การถอนเงินออกจากในบัญชีของผู้ใช้บัตรอย่างเช่นบัตรเอทีเอ็ม แต่เป็นการให้เงินสินเชื่อในวงเงินจำกัดที่ธนาคารได้รับค่าตอบแทนเป็นดอกเบี้ย บัตรเงินสดจึงมีลักษณะเหมือนบัตรเครดิตมาก แต่การใช้งานนั้นจะต้องใช้ถอนเงินผ่านเครื่องจ่ายเงินอัตโนมัติเท่านั้น ไม่สามารถใช้ชำระค่าสินค้าหรือบริการผ่านเครื่องรูดบัตรอัตโนมัติ (EDC) ได้อย่างบัตรเครดิตหรือบัตรเดบิต

2.1.2.2.2 บัตรอิเล็กทรอนิกส์ประเภทฝังชิปอีเอ็มวี (EMV Chip)

ชิปอีเอ็มวี (EMV Chip) เป็นเทคโนโลยีที่ฝังชิปเข้ากับบัตรเครดิตและเริ่มกลายมาเป็นมาตรฐานสากลในการรับจ่ายเงินด้วยบัตรเครดิต บัตรเดบิต หรือบัตรเติมเงินมากขึ้น โดยระบบชิปอีเอ็มวีจะทดแทนระบบแถบแม่เหล็กของบัตรรุ่นเก่าและเพื่อเพิ่มความปลอดภัยให้สูงขึ้นจากการขโมยข้อมูลจากเครื่องดูดข้อมูลแถบรหัสแม่เหล็ก โดยชิปอีเอ็มวีนี้จะสามารถเก็บข้อมูลส่วนตัวของลูกค้าไว้ในคอมพิวเตอร์ชิป (Computer Chip) ที่ฝังติดกับบัตรซึ่งทำให้ยากแก่การปลอมแปลงเป็นอย่างมากและง่ายต่อการตรวจสอบว่าบัตรเป็นของจริงหรือไม่เมื่อเทียบกับบัตรแบบใช้แถบแม่เหล็กที่ใช้กันอยู่ในปัจจุบัน ซึ่งอาจเรียกได้ในชื่ออื่นๆ เช่น บัตรชิปกับพิน (Chip and PIN Card) หรือบัตรชิปกับลายมือชื่อ (Chip and Signature Card)

บรรดาบัตรเอทีเอ็ม บัตรเดบิต บัตรเครดิต และบัตรเงินสด ของธนาคารพาณิชย์ในประเทศไทยในปัจจุบันทุกประเภทได้มีการติดตั้งชิปอีเอ็มวีนี้ไว้หมดแล้วตามการผลักดันของธนาคารแห่งประเทศไทย สมาคมธนาคารไทยและสถาบันการเงินต่างๆ ที่ทยอยให้ประชาชนปรับเปลี่ยนบัตรอิเล็กทรอนิกส์จากรูปแบบบัตรแถบรหัสแม่เหล็ก (Magnetic Stripe Card) ให้เป็นรูปแบบชิปการ์ด (Chip Card) ซึ่งมีกำหนดภายในวันที่ 15 มกราคม 2563 เพื่อยกระดับความปลอดภัยในการใช้บัตรอิเล็กทรอนิกส์ เช่น การป้องกันการปลอมแปลงบัตร (Counterfeit Card Fraud) และการโจรกรรมข้อมูล (Skimming) อันนำไปสู่การทำบัตรปลอมและใช้บัตรปลอมนั้นทำธุรกรรมทางการเงินผ่านเครื่องจ่ายเงินอัตโนมัติ[19]

จากรายงานฉบับที่ 4 เรื่องการฉ้อโกงบัตร ของธนาคารกลางแห่งสหภาพยุโรป (European Central Bank) ในเดือนกรกฎาคม ค.ศ. 2015[20] พบว่าการนำเทคโนโลยีชิปอีเอ็มวีมาใช้กับบัตรอิเล็กทรอนิกส์แทนการใช้แถบแม่เหล็กนั้น ช่วยลดการฉ้อโกงบัตรได้อย่างมากภายในระบบการทำธุรกรรมทางการเงินของกลุ่มประเทศยุโรป (Single Euro Payments Area : SEPA) แต่หากเป็นทำธุรกรรมทางการเงินนอกระบบของกลุ่มประเทศยุโรป ซึ่งยังต้องอาศัยระบบแถบแม่เหล็กติดตั้งควบคู่กับบัตรอิเล็กทรอนิกส์ไปด้วยจึงทำให้ยังคงมีการกระทำการฉ้อโกงบัตรโดยวิธีการปลอมแปลงได้อยู่โดยอาศัยเครื่องดูดข้อมูลแถบรหัสแม่เหล็ก

---

[19] ธนาคารแห่งประเทศไทย, "ข่าวธนาคารแห่งประเทศไทย ฉบับที่49/2562" [ออนไลน์], เข้าถึงเมื่อ 22 กรกฎาคม 2563. แหล่งที่มา: https://www.bot.or.th/Thai/PressandSpeeches/Press/News2562/n4962t.pdf.

[20] European Central Bank, "Fourth Report on Card Fraud" [Online], Accessed: 20 February 2018. Available from: https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf.

ตารางที่ 2 แสดงจำนวนบัตรอิเล็กทรอนิกส์ที่ใช้ในประเทศไทย พ.ศ. 2558 ถึง พ.ศ. 2562[21]

(หน่วย : ใบ)

ประเภทของบัตร	2562	2561	2560	2559	2558
บัตรเครดิต	23,998,653	22,105,472	20,334,780	20,136,341	18,974,195
บัตรเอทีเอ็ม	15,318,234	7,080,324	8,758,043	10,791,481	13,397,755
บัตรเดบิต	64,773,018	57,407,185	54,329,727	50,199,427	46,989,719
รวมทั้งสิ้น	104,089,905	86,592,981	83,422,550	81,127,249	79,361,669

2.2 ลักษณะการกระทำความผิดที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์

บัตรอิเล็กทรอนิกส์นับเป็นสิ่งที่สำคัญในการใช้งานในชีวิตประจำวันของบุคคล กล่าวคือ นอกจากจะเป็นสิ่งที่ใช้แทนการแสดงตัวตนของเจ้าของบัตรอิเล็กทรอนิกส์แล้ว ด้วยพัฒนาการทางเทคโนโลยีที่ผ่านมาทำให้บัตรอิเล็กทรอนิกส์ยังสามารถใช้งานในการทำธุรกรรมทางการเงินที่มีความหลากหลาย สะดวกและรวดเร็ว อันเป็นคุณประโยชน์ที่สำคัญที่สุดที่ทำให้เกิดความนิยมในการใช้งานบัตรอิเล็กทรอนิกส์โดยแพร่หลายจนถึงปัจจุบัน จนอาจกล่าวได้ว่าบัตรอิเล็กทรอนิกส์เป็นกระเป๋าเงินใบที่สองอันเป็นเงินที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์นอกจากกระเป๋าเงินสดของบุคคลทุกคนก็ว่าได้ ด้วยประโยชน์ที่มีอันมหาศาลของบัตรอิเล็กทรอนิกส์นี้เองจึงเป็นสิ่งล่อให้เกิดการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์อย่างต่อเนื่องดังแสดงจากตารางสถิติดังต่อไปนี้

[21] ธนาคารแห่งประเทศไทย, "จำนวนบัตรพลาสติก" [ออนไลน์], เข้าถึงเมื่อ 22 กรกฎาคม 2563. แหล่งที่มา: https://www.bot.or.th/App/BTWS_STAT/statistics/ReportPage.aspx?reportID=685&language=th.

ตารางที่ 3 แสดงสถิติการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ (ตามประมวลกฎหมายอาญา มาตรา 269/1 – 269/7) ทั่วทั้งประเทศ ของศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ[22]

(หน่วย : ราย)

รายการ	ปี 2562	ปี 2561	ปี 2560	ปี 2559	ปี 2558
รับแจ้ง	220	290	152	116	175
จับกุม	154	193	101	68	113
คิดเป็นร้อยละ	70	66.55	66.44	58.62	64.57

การกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตั้งแต่ในอดีตจนถึงปัจจุบันนั้นมีหลายลักษณะด้วยกันอันเกิดจาการพัฒนาทางเทคโนโลยีที่ทำให้อาชญากรคิดค้นวิธีการใหม่ๆ ในการกระทำความผิดขึ้นเพื่อหวังผลประโยชน์จากบัตรอิเล็กทรอนิกส์เหล่านั้น โดยรูปแบบการกระทำความผิดที่เกิดขึ้นก่อนวันที่ 23 ตุลาคม พ.ศ. 2547 อันเป็นวันที่ได้มีพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547 ใช้บังคับนั้น การกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์จะแบ่งได้เป็น 4 ลักษณะใหญ่ๆ คือ

2.2.1 การลักบัตรอิเล็กทรอนิกส์

การลักบัตรอิเล็กทรอนิกส์ เป็นการกระทำต่อตัวบัตรที่เป็นเอกสารหรือพลาสติก อันเป็นความผิดฐานลักทรัพย์ ตามประมวลกฎหมายอาญา มาตรา 334 การลักบัตรอิเล็กทรอนิกส์นั้นนับเป็นวิธีการที่ง่ายที่สุดในการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ เพราะผู้กระทำไม่จำต้องใช้เครื่องมือหรืออุปกรณ์ใดๆ เลยประกอบการกระทำความผิดดังกล่าว การลักบัตรอิเล็กทรอนิกส์ปรากฏตามคำพิพากษาศาลฎีกา ตัวอย่างเช่น

คำพิพากษาศาลฎีกาที่ 9/2543 “การที่จำเลยลักเอาบัตรเอ.ที.เอ็ม.ไปจากผู้เสียหายแล้วนำบัตรเอ.ที.เอ็มดังกล่าวไปลักเอาเงินของผู้เสียหาย โดยผ่านเครื่องฝากถอนเงินนั้น ทรัพย์ที่จำเลยลัก

[22] ศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ, "สถิติฐานความผิดคดีอาญา" [ออนไลน์], เข้าถึงเมื่อ 2 สิงหาคม 2563. แหล่งที่มา: http://pitc.police.go.th/dirlist/dirlist.php?dir=/crimes.

เป็นทรัพย์คนละประเภทและเป็นความผิดสำเร็จในตัวต่างกรรมต่างวาระ การลักเอาบัตรเอ.ที.เอ็ม. ไปกับการลักเงินจึงเป็นความผิดหลายกรรม

การที่จำเลยลักเอาบัตรเอ.ที.เอ็ม. ของผู้เสียหายไปนั้นเป็นความผิดทั้งฐานเอาไปเสียซึ่งเอกสารของผู้อื่นตามประมวลกฎหมายอาญา มาตรา 188 ซึ่งเป็นบทที่มีโทษหนักกว่าความผิดฐานลักทรัพย์ตามมาตรา 334 ต้องลงโทษจำเลยตามมาตรา 188

บัตรเอ.ที.เอ็ม. ของผู้เสียหาย 2 ใบ เป็นบัตรต่างธนาคารกัน และเงินฝากของผู้เสียหายที่ถูกลักไปก็เป็นเงินฝากในบัญชีต่างธนาคารกันด้วย เจตนาในการกระทำผิดของจำเลยจึงแยกจากกันได้ตามความมุ่งหมายในการใช้บัตรแต่ละใบการกระทำของจำเลยที่ใช้บัตรเอ.ที.เอ็ม. 2 ใบ ของผู้เสียหายแล้วลักเอาเงินฝากของผู้เสียหายต่างบัญชีกันแม้จะทำต่อเนื่องกันก็เป็นความผิดสองกรรม”

คำพิพากษาดังกล่าวเป็นเรื่องลักบัตรเอ.ที.เอ็ม. (ATM Card) ซึ่งเป็นบัตรอิเล็กทรอนิกส์ประเภทหนึ่งไปเสียจากผู้เสียหายแล้วนำบัตรนั้นไปกดถอนเงินจากเครื่องจ่ายเงินอัตโนมัติ (Automatic teller machine: ATM) ซึ่งจากคำพิพากษาดังกล่าว สรุปได้ดังนี้คือ

(ก) การลักบัตรอิเล็กทรอนิกส์ เป็นความผิดฐานลักทรัพย์ ตามประมวลกฎหมายอาญา มาตรา 334 และยังเป็นความผิดฐานเอาไปเสียซึ่งเอกสารของผู้อื่นตาม มาตรา 188 อีกด้วยตามคำพิพากษาฉบับนี้และคำพิพากษาศาลฎีกาที่ 6820/2552

(ข) การลักบัตรอิเล็กทรอนิกส์แล้วนำบัตรอิเล็กทรอนิกส์ที่ลักไปใช้ เป็นความผิดคนละกรรม

(ค) การใช้บัตรอิเล็กทรอนิกส์ต่างใบ หรือต่างธนาคารกัน ย่อมเป็นความผิดคนละกรรม

นอกจากคำพิพากษาดังกล่าวแล้วยังมีคำพิพากษากรณีลักบัตรอิเล็กทรอนิกส์อื่นๆ อีก เช่น คำพิพากษาศาลฎีกาที่ 2512/2550 และคำพิพากษาศาลฎีกาที่ 464/2551 ซึ่งนอกจากจำเลยจะกระทำความผิดในส่วนอาญาแล้ว พนักงานอัยการก็อาศัยอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 43 มีคำขอให้เรียกทรัพย์สินหรือใช้ราคาทรัพย์แทนผู้เสียหายจากการที่จำเลยได้ใช้บัตรอิเล็กทรอนิกส์ไปตามจำนวนวงเงินที่เบิกถอนไปจริงด้วย ดังในคำพิพากษาศาลฎีกาที่ 52/2553

คำพิพากษาศาลฎีกาที่ 52/2553 “โจทก์ฟ้องขอให้ลงโทษจำเลยฐานนำบัตรอิเล็กทรอนิกส์ไปใช้เบิกถอนเงินสดจำนวน 100,000 บาท ของผู้เสียหายที่ 2 ไป อันเป็นความผิดตาม ป.อ. มาตรา 269/5 และมาตรา 269/7 เมื่อตามคำฟ้องโจทก์ได้กล่าวบรรยายว่า จำเลยได้ใช้บัตรอิเล็กทรอนิกส์ของธนาคาร ซ. ซึ่งได้ออกให้แก่ผู้เสียหายที่ 2 อันเป็นทรัพย์ส่วนหนึ่งที่จำเลยได้ลักไปเพื่อใช้ประโยชน์ในการเบิกถอนเงินสด ถอนเงินสดจำนวน 100,000 บาท ไปจากวงเงินเครดิตของผู้เสียหายที่ 2 โดยมิชอบ ก่อให้เกิดความเสียหายแก่ผู้เสียหายและธนาคาร ซ. และยังมีคำขอท้ายฟ้องขอให้บังคับจำเลย

คืนเงินจำนวนดังกล่าวด้วย ดังนั้น ย่อมแปลคำฟ้องของโจทก์ได้ว่า โจทก์มุ่งประสงค์ที่จะให้ลงโทษจำเลยฐานลักเงินของผู้เสียหายที่ 2 อยู่ด้วย เพียงแต่วิธีการลักเงินดังกล่าวก็โดยการใช้บัตรอิเล็กทรอนิกส์เบิกถอนเงินสดผ่านเครื่องฝาก-ถอนเงินอัตโนมัตินั่นเอง จึงเป็นความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์และความผิดฐานลักทรัพย์ด้วยแล้ว ซึ่งตาม ป.วิ.อ. มาตรา 43 บัญญัติให้พนักงานอัยการมีอำนาจขอให้เรียกทรัพย์สินหรือใช้ราคาแทนผู้เสียหายที่ 2 โจทก์จึงมีอำนาจขอให้จำเลยคืนหรือใช้ราคาทรัพย์แทนผู้เสียหายที่ 2 ได้”

2.2.2 การปลอมเอกสารที่เป็นบัตรอิเล็กทรอนิกส์

ก่อนที่ได้มีการพัฒนาของเทคโนโลยีให้สามารถทำการปลอมบัตรอิเล็กทรอนิกส์ได้ทั้งตัวบัตรอิเล็กทรอนิกส์และข้อมูลที่บรรจุไว้ในบัตรอิเล็กทรอนิกส์นั้น เดิมการปลอมบัตรอิเล็กทรอนิกส์ส่วนใหญ่จะเป็นการปลอมบัตรอิเล็กทรอนิกส์ที่ใช้ยืนยันตัวบุคคลผู้เป็นเจ้าของบัตรใบนั้น โดยการปลอมพื้นผิวของบัตรให้เสมือนบัตรที่แท้จริง ซึ่งผู้กระทำต้องอาศัยอุปกรณ์เบื้องต้นซึ่งไม่จำต้องมีการทำงานที่ซับซ้อน เช่น กล้องถ่ายรูป เครื่องพิมพ์ภาพและเครื่องคอมพิวเตอร์ ในการกระทำความผิดร่วมด้วย ซึ่งอาจมีวิธีที่แตกต่างกันได้หลายแบบ เช่น การถ่ายรูปบัตรที่แท้จริงแล้วพิมพ์ออกมาติดทับไว้กับบัตรอิเล็กทรอนิกส์อีกใบหนึ่งหรือติดกับบัตรพลาสติกขาว การกระทำดังกล่าวนับว่าเป็นการปลอมเอกสารตามประมวลกฎหมายอาญา มาตรา 264 ดังตัวอย่างปรากฏตามคำพิพากษาศาลฎีกา เช่น

คำพิพากษาศาลฎีกาที่ 4766/2538 “จำเลยนำภาพถ่ายของ ม. มาตัดให้พอดีกับภาพถ่ายในบัตรประจำตัวประชาชนของ น. ที่แท้จริงแล้วนำภาพถ่ายที่ตัดแล้วปิดทับภาพถ่ายของ น. ที่ติดอยู่ในบัตรประจำตัวประชาชนของ น. ดังกล่าวแล้วถ่ายภาพบัตรและนำภาพถ่ายดังกล่าวอัดพลาสติกมอบให้ ม. โดยคิดค่าทำ 15 บาทถือได้ว่าจำเลยกระทำโดยมีเจตนาเพื่อให้ผู้พบเห็นบัตรประจำตัวประชาชนดังกล่าวหลงเชื่อว่าภาพถ่ายของ ม. ในบัตรประจำตัวประชาชนที่ถ่ายมาเป็นภาพถ่ายของ น. โดยมีวันเดือนปีเกิดและภูมิลำเนาตามที่ระบุไว้ในบัตรดังกล่าวเป็นบัตรประจำตัวประชาชนที่แท้จริงจึงเป็นความผิดฐานปลอมเอกสาร บัตรประจำตัวประชาชนเป็นเอกสารซึ่งเจ้าพนักงานสำนักทะเบียนบัตรประชาชนกระทรวงมหาดไทยได้ทำขึ้นจึงเป็นเอกสารราชการตามนิยามของประมวลกฎหมายอาญามาตรา 1(8) แม้บัตรประชาชนที่จำเลยทำปลอมขึ้นนั้นจะเป็นเพียงภาพถ่ายเอกสารแต่การกระทำของจำเลยมีลักษณะเพื่อการใช้อย่างบัตรประจำตัวประชาชนฉบับที่แท้จริงจึงมีความผิดฐานปลอมเอกสารราชการ”

จากคำพิพากษาศาลฎีกาดังกล่าว การปลอมบัตรประจำตัวประชาชนซึ่งเป็นบัตรอิเล็กทรอนิกส์ประเภทหนึ่ง นอกจากจะเป็นความผิดฐานปลอมเอกสาร ตามประมวลกฎหมายอาญา มาตรา 264 แล้ว ยังเป็นการปลอมเอกสารราชการด้วย ตามมาตรา 265

คำพิพากษาศาลฎีกาที่ 5598/2540 “จำเลยได้ปลอมบัตรเครดิตธนาคารกรุงไทย จำกัด (มหาชน) ใช้บัตรเครดิตดังกล่าวรูดกับเครื่องรูดบัตรเครดิตซึ่งธนาคารให้ไว้แก่จำเลยและปลอมเซลล์สลิปของบุคคลหลายคนแสดงว่าผู้เป็นเจ้าของบัตรเครดิตได้ซื้อหรือใช้บริการด้วยบัตรเครดิตดังกล่าว... จำเลยมีความผิดตามประมวลกฎหมายอาญามาตรา 265, 268 วรรคแรก ประกอบมาตรา 265 แต่การใช้เอกสารสิทธิปลอมเกิดจากการทำปลอมเอกสารสิทธิด้วยให้ลงโทษฐานใช้เอกสารสิทธิปลอม”

คำพิพากษาดังกล่าวเป็นเรื่องปลอมบัตรเครดิต แล้วนำไปรูดกับเครื่องรูดบัตรเครดิตซึ่งธนาคารให้ไว้แก่จำเลย แล้วทำการปลอมเซลล์สลิปขึ้นเพื่อแสดงว่าผู้เป็นเจ้าของบัตรเครดิตได้ซื้อหรือใช้บริการด้วยบัตรเครดิตที่ปลอมขึ้นนั้น ซึ่งจากคำพิพากษาดังกล่าว สรุปได้ดังนี้คือ

(ก) การปลอมบัตรอิเล็กทรอนิกส์ เป็นความผิดฐานปลอมเอกสาร ตามประมวลกฎหมายอาญา มาตรา 264 และการปลอมบัตรเครดิตนับว่าเป็นการปลอมเอกสารสิทธิด้วย ตามมาตรา 265 ทั้งคำพิพากษาศาลฎีกาที่ 15397/2557 ก็ตัดสินในลักษณะเดียวกัน โดยให้การปลอมบัตรเอทีเอ็มเป็นการปลอมเอกสารสิทธิด้วย

(ข) แต่เมื่อนำเอกสารนั้นออกใช้จึงลงโทษฐานใช้เอกสารปลอมเพียงมาตราเดียว ตามมาตรา 268

นอกจากคำพิพากษาดังกล่าวแล้วยังมีคำพิพากษากรณีปลอมเอกสารที่เป็นบัตรอิเล็กทรอนิกส์อื่นๆ อีก เช่น คำพิพากษาศาลฎีกาที่ 7904/2543 และ คำพิพากษาศาลฎีกาที่ 5345/2550

การปลอมเอกสารในอีกกรณี คือการนำสำเนาข้อมูลในแถบแม่เหล็กของบัตรอิเล็กทรอนิกส์ที่แท้จริง มาใส่ลงในแถบแม่เหล็กของนำบัตรพลาสติกขาว (White Card) ซึ่งเป็นบัตรที่ไม่ปรากฏตัวเลขหรือตัวอักษรใดๆ บนบัตรนั้นเลย อันทำให้ไม่มีผู้ใดหลงเชื่อว่าเป็นบัตรที่แท้จริง แต่ผู้กระทำก็ยังมีความผิดฐานปลอมเอกสารสิทธิ ตามมาตรา 265 ตามความเห็นของ นายดิเรก สุนทรเกตุ อดีตอัยการสูงสุด ตามคำสั่งชี้ขาดความเห็นแย้งที่ 38/2542 ความว่า “ผู้ต้องหาซื้อข้อมูลในแถบแม่เหล็กที่มีผู้ลักลอบบันทึกจากแถบแม่เหล็กของบัตรเครดิตที่แท้จริง แล้วนำมาบันทึกข้อมูลบนแถบแม่เหล็กบนบัตรไวด์การ์ด ซึ่งเป็นบัตรที่ยังไม่มีการพิมพ์ด้านหน้าบัตรให้เหมือนบัตรเครดิตของจริงเพื่อหาร้านค้าที่

ให้ความร่วมมือในการให้ใช้เครื่องรูดบัตรและตกลงแบ่งผลประโยชน์กัน ด้วยจุดประสงค์เพื่อที่จะให้สถาบันผู้ออกบัตรเครดิตหลงเชื่อว่าข้อมูลที่ทำปลอมบนแถบแม่เหล็กเป็นเอกสารที่แท้จริง ถือได้ว่าการกระทำดังกล่าวเข้าลักษณะการปลอมเอกสารสิทธิแล้ว”[23]

2.2.3 การยักยอกบัตรอิเล็กทรอนิกส์

การยักยอกบัตรอิเล็กทรอนิกส์ เป็นความผิดตามประมวลกฎหมายอาญา มาตรา 352 ซึ่งเป็นกรณีที่ผู้มีสิทธิใช้บัตรอิเล็กทรอนิกส์ปล่อยให้บัตรนั้นอยู่ในความครอบครองของบุคคลใด แล้วบุคคลนั้นนำบัตรอิเล็กทรอนิกส์นั้นไปใช้เสียไม่ตรงตามความยินยอมของผู้มีสิทธิใช้บัตรดังกล่าว ซึ่งกว่าผู้มีสิทธิใช้บัตรจะทราบเรื่องถึงการยักยอกวงเงินในบัตร ก็ต่อเมื่อมีการแจ้งหนี้จากธนาคารเจ้าของบัตรนั้นแล้ว ซึ่งโดยปกติแล้วมักเกิดกรณีดังกล่าวขึ้นกับการชำระค่าสินค้าหรือบริการ ณ จุดชำระเงิน (Point of Sale) ที่พนักงานของร้านค้าหรือโรงแรมจะนำบัตรอิเล็กทรอนิกส์ไปทำธุรกรรมกับเครื่องรูดบัตร (EDC) ซึ่งพนักงานนั้นจะต้องคืนบัตรอิเล็กทรอนิกส์ดังกล่าวให้โดยไม่สามารถแสวงหาประโยชน์ใดๆ เพิ่มเติมแก่บัตรอิเล็กทรอนิกส์ใบนั้น เทียบได้กับเรื่องฝากทรัพย์ ตามคำพิพากษาศาลฎีกาที่ 2711/2529 ที่ว่า “ผู้รับฝากมีหน้าที่จะต้องคืนทรัพย์ที่รับฝากแก่ผู้ฝากผู้รับฝากจะนำทรัพย์ออกใช้สอยหรือมอบให้ผู้อื่นโดยไม่ได้รับความยินยอมจากผู้ฝากหาได้ไม่... หากผู้รับฝากยักยอกเอาไปโดยทุจริตไม่ส่งคืนทรัพย์ที่รับฝากไว้ให้แก่ผู้ฝากได้... ผู้รับฝากจึงมีความผิดฐานยักยอก ตามประมวลกฎหมายอาญา มาตรา 352” ซึ่งหากพนักงานนำบัตรอิเล็กทรอนิกส์ไปกดจ่ายเงินมากกว่าค่าสินค้าหรือบริการ หรือนำเครื่องดูดข้อมูลบัตรอิเล็กทรอนิกส์ (Skimmer) มาใช้เพื่อดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ไป ก็อาจจะถือว่าการกระทำดังกล่าวเป็นการเบียดบังเอาทรัพย์นั้นเป็นของตนหรือบุคคลที่สามโดยทุจริตอันเป็นความผิดฐานยักยอกทรัพย์ได้

นอกจากการณีการยักยอกบัตรอิเล็กทรอนิกส์ ณ จุดชำระเงินแล้ว ยังพบการกระทำความผิดในการยักยอกบัตรอิเล็กทรอนิกส์ในรูปแบบอื่นๆ อีกด้วย ตัวอย่างเช่น พนักงานห้างสรรพสินค้าเก็บกระเป๋าลูกค้าที่มาใช้บริการได้ แล้วนำบัตรเครดิตที่อยู่ในกระเป๋าของลูกค้าไปใช้ซื้อสินค้าภายในห้าง[24]

---

[23] สำนักงานอัยการพิเศษฝ่ายสารสนเทศ, อัยการนิเทศ, 6 (2544).

[24] โพสต์ทูเดย์, "จับพนักงานห้างรูดบัตรเครดิตสาวมะกันเกลี้ยง" [ออนไลน์], เข้าถึงเมื่อ 2 สิงหาคม 2563. แหล่งที่มา: https://www.posttoday.com/social/general/47753.

พนักงานแผนกธุรการของบริษัทแอบนำบัตรกดเงินสดที่ธนาคารเพิ่งส่งใส่ซองจดหมายให้แก่หัวหน้าตนเองไปกดเงินสดแล้วนำไปใช้[25]

2.2.4 การฉ้อโกงบัตรอิเล็กทรอนิกส์

การฉ้อโกงบัตรอิเล็กทรอนิกส์ อาจเกิดขึ้นจากการกระทำความผิดในรูปแบบต่างๆ ข้างต้น[26] จนได้บัตรอิเล็กทรอนิกส์ที่แท้จริงหรือบัตรปลอมมาแล้ว ต่อมาผู้กระทำซึ่งเป็นผู้ไม่มีสิทธิจะใช้บัตรอิเล็กทรอนิกส์ดังกล่าวได้นำบัตรอิเล็กทรอนิกส์นั้นออกใช้ อันเป็นการทุจริต หลอกลวงโดยแสดงข้อความอันเป็นเท็จต่อธนาคารเจ้าของบัตรหรือผู้ออกบัตรให้ ว่าตนเองเป็นผู้มีสิทธิใช้ จึงมีความผิดฐานการฉ้อโกงตามประมวลกฎหมายอาญา มาตรา 341 ซึ่งการแสดงตนเป็นบุคคลผู้มีสิทธิใช้นี้ เป็นการกระทำความผิดฐานฉ้อโกงโดยแสดงตนเป็นคนอื่น ตามมาตรา 342(1) ด้วย ซึ่งข้อหาฉ้อโกงนี้ธนาคารผู้เป็นเจ้าของบัตรเท่านั้นที่เป็นผู้เสียหาย ตามนัยของคำพิพากษาศาลฎีกาที่ 4018/2542

คำพิพากษาศาลฎีกาที่ 4018/2542 “จำเลยที่ 1 นำใบบันทึกรายการขายปลอมไปใช้เบิกเงินจากธนาคารผู้เสียหายจึงเป็นความผิดฐานใช้เอกสารสิทธิปลอมและฉ้อโกงตามประมวลกฎหมายอาญามาตรา 268 วรรคแรก ประกอบมาตรา 265, 341 การที่จำเลยที่ 1 นำใบบันทึกรายการขายปลอมไปใช้เบิกเงินจากธนาคารจนได้รับเงินจากธนาคารแล้ว ธนาคารจึงเป็นผู้เสียหายไม่ใช่ผู้ถือบัตรเครดิตที่ถูกปลอมลายมือชื่อเป็นผู้เสียหาย”

คำพิพากษาศาลฎีกาที่ 2766/2546 “จำเลยทั้งสองได้นำบัตรเครดิตของธนาคาร ย. ซึ่งออกให้แก่ ด. ไปซื้อสินค้าที่ร้าน ซ. โดยร่วมกันหลอกลวงพนักงานขายว่าจำเลยที่ 1 ชื่อ ด. จำเลยทั้งสองได้ชำระราคาสินค้าด้วยบัตรเครดิตดังกล่าว โดยจำเลยที่ 1 ปลอมลายมือชื่อของ ด. ลงในเอกสารสิทธิบันทึกการขายในช่องลายมือชื่อผู้ถือบัตรแล้วจำเลยทั้งสองร่วมกันส่งมอบบันทึกการขายดังกล่าวแก่พนักงานขายของร้าน ซ. ทรัพย์ที่ได้จากการกระทำความผิด เป็นสินค้าที่จำเลยทั้งสองซื้อจากร้าน ซ. คือ โทรทัศน์สีและเครื่องเล่นวีดีโอเทปฉะนั้น การกระทำของจำเลยทั้งสองจึงเป็นความผิด” คดีนี้ศาลฎีกาพิพากษายืนตามศาลชั้นต้นที่ให้ลงโทษจำเลยฐานฉ้อโกง เป็นกระทงหนึ่งในนอกเหนือจากความผิดอื่นๆ ด้วย

---

[25] ข่าวเด็ดเจ็ดสี, "ตร.รวบสามีภรรยา คดีบัตรเครดิต ยักยอกทรัพย์" [ออนไลน์], เข้าถึงเมื่อ 2 สิงหาคม 2563. แหล่งที่มา: https://news.ch7.com/detail/366214.

[26] โปรดดูหัวข้อที่ 2.2.1 ถึงหัวข้อที่ 2.2.3 คือ การลักบัตร การปลอมเอกสารที่เป็นบัตร และการยักยอกบัตรอิเล็กทรอนิกส์

นอกจากคำพิพากษาดังกล่าวแล้วยังมีคำพิพากษากรณีฉ้อโกงบัตรอิเล็กทรอนิกส์อื่นๆ อีก เช่น คำพิพากษาศาลฎีกาที่ 7001/2544 คำพิพากษาศาลฎีกาที่ 12582/2547 คำพิพากษาศาลฎีกาที่ 821/2552 และ คำพิพากษาศาลฎีกาที่ 9276/2553

เนื่องด้วยเทคโนโลยีที่พัฒนาขึ้นจึงส่งผลให้อาชญากรพยายามแสวงหาและนำเทคโนโลยีต่างๆ มาประยุกต์ใช้กับการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์มากยิ่งขึ้น จากการกระทำความผิดในรูปแบบเดิมดังที่กล่าวมาที่ผู้กระทำไม่จำต้องใช้อุปกรณ์ใดๆ เลยในการกระทำความผิด หรือใช้เพียงอุปกรณ์พื้นฐานที่สามารถหาได้รอบตัว โดยไม่ต้องทำการดัดแปลงอุปกรณ์ให้มีความเฉพาะ เช่น ใช้กล้องถ่ายภาพ เครื่องพิมพ์เอกสาร หรือเครื่องคอมพิวเตอร์ กลายมาเป็นการดัดแปลงอุปกรณ์ต่างๆ ขึ้นเฉพาะเพื่อใช้ในการกระทำความผิดในรูปแบบดังกล่าว เช่น การใช้เครื่องดึงข้อมูลบัตรอิเล็กทรอนิกส์ (Skimmer) การเขียนโปรแกรมที่เป็นไวรัส (Virus) หรือมัลแวร์ (Malware) เข้าไปในระบบคอมพิวเตอร์ เพื่อให้ตนเองได้ประโยชน์จากการกระทำความผิดมากยิ่งขึ้น เช่น ได้การปลอมบัตรอิเล็กทรอนิกส์ที่มีความเหมือนกับบัตรที่แท้จริงมากยิ่งขึ้น หรือได้ข้อมูลจากบัตรอิเล็กทรอนิกส์ที่แท้จริงเพื่อนำไปแสวงหาประโยชน์ต่างๆ ต่อไป เช่น นำไปทำบัตรปลอม นำไปจำหน่ายหรือโอน ให้แก่ผู้อื่น เนื่องด้วยการกระทำความผิดของบัตรอิเล็กทรอนิกส์ที่ซับซ้อนขึ้นเช่นนี้จึงทำให้ประมวลกฎหมายอาญาที่มีอยู่เดิมสามารถบังคับใช้ได้แต่เฉพาะกรณีในหัวข้อที่ 2.2.1 ถึงหัวข้อที่ 2.2.4 ข้างต้นเท่านั้น ไม่ครอบคลุมการกระทำความผิดที่เกิดขึ้นทั้งหมด[27] และเนื่องจากเป็นการกระทำความผิดที่เกิดขึ้นอย่างมากในปัจจุบัน เกิดผลร้ายแรงและสร้างความเสียหายในระดับสูง ประกอบกับเป็นการกระทำความผิดในระดับ “องค์กรอาชญากรรม” จึงสมควรให้มีบทบัญญัติเฉพาะในเรื่องการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ จึงได้นำมาสู่การแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547 โดยการเพิ่มคำนิยามของคำว่า “บัตรอิเล็กทรอนิกส์” ใน มาตรา 1(14) และเพิ่ม “ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์” ตั้งแต่มาตรา 269/1 ถึง 269/7 ไว้ในหมวด 4 ลักษณะ 7 ความผิดเกี่ยวกับการปลอมและการแปลง แห่งประมวลกฎหมายอาญา ซึ่งมีผลบังคับใช้เมื่อวันที่ 23 ตุลาคม พ.ศ. 2547

เมื่อพิจารณาบทบัญญัติ ตั้งแต่มาตรา 269/1 ถึงมาตรา 269/7 ที่ถูกเพิ่มเข้ามาแล้ว สามารถแบ่งการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์เพิ่มขึ้นได้อีกเป็น 4 ลักษณะใหญ่ๆ ดังนี้

---

[27] สุรศักดิ์ ลิขสิทธิ์วัฒนสกุล, คำอธิบายความผิดเกี่ยวกับการปลอมและการแปลงตามประมวลกฎหมายอาญา, พิมพ์ครั้งที่ 1 (กรุงเทพฯ: สำนักพิมพ์วิญญูชน, 2555), หน้า 155-156.

2.2.5 การกระทำความผิดที่เกี่ยวข้องกับฐานปลอมบัตรอิเล็กทรอนิกส์

2.2.5.1 ความผิดฐานปลอมบัตรอิเล็กทรอนิกส์

การปลอมบัตรอิเล็กทรอนิกส์เป็นการกระทำความผิดต่อเนื่องจากการกระทำความผิดอื่นๆ มาก่อนแล้วเพื่อนำบัตรอิเล็กทรอนิกส์ที่แท้จริงมาทำปลอมขึ้นก่อนที่จะนำบัตรปลอมดังกล่าวออกใช้งาน ซึ่งเป็นการกระทำความผิดที่เกิดขึ้นมากที่สุดและการที่จะต้องมีบทบัญญัติดังกล่าวขึ้นมาเป็นการเฉพาะนั้น เพราะการปลอมบัตรอิเล็กทรอนิกส์ในบางครั้งสภาพของบัตรที่ทำปลอมขึ้นมีลักษณะไม่เหมือนกับบัตรอิเล็กทรอนิกส์ต้นแบบเลยแต่มีการใช้งานที่เหมือนกัน เช่น มีลักษณะเป็นบัตรพลาสติกขาว (White Card) หรือเป็นการปลอมบัตรอิเล็กทรอนิกส์ที่เป็นข้อมูลรหัส ต่างๆ ที่ธนาคารได้ออกให้แก่ลูกค้า อันมีปัญหาทำให้ไม่สามารถบังคับใช้บทบัญญัติในประมวลกฎหมายอาญาที่มีอยู่เดิมได้ จึงบัญญัติมาตรา 269/1 ขึ้นเพื่อกำหนดให้การปลอมบัตรอิเล็กทรอนิกส์เป็นความผิดเฉพาะอีกมาตราหนึ่ง นอกจากที่ผู้กระทำจะมีความผิดฐานลักทรัพย์ ตามมาตรา 334 ฐานเอาไปเสียซึ่งเอกสารของผู้อื่น ตามมาตรา 188 ฐานปลอมเอกสาร ตามมาตรา 264 ฐานยักยอกทรัพย์ ตามมาตรา 352 ฐานฉ้อโกงโดยแสดงตนเป็นคนอื่น ตามมาตรา 342 (1) เป็นต้น

มาตรา 269/1 “ผู้ใดทำบัตรอิเล็กทรอนิกส์ปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด เติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใด ๆ ในบัตรอิเล็กทรอนิกส์ที่แท้จริง โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ถ้าได้กระทำเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นบัตรอิเล็กทรอนิกส์ที่แท้จริงหรือเพื่อใช้ประโยชน์อย่างหนึ่งอย่างใด ผู้นั้นกระทำความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงห้าปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนบาท”

การปลอมบัตรอิเล็กทรอนิกส์นั้นไม่จำต้องมีบัตรอิเล็กทรอนิกส์ที่แท้จริงอยู่ก่อนและไม่ต้องทำให้เหมือนของจริงก็ได้ โดยการเทียบเคียงคำพิพากษาศาลฎีกาที่ 1650/2493 และคำพิพากษาศาลฎีกาที่ 4495/2548 ในเรื่องการปลอมเอกสาร ดังนั้นแม้จะไม่ถูกต้องตามแบบบัตรอิเล็กทรอนิกส์ที่แท้จริงแต่ก็มีลักษณะหลายอย่างที่เหมือนกับของจริง อันทำให้หลงหรือเข้าใจผิดได้ ก็เป็นการปลอมบัตรอิเล็กทรอนิกส์แล้ว[28]

[28] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 316.

การปลอมบัตรอิเล็กทรอนิกส์ตามที่มาตรา 269/1 ได้กำหนดไว้สามารถแยกได้สองกรณี คือ

(ก) กรณีทำบัตรอิเล็กทรอนิกส์ปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด

การทำบัตรอิเล็กทรอนิกส์ปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใดนั้น มีวิธีการที่นิยมทำกัน 2 วิธี ก็คือ

(1) การนำข้อมูลที่ได้มาจากการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์อื่นๆ แล้วทำการคัดลอกข้อมูลเหล่านั้นลงในบัตรพลาสติกที่จะทำการปลอมขึ้น ด้วยวิธีการพิมพ์อักษรนูนโดยใช้เครื่องอัดลาย (Embossing Machine) และถ่ายข้อมูลลงในแหล่งบันทึกความจำของบัตรโดยใช้เครื่องถ่ายข้อมูลรหัส (Re-encoder) แล้วนำรูปของบัตรอิเล็กทรอนิกส์ใบอื่นมาพิมพ์ลงบนตัวบัตรหรืออาจใช้บัตรพลาสติกเปล่าหรือที่เรียกว่าบัตรพลาสติกขาว (White Card) ที่มีขนาดและความหนาเท่ากับบัตรอิเล็กทรอนิกส์ต้นฉบับก็ได้

(2) การทำบัตรอิเล็กทรอนิกส์ปลอมโดยการทำข้อมูลขึ้นเอง[29] คือ การใช้โปรแกรมคอมพิวเตอร์ในการสร้างข้อมูลของบัตรอิเล็กทรอนิกส์ขึ้นใหม่ทั้งหมดเพื่อนำไปทำการปลอมบัตรอิเล็กทรอนิกส์ต่อไป ตัวอย่างเช่น การนำหมายเลขบนบัตรเครดิตที่แท้จริงของธนาคารมาเข้าโปรแกรมคอมพิวเตอร์ที่ชื่อว่า Credit Master หรือ Credit Wizard ซึ่งโปรแกรมดังกล่าวจะสร้างหมายเลขบัตรเครดิตเพิ่มขึ้นเองแล้วนำหมายเลขที่ได้ไปคัดลอกลงในบัตรเหมือนวิธีที่ (1) ต่อไป

(ข) กรณีเติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใดๆ ในบัตรอิเล็กทรอนิกส์ที่แท้จริง

การกระทำดังกล่าวเป็นการแปลงบัตรอิเล็กทรอนิกส์ ซึ่งถือว่าเป็นการปลอมบัตรอิเล็กทรอนิกส์ด้วย[30] อันเป็นการบัญญัติกฎหมายให้สอดคล้องกับบทบัญญัติต่างๆ ที่เกี่ยวกับการปลอมและแปลง เช่น เรื่องปลอมเงินตรา ปลอมแสตมป์หรือตั๋ว[31]

การทำบัตรอิเล็กทรอนิกส์ปลอมโดยการเติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใดๆ ในบัตรอิเล็กทรอนิกส์ที่แท้จริง ตัวอย่างเช่น การใช้บัตรอิเล็กทรอนิกส์ที่แท้จริงแต่

---

[29] ทวียศ ศรีเกตุ, "ภัยร้ายจากบัตรเครดิต," บทความใช้เพื่อการนำออกอากาศทางสถานีวิทยุกระจายเสียงรัฐสภา รายการเจตนารมณ์กฎหมาย, สำนักงานเลขาธิการสภาผู้แทนราษฎร (2557).

[30] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 315.

[31] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, คำอธิบายความผิดเกี่ยวกับการปลอมและการแปลงตามประมวลกฎหมายอาญา, หน้า 163.

เปลี่ยนแปลงข้อมูลในบัตรนั้น (Allered Card)[32] โดยการนำบัตรที่หมดอายุการใช้งานหรือที่ถูกอายัดแล้วมาแก้ไขข้อมูลเสียใหม่ เช่น การแก้ไขเลขตัวนูนหน้าบัตรเสียใหม่ (Re-Emboss) โดยการรีดด้วยความร้อนให้ตัวนูนเดิมเรียบเสียก่อน แล้วปั้มเลขนูนชุดใหม่ลงไปแทน ประกอบกับการแก้ไขข้อมูลที่บรรจุในหน่วยบันทึกความจำของบัตร (Re-Encode) โดยการใช้เครื่อง Endoder Key บรรจุข้อมูลของบัตรอิเล็กทรอนิกส์อื่นเข้าไปแทนที่ชุดข้อมูลเดิม หรือการตัดรหัสแท่ง (Bar Code) ของสินค้าชิ้นหนึ่งไปติดกับสินค้าอีกชิ้นหนึ่ง การลงลายมือชื่อปลอมด้านหลังบัตรเครดิต[33]

2.2.5.2 ความผิดฐานนำเข้าในหรือส่งออกไปนอกราชอาณาจักรซึ่งบัตรอิเล็กทรอนิกส์ปลอม

เมื่อได้ทำการปลอมบัตรอิเล็กทรอนิกส์แล้ว บัตรอิเล็กทรอนิกส์ที่ทำปลอมขึ้นหากมีการนำเข้าในหรือส่งออกไปนอกราชอาณาจักรก็จะเป็นความผิดด้วยตามมาตรา 269/3

มาตรา 269/3 “ผู้ใดนำเข้าในหรือส่งออกไปนอกราชอาณาจักรซึ่งสิ่งใด ๆ ตามมาตรา 269/1 ... ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบปี และปรับตั้งแต่หกหมื่นบาทถึงสองแสนบาท”

ซึ่งคำว่าราชอาณาจักรนั้น มีความหมายอย่างเดียวกับมาตรา 4 วรรคแรกเท่านั้น ไม่รวมเรือไทยหรืออากาศยานไทย และไม่รวมสถานทูตไทยในต่างประเทศ

เหตุที่ต้องมีการบัญญัติลักษณะความผิดดังกล่าว เพราะโดยปกติแล้วผู้กระทำความผิดมักจะนำบัตรอิเล็กทรอนิกส์ที่ได้ปลอมขึ้นไปใช้นอกราชอาณาจักรเพื่อให้ติดตามจับกุมผู้กระทำความผิดได้ยาก หรือที่พบบ่อยคือผู้กระทำความผิดที่เป็นชาวต่างชาติได้นำบัตรอิเล็กทรอนิกส์ปลอมของต่างประเทศมาใช้ในประเทศไทย ดังที่ปรากฏข่าวการจับกุมนักท่องเที่ยวต่างชาติ ตระเวน

[32] ทวียศ ศรีเกตุ, “ภัยร้ายจากบัตรเครดิต,” บทความใช้เพื่อการนำออกอากาศทางสถานีวิทยุกระจายเสียงรัฐสภา รายการเจตนารมณ์กฎหมาย, สำนักงานเลขาธิการสภาผู้แทนราษฎร (2557).

[33] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 316-317.

ใช้บัตรอิเล็กทรอนิกส์ปลอมในการเข้าพักโรงแรม ซื้อตั๋วเครื่องบิน ซื้อสินค้าต่างๆ[34] ตามแหล่งท่องเที่ยวในประเทศไทย[35]

ตัวอย่างการกระทำความผิดตามมาตรานี้ เช่น

คำพิพากษาศาลฎีกาที่ 3499/2552 “จำเลยที่ 1 กับพวกร่วมกันปลอม นำเข้า และใช้บัตรอิเล็กทรอนิกส์ปลอมที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ เพื่อใช้ประโยชน์ในการชำระค่าสินค้า ค่าบริการหรือหนี้อย่างอื่นแทนการชำระด้วยเงินสด อันเป็นความผิดตาม ป.อ. มาตรา 269/7 ” คดีนี้จำเลยมีความผิดฐานนำเข้าในหรือส่งออกไปนอกราชอาณาจักรซึ่งบัตรอิเล็กทรอนิกส์ปลอมนี้อีกกระทงหนึ่งด้วย แต่ต้องรับโทษหนักขึ้นตามมาตรา 269/7

2.2.5.3 ความผิดฐานใช้หรือมีไว้เพื่อใช้ซึ่งบัตรอิเล็กทรอนิกส์ปลอม

การใช้หรือมีไว้เพื่อใช้บัตรอิเล็กทรอนิกส์ปลอมนับเป็นการกระทำขั้นสุดท้ายของการปลอมบัตรอิเล็กทรอนิกส์ การใช้บัตรอิเล็กทรอนิกส์นั้นจะทำให้ผู้กระทำความผิดได้รับประโยชน์จากบัตรอิเล็กทรอนิกส์อย่างมาก เช่น นำบัตรอิเล็กทรอนิกส์ดังกล่าวไปซื้อสินค้าหรือบริการต่างๆ หรือแม้จะยังไม่ใช้แต่มีไว้เพื่อใช้ก็ถือว่าเป็นการกระทำที่ผู้กระทำผิดใกล้ชิดกับผลของการใช้มากที่สุดเพราะบัตรอิเล็กทรอนิกส์นั้นสามารถพกพาและใช้งานได้ง่าย ซึ่งผู้กระทำความผิดจะนำออกมาใช้เมื่อไหร่ก็ได้โดยไม่อาจถูกสังเกตเห็นว่ากำลังกระทำความผิดอยู่เลย ซึ่งบทบัญญัติของกฎหมายได้กำหนดให้การกระทำทั้งสองกรณีดังกล่าวบัญญัติอยู่ในมาตราเดียวกัน

มาตรา 269/4 วรรคแรก “ผู้ใดใช้หรือมีไว้เพื่อใช้ซึ่งสิ่งใดๆ ตามมาตรา 269/1 อันได้มาโดยรู้ว่าเป็นของที่ทำปลอมหรือแปลงขึ้น ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี หรือปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท หรือทั้งจำทั้งปรับ”

การกระทำความผิดดังกล่าวอาจกระทำแก่บัตรอิเล็กทรอนิกส์ที่ผู้อื่นทำปลอมให้หรือผู้กระทำอาจเป็นผู้ปลอมเองก็ได้ แต่ตามมาตรา 269/4 วรรคท้าย หากผู้กระทำความผิดที่ใช้หรือมีไว้เพื่อใช้ซึ่งบัตรอิเล็กทรอนิกส์ปลอมเป็นผู้ปลอมบัตรอิเล็กทรอนิกส์เองด้วย ให้ลงโทษตามมาตรา 269/4 แต่เพียงกระทงเดียวโดยไม่ต้องลงโทษฐานปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/1 อีก

---

[34] โพสต์ทูเดย์, "จับหนุ่มอินเดียใช้บัตรเครดิตปลอมรูดซื้อสินค้า" [ออนไลน์], เข้าถึงเมื่อ 6 สิงหาคม 2563. แหล่งที่มา: https://www.posttoday.com/social/local/341878.

[35] ไทยรัฐ, "จับมาเลย์แสบ! ทำบัตรเครดิตปลอม รูดข้ามโลก" [ออนไลน์], เข้าถึงเมื่อ 6 สิงหาคม 2563. แหล่งที่มา: https://www.thairath.co.th/news/local/516310.

กระทง อันเป็นหลักการเดียวกับความผิดฐานปลอมเอกสารที่ผู้ปลอมเอกสารและใช้เอกสารปลอมจะโดนลงโทษเพียงฐานใช้เอกสารปลอมเพียงกระทงเดียว[36]

ตัวอย่างการกระทำความผิดตามมาตรานี้ เช่น

คำพิพากษาศาลฎีกาที่ 16000/2553 “ศาลชั้นต้นพิพากษาว่า จำเลยกระทำความผิดหลายกรรมต่างกันให้เรียงกระทงลงโทษตาม ป.อ. มาตรา 91 ฐานปลอมบัตรอิเล็กทรอนิกส์ จำคุก 2 ปี ฐานมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ จำคุก 2 ปี และฐานใช้บัตรอิเล็กทรอนิกส์ปลอม จำคุก 3 ปี แต่ความผิดฐานใช้บัตรอิเล็กทรอนิกส์ปลอม ศาลชั้นต้นปรับบทว่าเป็นความผิดตาม ป.อ. มาตรา 269/5 ซึ่งไม่ถูกต้อง ศาลอุทธรณ์ภาค 1 ปรับบทว่าเป็นความผิดตาม ป.อ. มาตรา 269/4 วรรคแรก ให้ถูกต้องเท่านั้น”

2.2.5.4 ความผิดฐานจำหน่ายหรือมีไว้เพื่อจำหน่ายซึ่งบัตรอิเล็กทรอนิกส์ปลอม

การจำหน่ายหรือมีไว้เพื่อจำหน่ายบัตรอิเล็กทรอนิกส์ปลอมบัญญัติขึ้นเพราะการปลอมบัตรอิเล็กทรอนิกส์นั้น ผู้ทำปลอมอาจไม่ต้องการผลประโยชน์โดยตรงจากการใช้บัตรอิเล็กทรอนิกส์ก็ได้แต่ต้องการแลกกับเงินหรือผลประโยชน์อย่างอื่น และในการทำงานในรูปแบบองค์กรอาชญากรรมโดยมีการแบ่งหน้าที่กันทำนั้น บัตรอิเล็กทรอนิกส์ปลอมมักจะส่งกันเป็นทอดๆ ผู้ใช้บัตรอิเล็กทรอนิกส์ปลอมจึงมักจะไม่ใช่ผู้ปลอมบัตรอิเล็กทรอนิกส์ ดังนั้นบุคคลที่เป็นตัวกลางในการส่งมอบบัตรอิเล็กทรอนิกส์แม้จะไม่มีความผิดฐานใช้หรือมีไว้เพื่อใช้บัตรอิเล็กทรอนิกส์ปลอม แต่ก็อาจมีความผิดตามมาตรานี้ได้ เพราะการจำหน่าย หมายความว่า ส่งบัตรอิเล็กทรอนิกส์ปลอมไปยังบุคคลอื่นโดยจะมีค่าตอบแทนหรือไม่ก็ได้[37]

มาตรา 269/4 วรรคสอง “ผู้ใดจำหน่ายหรือมีไว้เพื่อจำหน่ายซึ่งสิ่งใด ๆ ที่ทำปลอมหรือแปลงขึ้นตามมาตรา ๒๖๙/๑ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี หรือปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท หรือทั้งจำทั้งปรับ”

ตามมาตรา 269/4 วรรคท้าย หากผู้กระทำความผิดที่จำหน่ายหรือมีไว้เพื่อจำหน่ายซึ่งบัตรอิเล็กทรอนิกส์ปลอมเป็นผู้ปลอมบัตรอิเล็กทรอนิกส์ด้วย ให้ลงโทษตามมาตรา 269/4 แต่เพียงกระทงเดียวโดยไม่ต้องลงโทษฐานปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/1 อีกกระทง

---

[36] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 327-330.

[37] เรื่องเดียวกัน, หน้า 328.

2.2.6 การกระทำความผิดที่เกี่ยวข้องกับฐานทำหรือมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์

2.2.6.1 ความผิดฐานทำเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์

การปลอมบัตรอิเล็กทรอนิกส์จะกระทำไม่ได้หากปราศจากเครื่องมือที่ใช้ในการปลอมบัตรอิเล็กทรอนิกส์ เพราะการปลอมบัตรอิเล็กทรอนิกส์นั้นจำต้องอาศัยเครื่องมือต่างๆ ที่ได้ทำขึ้นเฉพาะเพื่อใช้ในการปลอมบัตรอิเล็กทรอนิกส์ หรืออาศัยเครื่องมือเพื่อให้ได้ข้อมูลของบัตรอิเล็กทรอนิกส์แล้วนำข้อมูลนั้นไปใช้ในการทำบัตรอิเล็กทรอนิกส์ปลอมต่อไป เครื่องมือที่ใช้ในการปลอมบัตรอิเล็กทรอนิกส์จึงเป็นจุดเริ่มต้นของการทำบัตรอิเล็กทรอนิกส์ปลอม และเป็นจุดที่แยกการกระทำความผิดที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ออกจากการกระทำความผิดรูปแบบเดิมในหัวข้อที่ 2.2.1 ถึงหัวข้อที่ 2.2.4 ซึ่งเป็นการกระทำที่ไม่จำต้องอาศัยเครื่องมือใดๆ เลยในการกระทำความผิด หรือใช้เพียงเครื่องมือพื้นฐานทั่วๆ ไป โดยไม่จำต้องมีการดัดแปลงใดๆ แก่เครื่องมือเหล่านั้นให้มีลักษณะเฉพาะเลย

มาตรา 269/2 “ผู้ใดทำเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับ ให้ได้ข้อมูลในการปลอมหรือแปลงสิ่งใดๆ ซึ่งระบุไว้ใน มาตรา 269/1 ... ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงห้าปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนบาท”

เครื่องมือหรือวัตถุที่ใช้ในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ เช่น เครื่องคอมพิวเตอร์ แท่นปั๊มตัวอักษรนูนบนบัตร (Embossing Machine) เครื่องเคลือบนูนบนบัตร เครื่องพิมพ์บัตรพลาสติก เครื่องถ่ายข้อมูลรหัส (Re-encoder) เครื่อง Endoder Key บัตรพลาสติกเปล่าที่ใช้ใส่ข้อมูลบัตรอิเล็กทรอนิกส์ใบอื่น (White Card)[38]

เครื่องมือหรือวัตถุที่ใช้สำหรับให้ได้ข้อมูลบัตรอิเล็กทรอนิกส์ เช่น เครื่องดูดข้อมูลแถบรหัสแม่เหล็ก (Skimmer)[39] ซึ่งอาจเรียกว่า “เครื่องเก็บข้อมูล” ก็ได้[40] สมาร์ทโฟน (Smart

[38] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, คำอธิบายความผิดเกี่ยวกับการปลอมและการแปลงตามประมวลกฎหมายอาญา, หน้า 167.

[39] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 320.

[40] สมศักดิ์ เอี่ยมพลับใหญ่, กฎหมายอาญา ภาคความผิดเกี่ยวกับความเท็จ การปลอมและการแปลง, พิมพ์ครั้งที่ 1 (กรุงเทพฯ: นิติธรรม, 2554), หน้า 207.

phone)[41] กล้องขนาดจิ๋ว (Micro Camera) แป้นปุ่มกดปลอม (Keypad Overlays) โปรแกรมมัลแวร์หรือไวรัสคอมพิวเตอร์ (Malware or Virus Computer)

ยิ่งเทคโนโลยีพัฒนามากขึ้นเครื่องมือดังกล่าวเหล่านี้ก็พัฒนามากขึ้นตามไปด้วย เช่น เครื่องดูดข้อมูลบัตรอิเล็กทรอนิกส์เดิมนั้นสามารถคัดลอกข้อมูลได้จากแหล่งบันทึกข้อมูลประเภทแถบแม่เหล็ก (Magnetic Stripe) เท่านั้น แต่ในปัจจุบันเครื่องมือดังกล่าวมีการพัฒนาขึ้นและสามารถคัดลอกข้อมูลได้จากแหล่งบันทึกข้อมูลประเภทชิป (Chip) เพิ่มขึ้นด้วย[42]

การทำ คือ การผลิตหรือการทำให้มีขึ้น โดยอาศัยเจตนาธรรมดา ไม่จำต้องมีเจตนาพิเศษร่วมด้วย ซึ่งแตกต่างจากการมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ ในส่วนท้ายของมาตรา 269/2

ตัวอย่าง ขั้นตอนการทำเครื่องสกิมเมอร์[43]

ขั้นแรก ผู้กระทำผิดจะนำเครื่องสกิมเมอร์ทั่วไปมาถอดฝาออกแล้วเอาส่วนปลอกโลหะด้านนอกทิ้งไป แล้วใช้เฉพาะส่วนหัวอ่านและวงจรอิเล็กทรอนิกส์ซึ่งติดตั้งอยู่บนแกนพลาสติกซึ่งมีร่องสำหรับการรูดบัตรอยู่ตรงกลาง โดยเครื่องสกิมเมอร์แต่ละรุ่นและยี่ห้อนั้นเมื่อดูจากภายนอกจะมีขนาดเท่าๆ กัน แต่เมื่อแกะออกดูภายในจะมีขนาดของแผ่นวงจรไม่เท่ากัน ผู้กระทำผิดมักจะนิยมเลือกรุ่นที่มีแผ่นวงจรเล็กที่สุดและรุ่นที่มีส่วนเชื่อมต่อเพื่อใช้เสียบกับพอร์ทอนุกรม (RS-232) เพราะนำไปดัดแปลงได้ง่ายกว่า

ขั้นต่อมา ผู้กระทำผิดจะวิเคราะห์เครื่องสกิมเมอร์ว่าเมื่อรูดบัตรแล้วจะส่งข้อมูลเป็นสัญญาณไฟฟ้าออกมาในลักษณะใด การวิเคราะห์ทำได้โดยใช้เครื่องวิเคราะห์ตรรกะ (Logic Analyzer) ซึ่งเป็นเครื่องมือวัดที่มีใช้ในห้องปฏิบัติการทางอิเล็กทรอนิกส์ทั่วไป โดยใช้หัววัดเครื่องจับที่สายสัญญาณต่างๆ ของเครื่องสกิมเมอร์ เมื่อทำการรูดบัตรเครื่องสกิมเมอร์จะอ่านและส่งสัญญาณไปยังหน้าจอเครื่องซึ่งจะแสดงระดับสูงต่ำของสัญญาณไฟฟ้าออกมาเป็นภาพแผนภูมิตามช่วงเวลา

---

[41] It24hrs.com, "อุปกรณ์ที่ทำให้ Smartphone แปลงร่างเป็นเครื่องอ่านบัตรเครดิต เริ่มให้บริการในไทยแล้ว" [ออนไลน์], เข้าถึงเมื่อ 20 พฤศจิกายน 2560. แหล่งที่มา: https://www.it24hrs.com/2013/iphone-credit-card-reader-come-to-thailand/.

[42] Megan Geuss, “An ATM hack and a PIN-pad hack show chip cards aren’t impervious to fraud” [Online], Accessed: 25 July 2020. Available from: https://arstechnica.com/information-technology/2016/08/an-atm-hack-and-a-pin-pad-hack-show-chip-cards-arent-impervious-to-fraud/.

[43] ลาภลอย วานิชอังกูร, "สกิมเมอร์ : เทคโนโลยีโฉดเพื่อทรชน" [ออนไลน์], เข้าถึงเมื่อ 7 สิงหาคม 2563. แหล่งที่มา: https://www.kroobannok.com/33613.

(Timing Diagram) โดยผู้กระทำผิดจะทดสอบกับบัตรหลายๆ ใบเพื่อศึกษารูปแบบของสัญญาณเปรียบเทียบกัน ทำให้สามารถแปลตรรกะการทำงานของข้อมูลของบัตรได้ เมื่อผู้กระทำผิดเข้าใจรูปแบบของสัญญาณแล้ว ผู้กระทำผิดจะสร้างวงจรดิจิตอลเพื่อแปลงสัญญาณไฟฟ้านี้ให้อยู่ในรูปแบบที่นำไปจัดเก็บไว้ในหน่วยความจำของคอมพิวเตอร์ได้ โดยการใช้วงจรแปลงสัญญาณจากไมโครคอนโทลเลอร์ (Microcontroller) เช่น PIC16F688 และอาจทำการเพิ่มหน่วยความจำในเครื่องสกิมเมอร์ให้สามารถบันทึกข้อมูลจากบัตรอิเล็กทรอนิกส์ได้มากขึ้น และอาจติดตั้งหน้าจอเอลซีดี (LCD) ควบคู่ในการใช้งานเพื่อทำให้สามารถอ่านข้อมูลได้จากเครื่องสกิมเมอร์ได้โดยตรง

2.2.6.2 ความผิดฐานมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์

การมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ เป็นความผิดที่กำหนดอยู่ในส่วนท้ายของมาตรา 269/2 ซึ่งแม้ผู้กระทำความผิดมิได้เป็นผู้ทำเครื่องมือหรือวัตถุดังกล่าวแต่การมีก็นับว่าเป็นความผิดด้วย อันเป็นการบัญญัติกฎหมายให้สอดคล้องกับหมวดอื่นๆ ในลักษณะ 7 ความผิดเกี่ยวกับปลอมหรือแปลง[44]

มาตรา 269/2 “ผู้ใด... มีเครื่องมือหรือวัตถุเช่นว่านั้น เพื่อใช้หรือให้ได้ข้อมูลในการปลอมหรือแปลง... ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงห้าปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนบาท”

มี หมายถึงมีไว้ในครอบครอง[45] นอกจากเจตนาธรรมดาแล้วจะต้องมีเจตนาพิเศษเพื่อใช้หรือให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ ไม่ใช่มีไว้เพื่อสะสมโดยเห็นเป็นของแปลก[46] อันต่างจากการทำเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ที่มีเพียงเจตนาธรรมดาเท่านั้นไม่ต้องคำนึงถึงเจตนาพิเศษ และหากพิสูจน์เจตนาพิเศษได้แล้ว แม้ว่าผู้นั้นจะยังมิได้นำเครื่องมือหรือวัตถุดังกล่าวออกใช้ก็เป็นความผิดสำเร็จทันที เช่น ยังมิได้ติดตั้งเครื่องสกิมเมอร์

---

[44] ตามมาตรา 246 และ มาตรา 261

[45] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, คำอธิบายความผิดเกี่ยวกับการปลอมและการแปลงตามประมวลกฎหมายอาญา, หน้า 169.

[46] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 321.

เข้ากับตู้เอทีเอ็ม หรือยังมิได้ติดตั้งกับเครื่องรูดบัตรเครดิตก็ตาม[47] และการซื้อเครื่องมือดังกล่าวโดยให้ผู้ขายยึดถือไว้ให้ก็นับว่ามีการครอบครองแล้ว อันเป็นความผิดตามมาตรานี้ทันที[48]

เหตุที่ต้องมีการบัญญัติให้การมีนั้น จะต้องมีเจตนาพิเศษด้วยจึงจะเป็นความผิด เพราะเครื่องมือหรือวัตถุดังกล่าวหลายชนิดมีการใช้งานอยู่ทั่วไปซึ่งไม่เป็นความผิด เช่น เครื่องสกิมเมอร์หรือเครื่องรูดบัตรเครดิตที่ธนาคาร ห้างร้านและบุคคลทั่วไปได้ใช้ในการทำธุรกรรมทางการเงินในชีวิตประจำวัน[49] ดังนั้นการมีเครื่องมือหรือวัตถุใดๆ ซึ่งเป็นความผิดตามมาตรานี้ จึงต้องพิสูจน์ให้เห็นว่าผู้นั้นได้มีเจตนาพิเศษด้วย ซึ่งหากพนักงานสอบสวนพบเครื่องสกิมเมอร์เป็นพยานหลักฐานในการกระทำความผิดแต่เพียงอย่างเดียว จะยากในการพิสูจน์เจตนาพิเศษเพื่อเอาผิดกับบุคคลผู้มีเครื่องมือหรือวัตถุดังกล่าวเพราะไม่อาจทราบว่าการมีเครื่องสกิมเมอร์นั้นไว้ใช้งานธรรมดาหรือจะใช้ในการกระทำความผิด[50]

ตัวอย่างการกระทำความผิดตามมาตรานี้ เช่น

คำพิพากษาศาลฎีกาที่ 1969/2505 “บุคคลอื่นนำเครื่องมือไปทำเหรียญกษาปณ์ปลอมที่บ้านจำเลย... ได้ชื่อว่าจำเลยมีเครื่องมือไว้เพื่อใช้ในการปลอมเหรียญกษาปณ์แล้ว ” คำพิพากษาฉบับนี้เป็นเรื่องปลอมเงินตราที่นำมาเทียบเคียงกับมาตรานี้ได้ โดยศาลฎีกาตัดสินว่าเพียงแต่จำเลยรับฝากเครื่องมือไว้ก็มีความผิดฐานมีเครื่องมือสำหรับปลอมเงินตรา ตามมาตรา 246 แล้ว[51]

ความผิดตามมาตรานี้มักจะถูกตั้งเป็นข้อหาแก่ผู้กระทำความผิดมากที่สุด เพราะเมื่อมีการตรวจค้นเคหสถานในประเทศไทยที่กลุ่มอาชญากรต่างชาติได้ใช้ในการกบดานและดำเนินการ

---

[47] เรื่องเดียวกัน, หน้า 321.

[48] เรื่องเดียวกัน, หน้า 322.

[49] R&D smart shop, "เครื่องอ่านบัตรแม่เหล็ก" [ออนไลน์], เข้าถึงเมื่อ 20 พฤศจิกายน 2560. แหล่งที่มา: http://rd-comp.com/index.aspx?pid=dba21964-3b89-486b-969f-9cc86808d1ee&igid=13c1a775-8bde-494c-a208-0b826a843337.

[50] สัมภาษณ์ พงศ์พจน์ ธรรมากุลวิชช์, รองผู้กำกับการสอบสวน กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ, 17 ตุลาคม 2560.

[51] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 322.

กระทำความผิด มักจะพบเครื่องมือหรือวัตถุเหล่านั้นในสถานที่ดังกล่าวด้วย ซึ่งจะพบตามสถานที่ท่องเที่ยวหรือเมืองใหญ่ในประเทศไทย เช่น กรุงเทพ[52] เชียงใหม่[53] ภูเก็ต[54] และเมืองพัทยา[55]

2.2.6.3 ความผิดฐานนำเข้าในหรือส่งออกไปนอกราชอาณาจักรซึ่งเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์

การนำเข้าในหรือส่งออกไปซึ่งเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์บัตรอิเล็กทรอนิกส์ จะเป็นความผิดตามมาตรา 269/3

มาตรา 269/3 “ผู้ใดนำเข้าในหรือส่งออกไปนอกราชอาณาจักรซึ่งสิ่งใด ๆ ตาม... มาตรา 269/2 ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบปี และปรับตั้งแต่หกหมื่นบาทถึงสองแสนบาท”

ซึ่งคำว่าราชอาณาจักรนั้น มีความหมายอย่างเดียวกับมาตรา 4 วรรคแรกเท่านั้น ไม่รวมเรือไทยหรืออากาศยานไทย และไม่รวมสถานทูตไทยในต่างประเทศ

เหตุที่ต้องมีการบัญญัติลักษณะความผิดดังกล่าว เพราะเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ มักจะถูกนำมาเข้ามาพร้อมกับผู้กระทำความผิดที่แฝงตัวเป็นนักท่องเที่ยวชาวต่างชาติที่เข้ามาในประเทศไทยซึ่งเครื่องมือดังกล่าวนั้นในปัจจุบันสามารถหาซื้อได้จากเว็ปไซต์ที่ขายของผิดกฎหมายจากต่างประเทศ เช่น ประเทศจีน[56]

---

[52] Moneyhub, "มาอีกแล้ว! แก๊งสกิมเมอร์ปลอมบัตรเครดิตข้ามชาติ" [ออนไลน์], เข้าถึงเมื่อ 6 สิงหาคม 2563. แหล่งที่มา: https://moneyhub.in.th/article/skimmer-atm/.

[53] กรุงเทพธุรกิจ, "จับคาหนังคาเขาแก๊งสกิมเมอร์จีน ขณะติดอุปกรณ์คาตู้เอทีเอ็ม" [ออนไลน์], เข้าถึงเมื่อ 6 สิงหาคม 2563. แหล่งที่มา: https://www.bangkokbiznews.com/news/detail/759274.

[54] MGRonline, "ระวัง! แก๊งสกิมเมอร์ชาวจีนระบาดอีกแล้ว ตร.ภูเก็ตรวบได้ 2 คน ตระเวนกดเงินตู้เอทีเอ็ม" [ออนไลน์], เข้าถึงเมื่อ 6 สิงหาคม 2563. แหล่งที่มา: https://mgronline.com/south/detail/9600000065820.

[55] MGRonline, "รวบคู่หูแดนมังกรตั้งแก๊งสกิมเมอร์ดูดข้อมูลบัตรเอทีเอ็ม ตระเวนกดเงินสดใน จ.ชลบุรี" [ออนไลน์], เข้าถึงเมื่อ 6 สิงหาคม 2563. แหล่งที่มา: https://mgronline.com/local/detail/9620000111983.

[56] 77ข่าวเด็ด, "รวบแก๊งสกิมเมอร์ชาวจีนปลอมบัตรATM ตระเวนกดเงินสดทั่วชลบุรี" [ออนไลน์], เข้าถึงเมื่อ 6 สิงหาคม 2563. แหล่งที่มา: https://www.77kaoded.com/news/sangk/1036335.

2.2.7 การกระทำความผิดที่เกี่ยวข้องกับฐานใช้หรือมีไว้เพื่อนำออกใช้บัตรอิเล็กทรอนิกส์ที่แท้จริงของผู้อื่นโดยมิชอบ

2.2.7.1 ความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ

นอกจากการกระทำความผิดที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ปลอมตามหัวข้อที่ 2.2.5 แล้ว การใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นนั้นอาจจะมีความผิดได้ด้วย อันเป็นการใช้บัตรอิเล็กทรอนิกส์ที่แท้จริงของผู้อื่น คือ เป็นบัตรที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ แต่ผู้กระทำความผิดซึ่งมิได้รับอนุญาตจากผู้ออกบัตรและไม่ได้รับอำนาจจากผู้มีสิทธิใช้ ได้นำบัตรอิเล็กทรอนิกส์ดังกล่าวไปใช้อันเป็นการกระทำการที่มิชอบ[57]

มาตรา 269/5 “ผู้ใดใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

การกระทำดังกล่าวเพียงแต่น่าจะก่อให้เกิดความเสียหายก็เป็นความผิดสำเร็จแล้ว เทียบเคียงคำพิพากษาศาลฎีกาที่ 1281-1282/2538 เช่น นายม่วงมอบบัตรเอทีเอ็มของตนและรหัสบัตรดังกล่าวให้นายดำไปช่วยกดเงินให้จำนวนหนึ่งแต่นายดำไปกดเกินมาแล้วเก็บส่วนที่เกินไว้เอง นายดำมีความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบแล้วนอกจากความผิดอื่นๆ อันเกี่ยวกับทรัพย์[58]

ตัวอย่างการกระทำความผิดตามมาตรานี้ เช่น

คำพิพากษาศาลฎีกาที่ 6820/2552 “จำเลยเอาไปเสียซึ่งบัตรเครดิตวีซ่าการ์ดของบริษัท บ. ซึ่งออกให้แก่ น. แล้วใช้บัตรเครดิตวีซ่าการ์ดดังกล่าวชำระค่าสินค้าแทนการชำระด้วยเงินสดอันเป็นความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นชำระค่าสินค้า ค่าบริการหรือหนี้อื่นแทนการชำระด้วยเงินสดโดยมิชอบตาม ป.อ. มาตรา 269/5 และ มาตรา 269/7”

คำพิพากษาศาลฎีกาที่ 8833/2554 “จำเลยนำบัตรเอทีเอ็มของผู้เสียหายไปใช้เบิกถอนเงินสดและโอนเงินเข้าบัญชีเงินฝากของจำเลย” คดีนี้ศาลฎีกาตัดสินลงโทษตามมาตรา 269/5 ประกอบมาตรา 269/7

---

[57] คณิต ณ นคร, กฎหมายอาญาภาคความผิด, พิมพ์ครั้งที่ 11 (กรุงเทพฯ: วิญญูชน, 2559), หน้า 697.

[58] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 334.

มีคำพิพากษาอื่นๆ อีก เช่น คำพิพากษาศาลฎีกาที่ 2512/2550, คำพิพากษาศาลฎีกาที่ 20134/2556 และคำพิพากษาศาลฎีกาที่ 11227/2555

2.2.7.2 ความผิดฐานมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ

การมีบัตรอิเล็กทรอนิกส์ที่แท้จริงของผู้อื่นไว้เพื่อนำออกใช้นั้นจะเป็นความผิดเช่นเดียวกันกับการใช้บัตรอิเล็กทรอนิกส์ที่แท้จริงของผู้อื่นโดยมิชอบ แต่ประมวลกฎหมายอาญานั้นบัญญัติแยกการใช้และการมีไว้เพื่อนำออกใช้ออกเป็นคนละมาตรากัน เพราะมีอัตราโทษทางอาญาไม่เหมือนกัน ซึ่งน่าแปลกใจที่บทบัญญัติในมาตรา 269/5 และมาตรา 269/6 นี้ไม่ได้มีอัตราโทษที่เป็นไปในแนวทางเดียวกันกับบทบัญญัติในมาตราก่อนๆ คือมาตรา มาตรา 269/4 ซึ่งบัญญัติให้ไม่ว่าการใช้หรือมีไว้เพื่อใช้ หรือการจำหน่ายหรือมีไว้เพื่อจำหน่ายก็ต่างมีอัตราโทษเดียวกันทั้งสิ้น เมื่อผู้วิจัยได้ทำการศึกษาร่างกฎหมายอันเป็นที่มาของการแก้ไขประมวลกฎหมายอาญามาตรานี้จึงพบว่า เดิมนั้นร่าง... ของคณะรัฐมนตรี[59] และของสมาชิกสภาผู้แทนราษฎร[60] ได้บัญญัติให้ ผู้ใดใช้หรือมีไว้เพื่อใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ อยู่ในบทบัญญัติมาตราเดียวกันคือ มาตรา 269/5 ซึ่ง มาตรา 269/6 เดิมนั้นจะเป็นเรื่องเกี่ยวกับการใช้ข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ แต่โดนที่ประชุมคณะกรรมการแปรญัตติร่าง... ตัดทิ้งเสีย จึงจำเป็นต้องแยกมาตรา 269/5 ออกให้เรื่องการใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ อยู่ในมาตรา 269/5 และให้เรื่องการมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ไปแทนที่มาตรา 269/6 เดิม พร้อมทั้งลดอัตราโทษลงด้วย[61]

มาตรา 269/6 “ผู้ใดมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/5 ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

ตัวอย่างการกระทำความผิดตามมาตรานี้ เช่น นายแดงสะสมรหัสผ่านบัตรเอทีเอ็มของบุคคลต่างๆ ไว้เป็นจำนวนมากเพื่อจะไปขโมยบัตรเอทีเอ็มของบุคคลต่างๆ เหล่านั้น แล้วนำบัตร

---

[59] ร่างพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่...) พ.ศ. ... ที่ นร 0503/2883 วันที่ 4 มีนาคม 2546 ลงชื่อ พันตำรวจโท ทักษิณ ชินวัตร เสนอโดยนายพงศ์เทพ เทพกาญจนา รัฐมนตรีว่าการกระทรวงยุติธรรมในสมัยนั้น

[60] ร่างพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่...) พ.ศ. ... วันที่ 25 มีนาคม 2546 ลงชื่อ นงค์นาถ เตชะไพบูลย์ สมาชิกสภาผู้แทนราษฎร พรรคชาติพัฒนา โดยมีสมาชิกสภาผู้แทนราษฎรรับรอง 20 ท่าน

[61] รายงานการประชุมสภาผู้แทนราษฎร ชุดที่ 21 ปีที่ 3 ครั้งที่ 22 (สมัยสามัญนิติบัญญัติ) เป็นพิเศษ วันที่ 15 ตุลาคม 2546 หน้า 103

มาใช้ถอนเงินจากเครื่องจ่ายเงินอัตโนมัติ การสะสมรหัสบัตรของนายแดงนั้นย่อมเป็นความผิดตามมาตรานี้[62]

หากผู้กระทำความผิดได้ใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/5 แล้ว ก็ไม่จำต้องปรับบทลงโทษฐานมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรานี้อีกเพราะการมีไว้เพื่อนำออกใช้ได้เกลื่อนกลืนไปกับการใช้แล้ว ตามนัยของคำพิพากษาศาลฎีกาที่ 2512/2550 และคำพิพากษาศาลฎีกาที่ 465/2551[63]

2.2.8 การกระทำความผิดที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์บางประเภทที่ผู้กระทำต้องรับโทษหนักขึ้น

บัตรอิเล็กทรอนิกส์บางประเภทนั้นได้รับการคุ้มครองตามประมวลกฎหมายอาญามากกว่าบัตรอิเล็กทรอนิกส์ประเภทอื่นๆ ซึ่งหากเกิดการกระทำความผิดขึ้นแก่บัตร อิเล็กทรอนิกส์ประเภทดังกล่าวแล้ว ผู้กระทำต้องรับโทษหนักขึ้น ตามมาตรา 269/7 อันเป็นเหตุฉกรรจ์ของมาตรา 269/1 ถึงมาตรา 269/6

มาตรา 269/7 “ถ้าการกระทำดังกล่าวในหมวดนี้ เป็นการกระทำเกี่ยวกับบัตรอิเล็กทรอนิกส์ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ เพื่อใช้ประโยชน์ในการชำระค่าสินค้า ค่าบริการหรือหนี้อื่นแทนการชำระด้วยเงินสด หรือใช้เบิกถอนเงินสด ผู้กระทำต้องระวางโทษหนักกว่าที่บัญญัติไว้ในมาตรานั้นๆ กึ่งหนึ่ง”

หลักสำคัญที่ผู้กระทำความผิดจะต้องรับโทษหนักขึ้นตามมาตรา 269/7 นี้ อยู่ที่ว่าในขณะที่กระทำความผิด ผู้กระทำต้องรู้ข้อเท็จจริงว่าบัตรอิเล็กทรอนิกส์ประเภทดังกล่าวใช้ประโยชน์ในการชำระค่าสินค้า ค่าบริการหรือหนี้อื่นแทนการชำระด้วยเงินสด หรือใช้เบิกถอนเงินสดด้วย ตามประมวลกฎหมายอาญา มาตรา 62 วรรคท้าย[64]

บัตรอิเล็กทรอนิกส์ที่ผู้กระทำความผิดจะต้องรับโทษหนักขึ้นตามมาตรา 269/7 นี้ เช่น บัตรเอทีเอ็ม (Automatic Teller Machine Card ; ATM) บัตรเดบิต (Debit Card) บัตรเครดิต (Credit Card) บัตรเงินสด (Cash Card) บัตรเติมเงินต่างๆ ซึ่งบัตรอิเล็กทรอนิกส์เหล่านี้เปรียบเสมือน

---

[62] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 335.

[63] เรื่องเดียวกัน, หน้า 338.

[64] เรื่องเดียวกัน, หน้า 336.

เป็นเงินในรูปแบบอิเล็กทรอนิกส์ของผู้มีสิทธิใช้ ดังนั้นการกระทำความผิดกับบัตรอิเล็กทรอนิกส์ประเภทดังกล่าวจึงสร้างความเสียหายให้แก่ผู้ออกบัตรให้และผู้มีสิทธิจะใช้อย่างมาก ไม่ต่างจากการขโมยเงินจากบุคคลเหล่านั้น กฎหมายจึงให้ความคุ้มครองมากกว่าบัตรอิเล็กทรอนิกส์ประเภทอื่นๆ

บทที่ 3
ปัญหาและอุปสรรคเกี่ยวกับการบังคับใช้กฎหมาย จากการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในปัจจุบัน

เมื่อได้ทราบความหมายของบัตรอิเล็กทรอนิกส์ ประเภทของบัตรอิเล็กทรอนิกส์และการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามที่ประมวลกฎหมายอาญาได้บัญญัติไว้ในบทที่ 2 แล้ว ในบทที่ 3 นี้จะกล่าวถึงการกระทำความผิดที่เกี่ยวกับบัตรอิเล็กทรอนิกส์อีกประการหนึ่งคือ การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ซึ่งเป็นขั้นตอนที่สำคัญอันกล่าวได้ว่าเป็นบ่อเกิดให้มีการกระทำการปลอมบัตรอิเล็กทรอนิกส์เกิดขึ้นต่อมา เพราะหากไม่มีการดึงข้อมูลออกมาจากบัตรอิเล็กทรอนิกส์อื่นๆ มาก่อนแล้ว ก็จะทำให้บัตรอิเล็กทรอนิกส์ที่ทำปลอมขึ้นนั้นไม่มีข้อมูลอันทำให้บัตรนั้นใช้งานไม่ได้ ซึ่งไม่ก่อให้เกิดประโยชน์แก่อาชญากรในการกระทำความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ดังกล่าวเลย ดังนั้น การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์จึงเป็นสิ่งที่สำคัญไม่น้อยกว่าการการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์รูปแบบต่างๆ[1] ซึ่งในบทที่ 3 นี้จะกล่าวถึงโดยเน้นเฉพาะการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ว่ามีรูปแบบอะไรบ้าง ปัญหาการปรับใช้บทบัญญัติในประมวลกฎหมายอาญาเรื่องการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์เพื่อลงโทษผู้กระทำความผิดลักษณะนี้เป็นอย่างไร และทำไมถึงไม่สามารถใช้บทบัญญัติอื่นๆ ในประมวลกฎหมายอาญาและกฎหมายอื่นๆ ที่เกี่ยวข้องในการลงโทษผู้กระทำความผิดได้

3.1 การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ เป็นลักษณะการกระทำความผิดที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์อันเป็นการกระทำการโดยมุ่งถึงการได้มาซึ่งข้อมูล รหัส หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ ที่ได้บันทึก พิมพ์ เก็บรักษา หรือบรรจุไว้ในบัตรอิเล็กทรอนิกส์ ไม่ว่าข้อมูลนั้นจะปรากฏให้เห็นได้ด้วยตาเปล่าจากพื้นผิวของบัตรอิเล็กทรอนิกส์นั้นเอง หรือที่ไม่อาจมองเห็นได้ด้วยตาเปล่าซึ่งจะต้องใช้อุปกรณ์อิเล็กทรอนิกส์อื่นๆ ในการแสดงผลของข้อมูลนั้นให้เห็นได้ด้วยตาอีกครั้งหนึ่ง เช่น ข้อมูลหรือรหัสที่ได้บันทึกไว้ในแถบแม่เหล็ก (Magnetic Stripe) หรือในชิป (Chip) ของบัตรอิเล็กทรอนิกส์ หรือข้อมูลบัตรอิเล็กทรอนิกส์ที่ได้บันทึกไว้ในระบบคอมพิวเตอร์

---

[1] โปรดดูหัวข้อที่ 2.2 ลักษณะการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์

การดึงข้อมูลในลักษณะนี้ต้องเป็นการกระทำต่อบัตรอิเล็กทรอนิกส์ของผู้อื่น เพื่อให้ได้มาซึ่งข้อมูลบัตรอิเล็กทรอนิกส์ในครั้งแรกเท่านั้น เปรียบได้กับการกระทำความผิดฐานลักทรัพย์ที่ผู้กระทำลงมือกระทำต่อทรัพย์ อันเป็นการกระทำที่มีลักษณะของการขวนขวายให้ได้มาซึ่งข้อมูลนั้นโดยอาศัยวิธีการดึงข้อมูลในรูปแบบต่างๆ[2] หากเป็นการได้มาซึ่งข้อมูลบัตรอิเล็กทรอนิกส์ในครั้งหลังจากที่เกิดการดึงข้อมูลบัตรอิเล็กทรอนิกส์ในครั้งแรกมาแล้ว จะไม่ถือว่าเป็นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ตามหัวข้อวิทยานิพนธ์ฉบับนี้ เพราะการได้มาซึ่งข้อมูลจากบัตรอิเล็กทรอนิกส์ในครั้งหลังที่นอกเหนือจากการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในครั้งแรกนั้นเปรียบได้กับความผิดฐานรับของโจรที่แม้วัตถุแห่งการกระทำความผิดจะเป็นข้อมูลจากบัตรอิเล็กทรอนิกส์ที่เหมือนกัน แต่ก็มีลักษณะและขั้นตอนในการกระทำความผิดที่แตกต่างกัน กล่าวคือ ด้วยคุณสมบัติพิเศษของการเป็นข้อมูลที่สามารถนำไปทำสำเนาให้เหมือนข้อมูลต้นฉบับได้เป็นอย่างมากมายมหาศาล การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในครั้งแรกจึงเสมือนเป็นการแสวงหาแม่พิมพ์ของข้อมูลซึ่งเป็นกระบวนการที่สำคัญในการกระทำความผิด อันเป็นบ่อเกิดให้เกิดการกระทำความผิดอื่นๆ ที่เกี่ยวกับบัตรอิเล็กทรอนิกส์ตามมาในภายหลัง ซึ่งนอกจากผู้กระทำจะต้องกระทำการในรูปแบบต่างๆ เพื่อขวนขวายให้ได้มาซึ่งข้อมูลแล้ว การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ยังแสดงถึงเจตนาที่ชั่วร้ายต่อข้อมูลบัตรอิเล็กทรอนิกส์ที่อยู่ในความครอบครองของผู้อื่นในขณะนั้นอีกด้วย ซึ่งการได้มาซึ่งข้อมูลบัตรอิเล็กทรอนิกส์ในครั้งหลังนั้นเป็นเพียงการทำสำเนาข้อมูลจากแม่พิมพ์ข้อมูลที่ผู้กระทำความผิดได้ดึงมาดังกล่าวเท่านั้นและไม่ต้องใช้ความขวนขวายในการให้ได้มาซึ่งข้อมูลดังเช่นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในครั้งแรก อีกทั้งผู้วิจัยเห็นว่าสามารถใช้ความผิดฐานมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/6 ลงโทษกับผู้ได้มาซึ่งข้อมูลบัตรอิเล็กทรอนิกส์ในครั้งหลังนั้นได้อยู่แล้ว ด้วยเหตุดังกล่าว การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์จึงเป็นการกระทำความผิดขั้นตอนหนึ่งในความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์อันมีลักษณะที่สำคัญ ซึ่งจะต้องทำการศึกษาวิจัยถึงปัญหาในการนำกฎหมายมาบังคับใช้กับการกระทำความผิดในลักษณะดังกล่าวต่อไป

คำว่า “ดึง” ข้อมูลจากบัตรอิเล็กทรอนิกส์นั้น เป็นคำที่ผู้วิจัยคิดขึ้นเพื่อใช้อธิบายถึงลักษณะและรูปแบบของการกระทำความผิดอันเป็นการกระทำเพื่อให้ได้มาซึ่งข้อมูลจากบัตรอิเล็กทรอนิกส์ซึ่งเป็นคำที่ไม่ปรากฏใช้ในกฎหมายอาญา เพราะผู้วิจัยเล็งเห็นว่าหากใช้คำอื่นๆ ที่นอกเหนือจากคำว่า “ดึง” ดังกล่าวแล้ว จะเป็นการสับสนต่อผู้ที่มาศึกษาวิทยานิพนธ์ฉบับนี้ได้ เช่น หากใช้คำว่า “ได้รับ” ข้อมูลบัตรอิเล็กทรอนิกส์แล้วอาจเกิดปัญหาได้ เพราะคำว่าได้รับในภาษาไทยนั้นแสดงถึงการที่ผู้กระทำความผิดได้กระทำการดึงข้อมูลบัตรอิเล็กทรอนิกส์ด้วยตนเอง หรือแสดงถึงการส่งต่อข้อมูลให้ผู้อื่นให้ได้รับข้อมูลบัตรอิเล็กทรอนิกส์นั้น ซึ่งผู้วิจัยได้กล่าวไปแล้วว่าการดึงข้อมูลจากบัตร

[2] ดูหัวข้อที่ 3.2 รูปแบบการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

อิเล็กทรอนิกส์ต้องเป็นการกระทำเพื่อให้ได้มาซึ่งข้อมูลบัตรอิเล็กทรอนิกส์ในครั้งแรกเท่านั้น ไม่รวมถึงการส่งต่อข้อมูลนั้นให้บุคคลอื่นๆ ด้วย หากใช้คำว่า “ลัก” หรือคำว่า “เอาไป” ก็จะเป็นการซ้ำซ้อนกับความผิดฐานลักทรัพย์ อันเป็นการเอาทรัพย์เคลื่อนที่ในลักษณะตัดกรรมสิทธิ์[3] ซึ่งแตกต่างจากการดึงข้อมูลบัตรอิเล็กทรอนิกส์ที่เป็นเพียงการทำสำเนาของข้อมูลจากบัตรอิเล็กทรอนิกส์เท่านั้น ไม่ใช่การเคลื่อนที่ของข้อมูล ทั้งลักษณะของข้อมูลนั้นยังไม่ถือว่าเป็นทรัพย์อีกด้วย[4] แม้ว่าทั้งการดึงข้อมูลและการลักทรัพย์จะทำให้ผู้กระทำความผิดได้สิ่งต่างๆ เพิ่มขึ้นในความครอบครองของตน แต่ในแง่ของผู้ถูกกระทำนั้น การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นเพียงการทำสำเนาข้อมูลไปจากบัตรอิเล็กทรอนิกส์ ซึ่งไม่ทำให้ผู้ถูกกระทำที่เป็นเจ้าของหรือผู้มีสิทธิใช้บัตร อิเล็กทรอนิกส์ต้องสูญเสียข้อมูลนั้นไปด้วย ต่างจากการลักทรัพย์ที่ทำให้ผู้ถูกกระทำเกิดความสูญเสียในทรัพย์ชิ้นนั้นไป ดังนั้นการใช้คำว่า “ลัก” หรือคำว่า “เอาไป” จึงไม่มีความเหมาะสมกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์และอาจทำให้สับสนกับความผิดฐานลักทรัพย์ ซึ่งมีองค์ประกอบความผิดที่แตกต่างกับการดึงข้อมูลบัตรอิเล็กทรอนิกส์เป็นอย่างมาก หากจะใช้คำว่า “ดักรับ” ก็จะเป็นการซ้ำซ้อนกับความผิดฐานกระทำการโดยมิชอบเพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่น ตามมาตรา 8 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อันเป็นการกระทำความผิดที่มีเครื่องคอมพิวเตอร์มาเกี่ยวข้องและต้องเป็นข้อมูลบัตรอิเล็กทรอนิกส์ที่อยู่ในระหว่างการส่งผ่านของเครื่องคอมพิวเตอร์ด้วยกัน ซึ่งความผิดฐานดักรับข้อมูลคอมพิวเตอร์ตามมาตราดังกล่าวจะสามารถบังคับใช้ได้เฉพาะรูปแบบของการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์โดยการใช้มัลแวร์หรือไวรัสคอมพิวเตอร์เท่านั้น ไม่รวมถึงการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในรูปแบบอื่นๆ ที่ไม่ได้อาศัยการดึงข้อมูลในระหว่างการส่งผ่านข้อมูลของเครื่องคอมพิวเตอร์ เช่น การใช้เครื่องสกิมเมอร์อันเป็นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์โดยตรง หรือการหลอกลวงให้ผู้เป็นเจ้าของหรือผู้มีสิทธิใช้บัตรหลงเชื่อ ดังนั้นการใช้คำว่า “ดักรับ” จึงไม่ครอบคลุมกับลักษณะการดึงข้อมูลอย่างครบถ้วนเช่นกัน ทั้งนี้อาจใช้คำว่า “คัดลอก” หรือคำอื่นๆ ที่คล้ายกันแทนคำว่า “ดึง” ก็ได้แต่ผู้วิจัยคิดว่าอาจจะมีปัญหาในการแปลความในภาษาไทยให้ผิดแผกไปเป็นเรื่องอื่นได้อีก เช่น หากใช้คำว่า “คัดลอก” ก็อาจมีผู้เห็นว่าซ้ำซ้อนกับความผิดฐานปลอมเอกสารได้

ผู้วิจัยจึงเห็นว่า การใช้คำว่า “ดึง” ข้อมูลจากบัตรอิเล็กทรอนิกส์จึงเป็นคำที่เหมาะสมที่สุดอันจะมีการตีความไปในทางอื่นที่นอกเหนือจากวัตถุประสงค์ในการศึกษาวิทยานิพนธ์ฉบับนี้ได้น้อย ป้องกันความสับสนของผู้ศึกษาวิทยานิพนธ์ฉบับนี้กับการกระทำความผิดในฐานอื่นๆ ในกฎหมาย

---

[3] ทวีเกียรติ มีนะกนิษฐ์, คำอธิบายกฎหมายอาญา ภาคความผิดและลหุโทษ, พิมพ์ครั้งที่ 17 (กรุงเทพฯ: สำนักพิมพ์วิญญูชน, 2562), หน้า 321- 324.

[4] โปรดดูคำอธิบายดังกล่าวเพิ่มเติมได้ในหัวข้อที่ 3.4.1.1 ความผิดฐานลักทรัพย์

อาญา และครอบคลุมกับลักษณะของการกระทำความผิดที่เกิดขึ้นอันเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้ครบถ้วน

3.2 รูปแบบการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้นสามารถกระทำการโดยอาศัยรูปแบบในการกระทำได้หลากหลายทั้งที่ใช้อุปกรณ์อิเล็กทรอนิกส์เข้าช่วยเหลือในการกระทำ หรือใช้โปรแกรมคอมพิวเตอร์หรือใช้การหลอกลวงต่างๆ เพื่อให้ผู้เป็นเจ้าของหรือผู้มีสิทธิใช้ข้อมูลบัตรอิเล็กทรอนิกส์นั้นหลงเชื่อ ซึ่งการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้นสามารถจำแนกตามรูปแบบวิธีการที่ใช้ในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้ ดังนี้

3.2.1 การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์โดยการใช้เครื่องดูดข้อมูลแถบรหัสแม่เหล็ก (Skimmer)

3.2.1.1 ความหมายของเครื่องดูดข้อมูลแถบรหัสแม่เหล็ก

เครื่องดูดข้อมูลแถบรหัสแม่เหล็ก (Skimmer) หรือเครื่องสกิมมิ่ง (Skimming Device) หรือสกิมเมอร์ (Skimmer) เป็นเครื่องมืออิเล็กทรอนิกส์ที่ถูกดัดแปลงขึ้นเพื่อทำการดึงข้อมูลจากหน่วยความจำของบัตรอิเล็กทรอนิกส์รูปแบบหนึ่งที่เรียกว่าการสกิมมิ่ง (Skimming) ซึ่งในทางข้อเท็จจริงและทางข้อกฎหมายของนานาประเทศนั้นก็ไม่สามารถกำหนดรูปลักษณ์ของเครื่องมือนี้ได้อย่างแน่นอนเพราะเป็นเครื่องมือที่มีการพัฒนารูปแบบอย่างต่อเนื่องอันมีรูปร่างและลักษณะแตกต่างกันไปตามความก้าวหน้าทางเทคโนโลยีที่อาชญากรจะใช้ในการกระทำความผิด โดยในระยะแรกที่มีการใช้งานนั้น เป็นเพียงการดัดแปลงเครื่องอ่านบัตรอิเล็กทรอนิกส์ที่มีไว้ใช้ในสำนักงานหรือในห้างร้านที่บุคคลสามารถเป็นเจ้าของได้โดยไม่มีความผิดและมีขายอยู่ทั่วไป[5] ซึ่งโดยหลักการพื้นฐานแล้วเครื่องสกิมเมอร์เป็นเพียงเครื่องมืออิเล็กทรอนิกส์ที่ประกอบไปด้วยองค์ประกอบที่สำคัญสองประการ คือ แหล่งพลังงานภายในจากแบตเตอรี่ขนาดเล็กหรือจากแหล่งภายนอก เช่น โซล่าเซลล์ (Solar Cell) เพื่อให้เครื่องสามารถทำงานต่อไปได้ด้วยกำลังไฟฟ้าและหน่วยความจำภายในเครื่องที่ใช้บันทึกข้อมูลจากการดึงข้อมูลบัตรอิเล็กทรอนิกส์ที่สามารถถ่ายโอนไปยังเครื่องมืออิเล็กทรอนิกส์อื่นๆ ต่อไป

---

[5] Aliexpress, "Card Skimmer" [Online], Accessed: 25 July 2020. Available from: https://www.aliexpress.com/w/wholesale-card-skimmer.html.

ได้[6] และโดยระยะหลังได้อาศัยความก้าวหน้าทางเทคโนโลยีอื่นๆ ให้ทำงานประกอบกันเพื่อให้สามารถใช้งานได้ดียิ่งขึ้น เช่น การนำเทคโนโลยีไร้สาย (Wireless) หรือบลูทูธ (Bluetooth) มาใช้หรือการย่อขนาดเครื่องให้มีขนาดเล็กลงหรือบางลงจนยากที่จะถูกตรวจสอบและพบเห็นได้ ดังนั้นเครื่องมือใดจะเรียกว่าเครื่องสกิมเมอร์จึงขึ้นอยู่กับหลักการพื้นฐานดังกล่าวและลักษณะการใช้งานเครื่องมือนั้นว่าเข้าลักษณะเป็นเครื่องสกิมเมอร์หรือไม่ อีกทั้งในปัจจุบันนั้นแม้ว่าจะได้มีการเปลี่ยนรูปแบบบัตรอิเล็กทรอนิกส์จากประเภทแถบแม่เหล็กเป็นประเภทชิปการ์ดแล้วก็ยังพบว่ามีการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์โดยอาศัยเครื่องสกิมเมอร์ได้อยู่ เช่น ในประเทศอังกฤษ[7] ประเทศออสเตรเลีย[8] และการทดสอบโดยผู้เชี่ยวชาญจาก NCR Corporation[9] ซึ่งเป็นบริษัทที่ให้บริการด้านระบบซอฟแวร์และเทคโนโลยีการชำระเงินของสหรัฐอเมริกา

3.2.1.2 ประเภทของเครื่องดูดข้อมูลแถบรหัสแม่เหล็ก

เครื่องดูดข้อมูลแถบรหัสแม่เหล็กนั้นสามารถแยกประเภทตามการใช้งานออกได้เป็น 3 ประเภทดังนี้

3.2.1.2.1 ประเภทติดตั้งกับเครื่องจ่ายเงินอัตโนมัติ (ATM Skimmer)

การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ที่พบเป็นส่วนใหญ่มักกระทำโดยผ่านการติดตั้งเครื่องดูดข้อมูลแถบรหัสแม่เหล็กบนเครื่องจ่ายเงินอัตโนมัติ (Automated teller machine : ATM) โดยจะเรียกการกระทำในลักษณะดังกล่าวว่าเอทีเอ็มสกิมมิ่ง (ATM Skimming) ซึ่งเครื่องดูดข้อมูลแถบรหัสแม่เหล็กจะทำการติดตั้งไว้ที่ช่องสอดบัตรของเครื่องจ่ายเงินอัตโนมัติดังกล่าว โดยการครอบทับช่องเสียบบัตรซึ่งอาชญากรจะทำการดัดแปลงโดยทำให้มีรูปร่างลักษณะคล้ายกับฝาครอบ

---

[6] สัมภาษณ์ วิวัฒน์ สิทธิสรเดช, นักวิทยาศาสตร์ กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง สำนักงานตำรวจแห่งชาติ, 12 มกราคม 2561.

[7] Megan Geuss, "Why Aren't Chip Credit Cards Stopping "Card Present" Fraud in the Us?" [Online], Accessed: 25 July 2020. Available from: https://arstechnica.com/information-technology/2018/11/why-arent-chip-credit-cards-stopping-card-present-fraud-in-the-us/.

[8] Australian Payments Network Limited, "Australian Payment Card Fraud 2018" [Online], Accessed: 25 July 2020. Available from: https://www.auspaynet.com.au/sites/default/files/2018-08/AustralianPaymentCardFraud-2018-eport.pdf.

[9] Megan Geuss, "An ATM hack and a PIN-pad hack show chip cards aren't impervious to fraud" [Online], Accessed: 25 July 2020. Available from: https://arstechnica.com/information-technology/2016/08/an-atm-hack-and-a-pin-pad-hack-show-chip-cards-arent-impervious-to-fraud/.

บนเครื่องจ่ายเงินอัตโนมัติเพื่อนำไปติดตั้งไว้โดยที่ไม่ถูกสังเกตหรือให้มีขนาดเล็กลงหรือบางลงจนสามารถสอดแทรกเข้าไปในช่องเสียบบัตรเดิมของเครื่องจ่ายเงินอัตโนมัตินั้นได้ซึ่งทำให้ตรวจสอบยากยิ่งขึ้นเพื่อใช้ดึงข้อมูลจากแถบแม่เหล็กด้านหลังบัตรอิเล็กทรอนิกส์ โดยเครื่องสกิมเมอร์จะเริ่มทำงานหลังจากได้มีการการสอดบัตรอิเล็กทรอนิกส์ เช่น บัตรเอทีเอ็ม บัตรเดบิต หรือบัตรเครดิต เข้าไปในช่องสอดบัตรของเครื่องจ่ายเงินอัตโนมัติและผู้ใช้บัตรได้กดรหัสผ่านเรียบร้อยแล้วและเครื่องสกิมเมอร์จะทำการบันทึกข้อมูลของบัตรอิเล็กทรอนิกส์ในนั้นเมื่อผู้ใช้บัตรได้ดึงบัตรออกด้วยความรวดเร็วในลักษณะเป็นการรูดครั้งเดียวโดยไม่หยุดชะงักผ่านช่องเสียบบัตรของเครื่องจ่ายเงินอัตโนมัติหลังการใช้งาน[10] พร้อมกับการติดตั้งกล้องขนาดจิ๋ว (Micro Camera) ไว้ในบริเวณใกล้เคียงโดยหันหน้ากล้องไปที่แป้นปุ่มกดรหัสของเครื่องจ่ายเงินอัตโนมัติเพื่อบันทึกว่าผู้ใช้บัตรนั้นได้กดรหัสผ่านอะไรบ้างในการเปิดใช้งานบัตรอิเล็กทรอนิกส์ โดยกล้องขนาดจิ๋วนี้ส่วนใหญ่จะมีขนาดเล็กและผู้กระทำความผิดจะซ่อนได้อย่างแนบเนียนยากต่อการสังเกต เช่น ซ่อนไว้ด้านบนผนังหรือข้างแป้นปุ่มกดของเครื่องเอทีเอ็ม หรือซ่อนไว้โดยติดตั้งบนกล่องแจกโบรชัวร์ของธนาคารที่อยู่ใกล้เคียงกับเครื่องนั้น หรือ ทำการติดตั้งแป้นปุ่มกดปลอม (Keypad Overlays) ครอบลงบนแป้นปุ่มกดที่แท้จริงของเครื่องจ่ายเงินอัตโนมัติ ซึ่งจะบันทึกรหัสนั้นไว้เมื่อผู้ใช้บัตรได้กดรหัสของบัตรลงบนแป้นปุ่มกดปลอม โดยอาชญากรจะมาถอดเครื่องสกิมเมอร์ดังกล่าวพร้อมอุปกรณ์อื่นๆ ออกไปเพื่อนำข้อมูลทั้งสองส่วนนี้ไปใช้ในการทำบัตรปลอมและนำไปกดเงินจากเครื่องจ่ายเงินอัตโนมัติต่อไป

มีข้อสังเกตว่าเครื่องมือที่เกี่ยวข้องที่ใช้ร่วมกันกับเครื่องดูดข้อมูลแถบรหัสแม่เหล็กนั้น เช่น กล้องขนาดจิ๋ว แป้นปุ่มกดปลอม จนถึงเครื่องคอมพิวเตอร์ และเครื่องถ่ายข้อมูลรหัส (Re-encoder) ที่ใช้ถ่ายข้อมูลที่ได้มาจากการดึงนั้นลงในบัตรพลาสติกที่จะทำการปลอม โดยปรกติแล้วการเป็นเจ้าของเครื่องมือเหล่านี้ไม่ถือว่าเป็นความผิดตามกฎหมาย เว้นแต่จะสามารถพิสูจน์เจตนาภายในของผู้กระทำได้ว่ามีเจตนาพิเศษ “เพื่อใช้หรือให้ได้ข้อมูลในการปลอมหรือแปลง” ด้วย ผู้ที่มีเครื่องมือเหล่านี้จึงจะมีความผิดตามมาตรา 269/2 แห่งประมวลกฎหมายอาญา[11]

[10] Deenamtang, "การป้องกัน การ Skimming ขโมยข้อมูล บัตร ATM หรือ บัตร Credit" [ออนไลน์], เข้าถึงเมื่อ 25 กรกฎาคม 2563. แหล่งที่มา: https://www.deenamtang.com/14928366/การป้องกัน-การ-skimming-ขโมยข้อมูล-บัตร-atm-หรือ-บัตร-credit.

[11] สมศักดิ์ เอี่ยมพลับใหญ่, กฎหมายอาญา ภาคความผิดเกี่ยวกับความเท็จ การปลอมและการแปลง, พิมพ์ครั้งที่ 1 (กรุงเทพฯ: สำนักพิมพ์นิติธรรม, 2554), หน้า 208.

3.2.1.2.2 ประเภทใช้งานในขนาดพกพา (Handheld Skimmer)

เครื่องดูดข้อมูลแถบรหัสแม่เหล็กนั้นนอกจากจะมีประเภทที่ใช้ติดตั้งกับเครื่องมืออิเล็กทรอนิกส์อื่นแล้ว ยังมีประเภทขนาดพกพาหรือเครื่องแฮนด์เฮลด์สกิมเมอร์ (Handheld Skimmer) ซึ่งเป็นเครื่องดูดข้อมูลแถบรหัสแม่เหล็กขนาดเล็กที่สามารถพกพาได้ซึ่งอาชญากรมักจะถือไว้ในฝ่ามือและนำบัตรของเหยื่อมารูดผ่านเครื่องดังกล่าวพร้อมทั้งแอบดูรหัสบัตรจากด้านหลังบัตรโดยไม่ให้เหยื่อสังเกตเห็น ซึ่งอาจเกิดการกระทำผิดขึ้นที่ใดก็ได้ ไม่ว่าจะเป็นร้านค้า ร้านอาหาร สถานีบริการน้ำมัน หรืออาชญากรอาจแอบอ้างเป็นพนักงานธนาคารยืนหน้าตู้เอทีเอ็มเพื่อขอดูบัตรของเหยื่อหรืออาจทำทีเสนอความช่วยเหลือแก่เหยื่อหากบัตรที่ใช้งานติดขัด[12] แล้วทำการดึงข้อมูลผ่านเครื่องแฮนด์เฮลด์สกิมเมอร์เมื่อเหยื่อเผลอด้วยความรวดเร็ว[13]

3.2.1.2.3 ประเภทติดตั้งกับปั๊มแก๊ส (Gas Pump Skimmer)[14]

กรณีดังกล่าวมักพบได้บ่อยครั้งในประเทศที่ผู้ใช้บริการปั๊มน้ำมันจะต้องบริการตนเอง (Self Service) เช่น สหรัฐอเมริกา ที่มีเหยื่อจากการกระทำดังกล่าวมากถึง 23 เปอร์เซ็นต์ของผู้ใช้งานปั๊มน้ำมันทั้งหมดในปี 2019[15] โดยที่ผู้เติมน้ำมันจะต้องกดเติมน้ำมันและต้องจ่ายเงินค่าน้ำมันผ่านเครื่องปั๊มน้ำมันด้วยตนเอง โดยอาชญากรอาจลักลอบนำไปติดตั้งเองหรือติดสินบนพนักงานในปั๊มน้ำมันที่มีพนักงานคอยบริการรูดบัตรให้ ซึ่งเครื่องดูดข้อมูลดังกล่าวมีความคล้ายคลึงกับประเภทที่ติดตั้งกับเครื่องจ่ายเงินอัตโนมัติ คือเป็นการติดตั้งเครื่องสกิมเมอร์ไว้ที่ช่องเสียบบัตรของปั๊มน้ำมันพร้อมกับติดตั้งแป้นปุ่มกดปลอมครอบแป้นปุ่มกดที่แท้จริงไว้ด้วย แล้วเชื่อมต่อกับแหล่งพลังงานไฟฟ้าของปั๊มน้ำมันทำให้เครื่องสกิมเมอร์ลักษณะนี้ทำงานได้อย่างต่อเนื่องโดยไม่ต้องอาศัยแบตเตอรี่ และพบว่ามีการใช้เทคโนโลยีไร้สาย (Wireless) แบบบลูทูธ (Bluetooth) หรือแบบข้อความมือถือ (SMS) ในการส่งผ่านข้อมูลที่เครื่องสกิมเมอร์นั้นดึงมาได้ให้กับอาชญากรในระยะไกล

---

[12] โพสต์ทูเดย์, "จับโจรฝรั่งเศสฉกข้อมูลบัตรเครดิตจับโจรฝรั่งเศสฉกข้อมูลบัตรเครดิต" [ออนไลน์], เข้าถึงเมื่อ 25 กรกฎาคม 2563. แหล่งที่มา: https://www.posttoday.com/social/general/279509.

[13] ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย, "กลโกงบัตรต่างๆ" [ออนไลน์], เข้าถึงเมื่อ 20 กุมภาพันธ์ 2561. แหล่งที่มา: https://www.1213.or.th/th/finfrauds/CardFraud/Pages/CardFraud.aspx.

[14] Brian Krebs, "Gas Theft Gangs Fuel Pump Skimming Scams" [Online], Accessed: 25 July 2020. Available from: https://krebsonsecurity.com/tag/gas-pump-skimmers/.

[15] Los Angeles and Southern California News, "How to Spot a Gas Pump Skimmer" [Online], Accessed: 25 July 2020. Available from: https://abc7chicago.com/gas-skimmer-pump-credit-card-quick-tip/5413649/.

ซึ่งอาชญากรไม่จำต้องมาถอดเก็บเครื่องดังกล่าวออกไปเลยอันเป็นการลดความเสี่ยงในการถูกพบเห็นและถูกจับกุม

3.2.1.2.4 ประเภทใช้งานที่จุดชำระเงิน (Point of Sale Skimmer)[16]

กรณีดังกล่าวเป็นการใช้เครื่องสกิมเมอร์ ณ จุดชำระเงินหรือจุดที่ลูกค้าของธนาคารหรือห้างร้านมาทำธุรกรรมกับอาชญากรที่เป็นพนักงานธนาคารหรือห้างร้านนั้นๆ (Clerk Skim) โดยการใช้บัตรอิเล็กทรอนิกส์ในการชำระเงินค่าสินค้าหรือบริการ เช่น การใช้บัตรเครดิตในการซื้อสินค้าที่พนักงานจะนำบัตรเครดิตไปเข้าเครื่องจ่ายเงินแล้วนำใบเสร็จมาให้ลงลายมือชื่อ หรือเกิดจากการสับเปลี่ยนเครื่องชำระเงินด้วยบัตรอิเล็กทรอนิกส์ของจริงกับเครื่องสกิมเมอร์โดยอาศัยจังหวะเผลอของพนักงานดังกล่าว (POS Swaps)[17] ซึ่งหลักการทำงานนั้นยังมีรูปแบบพื้นฐานเดียวกันกับเครื่องสกิมเมอร์ทั่วๆ ไป คือ ภายในมีแบตเตอรี่และแหล่งบันทึกข้อมูลและภายนอกมีแป้นปุ่มกดปลอมที่คอยบันทึกรหัสบัตรอิเล็กทรอนิกส์ดังกล่าวไว้

3.2.2 การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์โดยการใช้มัลแวร์หรือไวรัสคอมพิวเตอร์ (Malware or Virus Computer)

ด้วยเทคโนโลยีที่พัฒนาขึ้น นอกจากการใช้เครื่องดูดข้อมูลแถบรหัสแม่เหล็กแล้วยังพบว่าผู้กระทำความผิดอาจใช้โปรแกรมประเภทมัลแวร์ (Malware) หรือเรียกชื่อในลักษณะอื่นๆ ที่เป็นโปรแกรมในลักษณะเดียวกันนี้ว่าเป็น ไวรัสคอมพิวเตอร์ (Virus) วอร์ม (Worm) โทรจัน (Trojan) สปายแวร์ (Spyware) เป็นต้น ซึ่งเป็นโปรแกรมคอมพิวเตอร์ที่บุกรุกเข้าไปในเครื่องคอมพิวเตอร์โดยมิได้รับความยินยิมจากผู้ใช้ โดยมีความสามารถในการทำสำเนาตัวเองและสอดแทรกตัวสำเนานั้นเข้าไปในรหัสคอมพิวเตอร์ที่เป็นส่วนของข้อมูลเอกสารหรือที่เป็นระบบปฏิบัติการได้ ซึ่งเปรียบเสมือนกับไวรัสในทางชีววิทยาที่สามารถแพร่กระจายตัวเข้าไปในเซลล์ของสิ่งมีชีวิตในลักษณะเดียวกัน ซึ่งมัลแวร์หรือไวรัสนั้นมีอยู่หลายชนิด บางชนิดเพียงก่อให้เกิดความรำคาญแก่การใช้งานเครื่องคอมพิวเตอร์ หรือบางชนิดก็ใช้ในการทำลายข้อมูล หรือการดึงข้อมูลอย่างในลักษณะที่กล่าวถึงนี้

---

[16] Brian Krebs, "Simple but Effective Point-of-Sale Skimmer" [Online], Accessed: 25 July 2020. Available from: https://krebsonsecurity.com/tag/pos-skimmer/.

[17] Robert Siciliano, "Point of Sale Skimming Attacks and Pci Standards" [Online], Accessed: 25 July 2020. Available from: https://www.thebalance.com/what-are-point-of-sale-skimming-attacks-and-pci-1947471.

เป็นต้น ซึ่งจะฝังตัวอยู่ในหน่วยความจำของเครื่องคอมพิวเตอร์และจะทำงานเมื่อมีการเรียกใช้งานโปรแกรมหรือไฟล์ใดๆ ในเครื่องคอมพิวเตอร์ดังกล่าว[18] ซึ่งในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ที่อยู่ในคอมพิวเตอร์หรือระบบคอมพิวเตอร์นี้ ผู้กระทำความผิดจะทำการติดตั้งมัลแวร์หรือไวรัสนั้นลงไปในเครื่องกดเงินอัตโนมัติผ่านช่องสอดบัตรอิเล็กทรอนิกส์ หรือผ่านการส่งเป็นสแปมอีเมล (Spam Email) เข้าไปในเครื่องคอมพิวเตอร์ของเหยื่อ เพื่อให้มัลแวร์หรือไวรัสนั้นทำการดึงข้อมูลที่ได้บันทึกไว้ในเครื่องจ่ายเงินอัตโนมัติหรือเครื่องคอมพิวเตอร์เมื่อคอมพิวเตอร์นั้นได้มีการบันทึกหรืออ่านข้อมูลจากบัตรอิเล็กทรอนิกส์จากการใช้งานบัตรดังกล่าว และส่งข้อมูลที่ได้รับมานั้นกลับไปยังเครื่องคอมพิวเตอร์ของผู้กระทำความผิด อีกทั้งทำสำเนาตัวเองเพื่อกระจายเข้าสู่เครื่องคอมพิวเตอร์หรือเครื่องจ่ายเงินอัตโนมัติเครื่องอื่นๆ ผ่านระบบเครือข่ายอินเตอร์เน็ต[19] ต่อไป ซึ่งอาจพบการใช้มัลแวร์หรือไวรัสดังกล่าวได้ที่จุดชำระเงิน (POS Malware)[20] ของห้างร้านต่างๆ ได้ด้วยเช่นกัน

การขูดหน่วยความจำ (Memory Scrapers) คือประเภทของมัลแวร์ที่พบได้บ่อยในการใช้ดึงข้อมูลบัตรอิเล็กทรอนิกส์จากแรม (Random Access Memory : RAM) ของเครื่องคอมพิวเตอร์ ณ จุดชำระเงิน ซึ่งมีหลากหลากโปรแกรมด้วยกัน เช่น Torpig Blackshades SpyEye Citadel POSCardStealer Alina และ ProjectHook โดยมีการใช้เทคนิคต่างๆ ร่วมด้วย เช่น การฉีดผ่านระบบเว็บ (Web Injects) การบันทึกการกดแป้นพิมพ์ (Keystroke Loggers) และการใช้ตัวจับบัตรเครดิต (Credit Card Grabbers)[21]

ตัวอย่างการกระทำความผิดในกรณีนี้ เช่น ในคดี United States v. Bonilla (2009)[22] ซึ่งผู้กระทำความผิดได้ติดตั้งโปรแกรมมัลแวร์ลงในคอมพิวเตอร์ที่ใช้ในโรงแรมหลายแห่งในพื้นที่ ด้วยผลจากการนั้นทำให้ผู้กระทำความผิดได้รับข้อมูลส่วนบุคคลและข้อมูลทางการเงินของลูกค้าที่เข้ามาพักในโรงแรมและใช้งานเครื่องคอมพิวเตอร์ดังกล่าวเป็นจำนวนมาก เช่น รหัสในการเข้าใช้งาน บัญชีธนาคาร ต่อมาผู้กระทำความผิดนั้นได้นำข้อมูลที่ได้ไปในการทำบัตรเครดิตปลอมและใช้บัตรปลอมนั้น

---

[18] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, หน้า 261.

[19] Pwchk.com, "Atm Fraud: Do You Know If Your Customer's Card Data Has Been Compromised?" [Online], Accessed: 25 November 2017. Available from: https://www.pwchk.com/en/risk-assurance/ra-atm-fraud-aug2016.pdf.

[20] Robert Siciliano, "Point of Sale Skimming Attacks and PCI Standards" [Online], Accessed: 25 July 2020. Available from: https://www.thebalance.com/what-are-point-of-sale-skimming-attacks-and-pci-1947471.

[21] Joana Vasiu and Lucian Vasiu, "Riders on the Storm: An Analysis of Credit Card Fraud Cases," Suffolk Journal of Trial & Appellate Advocacy, 20 (2015): 203-204.

[22] United States v. Bonilla (11th Cir. 2009)

หรือเข้าบัญชีของลูกค้าจากรหัสที่ได้รับดังกล่าวนั้นเพื่อโอนเงินให้แก่ตนเอง ในการซื้ออุปกรณ์อิเล็กทรอนิกส์ สินค้าฟุ่มเฟือย นำไปใช้จ่ายในประเทศและนำไปใช้ในการท่องเที่ยวต่างประเทศ

3.2.3 การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์โดยการหลอกลวงอื่นๆ

การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นอกจากการใช้เครื่องสกิมเมอร์ การใช้มัลแวร์หรือไวรัสคอมพิวเตอร์แล้ว ยังมีการหลอกลวงอื่นๆ ซึ่งมักจะเป็นรูปแบบของการหลอกลวงผู้เป็นเจ้าของบัตรอิเล็กทรอนิกส์ให้หลงผิดหรือเข้าใจผิด โดยมีการกระทำที่พบได้ดังนี้

3.2.3.1 การหลอกลวงโดยการสอบถามทางโทรศัพท์ (Call - Centre Scammers)

การหลอกลวงโดยการสอบถามทางโทรศัพท์เป็นวิธีการหนึ่งที่พบการกระทำความผิดอย่างมากในประเทศไทย ซึ่งประเทศไทยและประเทศที่อยู่ในภูมิภาคเอเชียตะวันออกเฉียงใต้มักเป็นแหล่งกบดานที่สำคัญของกลุ่มมิจฉาชีพดังกล่าวโดยเป็นการร่วมมือระหว่างชาวต่างชาติและคนไทย[23] เช่น ชาวฝรั่งเศส ชาวเบลเยี่ยม ชาวจีน ชาวตุรกี โดยใช้วิธีการโทรศัพท์ไปหลอกลวงเหยื่อผู้เสียหายโดยการปลอมเป็นเจ้าหน้าที่ธนาคาร เจ้าหน้าสรรพากรหรือตำรวจ โดยการหลอกลวงว่าบัญชีของเหยื่อนั้นมีเหตุขัดข้อง ถูกอายัด ติดหนี้บัตรเครดิต ข้อมูลในบัญชีสูญหาย หรือเกี่ยวข้องกับองค์กรอาชญากรรมประเภทยาเสพติดหรือการฟอกเงิน[24] เพื่อให้เหยื่อนั้นบอกเลขบัตรประจำตัวประชาชน เลขบัญชี ชื่อบัญชี รหัสบัตรอิเล็กทรอนิกส์ต่างๆ ให้ ซึ่งมักมีเป้าหมายเป็นผู้สูงอายุที่เกษียณแล้วเพราะเหยื่อเหล่านี้มักจะมีเงินเก็บในบัญชีธนาคารจำนวนมาก[25]

---

[23] Bangkokpost, "Cops Nab 10 for Call Centre Fraud Scam" [Online], Accessed: 25 July 2020. Available from: https://www.bangkokpost.com/thailand/general/1832039/cops-nab-10-for-call-centre-fraud-scam.

[24] ธนาคารไทยพาณิชย์, "กลโกงแก๊งคอลเซ็นเตอร์ รู้ทันไม่เสียที" [ออนไลน์], เข้าถึงเมื่อ 25 กรกฎาคม 2563. แหล่งที่มา: https://www.scb.co.th/th/personal-banking/stories/gang-callcenter.html.

[25] Hua Hin Today, "Call Center Scam" [Online], Accessed: 25 July 2020. Available from: https://www.huahintoday.com/sports/call-center-scam/.

3.2.3.2 การหลอกลวงโดยการปลอมเว็บไซต์ (Fake, Fraudulent or Scam Websites)

การหลอกลวงโดยการปลอมเว็บไซต์ คือ การหลอกลวงเหยื่อผู้เป็นเจ้าของบัตรอิเล็กทรอนิกส์โดยการใช้หน้าเว็บไซต์ปลอมเพื่อให้เหยื่อเข้าใจว่าหน้าเว็บไซต์ดังกล่าวเป็นหน้าเว็บไซต์ที่แท้จริง ซึ่งเว็บไซต์ปลอมดังกล่าวจะมีช่องให้ผู้เป็นเจ้าของบัตรอิเล็กทรอนิกส์กรอกข้อมูล ไม่ว่าจะเป็น ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) หมายเลขบัตรเครดิต วันหมดอายุ รหัส CVV ของบัตร เป็นต้น โดยที่เว็บไซต์ปลอมดังกล่าวจะมีชื่อที่อยู่เว็บไซต์ (Domain Name) แตกต่างจากเว็บไซต์ที่แท้จริงของธนาคารหรือห้างร้านเหล่านั้น[26] แต่อาจมีความคล้ายคลึงกันจนยากที่จะแยกได้ว่าเว็บไซต์ใดคือเว็บไซต์ที่แท้จริง จนทำให้ธนาคารพาณิชย์ต่างๆ ที่มีหน้าเว็บไซต์ของตนเองจำเป็นต้องออกมาชี้แจงแก่ลูกค้าของตนถึงข้อสังเกตเว็บไซต์ที่แท้จริง[27]

3.2.3.3 การหลอกลวงโดยการส่งจดหมายอิเล็กทรอนิกส์ปลอม (Phishing)

การหลอกลวงโดยการส่งจดหมายอิเล็กทรอนิกส์ปลอมหรือฟิชชิ่ง (Phishing) เป็นคำพ้องเสียงมาจากคำว่าฟิชชิ่ง (Fishing) ที่แปลว่าการตกปลาให้มาติดเบ็ด ซึ่งเป็นการสร้างสถานการณ์โดยการส่งข้อความหรืออีเมลเข้าสู่อีเมลของผู้ใช้บัตรอิเล็กทรอนิกส์ โดยอ้างว่าข้อมูลของเหยื่อนั้นโดนใช้งานโดยผู้ใช้อื่น ซึ่งให้เหยื่อนั้นรีบเปลี่ยนข้อมูลส่วนตัวโดยทันทีตามเว็บไซต์ปลอมที่ได้แนบมาด้วย และโดยใช้การกล่าวอ้าง ตราโลโก้ (Logo) หรือรูปแบบเว็บไซต์ ให้ดูเหมือนว่ามาจากหน่วยงานหรือองค์กรที่แท้จริง ซึ่งทำให้เยื่อที่หลงเชื่อทำการกรอกข้อมูลส่วนตัวต่างๆ ไม่ว่าจะเป็น ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) หมายเลขบัตรเครดิต วันหมดอายุ รหัส CVV ของบัตร เป็นต้น ลงในเว็บไซต์ปลอมนั้น หรือส่งโปรแกรมที่มีมัลแวร์หรือไวรัสคอมพิวเตอร์เพื่อให้ติดตั้งลงบนเครื่องคอมพิวเตอร์อันจะทำการดึงข้อมูลบัตรอิเล็กทรอนิกส์ เมื่อเหยื่อได้กรอกลงไปในเว็บไซต์ต่างๆ เป็นต้น[28]

---

[26] Australian competition and consumer commission, "Online Shopping Scams" [Online], Accessed: 25 July 2020. Available from: https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/online-shopping-scams.

[27] ธนาคารกรุงไทย, "เตือนเว็บไซต์ปลอม หลอกโจรกรรมข้อมูลส่วนตัว" [ออนไลน์], เข้าถึงเมื่อ 25 กรกฎาคม 2563. แหล่งที่มา: https://krungthai.com/th/content/financial-partner/security-tips-for-digital-life/web-phishing.

[28] บรรณศักดิ์ ยุวมิตร, "Phishing คืออะไร ป้องกันอย่างไร" [ออนไลน์], เข้าถึงเมื่อ 25 กรกฎาคม 2563. แหล่งที่มา: https://www.catcyfence.com/it-security/article/what-is-phishing/.

3.3 ปัญหาการขาดบทบัญญัติในการลงโทษสำหรับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

3.3.1 ปัญหาจากคำนิยาม ตามมาตรา 1(14)

จากความหมายของคำว่า “บัตรอิเล็กทรอนิกส์” ตามมาตรา 1(14) ทั้ง (ก) และ (ข) พบว่า มาตรา 1(14)(ก) นั้นระบุให้ “เอกสารหรือวัตถุอื่นใด” เป็น “บัตรอิเล็กทรอนิกส์” โดยมุ่งถึงตัวบัตรที่เป็นกายภาพ หรือรูปธรรมเป็นสำคัญ และมาตรา 1(14)(ข) ระบุให้ “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” เป็น “บัตรอิเล็กทรอนิกส์” ด้วย โดยมุ่งถึงข้อมูลเกี่ยวกับบัตรนั้นที่เป็นนามธรรมเป็นสำคัญ แต่เนื่องจาก มาตรา 1(14)(ข) ได้ระบุเพิ่มเติมต่อไปด้วยว่าข้อมูลที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้นั้นต้อง “มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้” ด้วยจึงจะเข้าความหมายของคำว่า “บัตรอิเล็กทรอนิกส์”

ผลดังกล่าวจึงทำให้ “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” ที่ “มีการออกเอกสารหรือวัตถุอื่นใดให้” ด้วยนั้น ไม่เป็น “บัตรอิเล็กทรอนิกส์” ตามคำนิยามใน มาตรา 1(14) ซึ่งส่งผลให้ “เอกสารหรือวัตถุอื่นใด” ตามมาตรา 1(14)(ก) ที่เป็น “บัตรอิเล็กทรอนิกส์” ที่มี “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” อยู่ในตัวบัตรที่มีการ “ออกเอกสารหรือวัตถุอื่นใดให้” ด้วยนั้น ถูกตีความโดยนักกฎหมายไทยหลายท่าน[29] ว่า “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” ที่อยู่ในบัตรที่มีการออกให้นั้น ไม่เป็น “บัตรอิเล็กทรอนิกส์” ในความหมายตามมาตรา 1(14) ด้วย

นั่นหมายความว่า หากมีการกระทำความผิดแก่ “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” ที่อยู่ในบัตร “ที่มีการออกให้” นั้น ไม่ว่าข้อมูลดังกล่าวจะปรากฏอยู่บนตัวพื้นผิวของบัตรใบนั้น[30] หรือเป็นข้อมูลที่ถูกจัดเก็บในหน่วยบันทึกความจำของบัตรนั้น ก็จะไม่เป็นการกระทำความผิดต่อ “บัตรอิเล็กทรอนิกส์” ตามประมวลกฎหมายอาญา อันส่งผลให้บทบัญญัติที่มีวัตถุแห่งการกระทำเป็น “บัตรอิเล็กทรอนิกส์” ในภาค 2 ลักษณะ 7 หมวด 4 ใน “ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์” ที่ได้แก้ไขเพิ่มเติมใน พ.ศ.2547 ตั้งแต่มาตรา 269/1 ถึง มาตรา 269/7 นั้น ไม่สามารถใช้ในการลงโทษแก่ผู้กระทำความผิดได้โดยตรง ทั้งที่บทบัญญัติในหมวดดังกล่าวที่ได้แก้ไขเพิ่มเติมขึ้นนั้น มีวัตถุประสงค์เพื่อ “กำหนดความผิดอาญาสำหรับการกระทำ

---

[29] เช่น ดร.เกียรขจร วัจนะสวัสดิ์, วีระวัฒน์ ปวาราจารย์, สมศักดิ์ เอี่ยมพลับใหญ่, สมศักดิ์ เธียรจรูญกุล

[30] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, พิมพ์ครั้งที่ 6 (กรุงเทพฯ: กรุงสยามพับลิชชิ่ง, 2557), หน้า 306.

ความผิดเกี่ยวกับบัตรและข้อมูลอิเล็กทรอนิกส์” อันเป็น “การกระทำความผิดเกี่ยวกับบัตรและลักลอบนำข้อมูลอิเล็กทรอนิกส์ของผู้อื่นมาใช้”[31] ซึ่งได้ระบุเป็นหมายเหตุท้าย พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547 โดยให้มีการกำหนดฐานความผิดเกี่ยวกับ “บัตร” และ “ข้อมูลอิเล็กทรอนิกส์” ในบัตรนั้นด้วย แต่เนื่องจากลักษณะการกำหนดความหมายในมาตรา 1(14) นั้นเอง ทำให้ไม่ครอบคลุม “ข้อมูลอิเล็กทรอนิกส์” ในบัตร “ที่มีการออกเอกสารหรือวัตถุอื่นใดให้” ด้วย การบัญญัติกฎหมายกล่าวจึงไม่ครอบคลุมการกระทำความผิดโดยตรง[32] ทั้งหมดที่เกิดขึ้นในทางข้อเท็จจริงอันเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

3.3.2 ปัญหาการนำบทบัญญัติในหมวดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์มาใช้กับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

หากพิจารณาความผิดทุกมาตราในหมวดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ จะพบว่าหากวัตถุแห่งการกระทำความผิดใดเข้าความหมายของคำว่า “บัตรอิเล็กทรอนิกส์” ตามมาตรา 1(14) แล้ว ไม่ว่าจะใน (ก) (ข) หรือ (ค) ก็ตาม ผู้กระทำความผิดต้องถูกลงโทษตามมาตราต่างๆ ที่ได้บัญญัติไว้ในหมวดดังกล่าวได้ทุกมาตรา เช่น ความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/1 ฐานทำหรือมีเครื่องมือในการปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/2 หรือฐานใช้หรือมีไว้เพื่อใช้บัตรอิเล็กทรอนิกส์ปลอม ตามมาตรา 269/4

ปัญหาต่อมาจึงเป็นปัญหาที่เกี่ยวเนื่องมาจากความหมายของคำว่า “บัตรอิเล็กทรอนิกส์” ตามหัวข้อที่ 3.3.1 ซึ่งเป็นปัญหาว่าการกระทำความผิดอันเป็นการทำต่อ “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” ที่อยู่ในบัตร “ที่มีการออกเอกสารหรือวัตถุอื่นใดให้” ซึ่งไม่เป็น “บัตรอิเล็กทรอนิกส์” ตามคำนิยามในมาตรา 1(14) นั้น หากมีการกระทำการดึงข้อมูลใดๆ ที่อยู่ในบัตรอิเล็กทรอนิกส์ดังกล่าว จะสามารถนำบทบัญญัติมาตราใดในหมวดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ตามประมวลกฎหมายอาญา มาปรับใช้เพื่อลงโทษผู้กระทำได้บ้างหรือไม่ เพียงใด และจะเกิดอุปสรรคในการนำมาปรับใช้อย่างไร

---

[31] หมายเหตุท้าย พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547

[32] แม้ไม่ครอบคลุมโดยตรงแต่อาจอาศัยการตีความบทบัญญัติอื่นๆ เพื่อลงโทษผู้กระทำความผิดได้ซึ่งจะขัดกับหลัก “กฎหมายอาญาต้องตีความอย่างเคร่งครัด” เช่น การนำมาตรา 269/2 มาปรับใช้เพื่อลงโทษผู้กระทำความผิด

3.3.2.1 การนำความผิดฐานปลอมบัตรอิเล็กทรอนิกส์มาปรับใช้

การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ จะถือว่าเป็นความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/1 หรือไม่ ซึ่งการจะพิจารณาปัญหาดังกล่าว จำต้องพิจารณาถึงองค์ประกอบภายนอกส่วนของการกระทำในความผิดฐานปลอมเอกสารเสียก่อน ซึ่งมาตรา 269/1 นั้นมีองค์ประกอบภายนอกส่วนของการกระทำ แบ่งออกได้เป็น 2 ลักษณะดังนี้[33]

(ก) ทำบัตรอิเล็กทรอนิกส์ปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด

การทำบัตรอิเล็กทรอนิกส์ปลอม ตามมาตรา 269/1 นั้น เป็นความผิดทำนองเดียวกันกับการปลอมเอกสาร ตามมาตรา 264[34] และมีความคล้ายคลึงกัน[35] ดังนั้นในการพิจารณาการกระทำที่เป็นการทำบัตรอิเล็กทรอนิกส์ปลอมนี้ จึงสามารถนำวิธีการในการปลอมเอกสารมาพิจารณาประกอบกันได้ เพื่อพิจารณาว่าการดึงข้อมูลจะเป็นการทำบัตรอิเล็กทรอนิกส์ปลอม อันเป็นความผิดฐานปลอมบัตรอิเล็กทรอนิกส์หรือไม่

ลักษณะของการดึงข้อมูลบัตรอิเล็กทรอนิกส์นั้น เป็นการกระทำในรูปแบบต่างๆ เพื่อให้ได้มาซึ่งข้อมูลที่บันทึกไว้ในบัตรอิเล็กทรอนิกส์ อันเป็นการคัดลอกหรือทำสำเนาข้อมูลในบัตรอิเล็กทรอนิกส์ ซึ่งโดยปกติแล้วหากเป็นเรื่องเอกสาร การทำสำเนาเอกสารย่อมเป็นความผิดฐานปลอมเอกสาร ตามมาตรา 264 ได้[36] หากใช้เหตุผลดังกล่าวเพียงประการเดียว การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ซึ่งมีลักษณะเป็นการคัดลอกหรือทำสำเนาข้อมูลเช่นกัน ก็ย่อมเป็นความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/1 ด้วยซึ่งนักกฎหมายบางส่วนอาจจะมีความเห็นไปในแนวทางดังกล่าว แต่จากการศึกษาวิจัยพบว่า ผลสรุปดังกล่าวนั้นไม่น่าจะถูกต้องด้วยเหตุผลอันแสดงได้ดังนี้

---

[33] มาตรา 269/1 “ผู้ใดทำบัตรอิเล็กทรอนิกส์ปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด เติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใด ๆ ในบัตรอิเล็กทรอนิกส์ที่แท้จริง โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ถ้าได้กระทำเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นบัตรอิเล็กทรอนิกส์ที่แท้จริงหรือเพื่อใช้ประโยชน์อย่างหนึ่งอย่างใด ผู้นั้นกระทำความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงห้าปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนบาท”

[34] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, คำอธิบายความผิดเกี่ยวกับการปลอมและการแปลงตามประมวลกฎหมายอาญา, พิมพ์ครั้งที่ 1 (กรุงเทพฯ: สำนักพิมพ์วิญญูชน, 2555), หน้า 163.

[35] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 314.

[36] เรื่องเดียวกัน, หน้า 163.

1. คุณธรรมทางกฎหมายในความผิดฐานปลอมเอกสาร คือ ความน่าเชื่อถือไว้วางใจต่อเอกสาร[37] และคุณธรรมทางกฎหมายในความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ คือ ความมั่นคงและความเชื่อถือในการใช้บัตรอิเล็กทรอนิกส์หรือในข้อมูลของบัตรอิเล็กทรอนิกส์[38] ซึ่งการกระทำการปลอมนั้นจะกระทบต่อการใช้งานสิ่งต่างๆ เหล่านี้ในฐานะหลักฐานในการอ้างอิง ลดความยอมรับ ความน่าเชื่อถือของตัวบัตรอิเล็กทรอนิกส์หรือข้อมูลในบัตรอิเล็กทรอนิกส์ที่ได้รับความคุ้มครองลงไป[39] ดังนั้น การอ่านเอกสาร การดูข้อมูลในบัตรอิเล็กทรอนิกส์หรือแม้กระทั่งการดึงเอาข้อมูลจากบัตรอิเล็กทรอนิกส์ไปโดยที่ยังไม่ได้กระทำสิ่งใดเพิ่มเติมแต่เพียงเท่านี้ น่าจะไม่กระทบต่อคุณธรรมทางกฎหมายดังกล่าวและไม่เป็นความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ในขณะที่การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์จะมุ่งถึงการคุ้มครองข้อมูลส่วนบุคคลในฐานะสิทธิมนุษยชนขั้นพื้นฐานที่สำคัญในความเป็นส่วนตัวของประชาชน (Privacy Right) ตั้งแต่แรก เช่น ในสหรัฐอเมริกานั้นเพียงแต่การอ่าน (Reading) ก็ถือว่าการคุ้มครองข้อมูลของบุคคลได้ถูกกระทบแล้ว[40] คุณธรรมหรือความคุ้มครองทางกฎหมายจึงแตกต่างกัน

2. บทบัญญัติความผิดต่างๆ ในหมวดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตั้งแต่มาตรา 269/1 ถึง มาตรา 269/7 มีลักษณะที่ล้อกับบทบัญญัติในหมวดอื่นๆ ในลักษณะที่ 7 ความผิดเกี่ยวกับการปลอมและการแปลง ตามประมวลกฎหมายอาญา ทำให้มีลักษณะการเรียงมาตราและการใช้คำในบทบัญญัติที่ใกล้เคียงกันภายในลักษณะดังกล่าว แต่ความพิเศษที่ทำให้หมวดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์แตกต่างไปจากหมวดอื่นๆ นั่นก็คือ บัตรอิเล็กทรอนิกส์นั้นประกอบไปด้วยลักษณะที่แตกต่างกันถึง 3 แบบด้วยกันคือ (1) บัตรหรือวัตถุอื่นใดในลักษณะที่จับต้องได้ (Physical Cards) ในมาตรา 1(14)(ก) หรือ (2) ข้อมูล รหัส หมายเลขชุดทางอิเล็กทรอนิกส์ใดๆ ในลักษณะที่จับต้องไม่ได้ (Virtual Cards) ในมาตรา 1(14)(ข) หรือ (3) เอกลักษณ์ทางชีวภาพของบุคคลในลักษณะที่เป็นส่วนหนึ่งของมนุษย์ (Biometric data) ในมาตรา 1(14)(ค) อันส่งผลให้การปลอมบัตรอิเล็กทรอนิกส์มีลักษณะการกระทำที่พิเศษกว่าการปลอมในหมวดอื่นๆ ในกฎหมาย

---

[37] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, คำอธิบายความผิดเกี่ยวกับการปลอมและการแปลงตามประมวลกฎหมายอาญา, หน้า 119.

[38] คณิต ณ นคร, กฎหมายอาญาภาคความผิด, พิมพ์ครั้งที่ 11 (กรุงเทพฯ: สำนักพิมพ์วิญญูชน, 2559), หน้า 685.

[39] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, คำอธิบายความผิดเกี่ยวกับการปลอมและการแปลงตามประมวลกฎหมายอาญา, หน้า 163.

[40] Charles Doyle, “Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws” [Online], Accessed: 20 October 2020. Available from: https://www.everycrsreport.com/files/20141015_97-1025_31056cd16cc55cc39047e24e327a15875045157f.pdf.

ลักษณะเดียวกัน กล่าวคือ หากเป็นการปลอมเงินตรา ดวงตา แสตมป์ ตั๋ว เอกสารหรือหนังสือเดินทาง เพียงแค่ทำการคัดลอกหรือทำสำเนาขั้นตอนเดียวก็เป็นอันเสร็จสิ้น ในขณะที่การปลอมบัตรอิเล็กทรอนิกส์นั้นอย่างน้อยต้องมีขั้นตอนการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์อื่นๆ มาก่อนจึงจะนำมาทำบัตรอิเล็กทรอนิกส์ปลอมต่อไปได้ ความผิดสำเร็จฐานปลอมใดๆ เมื่อล้อตัวบทกฎหมายกันมา จึงควรพิจารณาถึงผลลัพธ์สุดท้ายของขั้นตอนการปลอมนั้นเป็นสำคัญเหมือนกัน นั่นคือ บัตรอิเล็กทรอนิกส์ปลอมที่พร้อมใช้งานได้ ทำนองเดียวกันกับเงินตราปลอม ดวงตาปลอม แสตมป์ปลอม ตั๋วปลอม เอกสารปลอมหรือหนังสือเดินทางปลอม ซึ่งการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ที่ยังเป็นขั้นตอนในลำดับต้นๆ ของการทำบัตรอิเล็กทรอนิกส์ปลอมเช่นนี้ ไม่ควรที่จะแปลความให้ต้องมีความรับผิดเช่นเดียวกับความผิดสำเร็จฐานปลอมเหล่านั้น ในความเห็นของผู้วิจัยคือ อาจลงโทษได้แค่เพียงการพยายามกระทำความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ซึ่งไม่เหมาะสม หากต้องการกำหนดให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์มีความผิดด้วยแล้ว บทบัญญัติของกฎหมายควรแยกเป็นบทบัญญัติอันเฉพาะเพื่อความชัดเจนในการลงโทษทางอาญา

3. โดยทั่วไปแล้วลักษณะของข้อมูลนั้นย่อมส่งกันไปมาด้วยแต่การทำสำเนา ดังนั้น การตีความว่า การทำสำเนาข้อมูลบัตรอิเล็กทรอนิกส์เป็นความผิดฐานปลอมบัตรอิเล็กทรอนิกส์นั้น จะทำให้บทบัญญัติในความผิดฐานมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/6 ไม่มีที่ใช้ เพราะเมื่อเกิดการกระทำความผิดที่เป็นการทำสำเนาข้อมูลบัตรอิเล็กทรอนิกส์ทุกครั้ง ย่อมถูกตีความว่าเป็นความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ทุกครั้งไป ซึ่งในความเป็นจริง ควรที่จะให้การทำสำเนาข้อมูลบัตรอิเล็กทรอนิกส์ใดๆ โดยมิชอบ มีความผิดเพียงฐานมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ หากมีการนำข้อมูลนั้นไปทำบัตรอิเล็กทรอนิกส์ปลอมในรูปแบบเอกสารหรือวัตถุอื่นใดอีกครั้ง จึงควรมีความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ซึ่งมีโทษรุนแรงขึ้น การตีความในลักษณะนี้จึงจะสอดคล้องกับบทบัญญัติกฎหมายในหมวดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์และถูกต้องตามหลักกฎหมายมากกว่า

4. จากการศึกษาในทางตำราอย่างถี่ถ้วนเกี่ยวกับความผิดฐานปลอมบัตรอิเล็กทรอนิกส์นั้นพบว่า ตำราของนักกฎหมายหลายๆ ท่านยังไม่ยืนยันให้การดึงข้อมูลจะเป็นความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ด้วย แม้ในทางตำราจะไม่มีการกล่าวถึงการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์อย่างชัดแจ้ง แต่ผู้วิจัยได้พิจารณาจากการยกตัวอย่างประกอบคำอธิบายในความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ในตำราเหล่านั้น เช่น “ได้รหัสเอทีเอ็มของผู้อื่นมาแล้วและมากดเปลี่ยนรหัสใหม่เพื่อนำไปใช้เบิกถอนเงินสดจากเครื่องจากเงินอัตโนมัติอาจเป็นความผิดฐานปลอมบัตร

อิเล็กทรอนิกส์ได้”[41] ตัวอย่างนี้มีการกดเปลี่ยนรหัสใหม่อันแสดงถึงการปลอมเอกสารในขั้นตอนหลังจากที่ได้รหัสเอทีเอ็มมา แต่ไม่ยืนยันว่าหากได้รหัสมาแล้วนำไปกดเงินเลยทันทีจะเป็นความผิดฐานปลอมบัตรอิเล็กทรอนิกส์หรือไม่ หรือ “นายแดงแอบดักฟังทางโทรศัพท์ในขณะที่ธนาคารบอกหมายเลขให้นายดำซึ่งเป็นลูกค้าธนาคารและนายแดงจดจำและนำไปใช้โดยมิชอบ นายแดงมีความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/5”[42] ตัวอย่างนี้การจดของนายแดงก็นับเป็นการทำสำเนาข้อมูลนั้นแล้วแต่กลับไม่ยืนยันว่านายแดงมีความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ด้วย หรือ “แอบจดจำหมายเลขบัตรเครดิตและวันหมดอายุของบัตรเครดิตของผู้อื่นและนำข้อมูลนั้นไปใช้โดยมิชอบ”[43] ก็ไม่ยืนยันว่ามีความผิดฐานปลอมบัตรอิเล็กทรอนิกส์เช่นกัน

ด้วยเหตุที่กล่าวมาข้างต้นผู้วิจัยจึงเห็นว่า การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ยังไม่เข้าองค์ประกอบภายนอกส่วนการกระทำในลักษณะ (ก) นี้ของความผิดฐานปลอมบัตรอิเล็กทรอนิกส์

(ข) เติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใดๆ ในบัตรอิเล็กทรอนิกส์ที่แท้จริง

การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ เป็นการกระทำในรูปแบบต่างๆ เพื่อให้ได้มาซึ่งข้อมูลที่บันทึกไว้ในบัตรอิเล็กทรอนิกส์ การดึงข้อมูลออกมาจากบัตรจึงไม่ใช่การเติมข้อมูลลงไปในบัตรอิเล็กทรอนิกส์ แต่การดึงข้อมูลออกมานั้นจะถือว่าเป็นการตัดทอนหรือแก้ไขด้วยประการใดๆ ในบัตรอิเล็กทรอนิกส์ที่แท้จริง อันเป็นความผิดฐานปลอมบัตรอิเล็กทรอนิกส์หรือไม่

ปัญหาในประเด็นนี้จากการศึกษาวิจัยพบว่า การดึงข้อมูลบัตรอิเล็กทรอนิกส์นั้นเป็นการคัดลอกหรือทำสำเนาข้อมูลในบัตรอิเล็กทรอนิกส์ที่แท้จริง ซึ่งวิธีการดังกล่าวมิได้ส่งผลให้ข้อมูลในบัตรอิเล็กทรอนิกส์ที่แท้จริงอันเป็นต้นฉบับนั้นได้รับการเปลี่ยนแปลงหรือเปลี่ยนสภาพไปจากการกระทำดังกล่าว ดังนั้น การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์จึงไม่อาจทำให้เกิดการตัดทอนหรือแก้ไขด้วยประการใดๆ แก่ข้อมูลในบัตรอิเล็กทรอนิกส์ที่แท้จริงได้เลย จึงทำให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ไม่เข้าองค์ประกอบภายนอกส่วนการกระทำในลักษณะ (ข) นี้ของความผิดฐานปลอมบัตรอิเล็กทรอนิกส์เช่นกัน

---

[41] ทวีเกียรติ มีนะกนิษฐ์, คำอธิบายกฎหมายอาญา ภาคความผิดและลหุโทษ, หน้า 182.

[42] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 347.

[43] เรื่องเดียวกัน, หน้า 348.

ดังนั้นจึงสรุปได้ว่า ไม่อาจนำความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/1 มาปรับใช้เพื่อลงโทษในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้ เพราะลักษณะการกระทำไม่เข้าองค์ประกอบภายนอกส่วนการกระทำในความผิดฐานดังกล่าว

3.3.2.2 การนำความผิดฐานทำหรือมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลงหรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์มาปรับใช้

จากการศึกษาถึงลักษณะของ “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” ที่อยู่ในบัตร “ที่มีการออกเอกสารหรือวัตถุอื่นใดให้” พบว่า คุณสมบัติโดยทั่วไปของข้อมูลอิเล็กทรอนิกส์ที่อยู่ในบัตรอิเล็กทรอนิกส์นั้น ข้อมูลจะต้องถูกบรรจุในแหล่งบันทึกความจำใดๆ ก็ตามไม่ว่าจะเป็นการบันทึกลงในแถบแม่เหล็กของบัตร (Magnetic Stripe) หรือในชิป (Chip) ของบัตรใบนั้น หรือหากมีการโอนถ่ายหรือคัดลอกไปยังเครื่องมืออิเล็กทรอนิกส์อื่นๆ ข้อมูลนั้นก็จะต้องไปบันทึกอยู่ในหน่วยความจำในเครื่องมืออิเล็กทรอนิกส์นั้นๆ เช่น ในฮาร์ดไดร์ (Hard Drive) ของเครื่องคอมพิวเตอร์ จึงสรุปได้ในเบื้องต้นว่า โดยลักษณะทั่วไปของข้อมูลนั้นต้องอยู่ในแหล่งบันทึกไม่ว่าที่ใดที่หนึ่ง จะอยู่ลอยๆ ในอากาศไม่ได้[44]

เมื่อพิเคราะห์มาตรา 269/2 ที่ระบุว่า[45] ผู้ใดมีเครื่องมือหรือวัตถุ... เพื่อใช้หรือให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ แล้วพบว่า เครื่องมือประเภทนี้ได้ถูกบัญญัติไว้กว้างๆ อาจจะเป็น เครื่องคอมพิวเตอร์ โทรศัพท์ เครื่องดูดข้อมูลบัตรอิเล็กทรอนิกส์หรือเครื่องสกิมเมอร์ (Skimmer) กล้องบันทึกขนาดจิ๋ว ซึ่งผู้ที่มีเครื่องมือพวกนี้อาจมีความผิดตามมาตรา 269/2 นี้ได้ เพราะเครื่องมือพวกนี้ส่วนใหญ่แล้วมักจะมีแหล่งบันทึกความจำอยู่ในเครื่องนั้นด้วย ซึ่งหากมีข้อมูลจากการกระทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้นได้บันทึกอยู่ในเครื่องมือดังกล่าวด้วย ก็อาจตีความได้ว่า ผู้นั้นมีเครื่องมือหรือวัตถุ...เพื่อใช้หรือให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/2 เพื่อลงโทษผู้กระทำการดึงข้อมูลออกจากบัตรอิเล็กทรอนิกส์ได้

---

[44] สัมภาษณ์ วิวัฒน์ สิทธิสรเดช, นักวิทยาศาสตร์ กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง สำนักงานตำรวจแห่งชาติ, 12 มกราคม 2561. และ ผู้วิจัยเห็นว่า การใช้ความจำก็เป็นแหล่งบันทึกข้อมูลเช่นกัน โดยใช้สมอง แต่การกระทำความผิดแก่ข้อมูลในสมอง ในปัจจุบันเทคโนโลยียังไม่สามารถขโมยหรือดึงข้อมูลออกมาจากสมองมนุษย์ได้ จึงต้องใช้การเค้นเอาข้อมูลนั้น อันอาจเป็นความผิด ฐานข่มขืนใจผู้อื่น ตามมาตรา 309

[45] มาตรา 269/2 “ผู้ใดทำเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงสิ่งใดๆ ซึ่งระบุไว้ในมาตรา 269/1 หรือมีเครื่องมือหรือวัตถุเช่นว่านั้น เพื่อใช้หรือให้ได้ข้อมูลในการปลอมหรือแปลง ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงห้าปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนบาท”

แต่ที่น่าสังเกตก็คือโดยปรกติแล้วเครื่องมือหรือวัตถุดังกล่าวนั้น แม้จะไม่มีข้อมูลใดๆ อยู่ในแหล่งบันทึกความจำเลยก็ตาม หรืออาจกล่าวได้ว่าผู้กระทำยังไม่ได้ใช้เครื่องมือหรือวัตถุนั้นไปทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เลย แต่มาตรา 269/2 บัญญัติว่า หากผู้กระทำมีเจตนาพิเศษเพื่อใช้หรือให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์แล้ว ผู้กระทำที่มีเครื่องมือหรือวัตถุนั้นก็จะมีความผิด ตามมาตรา 269/2 เช่นเดียวกัน ตัวอย่างเช่น คอมพิวเตอร์เปล่าที่ไม่มีข้อมูลบัตรอิเล็กทรอนิกส์อยู่เลยที่คนร้ายใช้พกพาไปในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ หรือกล้องขนาดจิ๋วที่คนร้ายมีในการใช้งานที่ยังไม่ทำการถ่ายภาพข้อมูลในกล้องนั้นเลย หรือ เครื่องสกิมเมอร์เปล่าที่ยังไม่มีข้อมูลบัตรอิเล็กทรอนิกส์เลยเพราะยังไม่ได้มีการใช้ติดตั้งกับเครื่องจ่ายเงินอัตโนมัติ

ดังนั้นหากศาลได้ตีความว่า แม้ข้อมูลที่อยู่ในบัตร “ที่มีการออกเอกสารหรือวัตถุอื่นใดให้” ไม่เป็น “บัตรอิเล็กทรอนิกส์” ตามมาตรา 1(14) แต่เนื่องจากพบว่ามีข้อมูลของบัตรอิเล็กทรอนิกส์นั้นอยู่ในแหล่งบันทึกความจำของเครื่องมือหรือวัตถุใดๆ ที่ผู้กระทำความผิดใช้ แสดงว่าผู้กระทำมีเจตนาพิเศษเพื่อใช้หรือให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/2 ด้วย ซึ่งศาลอาจตีความขยายไปให้มีการลงโทษตามมาตรานี้ได้ แต่การตีความดังกล่าวนั้นอาจเกิดปัญหาในด้านต่างๆ ดังต่อไปนี้

3.3.2.1 ด้านวัตถุแห่งการกระทำ

องค์ประกอบความผิดของ มาตรา 269/2 มีวัตถุแห่งการกระทำคือ “เครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลง” ไม่ได้ระบุเจาะจงว่าวัตถุแห่งการกระทำเป็น “ข้อมูล” โดยตรง และการมีหรือไม่มี “ข้อมูล” อยู่ในเครื่องมือหรือวัตถุ ตามมาตรา 269/2 ดังกล่าว เป็นเพียงการพิสูจน์ถึงเจตนาพิเศษ “เพื่อใช้หรือให้ได้ข้อมูลในการปลอมหรือแปลง” เท่านั้น ว่าถ้ายิ่งมี “ข้อมูล” อยู่ในเครื่องมือหรือวัตถุที่ใช้ในการกระทำความผิดด้วย เจตนาพิเศษก็ยิ่งพิสูจน์ได้ชัดยิ่งขึ้น อันนำไปสู่การตัดสินลงโทษผู้กระทำผิดฐานมีเครื่องมือหรือวัตถุนั้น ตามมาตรา 269/2 ได้อย่างปราศจากข้อสงสัย แต่แม้ไม่ได้มี “ข้อมูล” อยู่ในตัวเครื่องมือหรือวัตถุดังกล่าว โจทก์ก็ย่อมนำสืบประกอบพยานหลักฐานอื่นๆ ให้ศาลเชื่อได้ว่า ผู้กระทำมีเจตนาพิเศษเช่นว่านั้นจริง เช่น มีประจักษ์พยานพบเห็นจำเลยขณะทำการติดตั้งเครื่องสกิมเมอร์เปล่า หรือจำเลยเป็นนักท่องเที่ยวต่างชาติที่ไม่ได้ประกอบธุรกิจใดๆ ในประเทศไทยแต่จำเลยพกเครื่องสกิมเมอร์เปล่าไปในย่านแหล่งท่องเที่ยว หรือฟังจากพยานซัดทอดจากพวกของจำเลยด้วยกันประกอบพยานหลักฐานอื่นๆ เช่น ภาพกล้องวงจรปิด อันใช้ลงโทษผู้กระทำความผิดได้อยู่ จึงกล่าวสรุปได้ว่า “ข้อมูล” ในเครื่องมือหรือวัตถุเหล่านั้นเป็นเพียงการนำสืบพิสูจน์ถึงเจตนาพิเศษให้ง่ายขึ้นเท่านั้น แต่กฎหมายไม่ได้บัญญัติ

ให้ “ข้อมูล” เป็นองค์ประกอบความผิดในมาตรา 269/2 ด้วย มิฉะนั้น กฎหมายคงต้องบัญญัติกำหนดลงไป เช่นว่า “ผู้ใด...มีเครื่องมือหรือวัตถุ หรือข้อมูล เพื่อใช้หรือให้ได้ข้อมูลสำหรับการปลอมหรือแปลง” แล้ว

3.3.2.2 ด้านหลักกฎหมายอาญา

หลักไม่มีความผิดและไม่มีโทษโดยไม่มีกฎหมาย (Nullum crimen, nulla poena, sine lege) หรือที่เรียกย่อๆ ว่า หลักไม่มีโทษโดยไม่มีกฎหมาย (Nulla poena, sine lege : No punishment without law) อันมีความหมายว่า ประชาชนจะต้องรับโทษก็แต่เฉพาะกรณีที่ตนได้กระทำการอันกฎหมายกำหนดว่าเป็นความผิดและกำหนดโทษไว้ชัดแจ้งเท่านั้น จึงเท่ากับเป็นการป้องกันมิให้เจ้าหน้าที่ของรัฐใช้อำนาจจนเกินขอบเขต จนนักนิติศาสตร์ได้กล่าวว่าหลักการดังกล่าวเป็นหลักประกันในกฎหมายอาญาและเป็นหัวใจของกฎหมายอาญาเสียทีเดียว[46] สำหรับประเทศไทยได้บัญญัติหลักกฎหมายดังกล่าวไว้ในประมวลกฎหมายอาญามาตรา 2 วรรคแรก ความว่า

“บุคคลจักต้องรับโทษในทางอาญาต่อเมื่อได้กระทำการอันกฎหมายที่ใช้ในขณะกระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแก่ผู้กระทำความผิดนั้น ต้องเป็นโทษที่บัญญัติไว้ในกฎหมาย”

อีกทั้งยังได้บัญญัติรับรองหลักการนี้อีกชั้นหนึ่งในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 29 วรรคแรก ความว่า

“บุคคลไม่ต้องรับโทษอาญา เว้นแต่ได้กระทำการอันกฎหมายที่ใช้อยู่ในเวลาที่กระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแก่บุคคลนั้นจะหนักกว่าโทษที่บัญญัติไว้ในกฎหมายที่ใช้อยู่ในเวลาที่กระทำความผิดมิได้”

จากหลักไม่มีโทษโดยไม่มีกฎหมาย สามารถจำแนกรายละเอียดหรือแยกลักษณะสำคัญได้ ดังนี้[47]

---

[46] คณิต ณ นคร, ประมวลกฎหมายอาญา หลักกฎหมายและพื้นฐานการเข้าใจ, พิมพ์ครั้งที่ 5 (กรุงเทพฯ: นิติธรรม, 2538), หน้า 173.

[47] เรื่องเดียวกัน, หน้า 174.

(ก) กฎหมายอาญาต้องชัดเจนแน่นอน

ด้วยหลัก ไม่มีโทษโดยไม่มีกฎหมาย เป็นหลักที่มีขึ้นเพื่อคุ้มครองเสรีภาพของประชาชน ดังนั้นการบัญญัติถ้อยคำในกฎหมายอาญาจึงต้องบัญญัติให้มีความชัดเจนแน่นอน และต้องพยายามหลีกเลี่ยงถ้อยคำที่จะทำให้เกิดการตัดสินคดีที่ขึ้นอยู่กับความรู้สึกที่เป็นอัตวิสัย (Subjective) และอำเภอใจของผู้พิจารณาคดี เพราะมิฉะนั้นหลักประกันของประชาชนจะหมดไป กฎหมายหมายอาญาจึงเป็นบทกฎหมายที่ต้องตีความโดยเคร่งครัด เพราะเป็นบทกฎหมายที่จำกัดสิทธิเสรีภาพของบุคคลที่รัฐธรรมนูญยินยอมให้ทำได้แต่ต้องอาศัยกฎหมาย ทั้งมีหลักกฎหมายอาญาว่า บุคคลทุกคนซึ่งต้องหาว่ากระทำผิดอาญา ต้องมีสิทธิได้รับการสันนิษฐานว่าเป็นผู้บริสุทธิ์ จนกว่าจะพิสูจน์ตามกฎหมายได้ว่ามีความผิด และมาตรา 2 ในประมวลกฎหมายอาญา มีข้อความว่า “โทษที่จะลงแก่ผู้กระทำความผิดนั้น ต้องเป็นโทษที่บัญญัติไว้ในกฎหมาย” ดังนั้นการลงโทษบุคคลโดยตีความโดยขยายความจะกระทำไม่ได้ ในเมื่อ “ข้อมูล” ที่อยู่ในบัตร “ที่มีการออกให้” ไม่เป็น “บัตรอิเล็กทรอนิกส์” อันมีนิยามของกฎหมายแยกกันชัดเจนแล้วตามมาตรา 1(14) การอนุโลมให้เป็นการกระทำดังกล่าวแก่ “ข้อมูล” นั้น เป็นความผิดตามบทบัญญัติอื่นๆ อีกจึงเป็นการมิชอบ[48]

(ข) ห้ามใช้กฎหมายที่ใกล้เคียงอย่างยิ่งลงโทษทางอาญาแก่บุคคล

ในระบบกฎมายลายลักษณ์อักษรส่วนใหญ่ มักจะเกิดปัญหาเสมอว่า เมื่อเกิดคดีขึ้นแล้วและเป็นกรณีที่กฎหมายลายลักษณ์อักษรไม่ได้บัญญัติไว้โดยตรง ศาลจะปฏิเสธคดีโดยอ้างว่ากฎหมายไม่ได้บัญญัติไว้หรือกฎหมายบัญญัติไว้ไม่ชัดเจนไม่ได้ และเป็นหน้าที่ของศาลที่จะต้องพยายามหาบทบัญญัติมาปรับกับคดีที่เกิดขึ้นอยู่เสมอ[49] วิธีแก้ปัญหาในกรณีดังกล่าวคือ การใช้กฎหมายโดยการเทียบเคียงหลักกฎหมายที่ใกล้เคียงอย่างยิ่ง (Analogy) หมายถึงการให้เหตุผลโดยอ้างความคล้ายคลึงกันย่อมมีความหมายอย่างเดียวกัน (Argumentum a simile) วิธีการคือนำข้อเท็จจริงที่เกิดขึ้นในคดีมาเทียบเคียงองค์ประกอบที่บัญญัติไว้ในกฎหมายที่ใกล้เคียงอย่างยิ่ง โดยพิจารณาว่าข้อเท็จจริงนั้นมีความคล้ายคลึงกับองค์ประกอบของกฎหมายที่ใกล้เคียงนั้น ถึงขนาดหรือตรงกันในสาระสำคัญหรือไม่ จึงจะให้มีผลทางกฎหมายอย่างเดียวกัน เพราะ “สิ่งที่เหมือนกันควร

[48] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 348.

[49] สมยศ เชื้อไทย, คำอธิบายวิชากฎหมายแพ่ง : หลักทั่วไป, พิมพ์ครั้งที่ 25 (กรุงเทพฯ: วิญญูชน, 2562), หน้า 192.

ได้รับการปฏิบัติอย่างเดียวกันหรือเท่าเทียมกัน”[50] ซึ่งหลักเกณฑ์ดังกล่าวได้รับการบัญญัติไว้ในประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 4 วรรคสอง อีกด้วย[51]

แต่สำหรับในทางอาญานั้น การจะลงโทษบุคคลใดได้ก็ต่อเมื่อมีกฎหมายลายลักษณ์อักษรบัญญัติไว้โดยตรงเท่านั้น จักนำหลักกฎหมายที่ใกล้เคียงอย่างยิ่งมาปรับกับข้อเท็จจริงในคดีที่ไม่มีกฎหมายบัญญัติกำหนดไว้โดยตรงเพื่อลงโทษบุคคลไม่ได้ เพราะไม่ต้องตามบทบัญญัติแห่งตัวอักษรและเจตนารมณ์ในเรื่องนั้นๆ ทั้งยังเป็นการกระทบสิทธิเสรีภาพของประชาชนเป็นอย่างมากและจะทำให้ขาดหลักเกณฑ์ที่แน่นอนในการพิจารณาคดี[52] ดังเช่น เรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นี้จะนำความผิดฐานมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/2 โดยเห็นว่าเป็นบทบัญญัติที่มีคำว่า “ข้อมูล” อยู่ในบทบัญญัติดังกล่าวจึงลงโทษผู้กระทำการการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในฐานนี้ซึ่งเป็นการนำหลักการใช้กฎหมายโดยการเทียบเคียงหลักกฎหมายที่ใกล้เคียงอย่างยิ่งมาใช้นั้น จึงไม่เป็นการถูกต้องตามหลักกฎหมายอาญา ทั้งจะนำความผิดในประมวลกฎหมายอาญาในฐานอื่นๆ เช่น ฐานลักทรัพย์ ฐานปลอมเอกสาร (ซึ่งจะกล่าวต่อไปในหัวข้อที่ 3.3) มาใช้ลงโทษผู้กระทำก็ไม่ได้อีกเช่นกัน

3.3.2.3 ด้านฐานของการกระทำ

หากกฎหมายประสงค์ให้การกระทำต่อ “ข้อมูล” ที่บรรจุอยู่ในเครื่องมือหรือวัตถุเหล่านั้นเป็นความผิดอีกฐานหนึ่ง กฎหมายก็ต้องบัญญัติฐานของการกระทำผิดที่เป็นข้อมูลไว้แยกออกจากฐานมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/2 ให้ชัดเจนเหมือนดังเช่น ฐานปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/1 ฐานนำเข้าในหรือส่งออกไปนอกราชอาณาจักรซึ่งบัตรอิเล็กทรอนิกส์ปลอม ตามมาตรา 269/3 ฐานใช้หรือมีไว้เพื่อใช้ซึ่งบัตรอิเล็กทรอนิกส์ปลอม ตามมาตรา 269/4 หรือฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/5 แต่บทบัญญัติของกฎหมายกลับบัญญัติให้ไม่ว่าเครื่องมือหรือวัตถุนั้นจะมีข้อมูลจากการดึงจากบัตรอิเล็กทรอนิกส์หรือไม่ ก็ลงโทษผู้กระทำความผิดโดยเจาะจงลงว่าเป็นฐาน “มีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการ

---

[50] เรื่องเดียวกัน.

[51] ป.พ.พ. มาตรา 4 วรรคสอง “เมื่อไม่มีบทกฎหมายที่จะยกมาปรับคดีได้ ให้วินิจฉัยคดีนั้นตามจารีตประเพณีแห่งท้องถิ่น ถ้าไม่มีจารีตประเพณีเช่นว่านั้น ให้วินิจฉัยคดีอาศัยเทียบบทกฎหมายที่ใกล้เคียงอย่างยิ่ง และถ้าบทกฎหมายเช่นนั้นก็ไม่มีด้วย ให้วินิจฉัยตามหลักกฎหมายทั่วไป”

[52] แสวง บุญเฉลิมวิภาส, หลักกฎหมายอาญา, พิมพ์ครั้งที่ 1 (กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2539), หน้า 19.

ปลอมหรือแปลงบัตรอิเล็กทรอนิกส์” เพียงฐานเดียวเท่านั้นตามประมวลกฎหมายอาญาที่ได้แก้ไขเพิ่มเติมใน พ.ศ. 2547 ซึ่งต่างจากร่าง... ที่ได้เสนอให้แก่ที่ประชุมสภาผู้แทนราษฎร ที่ได้บัญญัติให้การกระทำความผิดต่อข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์เป็นฐานความผิดอีกฐานหนึ่ง เช่น ฐานใช้หรือมีไว้เพื่อใช้ข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ซึ่งจะแยกต่างหากจากการกระทำความผิดฐานอื่นๆ ดังที่ปรากฏในปัจจุบันด้วย (อันจะกล่าวโดยละเอียดในหัวข้อ 3.3.3 ต่อไป)

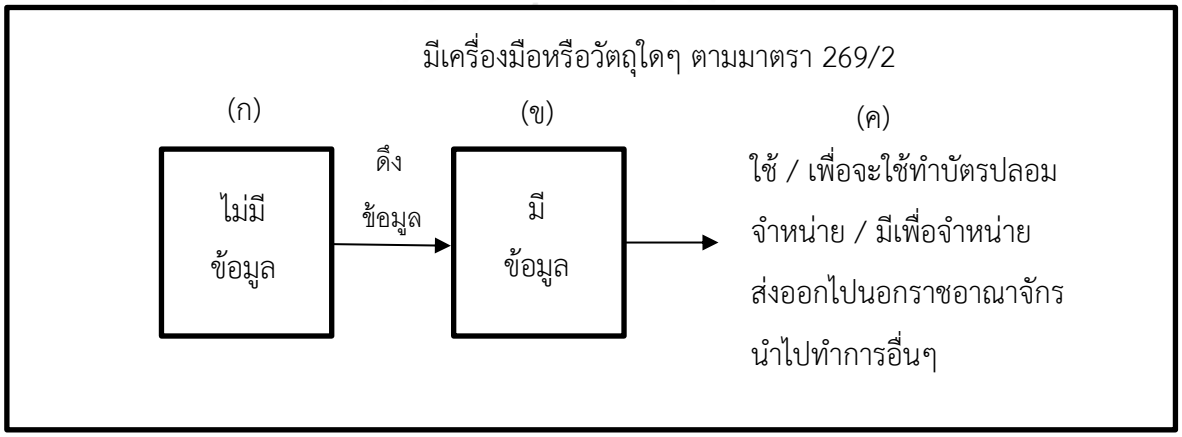
3.3.2.4 ด้านกรรมของการกระทำความผิด

จากการที่ไม่ได้แยกการกระทำผิดออกเป็นฐานต่างๆ ดังในหัวข้อที่ 3.3.2.3 นั้นทำให้

(ก) การมีเครื่องมือหรือวัตถุ ตามมาตรา 269/2 เปล่าๆ โดยที่ยังไม่ได้ใช้ดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

(ข) ต่อมา การมีเครื่องมือหรือวัตถุ ตามมาตรา 269/2 แต่มีข้อมูลอยู่ในเครื่องมือหรือวัตถุนั้น เพราะได้ใช้ในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ไปแล้ว

(ค) ต่อมา การมีเครื่องมือหรือวัตถุ ตามมาตรา 269/2 แต่มีข้อมูลอยู่ในเครื่องมือหรือวัตถุนั้น เพราะได้ใช้ในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ไปแล้ว แล้วจะนำข้อมูลนั้นไปทำการใดต่อ เช่น นำไปใช้หรือเพื่อจะใช้ทำบัตรอิเล็กทรอนิกส์ปลอม หรือนำข้อมูลนั้นไปจำหน่ายหรือมีไว้เพื่อจำหน่าย หรือนำข้อมูลนั้นส่งออกไปนอกราชอาณาจักร



ทั้งสามการกรณีดังกล่าวอันเป็นการกระทำที่ต่อเนื่องกันเหล่านี้ ผู้กระทำก็จะมีความผิดฐานมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/2 เพียงกรรมเดียวเท่านั้น โดยไม่ต้องคำนึงว่าผู้กระทำจะมี

ข้อมูลที่ได้มาจากการดึงจากบัตรอิเล็กทรอนิกส์ หรือจะนำข้อมูลนั้นไปกระทำการใดต่อไปหรือไม่ ดังนั้นคำว่า “ข้อมูล” ในมาตรา 269/2 จึงไม่ใช่ตัวแปรของการลงโทษผู้กระทำความผิด เพราะมาตรา 269/2 นั้นมุ่งพิจารณาเพียงแค่การ “มีเครื่องมือหรือวัตถุ” เท่านั้น ไม่ใช่การมีข้อมูลของบัตรอิเล็กทรอนิกส์ ดังนั้นจึงจะลงโทษผู้ที่มีข้อมูลจากการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ให้ต้องรับผิดตามมาตรา 269/2 ไม่ได้ ซึ่งโดยที่จริงแล้วการกระทำต่างๆ ตาม (ก) (ข) และ (ค) เหล่านี้ควรจะเป็นความผิดหลายกรรมต่างกันดังเช่นความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ทั่วๆ ไป[53]

3.3.2.5 ด้านอัตราโทษ

จากการลงโทษฐานมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/2 เพียงแค่กรรมเดียว ตามหัวข้อที่ 3.3.2.4 แม้ว่าในความเป็นจริงแล้วการกระทำความผิดนั้นอาจแยกออกจากกันได้เป็นหลายกรรมต่างกันก็ตาม ทำให้การลงโทษผู้กระทำความผิดจึงจำกัดอยู่ที่ จำคุกตั้งแต่หนึ่งปีถึงห้าปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนบาท อันเป็นโทษขั้นต่ำที่สุดของหมวด “ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์” ที่ศาลจะลงได้โดยใช้ดุลพินิจ เนื่องจากถือว่าเป็นการกระทำเพียงกรรมเดียว ศาลจึงไม่สามารถลงโทษผู้นั้นทุกกรรมเรียงกระทงความผิดได้ดังที่บัญญัติไว้ในมาตรา 91 และผลจากการลงโทษเพียงกรรมเดียวในความผิดตามมาตรา 269/2 ซึ่งมีอัตราโทษขั้นสูงเพียงห้าปีเช่นนี้ ทำให้เข้าหลักเกณฑ์ของมาตรา 56 ที่จะรอการลงโทษหรือรอการกำหนดโทษไว้ ซึ่งหากทำให้ผู้ได้รับโทษนั้นให้การรับสารภาพและมีเหตุบรรเทาโทษตามมาตรา 78 ด้วยอันทำให้ศาลเห็นสมควรลดโทษไม่เกินกึ่งหนึ่งด้วยแล้ว ศาลย่อมจะมีแนวโน้มที่จะรอการกำหนดโทษหรือรอการลงโทษไว้ก่อน ซึ่งขัดกับเจตนารมณ์ในการยกร่างกฎหมายในหมายเหตุ[54] ว่าการลักลอบนำข้อมูลอิเล็กทรอนิกส์ของผู้อื่นมาใช้เป็นการส่งผลกระทบต่อเศรษฐกิจและผู้บริโภคในวงกว้าง จึงเห็นสมควรกำหนดโทษความผิดลักษณะนี้ให้เหมาะสม ดังนั้นการรอการกำหนดโทษหรือรอการลงโทษจากเหตุผลดังกล่าวจึงเสมือนเป็นข้อผูกมัดที่ศาลต้องใช้เสมอไปจากปัญหาในทางกฎหมาย อันเป็นการเปิดโอกาสให้ผู้กระทำความผิดไม่เกรงกลัวต่อกฎหมายและยอมเสี่ยงในการกระทำความผิดเพื่อแลกกับประโยชน์ที่ได้อันมหาศาลจากการนำข้อมูลที่ได้มาเหล่านั้นไปแสวงหาผลประโยชน์ต่อไป

---

[53] คำพิพากษาศาลฎีกาที่ 6820/2552 “นำบัตรวีซ่าการ์ดใช้ชำระค่าสินค้าแทนเงินสดรวม 3 ครั้งย่อมเป็นความผิดหลายกรรม หาใช่กรรมเดียวไม่” และฎีกาที่ 2512/2550 “จำเลยกระทำความผิดโดยมีเจตนาต่างกัน การกระทำของจำเลยย่อมเป็นความผิดหลายกรรมหาใช่กรรมเดียว”

[54] พ.ร.บ. แก้ไขเพิ่มเติมประมวลกฎหมายอาญา ฉบับที่ 17 พ.ศ. 2547

3.3.2.6 ด้านเจตนารมณ์ในการยกร่างกฎหมาย

เมื่อวิเคราะห์ถึงถ้อยคำของเหตุผลของร่าง... ที่เสนอให้แก่ที่ประชุมสภาผู้แทนราษฎร ให้มีการบัญญัติกฎหมายและหมายเหตุท้าย พ.ร.บ. แก้ไขเพิ่มเติมประมวลกฎหมายอาญา ฉบับที่ 17 พ.ศ. 2547 ที่ระบุว่า

ปัจจุบันการใช้เอกสาร วัตถุอื่นใดหรือ “ข้อมูล” ในลักษณะบัตรอิเล็กทรอนิกส์ กำลังเพิ่มปริมาณและประเภทการใช้งานอย่างแพร่หลาย และได้มีการกระทำความผิดเกี่ยวกับบัตรและลักลอบนำ “ข้อมูล” อิเล็กทรอนิกส์ของผู้อื่นมาใช้ อันส่งผลกระทบต่อเศรษฐกิจและผู้บริโภคในวงกว้าง จึงสมควรกำหนดความผิดอาญาสำหรับการกระทำความผิดเกี่ยวกับบัตรและ “ข้อมูล” อิเล็กทรอนิกส์ดังกล่าวเพิ่มเติม “ให้ครอบคลุม” การกระทำความผิดในรูปแบบต่าง ๆ และให้มี “อัตราโทษเหมาะสมกับความร้ายแรง” ของการกระทำความผิด

ซึ่งเห็นได้ชัดว่าเจตนารมณ์ของกฎหมายที่ได้แก้ไขเพิ่มเติมนั้น ต้องการให้ “ข้อมูล” ไม่ว่าข้อมูลนั้นจะมีการออกเอกสารหรือวัตถุอื่นใดให้หรือไม่ก็ตาม ได้รับการคุ้มครองตามกฎหมายได้อย่างครอบคลุมถึงการกระทำความผิดในรูปแบบต่างๆ ในลักษณะเดียวกับที่กฎหมายได้คุ้มครองไว้แล้ว ตามมาตรา 269/1 ถึง มาตรา 269/7 ด้วย ดังนั้นการจะตีความกฎหมายเพื่อปรับบทลงโทษผู้กระทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์โดยใช้มาตรา 269/2 เพียงประการเดียวนั้น จึงไม่ครอบคลุมถึงการกระทำต่อข้อมูลในรูปแบบอื่นๆ ได้ อันขัดกับเจตนารมณ์ในการแก้ไขเพิ่มเติมกฎหมายและหมายเหตุในการยกร่างกฎหมายดังกล่าวที่ต้องการให้มีการกำหนดการกระทำความผิดเกี่ยวกับบัตรและ “ข้อมูล” อิเล็กทรอนิกส์ดังกล่าวเพิ่มเติม “ให้ครอบคลุม” การกระทำความผิดในรูปแบบต่างๆ มากยิ่งขึ้น

จากหัวข้อที่ 3.3.2.1 ถึง 3.3.2.6 ข้างต้น จึงสรุปได้ว่า หากศาลได้ตีความว่า แม้ข้อมูลที่อยู่ในบัตรอิเล็กทรอนิกส์ “ที่มีการออกเอกสารหรือวัตถุอื่นใดให้” ไม่เป็น “บัตรอิเล็กทรอนิกส์” ตามมาตรา 1(14) แต่ก็ยังฝืนปรับบทลงโทษโดยการนำมาตรา 269/2 มาใช้แก่การกระทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์แล้ว จะเป็นการไม่ถูกต้องตามเหตุผลดังที่ได้กล่าวมา

3.3.3 ปัญหาในชั้นยกร่างกฎหมายกับเรื่องข้อมูลในบัตรอิเล็กทรอนิกส์

จากการศึกษาไปถึงการยกร่างกฎหมายก่อนที่จะได้มีการบัญญัตินิยามของบัตรอิเล็กทรอนิกส์และความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ที่มีใช้ในปัจจุบันนั้นพบว่า ในชั้นรับหลักการแห่งร่างพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา มีร่าง... ที่ได้เสนอแก่ที่ประชุมสภาผู้แทนราษฎร

ในสมัยสามัญทั่วไปครั้งที่ 20 ในวันที่ 23 เมษายน 2546 จำนวน 2 ร่างด้วยกันคือ ร่าง...ของคณะรัฐมนตรีและของสมาชิกสภาผู้แทนราษฎร

ซึ่งคณะรัฐมนตรีได้เสนอร่าง...[55] ลงวันที่ 4 มีนาคม 2546 ในบันทึกหลักการและเหตุผลประกอบร่าง... ข้อ (3) นอกจากที่ได้เสนอจนมีการเพิ่มให้มีความผิดมาตราต่างๆ ดังที่ปรากฏในปัจจุบัน[56] แล้ว ได้ระบุว่าให้มีการกำหนดความผิดสำหรับการกระทำดังต่อไปนี้ด้วย คือ

(1) กำหนดความผิด “สำหรับการใช้...ข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ” โดยการเพิ่มมาตรา 269/6 ตามข้อ (3)(ง)

(2) กำหนดความผิด “สำหรับการมีไว้เพื่อใช้ซึ่ง...ข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ” โดยการเพิ่มมาตรา 269/6/1 ตามข้อ (3)(จ)

โดยในร่าง...ที่คณะรัฐมนตรีเสนอ ได้บัญญัติให้เพิ่มมาตรา 1(14) โดยให้ความหมายของคำว่า “บัตรอิเล็กทรอนิกส์” ว่าหมายถึง

“เอกสารหรือวัตถุอื่นใด ไม่ว่าจะมีรูปลักษณะใด ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็ก ให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า และให้หมายความรวมถึง ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ แต่มีวิธีการใช้ในทำนองเดียวกัน”

และให้เพิ่มมาตรา 269/6 และ มาตรา 269/6/1 ซึ่งระบุว่า

มาตรา 269/6 “ผู้ใดใช้ข้อมูลบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

มาตรา 269/6/1 “ผู้ใดมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/5 หรือซึ่งข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/6 ในประการที่

---

[55] ร่างพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่...) พ.ศ. ... ที่ นร 0503/2883 วันที่ 4 มีนาคม 2546 ลงชื่อ พันตำรวจโท ทักษิณ ชินวัตร เสนอโดยนายพงศ์เทพ เทพกาญจนา รัฐมนตรีว่าการกระทรวงยุติธรรมในสมัยนั้น

[56] พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547

น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

ส่วนร่าง... ของสมาชิกสภาผู้แทนราษฎร[57] ลงวันที่ 25 มีนาคม 2546 มีหลักการและเหตุผลประกอบร่าง... และมีคำนิยามของคำว่า “บัตรอิเล็กทรอนิกส์” ในมาตรา 1(14) เหมือนกับร่าง...ของคณะรัฐมนตรี แต่ได้มีการเพิ่มมาตรา 269/6 โดยเป็นการรวมมาตรา 269/6 และมาตรา 269/6/1 ของร่างคณะรัฐมนตรีเข้าด้วยกัน เป็นมาตราเดียวกัน ระบุว่า

มาตรา 269/6 “ผู้ใดใช้หรือมีไว้เพื่อใช้ข้อมูล หรือรหัสบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

ซึ่งในที่ประชุมสภาผู้แทนราษฎรในวันที่ 23 เมษายน 2546 นั้น ได้มีมติเห็นชอบรับร่างทั้ง 2 ฉบับ และตั้งคณะกรรมการคณะหนึ่งจำนวน 35 คนเพื่อแปรญัตติในการพิจารณาวาระที่ 2 โดยที่ประชุมมีมติเห็นชอบให้ใช้ร่างของคณะรัฐมนตรีเป็นหลักในการแปรญัตติ[58]

ในการแปรญัตติร่าง...ในวาระที่ 2 ในสมัยสามัญนิติบัญญัติ เป็นพิเศษ ครั้งที่ 22 วันที่ 15 ตุลาคม 2546 ได้มีการแก้ไขร่าง...เดิม ในมาตรา 1(14) โดยให้มาตรา 1(14) แยกออกเป็น 1(14)(ก) 1(14)(ข) และ 1(14)(ค) เหมือนเช่นที่มีในปัจจุบัน[59] และได้แก้ไขมาตรา 269/6 และมาตรา 269/6/1 โดยตัดเรื่องข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์ออกไป เหลือเพียงไว้แต่ว่า

มาตรา 269/6 “ผู้ใดมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/5 ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

อันมีข้อความเหมือนดังเช่นปัจจุบัน

ซึ่งในเรื่องนี้ในที่ประชุมสภาผู้แทนราษฎร นายวัฒนา เช่งไพเราะ สมาชิกสภาผู้แทนราษฎรกรุงเทพมหานคร เขตพระโขนง เขตวัฒนา พรรคเพื่อไทย ได้สงวนคำแปรญัตติและได้สอบถาม นายชูเกียรติ รัตนชัยชาญ ซึ่งเป็นกรรมาธิการคนหนึ่ง ว่าทำไมถึงตัดเรื่องที่เกี่ยวกับข้อมูลนั้นออกไป เพราะในร่าง...เดิม ตามมาตรา 269/5 จะเป็นเรื่องของการใช้บัตร ส่วนมาตรา 269/6 จะเป็นเรื่องของข้อมูล

---

[57] ร่างพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่...) พ.ศ. ... วันที่ 25 มีนาคม 2546 ลงชื่อ นงค์นาถ เตชะไพบูลย์ สมาชิกสภาผู้แทนราษฎร พรรคชาติพัฒนา โดยมีสมาชิกสภาผู้แทนราษฎรรับรอง 20 ท่าน

[58] รายงานการประชุมสภาผู้แทนราษฎร ชุดที่ 21 ปีที่ 3 ครั้งที่ 20 (สมัยสามัญทั่วไป) วันที่ 23 เมษายน 2546 หน้า 63

[59] พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547

ด้วย ซึ่งกรรมาธิการได้ให้เหตุผลว่า ร่างที่กรรมาธิการเสนอในวาระ 2 นี้ได้แยกคำนิยามของคำว่า “บัตรอิเล็กทรอนิกส์” ในมาตรา 1(14) เป็น (ก) (ข) และ (ค) ให้มีความละเอียดมากขึ้นแล้ว ซึ่งกรรมาธิการเห็นว่า “ข้อมูล รหัส หมายเลขบัญชี” นั้นเป็น “บัตรอิเล็กทรอนิกส์” อันอยู่ในความหมายของมาตรา 1(14)(ข) แล้ว จึงไม่จำเป็นต้องบัญญัติลงไปซ้ำอีก มาตรา และให้เหตุผลที่สำคัญว่า เพราะ “ความหมายของบัตรอิเล็กทรอนิกส์ดังกล่าวก็รวมถึงข้อมูลอยู่แล้ว”[60] และต่อมาที่ประชุมสมาชิกสภาผู้แทนราษฎรก็ได้เห็นชอบกับร่างดังกล่าว

ปัญหาคือ การเสนอร่าง...ตั้งแต่ชั้นรับร่างในวาระแรกจนถึงชั้นแปรญัตติในวาระที่สองก่อให้เกิดปัญหาทางกฎหมายประการใดและเนื้อหาของกฎหมายที่แท้จริงควรจะเป็นประการใด

เนื้อหาของกฎหมายที่แท้จริงควรจะบัญญัติอย่างไรนั้น สามารถพิจารณาจากเหตุผลของร่าง ... ที่เสนอให้แก่ที่ประชุมสภาผู้แทนราษฎร โดยร่าง... เสนอให้มีการบัญญัติกฎหมายโดยมีเหตุผลว่า

“เนื่องจากปัจจุบันการใช้เอกสาร วัตถุอื่นใดหรือข้อมูล ที่จัดทำขึ้นในลักษณะบัตรอิเล็กทรอนิกส์ เช่น บัตรเครดิต บัตรเดบิต บัตรสมาร์ทการ์ด หรือบัตรอื่นใดในลักษณะคล้ายกัน โดยมีวัตถุประสงค์เพื่อใช้ประโยชน์ในการชำระค่าสินค้า ค่าบริการ หรือหนี้อื่น หรือเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อย่างหนึ่งอย่างใด กำลังเพิ่มปริมาณและประเภทการใช้งานอย่างแพร่หลาย และปรากฏว่าได้มีการกระทำความผิดเกี่ยวกับบัตรและลักลอบนำข้อมูลอิเล็กทรอนิกส์ของผู้อื่นมาใช้อันส่งผลกระทบต่อเศรษฐกิจและผู้บริโภคในวงกว้าง สมควรกำหนดความผิดอาญาสำหรับการกระทำความผิดเกี่ยวกับบัตรและข้อมูลอิเล็กทรอนิกส์ดังกล่าวเพิ่มเติมให้ครอบคลุมการกระทำความผิดในรูปแบบต่างๆ และให้มีอัตราโทษเหมาะสมกับความร้ายแรงของการกระทำความผิด จึงจำเป็นต้องตราพระราชบัญญัตินี้”

เมื่ออ่านร่าง...ของคณะรัฐมนตรีในชั้นรับร่างแล้ว จะพบว่าการบัญญัติมาตรา 1(14) โดยให้ความหมายของคำว่า “บัตรอิเล็กทรอนิกส์” นั้น เนื้อหาส่วนใหญ่แทบจะไม่มีอะไรแตกต่างจากมาตรา 1(14) ที่ได้มีการแยกเป็น (ก) (ข) และ (ค) ในชั้นแปรญัตติอันเป็นความหมายที่ปรากฏในประมวลกฎหมายอาญาในปัจจุบัน เพียงแต่เป็นการแยกมาตรา 1(14) เดิม ออกเป็น 2 ตอน คือ ตอนต้นให้เป็นมาตรา 1(14)(ก) และ ตอนปลาย ตั้งแต่คำว่า “และให้หมายความรวมถึง” ให้เป็นมาตรา 1(14)(ข) โดยไม่ได้เปลี่ยนความหมายใดๆ อีก ทั้งได้บัญญัติเพิ่มให้มีมาตรา 1(14)(ค) ขึ้นมาเท่านั้น

---

[60] รายงานการประชุมสภาผู้แทนราษฎร ชุดที่ 21 ปีที่ 3 ครั้งที่ 22 (สมัยสามัญนิติบัญญัติ) เป็นพิเศษ วันที่ 15 ตุลาคม 2546 หน้า 103

การดังกล่าวทำให้เกิดข้อสังเกตคือ การแยกมาตรา 1(14) เดิม ให้ออกเป็น (ก) และ (ข) นั้น อาจส่งผลต่อการตีความกฎหมายได้ กล่าวคือเดิมนั้นข้อความในมาตรา 1(14) เป็นข้อความเดียวกันทั้งหมด ซึ่งการตีความว่าบัตรอิเล็กทรอนิกส์นั้นเมื่ออ่านข้อความทั้งหมดในมาตรา 1(14) เดิมประกอบกัน และนำเอาเหตุผลของร่าง... ตอนหนึ่งที่เขียนว่า “ปรากฏว่าได้มีการกระทำความผิดเกี่ยวกับบัตรและลักลอบนำข้อมูลอิเล็กทรอนิกส์ของผู้อื่นมาใช้...สมควรกำหนดความผิดอาญาสำหรับการกระทำความผิดเกี่ยวกับบัตรและข้อมูลอิเล็กทรอนิกส์...ให้ครอบคลุมการกระทำความผิดในรูปแบบต่างๆ” ดังนั้นเนื้อหาของกฎหมายที่แท้จริงแล้ว บัตรอิเล็กทรอนิกส์น่าจะหมายถึงเอกสารหรือวัตถุอื่นใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งรวมถึงข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ ที่อยู่ในบัตรนั้นด้วย เพียงแต่ผู้เสนอร่าง... เกรงว่าจะไม่ครอบคลุมถึงรูปแบบของบัตรอิเล็กทรอนิกส์ทั้งหมด จึงเพิ่มข้อความในตอนท้ายว่า “และให้หมายความรวมถึง ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้” ด้วยเท่านั้น แต่การแยกมาตรา 1(14) เดิม ให้ออกเป็น (ก) และ (ข) ทำให้มีการตีความกฎหมายแยกจากกันดังเช่นปรากฏในปัจจุบัน กล่าวคือตีความว่าบัตรอิเล็กทรอนิกส์คือ

(1) เอกสารหรือวัตถุอื่นใดซึ่งต้องมีการออกให้โดยไม่รวมถึงข้อมูลในเอกสารหรือวัตถุอื่นใดนั้นด้วย[61] ตามมาตรา (14)(ก) และ

(2) ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ ตามมาตรา (14)(ข)

ซึ่งการตีความกฎหมายดังกล่าวอันเนื่องจากการแยกบทบัญญัติของมาตรา 1(14) ในร่าง... ออกเป็นมาตรา 1(14)(ก) และ 1(14)(ข) ทำให้เกิดปัญหาดังที่กล่าวมาในข้อ 3.3.1

เมื่อพิจารณาต่อมาแล้วพบว่า ร่าง...เดิม ได้กำหนดให้มีบทบัญญัติต่างหากเกี่ยวกับการกระทำผิดอันมีวัตถุแห่งการกระทำเป็นข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์ เป็นเรื่องเฉพาะในมาตรา 269/6 และมาตรา 269/6/1 นั้นเพราะหากพิจารณาดูในคำนิยามคำว่า “บัตรอิเล็กทรอนิกส์” ในร่าง...เดิม ตามมาตรา 1(14) นั้น ผู้ร่างคงรู้ดีอยู่แล้วว่าอาจมีการตีความว่าข้อมูลในบัตรอิเล็กทรอนิกส์ที่มีการออกเอกสารหรือวัตถุอื่นใดให้ด้วยนั้นจะไม่เป็น “บัตรอิเล็กทรอนิกส์” ตามคำนิยามดังกล่าวด้วย ซึ่งปัจจุบันแนวคิดเช่นนี้ก็มีนักกฎหมายหลายท่านเห็นด้วย[62] จึงต้องมีการบัญญัติแยกออกมาเป็นการ

---

[61] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 306.

[62] เช่น ดร.เกียรขจร วัจนะสวัสดิ์, วีระวัฒน์ ปวาราจารย์, สมศักดิ์ เอี่ยมพลับใหญ่, สมศักดิ์ เธียรจรูญกุล

เฉพาะเพื่อตัดปัญหาและเพื่อความชัดเจน ให้มีการกระทำความผิดเกี่ยวกับการใช้ข้อมูลบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ และการมีไว้เพื่อนำออกใช้ซึ่งข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยไม่ชอบ ตามมาตรา 269/6 และมาตรา 269/6/1 ตามลำดับ[63] ซึ่งมีความสอดคล้องกับเหตุผลของร่าง... ตอนหนึ่งที่เขียนว่า “สมควรกำหนดความผิดอาญาสำหรับการกระทำความผิดเกี่ยวกับ... ข้อมูลอิเล็กทรอนิกส์... เพิ่มเติมให้ครอบคลุมการกระทำความผิดในรูปแบบต่างๆ” เนื้อหาของกฎหมายที่แท้จริงแล้วข้อมูลและรหัสบัตรอิเล็กทรอนิกส์ในรูปแบบต่างๆ จึงควรได้รับการคุ้มครองทางกฎหมายด้วย

ดังนั้นการที่กรรมาธิการในชั้นแปรญัตติร่าง...ได้เสนอร่าง...ใหม่ โดยการตัดมาตรา 269/6 และมาตรา 269/6/1 ทิ้งไปเพราะเห็นว่าซ้ำซ้อนกับมาตราอื่นและเห็นว่า “ความหมายของบัตรอิเล็กทรอนิกส์ก็รวมถึงข้อมูลอยู่แล้ว” นั้น นับว่าเป็นความเห็นที่คลาดเคลื่อนกับบทบัญญัติของกฎหมาย อันเป็นการทำให้บทบัญญัติของประมวลกฎหมายอาญาในปัจจุบันไม่ครอบคลุมถึงการกระทำความผิดที่มีวัตถุแห่งการกระทำเป็นข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์อย่างครบถ้วน กล่าวคือ แม้ความหมายของบัตรอิเล็กทรอนิกส์จะไม่รวมข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ โดยที่ได้มีการออกเอกสารหรือวัตถุอื่นใดให้ ตามมาตรา 1(14) แต่หากมาตรา 269/6 และมาตรา 269/6/1 ยังไม่ได้โดนตัดทิ้งออกไป ก็ยังสามารถนำบทบัญญัติดังกล่าวมาปรับใช้กับการกระทำความผิดที่มีวัตถุแห่งการกระทำที่เป็นข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์ได้อย่างครบถ้วนโดยมิต้องคำนึงถึงความหมายของมาตรา 1(14) เป็นสำคัญอีกต่อไป ดังนั้นการตัดบทบัญญัติดังกล่าวออกจึงทำให้เนื้อหาของกฎหมายที่แท้จริงนั้นเปลี่ยนไปและขัดกับเจตนารมของการยกร่างกฎหมายดังที่แสดงในเหตุผลของร่าง... ด้วย อันทำให้เกิดปัญหาการนำบทบัญญัติในเรื่องความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์มาใช้[64] กับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นต้นมา

[63] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 346.

[64] ดูหัวข้อที่ 3.3.2 ปัญหาการนำบทบัญญัติในหมวดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์มาใช้กับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

3.4 อุปสรรคในการนำบทบัญญัติอื่นที่มีลักษณะใกล้เคียงมาบังคับใช้แทน

นอกจากความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ที่บัญญัติในประมวลกฎหมายอาญา ภาค 2 ลักษณะ 7 หมวด 4 แล้ว บทบัญญัติของกฎหมายไทยลักษณะอื่นๆ ที่เกี่ยวข้องกับเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้น มีปรากฏอยู่กระจัดกระจายในกฎหมายหลายมาตราทั้งที่อยู่ในกฎหมายฉบับเดียวกันและต่างฉบับกัน ทำให้การแสวงหาบทบัญญัติที่เกี่ยวข้องเพื่อที่จะนำผู้กระทำความผิดในลักษณะนี้มาลงโทษ จำต้องศึกษาและวิเคราะห์เสียก่อนว่า บทบัญญัติของกฎหมายไทยในลักษณะอื่นๆ ที่มีใช้อยู่นั้นได้บัญญัติให้การกระทำความผิดในลักษณะนี้เป็นความผิดแล้วหรือไม่และครอบคลุมเพียงใดและจะสามารถใช้บทบัญญัติของกฎหมายอื่นๆ ที่มีอยู่แก้ไขปัญหาดังกล่าวได้หรือไม่ ซึ่งบทบัญญัติของกฎหมายไทยที่ใกล้เคียงที่ผู้วิจัยเห็นว่าจำต้องยกขึ้นพิจารณานั้น มีดังต่อไปนี้

3.4.1 ประมวลกฎหมายอาญา

ประมวลกฎหมายอาญาเป็นบทบัญญัติพื้นฐานของความรับผิดทางอาญาทั้งปวง จึงจำต้องยกขึ้นพิจารณาเป็นอันดับแรกว่า จะมีบทบัญญัติอื่นใดที่สามารถปรับใช้กับการกระทำความผิดที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้อีกบ้าง อันได้แก่

3.4.1.1 ความผิดฐานลักทรัพย์

การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้น มีปัญหาในการใช้บทบัญญัติในความผิดฐานลักทรัพย์ เพราะโดยลักษณะของความผิดนั้นมีแนวคำพิพากษาของศาลฎีกาที่ใช้เทียบเคียงได้และนำมาตีความได้ว่าการดึงข้อมูลจากบัตรจากบัตรอิเล็กทรอนิกส์กับการลักทรัพย์โดยนำบัตรอิเล็กทรอนิกส์ที่ทำปลอมขึ้นไปกดเงินออกจากตู้จ่ายเงินอัตโนมัตินั้นเป็นการกระทำความผิดต่างกรรมต่างวาระกัน[65] ซึ่งต้องมีการลงโทษทุกกรรมเรียงกระทงความผิดไปตามประมวลกฎหมายอาญามาตรา 91 จากแนวความคิดดังกล่าวทำให้ต้องพิจารณาว่าการกระทำความผิดโดยการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์จะเป็นความผิดฐานลักทรัพย์หรือไม่ก่อนเป็นอันดับแรก ซึ่งแยกต่างหากจากการนำข้อมูลที่ได้มาจากการดึง ไปทำการปลอมบัตรอิเล็กทรอนิกส์แล้วนำบัตรที่ทำการปลอมนั้นออกใช้

---

[65] เทียบเคียงกับคำพิพากษาศาลฎีกาที่ 300/2546, 2512/2550, 464/2551 และ 15397/2557 ที่วางหลักว่าการลักบัตรอิเล็กทรอนิกส์และการนำบัตรอิเล็กทรอนิกส์ที่ลักไปกดเงินออกจากตู้จ่ายเงินอัตโนมัติ ถือว่าผู้กระทำมีเจตนาต่างกัน การกระทำดังกล่าวจึงเป็นความผิดหลายกรรมต่างกัน ให้ลงโทษทุกกรรมเป็นกระทงความผิดไป ตามมาตรา 91

ความผิดฐานลักทรัพย์ บัญญัติอยู่ในมาตรา 334 ความว่า “ผู้ใดเอาทรัพย์ของผู้อื่นหรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วยไปโดยทุจริต ผู้นั้นกระทำความผิดฐานลักทรัพย์ ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินหกหมื่นบาท” ซึ่งสามารถแยกองค์ประกอบความผิดได้ดังนี้[66]

องค์ประกอบภายนอก

(1) ผู้ใด (ผู้กระทำ)

(2) เอาไป (การกระทำ)

(3) ทรัพย์ของผู้อื่น หรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วย (วัตถุแห่งการกระทำ)

องค์ประกอบภายใน

(1) เจตนา หมายถึง เจตนาธรรมดา คือ ประสงค์ต่อผล หรือเล็งเห็นผล

(2) เจตนาพิเศษ คือ โดยทุจริต

ความผิดฐานลักทรัพย์นั้น ต้องประกอบด้วยการกระทำที่สำคัญทางกายภาพ 2 ประการ คือ 1. การเอาไป และ 2. ต้องเอาไปซึ่งทรัพย์ของผู้อื่นหรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วย โดยต้องปรากฏว่าผู้อื่นนั้นได้ครอบครองทรัพย์นั้นอยู่ในขณะที่เอาไป ซึ่งบุคคลนั้นได้ใช้อำนาจครอบครองอยู่ตามความเป็นจริง โดยสามารถจัดการแก่ทรัพย์นั้นในทางหนึ่งทางใดก็ได้โดยไม่อาจถูกขัดขวางจากผู้อื่นและผู้กระทำความผิดได้เอาทรัพย์นั้นไปเสียจากความครอบครองของบุคคลนั้น[67]

3.4.1.1.1 ผู้กระทำ “เอาไป” ซึ่งทรัพย์นั้น

การเอาไปนั้น เป็นการเอาทรัพย์เคลื่อนที่ไปจากการครอบครองของผู้อื่นในลักษณะตัดกรรมสิทธิ์ตลอดไป หรือในลักษณะของการแย่งกรรมสิทธิ์และการครอบครอง[68] และเริ่ม

---

[66] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 3, พิมพ์ครั้งที่ 1 (กรุงเทพฯ: หจก.จิรรัชการพิมพ์, 2550), หน้า 19.

[67] หยุด แสงอุทัย, กฎหมายอาญา ภาค 2-3, พิมพ์ครั้งที่ 7 (กรุงเทพฯ: สำนักพิมพ์วิทยาลัยธรรมศาสตร์, 2538), หน้า 259-261.

[68] มนต์ชัย ชนินทรลีลา, คู่มือประมวลกฎหมายอาญา ภาค 2 ความผิด ภาค 3 ลหุโทษ พร้อมตัวอย่างย่อหลักกฎหมายจากคำพิพากษาศาลฎีกา,, พิมพ์ครั้งที่ 1 (กรุงเทพฯ: พลสยาม, 2547), หน้า 157.

เป็นการเอาไปเมื่อกรรมสิทธิ์และการครอบครองของบุคคลถูกกระทบ[69] อันต่างกับความผิดฐานยักยอกที่ไม่ได้ทำร้ายการครอบครองเพราะในความผิดฐานยักยอกนั้นผู้กระทำความผิดได้ครอบครองทรัพย์นั้นอยู่แล้ว[70] นั่นคือจะมีการ “เอาไป” ได้จะต้องปรากฏในเบื้องต้นก่อนว่าผู้อื่นนั้นได้ครอบครองทรัพย์ไว้ขณะที่มีการเอาไป การครอบครองนี้ไม่ได้หมายถึงสิทธิครอบครองในทางแพ่ง แต่เป็นศัพท์เฉพาะของประมวลกฎหมายอาญา หมายถึง บุคคลนั้นได้ใช้อำนาจปกครองทรัพย์อยู่ตามความเป็นจริงโดยการที่เขาสามารถจัดการแก่ทรัพย์นั้นในทางหนึ่งทางใดโดยไม่มีใครสามารถขัดขวางได้ ตามจารีตประเพณี ลักษณะของทรัพย์ วิธีที่เจ้าของหรือผู้ครอบครองทรัพย์อาจขัดขวางมิให้ผู้อื่นเข้าเกี่ยวข้องกับทรัพย์ ระยะทางใกล้ไกลระหว่างผู้ครอบครองกับทรัพย์นั้น และบุคคลดังกล่าวต้องมีเจตจำนง (will) ที่จะครอบครองทรัพย์นั้นด้วย[71]

สำหรับคำว่า “เอาไป” นั้นมีความเห็นของนักกฎหมายแบ่งออกเป็น 2 แนว คือ แนวความคิดแรก เป็นความเห็นของศาลฎีกาที่ถือว่าการเอาไปย่อมสำเร็จบริบูรณ์ต่อเมื่อผู้กระทำได้พาเอาทรัพย์นั้นเคลื่อนที่ไปในลักษณะที่พาเอาไปได้ ไม่ว่าจะเคลื่อนที่ได้เล็กน้อยเพียงใดก็ตาม แม้ยังไม่ได้เข้าครอบครองทรัพย์นั้นอย่างเด็ดขาดแต่สามารถควบคุมทิศทางการเคลื่อนที่ของทรัพย์นั้นได้แล้ว[72] ก็เท่ากับว่าเป็นการเอาไปอันกระทบต่อการครอบครองทรัพย์ของผู้อื่นแล้ว ส่วนแนวความคิดหลัง เป็นแนวความคิดเห็นในทางตำรากฎหมาย เห็นว่าการเอาไปย่อมสำเร็จบริบูรณ์ต่อเมื่อผู้กระทำความผิดได้ไปซึ่งการครอบครองทรัพย์นั้น คือมีอำนาจอันแท้จริงเหนือทรัพย์นั้น โดยพิจารณาจากจารีตประเพณี ลักษณะของทรัพย์ ความสามารถที่จะขัดขวางมิให้ผู้อื่นเข้ามาเกี่ยวข้องและระยะห่างของทรัพย์นั้นระหว่างผู้ครอบครองเดิมกับผู้กระทำความผิด ซึ่งความผิดจะสำเร็จได้โดยผู้กระทำมิจำต้องเอามือแตะต้องตัวทรัพย์ดังกล่าวเลย[73] ข้อสังเกตคือหากผู้กระทำมีอำนาจกระทำได้โดยการได้รับอนุญาตโดยตรงหรือโดยปริยายจากเจ้าของทรัพย์หรือผู้แทนเจ้าของทรัพย์แล้ว แม้จะเป็นการถือวิสาสะไปบ้าง การกระทำก็ไม่เป็นการเอาไปและไม่เป็นความผิดฐานลักทรัพย์[74]

---

[69] คณิต ณ นคร, กฎหมายอาญาภาคความผิด, หน้า 383.

[70] เรื่องเดียวกัน, หน้า 388.

[71] หยุด แสงอุทัย, กฎหมายอาญา ภาค 2-3, หน้า 283.

[72] จิตติ ติงศภัทิย์, คำอธิบายประมวลกฎหมายอาญา ภาค 2 ตอน 2 และภาค 3, พิมพ์ครั้งที่ 3 (กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2532), หน้า 2327-2328.

[73] ทวีเกียรติ มีนะกนิษฐ์, "ความผิดฐานลักทรัพย์," วารสารนิติศาสตร์, 16 (2529): 34.

[74] หยุด แสงอุทัย, กฎหมายอาญา ภาค 2-3, หน้า 284-285.

ประเด็นปัญหาที่ต้องพิจารณาคือ ข้อมูลที่อยู่ในบัตรอิเล็กทรอนิกส์นั้น จะสามารถมีการกระทำในลักษณะตามนิยามของคำว่า “เอาไป” อันจะเป็นความผิดฐานลักทรัพย์ได้หรือไม่

ดังที่ได้กล่าวมาแล้วว่า การเอาไปนั้น เป็นการเอาทรัพย์เคลื่อนที่ไปจากการครอบครองของผู้อื่นในลักษณะตัดกรรมสิทธิ์ตลอดไป หรือในลักษณะของการแย่งกรรมสิทธิ์และการครอบครอง และการกระทำที่เป็นการทำร้ายการครอบครองอย่างเดียว โดยไม่ทำร้ายกรรมสิทธิ์ ไม่เป็นการเอาไป[75] การทำร้ายกรรมสิทธิ์และการครอบครองจึงเป็นตัวแปรสำคัญของนิยามคำว่าเอาไป ซึ่งหากกระทบเพียงอย่างใดอย่างหนึ่งแล้วไม่ใช่การเอาไปอันเป็นความผิดฐานลักทรัพย์ แต่อาจเป็นความผิดประเภทอื่น[76] ดังนั้นนิยามคำว่า การเอาไป จึงมีประเด็นที่ต้องพิจารณาถึง 2 ส่วนประกอบกันดังนี้

1. กรรมสิทธิ์ของบุคคลถูกกระทบ

กรรมสิทธิ์ (Eigentum : ownership) ไม่ได้บัญญัติความหมายไว้ในประมวลกฎหมายอาญา ดังนั้นจึงต้องศึกษาความหมายจากประมวลกฎหมายแพ่งและพาณิชย์ ตามหลักที่ว่ากฎหมายต่างๆ เกี่ยวข้องซึ่งกันและกัน[77] ซึ่งตามประมวลกฎหมายแพ่งและพาณิชย์มาตรา 1295 กล่าวว่า “ทรัพยสิทธิทั้งหลายนั้น ท่านว่าจะก่อตั้งขึ้นได้แต่ด้วยอาศัยอำนาจในประมวลกฎหมายนี้หรือกฎหมายอื่น” ในเรื่อง กรรมสิทธิ์ นั้นได้บัญญัติไว้บรรพ 4 ของประมวลกฎหมายแพ่งและพาณิชย์จึงมีสภาพเป็นทรัพยสิทธิ (Real right)[78] อันเป็นสิทธิที่จะบังคับเอาแก่ตัวทรัพย์โดยตรง[79] และคำว่า ทรัพย์ ตามมาตรา 137 หมายถึง วัตถุมีรูปร่าง ดังนั้นกรรมสิทธิ์ จึงหมายถึง สิทธิในสิ่งที่มีรูปร่าง[80] และข้อมูลที่อยู่ในบัตรอิเล็กทรอนิกส์นั้นมีสภาพเป็นข้อมูลอิเล็กทรอนิกส์ประเภทหนึ่ง อาศัยความหมายจาก พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ซึ่งได้ให้คำนิยามคำว่า “อิเล็กทรอนิกส์” และ “ข้อมูลอิเล็กทรอนิกส์” ไว้ เมื่ออ่านประกอบกันแล้วจะได้ความหมายของคำ

---

[75] คณิต ณ นคร, กฎหมายอาญาภาคความผิด, หน้า 384.

[76] เช่น การกระทำที่ทำร้ายเพียงการครอบครอง โดยไม่ทำร้ายกรรมสิทธิ์ เป็นความผิดฐานโกงเจ้าหนี้ ตามมาตรา 349

[77] หยุด แสงอุทัย, กฎหมายอาญา ภาค 2-3, หน้า 287..

[78] ต่างจากบุคคลสิทธิ (Personal right) คือสิทธิที่มีอยู่เหนือบุคคล เป็นสิทธิที่บังคับเอาแก่ตัวบุคคลให้กระทำการหรือมิให้กระทำการอย่างใดอย่างหนึ่ง ซึ่งในลักษณะหนี้เรียกว่าสิทธิเรียกร้อง

[79] บัญญัติ สุชีวะ, คำอธิบายกฎหมายลักษณะทรัพย์, พิมพ์ครั้งที่ 15 (กรุงเทพฯ: กรุงสยามพับลิชชิ่ง, 2556), หน้า 60-63.

[80] คณิต ณ นคร, กฎหมายอาญาภาคความผิด, หน้า 382.

ว่า “ข้อมูลอิเล็กทรอนิกส์” ว่าหมายถึง “ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือ ประมวลผลด้วยวิธีการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่น แม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทาง แสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่างๆ เช่นว่านั้น” ในเมื่อข้อความจากการประยุกต์ใช้อิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า ไม่สามารถมองเห็นได้ด้วยตาเปล่าได้ จึงสรุปได้ว่าข้อมูลอิเล็กทรอนิกส์ เป็นสิ่งที่ไม่มีรูปร่าง ดังนั้นข้อมูลในบัตรอิเล็กทรอนิกส์ซึ่งเป็นสิ่งที่ไม่มีรูปร่าง บุคคลจึงไม่อาจมีกรรมสิทธิ์ในข้อมูลดังกล่าวได้ เมื่อไม่อาจมีกรรมสิทธิ์ได้แล้วทำร้ายกรรมสิทธิ์จากการกระทำการ “เอาไป” จึงไม่อาจเกิดขึ้นได้เลย หรือกล่าวอีกนัยหนึ่งได้ว่า ข้อมูลในบัตรอิเล็กทรอนิกส์ไม่อาจมีการกระทำการ “เอาไป” ในความผิดฐานลักทรัพย์ได้นั่นเอง

2. การครอบครองของบุคคลถูกกระทบ

การเอาไปจะสำเร็จบริบูรณ์เมื่อการครอบครองเก่าหมดไปและการครอบครองใหม่เข้ามาแทนที่[81] แต่ว่าในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้น ลักษณะการกระทำเป็นเพียงการทำสำเนา (Copy) อันเป็นคุณสมบัติเฉพาะตัวของข้อมูลอิเล็กทรอนิกส์ที่สามารถจำลองตนเองเสมือนต้นฉบับได้ (Duplicate) โดยไม่มีที่สิ้นสุดและไม่ผิดเพี้ยนหรือที่เรียกว่าการสำเนาข้อมูล (Data backup) การครอบครองข้อมูลในบัตรอิเล็กทรอนิกส์จึงไม่อาจถูกกระทบได้[82] เพราะบุคคลที่ยังครอบครองข้อมูลอยู่นั้นไม่ว่าจะเป็นธนาคารพาณิชย์ในฐานะผู้ออกบัตรให้หรือเจ้าของบัตรผู้เป็นเจ้าของข้อมูล ก็ยังคงได้ใช้อำนาจปกครองทรัพย์อยู่ตามความเป็นจริง ยังมีสิทธิเต็มที่ในการจัดการข้อมูลนั้นอันเป็นต้นฉบับในทางหนึ่งทางใดโดยไม่มีใครสามารถขัดขวางได้ จึงไม่ทำให้การครอบครองเก่าหมดไป เพียงแต่อาจมีการครอบครองใหม่โดยผู้กระทำความผิดจากการทำสำเนานั้น เมื่อการครอบครองไม่ถูกทำร้ายจึงไม่มีการ “เอาไป” อันเป็นความผิดฐานลักทรัพย์ แต่ศาลฎีกา[83] และนักกฎหมายส่วนใหญ่[84] มักไม่เห็นด้วยกับหลักการครอบครองเก่าหมดไปและการครอบครองใหม่แทนที่ แต่กลับเห็นว่าการเอาไปจะบริบูรณ์เมื่อผู้กระทำเอาทรัพย์เคลื่อนที่ในลักษณะเอาไปได้ไม่ว่าจะเคลื่อนได้เพียงเล็กน้อยก็ตาม[85] ซึ่งต้องเป็นการพาทรัพย์เคลื่อนที่ไปในลักษณะที่เป็นการตัดกรรมสิทธิ์ของ

---

[81] เรื่องเดียวกัน, หน้า 385.

[82] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, พิมพ์ครั้งที่ 1 (กรุงเทพฯ: กรุงสยาม พับลิชชิ่ง, 2559), หน้า 149.

[83] คำพิพากษาศาลฎีกาที่ 2074/2514

[84] จิตติ ติงศภัทิย์, คำอธิบายประมวลกฎหมายอาญา ภาค 2 ตอน 2 และภาค 3, พิมพ์ครั้งที่ 7 (กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2553), หน้า 540.

[85] คณิต ณ นคร, กฎหมายอาญาภาคความผิด, หน้า 383.

เจ้าของทรัพย์ตลอดไปและทำให้ทุกๆจุดของทรัพย์นั้นได้เคลื่อนที่จากที่แต่ละจุดของทรัพย์ที่ตั้งอยู่ (every part of the property must be moved)[86] อย่างไรก็ดีหากใช้เกณฑ์ตามความเห็นดังกล่าว วินิจฉัย การทำสำเนาข้อมูลก็ไม่ได้ทำให้ข้อมูลเคลื่อนที่จากแหล่งหนึ่งไปสู่อีกแหล่งหนึ่ง ข้อมูลแหล่งเดิมก็ยังคงอยู่และไม่หายไป เมื่อไม่มีการพาทรัพย์เคลื่อนที่การเอาไปจึงไม่เกิดขึ้นเช่นเดียวกัน

3.4.1.1.2 ทรัพย์ของผู้อื่นหรือผู้อื่นเป็นเจ้าของรวมอยู่ด้วย

วัตถุแห่งการกระทำความผิดฐานลักทรัพย์ คือ ทรัพย์ของผู้อื่น หรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วย ดังนั้นจึงต้องพิจารณาถึงความหมายของคำว่า “ทรัพย์”[87] เสียก่อน ซึ่งประมวลกฎหมายอาญาไม่ได้มีบทนิยาม คำว่า “ทรัพย์” ไว้ ดังนั้น “ทรัพย์” จึงต้องมีความหมายเดียวกันกับประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 137 ซึ่งได้บัญญัติว่า “อันว่าทรัพย์นั้น ได้แก่ วัตถุมีรูปร่าง” ซึ่งศาลฎีกาของประเทศไทยนั้นเห็นพ้องด้วย[88] ซึ่งทรัพย์ในเรื่องการกระทำความผิดเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้นสามารถพิจารณาแยกออกมาได้ 2 กรณี ดังนี้

(1) การกระทำความผิดต่อตัวบัตรอิเล็กทรอนิกส์

บัตรอิเล็กทรอนิกส์ ที่มีลักษณะทางกายภาพซึ่งเป็นวัตถุที่มีรูปร่าง อันได้แก่ บัตรอิเล็กทรอนิกส์ตามคำนิยามของมาตรา 1(14)(ก) คือ “เอกสารหรือวัตถุอื่นใดไม่ว่าจะมีรูปลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า” อาทิ บรรดาบัตรประเภทต่างๆ เช่น บัตรเครดิต บัตรเดบิต บัตรเอทีเอ็ม บัตรซิมการ์ด บัตรสมาร์ตการ์ด[89] และบัตรอิเล็กทรอนิกส์ตามมาตรา 1(14)(ค) คือ “สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของนั้น” อาทิ ลายนิ้วมือ ลายมือ ลายเท้า อวัยวะนัยน์ตา ซึ่งเป็นส่วนของ

---

[86] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 3, หน้า 78.

[87] เรื่องเดียวกัน, หน้า 20.

[88] หยุด แสงอุทัย, กฎหมายอาญา ภาค 2-3, พิมพ์ครั้งที่ 11 (กรุงเทพฯ: โรงพิมพ์มหาวิทยาลัยธรรมศาสตร์, 2553), หน้า 286.

[89] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 304.

ร่างกาย หากได้มีการแยกออกมาจากร่างกายแล้ว[90] ต่างก็เป็นทรัพย์ที่เป็นวัตถุแห่งการกระทำความผิดฐานลักทรัพย์ จึงมีการลักกันได้[91]

(2) การกระทำความผิดต่อข้อมูลซึ่งอยู่ในบัตรอิเล็กทรอนิกส์

ข้อมูลซึ่งอยู่ในบัตรอิเล็กทรอนิกส์นั้น โดยสภาพเป็นวัตถุที่ไม่มีรูปร่าง ซึ่งจะเป็นทรัพย์ที่มีการลักกันได้หรือไม่นั้น การพิจารณาดังกล่าวจึงต้องอาศัยการเทียบเคียงจากประเด็นทางกฎหมายที่เคยได้มีข้อโต้แย้งเกิดขึ้นมาก่อนแล้วนั่นก็คือความผิดเรื่องการลักกระแสไฟฟ้า โดยแนวความเห็นของนักกฎหมายในเรื่องการลักกระแสไฟฟ้านั้นแบ่งออกเป็น 2 ฝ่าย ฝ่ายแรกซึ่งเป็นความเห็นของนักกฎหมายเยอรมันและสวิสเห็นว่า คำว่าทรัพย์ต้องอาศัยความหมายเช่นเดียวกับบทบัญญัติในประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 137 ซึ่งหมายถึงเฉพาะแต่วัตถุมีรูปร่างเท่านั้น กระแสไฟฟ้าซึ่งเป็นวัตถุที่ไม่มีรูปร่าง เป็นแต่เพียงพลังงาน[92] จึงไม่ใช่ทรัพย์ ดังนั้นประเทศเยอรมันและสวิสจึงไม่ถือว่าการลักกระแสไฟฟ้าเป็นความผิดฐานลักทรัพย์ และได้มีบทบัญญัติพิเศษเพื่อลงโทษความผิดฐานเอาพลังงานของผู้อื่นไปใช้โดยไม่มีอำนาจ[93] ซึ่งศาสตราจารย์ ดร.คณิต ณ นคร ก็เห็นด้วยกับฝ่ายนี้ เพราะเห็นว่าคุณธรรมทางกฎหมาย (Rechtsgut : legal interest) ของความผิดฐานลักทรัพย์ประการหนึ่งคือ “กรรมสิทธิ์” (Eigentum : ownership) ซึ่งเป็นสิทธิในทรัพย์ (Dingliches Recht : real right) หรือสิทธิในสิ่งที่มีรูปร่างเท่านั้น “สิทธิในไฟฟ้า” ซึ่งเป็นสิ่งที่ไม่มีรูปร่าง จึงไม่ใช่ “กรรมสิทธิ์” การลักกระแสไฟฟ้าจึงเป็นความผิดฐานลักทรัพย์ไม่ได้[94] แตกต่างจากฝ่ายหลังที่เห็นว่าทรัพย์นั้นคือบรรดาสิ่งอันบุคคล สามารถมีกรรมสิทธิ์ถืออำนาจเป็นเจ้าของได้ ไม่ว่าจะเคลื่อนที่ได้หรือเคลื่อนที่ไม่ได้ก็ดี[95] ซึ่งศาสตราจารย์จิตติ ติงศภัทิย์ มีความเห็นว่า คำว่าทรัพย์นั้นหมายความรวมถึงสิ่งที่ไม่มีรูปร่างดังเช่นกระแสไฟฟ้าด้วยเพราะคำว่าทรัพย์และทรัพย์สินที่ใช้ในประมวลกฎหมายอาญา ยังมีการใช้ปะปนกันอยู่หาได้แยกจากกันโดยเคร่งครัด อีกทั้งกระแสไฟฟ้าแม้เป็นวัตถุที่ไม่มีรูปร่าง แต่มีราคาถือเอาได้และนำพาไปเสียจากเจ้าของได้โดยอาศัยเจตนาทุจริตแล้ว จึง

---

[90] หยุด แสงอุทัย, กฎหมายอาญา ภาค 2-3, หน้า 286.

[91] คำพิพากษาศาลฎีกาที่ 2512/2550 “จำเลยได้ลักทรัพย์และเอาไปเสียซึ่งบัตรอิเล็กทรอนิกส์ของธนาคาร ก. ที่ออกให้แก่ผู้เสียหายไปโดยทุจริต ในประการที่น่าจะเกิดความเสียหายแก่ผู้เสียหาย ธนาคาร ก. ผู้อื่นและประชาชน ความผิดดังกล่าวย่อมสำเร็จเมื่อจำเลยลักเอาบัตรดังกล่าวไป”

[92] หยุด แสงอุทัย, กฎหมายอาญา ภาค 2-3, หน้า 260 และ คณิต ณ นคร, กฎหมายอาญาภาคความผิด, พิมพ์ครั้งที่ 5 (กรุงเทพฯ: สำนักพิมพ์วิทยาลัยธรรมศาสตร์, 2537), หน้า 135.

[93] หยุด แสงอุทัย, กฎหมายอาญา ภาค 2-3, หน้า 286.

[94] คณิต ณ นคร, กฎหมายอาญาภาคความผิด, หน้า 382.

[95] พระยานิพนธ์พจนาตถ์, กฎหมายลักษณะอาญา รศ. 127 (พระนคร: กรุงเทพ-บรรณาคาร, 2478), หน้า 262.

ต้องมีความผิดฐานลักทรัพย์เหมือนเช่นกรณีลักทรัพย์ทั่วไปและในต่างประเทศเช่น ประเทศอังกฤษ อเมริกา อินเดีย และฝรั่งเศส การลักกระแสไฟฟ้าศาลก็จะลงโทษฐานลักทรัพย์เช่นเดียวกัน

ส่วนในประเทศไทยนั้น เดิมได้มีคำพิพากษาที่เกี่ยวข้องกับเรื่องการลักกระแสไฟฟ้าแบ่งออกเป็น 2 แนวทาง คำพิพากษาชุดแรก คือ คำพิพากษาฎีกาที่ 5354/2539 ที่ตัดสินว่า จำเลยนำโทรศัพท์มือถือมาทำการปรับจูนโดยใช้เครื่องดีเลอโค๊ดและก๊อปปี้คลื่นสัญญาณโทรศัพท์ของผู้เสียหายแล้วใช้โทรศัพท์มือถือดังกล่าวทำการรับส่งวิทยุคมนาคมโดยไม่ได้รับอนุญาตจากเจ้าพนักงานผู้ออกใบอนุญาตนั้น เป็นเพียงการทำการรับส่งวิทยุคมนาคม โดยอาศัยคลื่นสัญญาณโทรศัพท์ของผู้เสียหายโดยไม่ได้รับอนุญาต หรือเป็นการแย่งใช้คลื่นสัญญาณโทรศัพท์ของผู้เสียหายโดยไม่มีสิทธิ มิใช่เป็นการเอาทรัพย์ของผู้อื่นไปโดยทุจริต การกระทำของจำเลยตามฟ้องจึงไม่เป็นความผิดฐานลักทรัพย์ตาม ป.อ. มาตรา 334[96] และคำพิพากษาชุดต่อมา ได้แก่ คำพิพากษาฎีกาที่ 877/2501 และ 1880/2542 ที่ตัดสินว่า การลักกระแสไฟฟ้าย่อมเป็นผิดตามประมวลกฎหมายอาญามาตรา 334 หรือ 335 แล้วแต่กรณี[97] สัญญาณโทรศัพท์เป็นกระแสไฟฟ้าที่แปลงมาจากเสียงพูดเคลื่อนที่ไปตามสายลวดตัวนำจากที่หนึ่งไปยังอีกที่หนึ่ง จำเลย ลักเอาสัญญาณโทรศัพท์จากตู้โทรศัพท์สาธารณะซึ่งอยู่ในความครอบครองขององค์การโทรศัพท์แห่งประเทศไทยไปใช้เพื่อประโยชน์ของจำเลยโดยทุจริต จึงเป็นความผิดฐานลักทรัพย์เช่นเดียวกับการลักกระแสไฟฟ้า[98] โดยเฉพาะคำพิพากษาชุดหลังที่ได้ตัดสินว่าการลักกระแสไฟฟ้าเป็นความผิดฐานลักทรัพย์นี้ ศาสตราจารย์ ดร.คณิต ณ นคร กล่าวว่า ศาลฎีการะบุเพียงแต่ผลเท่านั้น โดยมิได้ระบุเหตุผลแห่งการตัดสินเลย กรณีจึงเป็นการฝ่าฝืนประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 186(6), 214, 215 และ 225 ที่เป็นพื้นฐานในการประกันการประสาทความยุติธรรมและเป็นการพิพากษาที่ขัดต่อ “หลักประกันในกฎหมายอาญา”[99] (Nullum crimen, nulla poena sine lege) ในข้อ “การห้ามใช้กฎหมายที่ใกล้เคียงอย่างยิ่งในกฎหมายอาญา” (Analogieverbot : prohibition of analogy)[100] อันเป็นหลักเกณฑ์อันสำคัญของมาตรา 2[101] ซึ่งคำพิพากษาทั้ง 2 แนวทางดังกล่าวนั้น ทำให้เกิดปัญหาในการใช้ความผิดฐานลัก

---

[96] คำพิพากษาศาลฎีกาที่ 5354/2539

[97] คำพิพากษาศาลฎีกาที่ 877/2501

[98] คำพิพากษาศาลฎีกาที่ 1880/2542

[99] คณิต ณ นคร, กฎหมายอาญาภาคความทั่วไป, พิมพ์ครั้งที่ 4 (กรุงเทพฯ: สำนักพิมพ์วิญญูชน, 2554), หน้า 65.

[100] คณิต ณ นคร, กฎหมายอาญาภาคความผิด, หน้า 381-382.

[101] มาตรา 2 วรรคแรก บัญญัติว่า “บุคคลจักต้องรับโทษในทางอาญาต่อเมื่อได้กระทำการอันกฎหมายที่ใช้ในขณะกระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแก่ผู้กระทำความผิดนั้น ต้องเป็นโทษที่บัญญัติไว้ในกฎหมาย”

ทรัพย์กับวัตถุที่ไม่มีรูปร่างอย่างยิ่ง และเป็นที่วิพากษ์วิจารณ์ในทางทฤษฎีกฎหมายอย่างมาก[102] อย่างไรก็ตาม ต่อมาได้มีคำพิพากษาฎีกาที่ 5161/2547 ที่ตัดสินว่า “การที่จำเลยนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลจากแผ่นบันทึกข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ของโจทก์ร่วม เป็นความผิดฐานลักทรัพย์หรือไม่ โจทก์ร่วมฎีกาว่า ข้อมูลในเครื่องคอมพิวเตอร์ของโจทก์ร่วมมีรูปร่างเป็นตัวอักษร ภาพ แผนผัง และตราสาร จึงเป็นทรัพย์ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 137 การที่จำเลยเอาข้อมูลของโจทก์ร่วมดังกล่าวไปจึงเป็นความผิดฐานลักทรัพย์ เห็นว่า ข้อมูล ตามพจนานุกรมให้ความหมายว่า "ข้อเท็จจริงหรือสิ่งที่ถือหรือยอมรับว่าเป็นข้อเท็จจริง สำหรับใช้เป็นหลักอนุมานหาความจริงหรือการคำนวณ" ส่วนข้อเท็จจริงหมายความว่า "ข้อความแห่งเหตุการณ์ที่เป็นมาหรือที่เป็นอยู่ตามจริง ข้อความหรือเหตุการณ์ที่จะต้องวินิจฉัยว่าเท็จหรือจริง" ดังนั้น ข้อมูลจึงไม่นับเป็นวัตถุมีรูปร่าง สำหรับตัวอักษร ภาพ แผนผัง และตราสารเป็นเพียงสัญลักษณ์ที่ถ่ายทอดความหมายของข้อมูลออกจากแผ่นบันทึกข้อมูลโดยอาศัยเครื่องคอมพิวเตอร์ มิใช่รูปร่างของข้อมูล เมื่อประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 137 บัญญัติว่า ทรัพย์ หมายความว่า วัตถุมีรูปร่าง ข้อมูลในแผ่นบันทึกข้อมูลจึงไม่ถือเป็นทรัพย์ การที่จำเลยนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลจากแผ่นบันทึกข้อมูลของโจทก์ร่วม จึงไม่เป็นความผิดฐานลักทรัพย์ตามฟ้อง ศาลล่างทั้งสองพิพากษายกฟ้อง ศาลฎีกาเห็นพ้องด้วย ฎีกาของโจทก์ร่วมทุกข้อฟังไม่ขึ้น” ดังนั้นจึงเป็นอันยุติว่า หากวัตถุแห่งการกระทำนั้นเป็นข้อมูลในแผ่นบันทึกซึ่งไม่มีรูปร่าง จึงไม่ใช่ทรัพย์ ทำนองเดียวกันกับข้อมูลซึ่งอยู่ในบัตรอิเล็กทรอนิกส์อันมีลักษณะอย่างเดียวกัน การคัดลอกข้อมูลจากบัตรอิเล็กทรอนิกส์จึงไม่เป็นความผิดฐานลักทรัพย์

3.4.1.2 ความผิดฐานปลอมเอกสาร

จากคำนิยามของคำว่า “บัตรอิเล็กทรอนิกส์” ประเภทหนึ่ง[103] ตามมาตรา 1(14)(ก)[104] ที่ให้ความหมายว่าคือ “เอกสาร” ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้โดยบันทึกข้อมูลหรือรหัสไว้ให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่

---

[102] ศิริภัทร ธรรมเขต, “ความผิดฐานลักทรัพย์ : ศึกษากรณีการลักทรัพย์ไม่มีรูปร่าง,” (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ มหาวิทยาลัยรามคำแหง, 2550), หน้า 1-165.

[103] มาตรา 1(14) “บัตรอิเล็กทรอนิกส์” แบ่งได้เป็น 3 ประเภท ตามความหมายในอนุมาตรา ก ข และ ค

[104] ประมวลกฎหมายอาญามาตรา 1(14)(ก) “บัตรอิเล็กทรอนิกส์ หมายความว่า เอกสารหรือวัตถุอื่นใดไม่ว่าจะมีรูปลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า”

สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า ประกอบกับแนวคำพิพากษาของศาลฎีกาที่วางหลักเพิ่มเติมว่า ตัวบัตรอิเล็กทรอนิกส์เป็นเอกสาร ตามมาตรา 1(7)[105] การปลอมบัตรอิเล็กทรอนิกส์จึงเป็นความผิดฐานปลอมเอกสารด้วย[106] อันกล่าวได้ว่า บัตรอิเล็กทรอนิกส์ที่อยู่ในรูปแบบเอกสารนั้นย่อมได้รับความคุ้มครองตามประมวลกฎหมายอาญาเรื่องความผิดเกี่ยวกับเอกสารแล้ว แต่เนื่องจากบัตรอิเล็กทรอนิกส์นั้นมักจะมีการบันทึกข้อมูลลงไปในบัตรเพื่อใช้งานควบคู่กันด้วย ซึ่งอาจมองเห็นด้วยตาเปล่า เช่น การพิมพ์อักษรนูนบนบัตร หรือที่มองไม่เห็นด้วยตาเปล่าโดยการฝังชิปหรือติดแถบแม่เหล็กที่เป็นแหล่งบันทึกข้อมูลดังกล่าว จึงมีปัญหาว่าหากเกิดการปลอมบัตรอิเล็กทรอนิกส์ที่เป็นเอกสารขึ้นแล้ว ความผิดฐานปลอมเอกสารจะสามารถใช้ให้ครอบคลุมไปถึงข้อมูลที่บันทึกอยู่ในบัตรอิเล็กทรอนิกส์นั้นได้หรือไม่เพียงใด ด้วยปัญหาดังกล่าวจึงจำต้องนำหลักเกณฑ์ของความผิดฐานปลอมเอกสารมาวิเคราะห์กับการกระทำความผิดในลักษณะการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ด้วย

เอกสารปลอมคือ เอกสารที่แสดงออกว่าผู้ใดทำเอกสารซึ่งแท้จริงแล้วผู้นั้นมิได้ทำเอกสารนั้นหรือมิได้ให้อำนาจผู้อื่นให้ทำเอกสารนั้น ไม่ว่าผู้ใดที่แสดงออกในเอกสารนั้นจะมีตัวตนอยู่จริงหรือไม่[107] จึงเป็นการหลอกในตัวผู้ทำเอกสารเพื่อให้เข้าใจว่าเป็นเอกสารที่คนอื่นทำขึ้น และไม่

---

[105] คำพิพากษาศาลฎีกาที่ 6820/2552 “การที่จำเลยเอาไปเสียซึ่งเอกสารบัตรเครดิตวีซ่าการ์ดของบริษัท บ. อันเป็นบัตรอิเล็กทรอนิกส์ และเอกสารตาม ป.อ. มาตรา 1 (7) ซึ่งออกให้แก่ น. ในประการที่น่าจะเกิดความเสียหายแก่ น. และบริษัท บ. แล้ว การกระทำของจำเลยจึงเป็นความผิดตามบทบัญญัติมาตรา 188

การที่จำเลยเอาไปเสียซึ่งบัตรเครดิตวีซ่าการ์ดของบริษัท บ. ซึ่งออกให้แก่ น. แล้วใช้บัตรเครดิตวีซ่าการ์ดดังกล่าวชำระค่าสินค้าแทนการชำระด้วยเงินสดอันเป็นความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นชำระค่าสินค้า ค่าบริการหรือหนี้อื่นแทนการชำระด้วยเงินสดโดยมิชอบตาม ป.อ. มาตรา 269/5 และ มาตรา 269/7 รวม 3 ครั้ง เมื่อปรากฏว่าโจทก์ฟ้องจำเลยแยกออกเป็นข้อๆ และการกระทำตามที่โจทก์บรรยายฟ้องมาในแต่ละข้อต่างเป็นความผิดสำเร็จในตัวเองต่างกรรมต่างวาระ ทั้งทรัพย์ที่จำเลยได้จากการกระทำผิดก็เป็นทรัพย์คนละประเภทแตกต่างกัน เมื่อจำเลยให้การรับสารภาพตามฟ้องถือได้ว่าจำเลยกระทำความผิดโดยมีเจตนาต่างกัน การกระทำของจำเลยฐานเอาไปเสียซึ่งเอกสารบัตรเครดิตกับฐานใช้บัตรเครดิตจึงเป็นความผิดหลายกรรมตาม ป.อ. มาตรา 91 และเมื่อข้อเท็จจริงฟังได้ตามฟ้องและคำให้การรับสารภาพของจำเลยว่าจำเลยนำบัตรเครดิตวีซ่าการ์ดดังกล่าวไปใช้ชำระค่าสินค้าโทรศัพท์เคลื่อนที่ กล้องวีดีโอและกล้องถ่ายรูปดิจิทัลแทนการชำระด้วยเงินสดจำนวน 3 คราว การกระทำของจำเลยในส่วนนี้จึงเป็นความผิด 3 กรรมต่างกัน”

[106] คำพิพากษาศาลฎีกาที่ 3873/2551 “การที่ธนาคารผู้ออกบัตร ATM ทั้งหลายต่างออกแบบให้ด้านหลังของบัตร ATM มีช่องให้เจ้าของบัตรลงลายมือชื่อไว้นั้น นอกจากจะมีวัตถุประสงค์มีไว้เพื่อระบุตัวเจ้าของบัตรแล้วยังอาจมีวัตถุประสงค์เป็นประการอื่น ๆ ด้วย การที่จำเลยปลอมลายมือชื่อของโจทก์ร่วมในบัตร ATM ของโจทก์ร่วม แม้ลายมือชื่อปลอมจะมิใช่สาระสำคัญของการใช้บัตร ATM ในการทำรายการเบิกถอนเงินที่ตู้เบิกถอนเงิน ATM ก็ตาม การกระทำของจำเลยที่ลงลายมือชื่อปลอมที่หลังบัตร ATM ของโจทก์ร่วมก็ถือได้ว่าน่าจะเกิดความเสียหายแก่โจทก์ร่วมและธนาคารผู้ออกบัตร และได้กระทำเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารแท้จริง อันเป็นการครบองค์ประกอบความผิดตาม ป.อ. มาตรา 264 วรรคแรก ประกอบมาตรา 265”

[107] คำพิพากษาศาลฎีกาที่ 278/2501

จำต้องมีเอกสารที่แท้จริงอยู่ก่อนไม่จำต้องทำให้เหมือนของจริง[108] และไม่ต้องคำนึงว่าข้อความที่เขียนลงในเอกสารนั้นจะจริงหรือเท็จแต่ประการใด[109] ซึ่งต่างกับเอกสารเท็จซึ่งเป็นเอกสารที่แสดงออกว่าบุคคลผู้ทำเอกสารได้ทำเอกสารนั้นขึ้นมาจริงๆ เพียงแต่ข้อความในเอกสารนั้นไม่ตรงกับความจริงอันเป็นข้อความเท็จ[110]

ความผิดฐานปลอมเอกสาร บัญญัติอยู่ในมาตรา 264 ความว่า “ผู้ใดทำเอกสารปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด เติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใด ๆ ในเอกสารที่แท้จริง หรือประทับตราปลอม หรือลงลายมือชื่อปลอมในเอกสาร โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ถ้าได้กระทำเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารที่แท้จริง ผู้นั้นกระทำความผิดฐานปลอมเอกสาร ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดกรอกข้อความลงในแผ่นกระดาษหรือวัตถุอื่นใด ซึ่งมีลายมือชื่อของผู้อื่นโดยไม่ได้รับความยินยอม หรือโดยฝ่าฝืนคำสั่งของผู้อื่นนั้น ถ้าได้กระทำเพื่อนำเอาเอกสารนั้นไปใช้ในกิจการที่อาจเกิดเสียหายแก่ผู้หนึ่งผู้ใดหรือประชาชน ให้ถือว่าผู้นั้นปลอมเอกสาร ต้องระวางโทษเช่นเดียวกัน”

จากบทบัญญัติดังกล่าวสามารถแยกได้ออกเป็น 2 กรณีคือ การปลอมเอกสารโดยตรง ตามวรรคแรก และไม่ใช่การปลอมเอกสารโดยตรง แต่ให้ถือว่าเป็นการปลอมเอกสาร ตามวรรคสอง ซึ่งตามวรรคสองนั้น องค์ประกอบภายนอกคือการกระทำการกรอกข้อความลงในแผ่นกระดาษหรือวัตถุอื่นใด ซึ่งมีลายมือชื่อของผู้อื่น แต่ผู้วิจัยต้องการศึกษาเฉพาะกรณีการดึงข้อมูลออกมา ไม่ใช่การกรอกข้อความลงไป ซึ่งต่างกันในลักษณะของการกระทำอย่างมากจึงไม่นำวรรคสองมาวิเคราะห์เพราะเห็นว่าไม่เกี่ยวข้องกับเรื่องที่กำลังศึกษา ดังนั้นสามารถแยกองค์ประกอบความผิดของวรรคแรกได้ดังนี้[111]

---

[108] จิตติ ติงศภัทิย์, กฎหมายอาญา ภาค 2 ตอน 1, พิมพ์ครั้งที่ 5 (กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2523), หน้า 1835.

[109] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 153.

[110] เรื่องเดียวกัน, หน้า 150-154.

[111] เรื่องเดียวกัน, หน้า 150.

องค์ประกอบภายนอก

(1) ผู้ใด (ผู้กระทำ)

(2) (การกระทำ)

(ก) ทำเอกสารปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด

(ข) เติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใดๆ ในเอกสารที่แท้จริง

(ค) ประทับตราปลอม หรือลงลายมือชื่อปลอมในเอกสาร

(3) เอกสาร (วัตถุแห่งการกระทำ)

(4) โดยประการที่น่าจะเกิดความเสียหายต่อผู้อื่นหรือประชาชน (พฤติการณ์ประกอบการกระทำ)

องค์ประกอบภายใน

(1) เจตนา หมายถึง เจตนาธรรมดา คือ ประสงค์ต่อผล หรือเล็งเห็นผล

(2) เจตนาพิเศษ คือ เพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารที่แท้จริง

จากบทบัญญัติดังกล่าวจะเห็นได้ว่าการปลอมเอกสารคือการกระทำอย่างใดอย่างหนึ่งต่อไปนี้ คือ 1. การทำเอกสารที่ไม่แท้จริงขึ้น กล่าวคือ การทำเอกสารปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด การประทับตราปลอมหรือการลงลายมือชื่อปลอม หรือ 2. การทำเอกสารที่แท้จริงให้ผิดไปจากเดิม กล่าวคือ การเติมหรือตัดทอนข้อความหรือแก้ไขด้วยประการใดๆ ในเอกสารที่แท้จริง ส่วนการตัดทอนแก้ไขเอกสารที่ตนเองทำขึ้นก่อนส่งมอบให้บุคคลอื่น ไม่เป็นการกระทำที่กระทบต่อคุณธรรมทางกฎหมายของความผิดฐานนี้ที่ปกป้องความมั่นคงและความเชื่อถือในการใช้เป็นพยานหลักฐาน จึงไม่ผิดฐานปลอมเอกสาร[112]

[112] คณิต ณ นคร, กฎหมายอาญาภาคความผิด, หน้า 664-665.

3.4.1.2.1 ความหมายของคำว่าเอกสาร

วัตถุแห่งการกระทำความความผิดฐานปลอมเอกสารคือ เอกสาร ดังนั้นจึงต้องพิจารณาก่อนว่าลักษณะและหลักเกณฑ์ของคำว่า เอกสาร นั้นหมายถึงอะไร เพื่อจะทำการวิเคราะห์ว่าข้อมูลในบัตรอิเล็กทรอนิกส์อยู่ในขอบข่ายอันจะถือว่าเป็นเอกสารหรือไม่ เพราะการดึงข้อมูลออกจากบัตรอิเล็กทรอนิกส์ย่อมเป็นการทำสำเนาให้ข้อมูลไปปรากฏบนวัตถุอีกแหล่งหนึ่ง ซึ่งจากลักษณะดังกล่าว ถ้าหากปรากฏว่าคำว่าเอกสารนั้น รวมไปถึงข้อมูลใดๆ ในบัตรอิเล็กทรอนิกส์ด้วย การทำสำเนาข้อมูลย่อมเป็นการปลอมเอกสาร อันจะทำให้บทบัญญัติความผิดเกี่ยวกับการปลอมเอกสารสามารถนำมาใช้กับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้

“เอกสาร” มีนิยามอยู่ในมาตรา 1(7) หมายความว่า “กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น”

จากบทนิยามดังกล่าวสามารถแยกออกพิจารณาเป็นข้อๆ ได้ดังนี้[113]

(ก) กระดาษหรือวัตถุอื่นใด

หมายความถึงสิ่งที่ใช้รองรับสำหรับทำให้ความหมายของถ้อยคำปรากฏขึ้น เอกสารนั้นไม่ใช่ตัวถ้อยคำที่แสดงความหมาย แต่มุ่งถึงวัตถุที่ทำให้ปรากฏความหมายขึ้น ซึ่งตามปกติแล้วคือ กระดาษ แต่อาจเป็นวัตถุอื่นได้ เช่น ไม้โลหะ ศิลา กำแพง เครื่องคอมพิวเตอร์ หรือแม้กระทั่ง หิมะ ทราย ตัวอักษรในอากาศ[114] ร่างกายของสัตว์ ร่างกายของคน

(ข) ทำให้ปรากฏ

หมายความว่าต้องมีการกระทำของบุคคลให้ปรากฏความหมายขึ้นบนกระดาษหรือวัตถุอื่นใดนั้น จะปรากฏโดยชั่วคราวหรือยั่งยืนก็ไม่สำคัญ แต่ต้องไม่ใช่การปรากฏขึ้นเองโดยไม่มีการกระทำของบุคคล เช่น ปรอทแสดงสภาพอากาศ นาฬิกาบอกเวลา มิเตอร์แสดงระยะทางและจำนวนค่าโดยสารในรถแท็กซี่

(ค) ความหมาย

คือสิ่งที่ทำให้ปรากฏขึ้นนั้นต้องแสดงความคิดของผู้ทำเอกสาร จะเป็นที่เข้าใจหรือไม่ก็ตาม เช่น รอยขีดที่จดคะแนนที่บ่งบอกความหมายว่ามีผู้ลงคะแนนกี่คน รหัสที่

---

[113] จิตติ ติงศภัทิย์, กฎหมายอาญา ภาค 2 ตอน 1, หน้า 1825-1834.

[114] เรื่องเดียวกัน, หน้า 1826.

เขียนไว้ที่สิ่งใดๆ แม้ไม่มีผู้ใดเข้าใจได้ แต่แสดงความหมายถึงการจัดประเภทสิ่งนั้นๆ ลายมือชื่อที่เขียนไว้โดยให้มีความหมายแสดงว่าเป็นเจ้าของ ภาพถ่ายลายพิมพ์นิ้วมือในการพิสูจน์หลักฐาน ภาพถ่ายบุคคลที่ปิดอยู่บนบัตรแสดงตัว

(ง) ด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น

หมายความว่า อ่านหรือเห็นความหมายได้โดยการสัมผัสทางตา รวมถึงอักษรที่ทำให้คนตาบอดอ่านผสมอักษรผ่านการสัมผัสด้วยมือซึ่งใช้แทนตาด้วย แต่การแสดงเครื่องหมายผ่านความร้อนและเย็น หรือใช้เสียง เช่น การอัดเทปอัดแผ่นเสียง หรือสิ่งที่ไม่มีรูปร่างและไม่สามารถมองเห็นด้วยตาได้ เช่น ข้อมูลในคอมพิวเตอร์[115] ไม่ใช่เอกสาร ดังนั้นการปรากฏความหมายโดยการรับรู้ผ่านประสาทสัมผัสทางตาจึงเป็นเกณฑ์สำคัญว่าสิ่งนั้นๆ เป็นเอกสารหรือไม่

(จ) โดยวิธีการพิมพ์ ถ่ายภาพหรือวิธีอื่น

หมายถึงวิธีจารึกเครื่องหมายให้ปรากฏบนวัตถุด้วยวิธีใดวิธีหนึ่ง เช่น การเขียน ตีตราข้อความ แกะสลัก พ่นสี พ่นควัน

(ฉ) อันเป็นหลักฐานแห่งความหมายนั้น

หมายความว่าต้องปรากฏคงทนอยู่ชั่วขณะหนึ่งแม้ไม่นาน คือต้องมีรูปร่าง เช่น อากาศยานทำอักษรในอากาศด้วยควัน การเขียนข้อความบนทราย บนหิมะ ภาพถ่ายหรือภาพยนตร์ที่แสดงการเคลื่อนไหว แต่ไม่ใช่การทำเครื่องหมายด้วยการคลื่นไหวของร่าง เช่น ยกมือยกไม้[116]

ส่วนคำว่า “ข้อมูล” ตามพจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554 ให้ความหมายว่า “ข้อเท็จจริง หรือสิ่งที่ถือหรือยอมรับว่าเป็นข้อเท็จจริง สำหรับใช้เป็นหลักอนุมานหาความจริงหรือการคำนวณ” อันมีลักษณะเป็นข้อมูลดิบ หรือข้อเท็จจริงต่างๆ ที่ใช้ในชีวิตประจำวัน อาจแทนที่ด้วยสัญลักษณ์ต่างๆ ที่แทนปริมาณหรือการกระทำต่างๆ ซึ่งยังไม่ผ่านการกลั่นกรองหรือประมวลผล และอาจอยู่ในรูปของตัวเลข ตัวอักษร ข้อความ ภาพ และเสียง เป็นต้น[117] แต่เนื่องจากข้อมูลที่อยู่ในบัตรอิเล็กทรอนิกส์รูปแบบเอกสารนั้นมีสภาพเป็นข้อมูลอิเล็กทรอนิกส์ประเภทหนึ่ง จึงต้องอาศัยความหมายจาก พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ซึ่งได้ให้คำ

---

[115] ทวีเกียรติ มีนะกนิษฐ์, คำอธิบายกฎหมายอาญา ภาคความผิดและลหุโทษ, หน้า 171.

[116] จิตติ ติงศภัทิย์, กฎหมายอาญา ภาค 2 ตอน 1, หน้า 1834.

[117] สุเนติ คงเทพ, กฎหมายเกี่ยวกับคอมพิวเตอร์, พิมพ์ครั้งที่ 2 (กรุงเทพฯ: มังกุ๊ดดิจิตอลเพรส, 2561), หน้า 151.

นิยามคำว่า “ข้อมูลอิเล็กทรอนิกส์” ว่าหมายถึง “ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร”

ในการวิเคราะห์ปัญหาว่าหลักเกณฑ์ของคำว่า เอกสาร จะครอบไปถึงข้อมูลที่อยู่ในบัตรอิเล็กทรอนิกส์หรือไม่นั้น สามารถจำแนกตามลักษณะของข้อมูลที่อยู่ในบัตรอิเล็กทรอนิกส์ในรูปแบบเอกสาร ได้เป็น 2 ลักษณะคือ

(1) ข้อมูลที่ปรากฏอยู่บนผิวของบัตรอิเล็กทรอนิกส์

ข้อมูลที่ปรากฏอยู่บนผิวของบัตรอิเล็กทรอนิกส์ในรูปแบบเอกสาร ไม่ว่าด้านหน้าหรือด้านหลัง และไม่ว่าบัตรอิเล็กทรอนิกส์นั้นเป็นกระดาษหรือวัตถุอื่นใด เช่น พลาสติก เหรียญทรงกลม ต่างก็เป็นการกระทำให้ปรากฏความหมายของบุคคล โดยวิธีพิมพ์ ถ่ายภาพหรือวิธีอื่นๆ อันเป็นตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น เช่น หมายเลขบัตรเอทีเอ็ม ตัวอักษรพิมพ์นูนบนบัตร วันที่บัตรหมดอายุ รูปถ่ายบนบัตร ชื่อ นามสกุล ที่อยู่ วันเดือนปีเกิด หมายเลขบัตรประชาชน ลายมือชื่อที่ลงไว้หลังบัตร หรือตราสัญลักษณ์แสดงถึงผู้ออกให้ ซึ่งสามารถอ่านหรือเห็นความหมายได้โดยการสัมผัสทางตาให้มนุษย์เข้าใจได้ ดังนั้น ข้อมูลที่ปรากฏอยู่บนผิวของบัตรอิเล็กทรอนิกส์จึงเป็นเอกสาร ที่ผู้ทำเอกสารการปลอมจะมีความผิดฐานปลอมเอกสารได้ ดังที่แนวคำพิพากษาของศาลฎีกาได้วางหลักไว้แล้ว[118]

[118] คำพิพากษาศาลฎีกาที่ 2409/2534 “บัตรประจำตัวประชาชนเป็นเอกสารที่เจ้าพนักงานสำนักงานทะเบียนบัตรประชาชนกระทรวงมหาดไทยได้ทำขึ้น บัตรประจำตัวประชาชนจึงเป็นเอกสารราชการตามบทนิยามของประมวลกฎหมายอาญา มาตรา 1(8) จำเลยที่ 1 ที่ 2 และที่ 5 กับพวกร่วมกันนำบัตรประจำตัวประชาชนของจำเลยที่ 1 ซึ่งเจ้าพนักงานได้ทำขึ้นสำหรับเป็นบัตรประจำตัวประชาชนของจำเลยที่ 1 ตามกฎหมาย มาทำปลอมให้หลงเชื่อว่าเป็นบัตรประจำตัวประชาชนของ ป. ที่แท้จริง แล้วสำเนาภาพถ่ายบัตรประจำตัวประชาชนที่ปลอมแล้วเอาไปใช้อ้างต่อโจทก์ร่วม จึงถือได้ว่าสำเนาภาพถ่ายบัตรประจำตัวประชาชนปลอมนั้นเป็นเอกสารราชการปลอมนั่นเอง จำเลยที่ 1 ที่ 2 และที่ 5 กับพวกจึงมีความผิดฐานร่วมกันปลอมและใช้เอกสารราชการปลอม”

คำพิพากษาศาลฎีกาที่ 3873/2551 “การที่ธนาคารผู้ออกบัตร ATM ทั้งหลายต่างออกแบบให้ด้านหลังของบัตร ATM มีช่องให้เจ้าของบัตรลงลายมือชื่อไว้นั้น นอกจากจะมีวัตถุประสงค์มีไว้เพื่อระบุตัวเจ้าของบัตรแล้วยังอาจมีวัตถุประสงค์เป็นประการอื่น ๆ ด้วย การที่จำเลยปลอมลายมือชื่อของโจทก์ร่วมในบัตร ATM ของโจทก์ร่วม แม้ลายมือชื่อปลอมจะมิใช่สาระสำคัญของการใช้บัตร ATM ในการทำรายการเบิกถอนเงินที่ตู้เบิกถอนเงิน ATM ก็ตาม การกระทำของจำเลยที่ลงลายมือชื่อปลอมที่หลังบัตร ATM ของโจทก์ร่วมก็ถือได้ว่าน่าจะเกิดความเสียหายแก่โจทก์ร่วมและธนาคารผู้ออกบัตร และได้กระทำเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารแท้จริง อันเป็นการครบองค์ประกอบความผิดตาม ป.อ. มาตรา 264 วรรคแรก ประกอบมาตรา 265”

(2) ข้อมูลที่บันทึกอยู่ในชิปหรือในแถบแม่เหล็กหรือในบัตรอิเล็กทรอนิกส์

ข้อมูลที่บันทึกอยู่ในชิปหรือในแถบแม่เหล็กหรือในบัตรอิเล็กทรอนิกส์รูปแบบเอกสาร แม้จะได้มีกระดาษหรือวัตถุอื่นใดรองรับแหล่งบันทึกข้อมูลนั้น ซึ่งข้อมูลอาจอยู่ในรูปของตัวเลข ตัวอักษร ข้อความ ภาพ และเสียง อันมีลักษณะคล้ายคลึงกับ ตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น ในลักษณะของเอกสารก็ตาม แต่มนุษย์ไม่สามารถอ่านหรือเห็นความหมายของข้อมูลที่บันทึกอยู่ได้โดยการสัมผัสทางตา จึงจำต้องมีการกระทำให้ปรากฏความหมายอีกครั้งหนึ่งโดยบุคคล เช่น การแตะ การสอด การรูด บัตรอิเล็กทรอนิกส์ดังกล่าวกับเครื่องมืออิเล็กทรอนิกส์ เช่น เครื่องรูดบัตรอัตโนมัติ (EDC) เครื่องอ่านบัตรสมาร์ทการ์ด (Smart card reader) เครื่องอ่านบัตรแถบแม่เหล็ก (Magnetic card reader) ให้ไปปรากฏอยู่บนอีกเครื่องมืออิเล็กทรอนิกส์หนึ่ง เช่น หน้าจอเครื่องคอมพิวเตอร์ ประกอบกับความหมายของ “ข้อมูลอิเล็กทรอนิกส์” นั้นเป็น ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือ ประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เมื่อข้อความจากการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่น แม่เหล็กไฟฟ้า ไม่สามารถมองเห็นได้ด้วยตาเปล่าได้ จึงสรุปได้ว่าข้อมูลอิเล็กทรอนิกส์เป็นสิ่งที่ไม่มีรูปร่าง อันขาดองค์ประกอบซึ่งเป็นสาระสำคัญของการเป็นเอกสาร ตามความเห็นของ ศาสตราจารย์ จิตติ ติงศภัทย์ ศาสตราจารย์ ดร.ทวีเกียรติ มีนะกนิษฐ์[119] และศาสตราจารย์ ดร.คณิต ณ นคร[120] ทั้งเจตนารมณ์ของเอกสารก็คือสิ่งที่มนุษย์ทำขึ้นเพื่อให้มนุษย์เอง “เข้าใจความหมายเพื่อเป็นหลักฐานแห่งความหมายที่ตนประสงค์ให้หมายถึง ว่าคืออะไร” แต่ ข้อมูล เป็น “สิ่งที่มนุษย์หรือเครื่องจักรหรือคอมพิวเตอร์เข้าใจหรือประมวลผลได้ (Processing)”[121] จากเหตุผลดังที่กล่าวมา จึงสรุปได้ว่า ข้อมูลที่บันทึกอยู่ในชิปหรือในแถบแม่เหล็กหรือในบัตรอิเล็กทรอนิกส์นั้นไม่เข้าหลักเกณฑ์ของคำว่าเอกสาร ดังนั้น เมื่อเกิดการกระทำความผิดโดยการดึงข้อมูลออกจากบัตรอิเล็กทรอนิกส์ แล้วทำให้เกิดสำเนาข้อมูลไปปรากฏบนวัตถุอีกแหล่งหนึ่ง สำเนาข้อมูลที่ได้จากการดึงนั้น ไม่ใช่เอกสาร จึงไม่เป็นการกระทำความผิดฐานปลอมเอกสาร

---

[119] ทวีเกียรติ มีนะกนิษฐ์, คำอธิบายกฎหมายอาญา ภาคความผิดและลหุโทษ, หน้า 171.

[120] คณิต ณ นคร, กฎหมายอาญาภาคความผิด, หน้า 663.

[121] สุเนติ คงเทพ, กฎหมายเกี่ยวกับคอมพิวเตอร์, หน้า 151.

3.4.1.2.2 ลักษณะการกระทำการปลอมเอกสารกับข้อมูลในบัตรอิเล็กทรอนิกส์

เนื่องจากมีแนวคำพิพากษาของศาลฎีกาวางหลักว่า การนำเอกสารไปถ่ายสำเนานั้น เป็นการกระทำการปลอมเอกสารโดยการทำเอกสารปลอมขึ้นทั้งฉบับ จึงจำต้องวิเคราะห์ต่อไปอีกว่า หากเกิดการนำบัตรอิเล็กทรอนิกส์มาถ่ายสำเนาขึ้นจะถือว่าเป็นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์อันเป็นการกระทำความผิดฐานปลอมเอกสารด้วยหรือไม่ ซึ่งถ้าหากการถ่ายสำเนาบัตรอิเล็กทรอนิกส์นั้นเป็นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ด้วย ย่อมสามารถนำความผิดฐานปลอมเอกสารมาปรับใช้ได้

โดยคำพิพากษาของศาลฎีกาเกี่ยวกับการถ่ายสำเนาเอกสารอันเป็นการปลอมเอกสารนั้นสามารถแบ่งได้ดังนั้น

(ก) นำเอกสารที่แท้จริงไปถ่ายสำเนา[122]

(ข) นำเอกสารที่แท้จริงไปถ่ายสำเนา แล้วแก้ไขข้อความในสำเนา[123]

(ค) นำเอกสารที่แท้จริงไปถ่ายสำเนา แล้วแก้ไขข้อความในสำเนาและนำไปถ่ายสำเนาอีก[124]

---

[122] คำพิพากษาศาลฎีกาที่ 2463/2548 “จำเลยถ่ายสำเนาเอกสารแผ่นป้ายแสดงการเสียภาษีรถยนต์ประจำปีและแผ่นป้ายประกันภัยคุ้มครองผู้ประสบภัยจากรถเป็นภาพสีให้ปรากฏข้อความที่มีสี ตัวอักษรและขนาดเหมือนฉบับที่แท้จริงแล้วนำไปติดที่รถยนต์บรรทุกและรถพ่วง มีลักษณะที่ทำให้หลงเชื่อว่าเป็นเอกสารที่แท้จริง โดยประการที่น่าจะเกิดความเสียหายแก่นายทะเบียนยานพาหนะจังหวัดนนทบุรี นายทะเบียนยานพาหนะจังหวัดพะเยา นายทะเบียนยานพาหนะกรุงเทพมหานคร นายทะเบียนกรมการประกันภัย หรือผู้อื่นได้ จึงเป็นการปลอมแปลงเอกสารขึ้นทั้งฉบับ หาใช่ว่าจำเลยจะต้องแก้ไขเปลี่ยนแปลงข้อความให้ผิดแผกแตกต่างไปจากต้นฉบับเอกสารที่แท้จริงไม่ การกระทำของจำเลยจึงเป็นความผิดฐานปลอมเอกสารตาม ป.อ. มาตรา 264 วรรคหนึ่ง”

[123] คำพิพากษาศาลฎีกาที่ 4073/2545 “จำเลยที่ 1 ถ่ายสำเนารายการจดทะเบียนรถจากฉบับที่แท้จริงซึ่งเป็นเอกสารราชการ แล้วแก้ไขรายการในช่องผู้ถือกรรมสิทธิ์เพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าสำเนาดังกล่าวมีข้อความตรงกับต้นฉบับ และน่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน เป็นการทำเอกสารปลอมขึ้นทั้งฉบับ แม้จำเลยที่ 1 จะไม่ได้แก้ไขรายการจดทะเบียนรถในเอกสารที่แท้จริง แต่การกระทำของจำเลยที่ 1 ก็เป็นความผิดฐานปลอมเอกสารราชการตามประมวลกฎหมายอาญา มาตรา 265 แล้ว”

[124] คำพิพากษาศาลฎีกาที่ 1572/2549 “จำเลยถ่ายสำเนาบัตรประจำตัวประชาชนจากฉบับที่แท้จริงซึ่งเป็นเอกสารราชการแล้วแก้ไขในช่องชื่อ ชื่อสกุล วันออกบัตร วันหมดอายุ และนำสำเนาบัตรประจำตัวประชาชนดังกล่าวไปถ่ายสำเนาเอกสารอีก เพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าสำเนาเอกสารดังกล่าวมีข้อความตรงกับต้นฉบับและน่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน เป็นการทำปลอมเอกสารขึ้นทั้งฉบับ แม้จำเลยจะมิได้แก้ไขในเอกสารที่แท้จริง การกระทำของจำเลยก็เป็นความผิดฐานปลอมบัตร

(ง) นำเอกสารปลอมไปถ่ายสำเนา แล้วถ่ายภาพสำเนานั้น[125]

จากคำพิพากษาทั้งหมดดังกล่าว ทำให้ได้หลักเกณฑ์องค์ประกอบภายนอกในการทำเอกสารปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใดที่เป็นการถ่ายสำเนาเอกสารได้ว่า การนำเอกสารที่แท้จริง หรือสำเนา หรือเอกสารปลอม ไปถ่ายสำเนาเอกสารโดยถ่ายสำเนาหรือถ่ายภาพให้เหมือนของจริง ทั้งสี ตัวอักษร และขนาด แม้จะมีการแก้ไขข้อความในสำเนาภายหลังก็ตาม ก็เป็นการทำเอกสารปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด อันเป็นความผิดฐานปลอมเอกสารได้ การแก้ไขข้อความในสำเนาแม้จะไม่ได้ทำลงในเอกสารที่แท้จริงก็ผิดฐานปลอมเอกสารได้เพราะการทำเอกสารปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใดไม่จำต้องทำลงในเอกสารที่แท้จริง ต่างไปจากการเติมหรือตัดทอนข้อความหรือแก้ไขด้วยประการใดๆ ซึ่งต้องกระทำลงในเอกสารที่แท้จริงเท่านั้นจึงจะเป็นความผิด

ในการวิเคราะห์ปัญหาว่าการนำบัตรอิเล็กทรอนิกส์มาถ่ายสำเนาจะเป็นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์อันเป็นการกระทำความผิดฐานปลอมเอกสารด้วยหรือไม่นั้น สามารถจำแนกตามลักษณะของข้อมูลที่อยู่ในบัตรอิเล็กทรอนิกส์ในรูปแบบเอกสาร ได้เป็น 2 ลักษณะคือ

(1) ข้อมูลที่ปรากฏอยู่บนผิวของบัตรอิเล็กทรอนิกส์

ดังที่ได้วิเคราะห์ไปแล้วว่าข้อมูลที่ปรากฏอยู่บนผิวของบัตรอิเล็กทรอนิกส์เป็นเอกสาร[126] ซึ่งการถ่ายสำเนาบัตรอิเล็กทรอนิกส์ย่อมเป็นการทำให้สำเนาซึ่งเป็นเอกสารนั้นปรากฏข้อความที่มีสี ตัวอักษรและขนาดเหมือนบัตรอิเล็กทรอนิกส์ที่เป็นเอกสารฉบับที่แท้จริง[127] จึงเป็นการทำเอกสารปลอมขึ้นทั้งฉบับ อันเป็นความผิดฐานปลอมเอกสารได้

ประจำตัวประชาชนอันเป็นเอกสารราชการและฐานใช้บัตรประจำตัวประชาชนอันเป็นเอกสารราชการปลอมตาม ป.อ. มาตรา 265, 268 วรรคหนึ่ง ประกอบมาตรา 265 พ.ร.บ.บัตรประจำตัวประชาชนฯ มาตรา 14 วรรคหนึ่ง (2) (3)"

[125] คำพิพากษาศาลฎีกาที่ 9026/2553 "หนังสือสัญญาซื้อขายที่ดินเป็นเอกสารสิทธิปลอมภาพถ่ายหนังสือสัญญาซื้อขายที่ดินดังกล่าวที่จำเลยถ่ายสำเนามา จึงเป็นเอกสารสิทธิปลอมด้วย เมื่อจำเลยนำภาพถ่ายหนังสือสัญญาซื้อขายที่ดินไปใช้อ้างเป็นเอกสารแนบท้ายคำร้องและคำฟ้องโดยรู้อยู่แล้วว่าหนังสือสัญญาซื้อขายที่ดินเป็นเอกสารปลอมการกระทำของจำเลยจึงเป็นการใช้เอกสารสิทธิปลอมแล้ว"

[126] โปรดดูหัวข้อที่ 3.4.1.2.1 ความหมายของคำว่าเอกสาร

[127] เทียบเคียง คำพิพากษาศาลฎีกาที่ 2463/2548

(2) ข้อมูลที่บันทึกอยู่ในชิปหรือในแถบแม่เหล็กหรือในบัตรอิเล็กทรอนิกส์

เมื่อมีการถ่ายสำเนาบัตรอิเล็กทรอนิกส์ แม้ว่าในสำเนาจะปรากฏว่ามีรูปชิปหรือแถบแม่เหล็กอยู่ด้วย แต่รูปชิปหรือแถบแม่เหล็กที่ปรากฏในสำเนาเปรียบเสมือนภาพๆ หนึ่งเท่านั้น อันเป็นส่วนที่ปรากฏออกมาภายนอกของแหล่งบันทึกข้อมูล ซึ่งมนุษย์ไม่สามารถอ่านหรือเห็นความหมายของข้อมูลที่บันทึกอยู่ในรูปชิปหรือแถบแม่เหล็กในสำเนานั้นได้โดยการสัมผัสทางตา รูปดังกล่าวจึงไม่ได้แสดงถึงความหมายของข้อมูลภายในแหล่งบันทึกว่าเป็นอย่างไร ซึ่งอาจอยู่ในรูปของตัวเลข ตัวอักษร ข้อความ ภาพ หรือเสียงก็ได้ การถ่ายสำเนาเอกสารจึงเป็นเพียงการทำให้ปรากฏองค์ประกอบภายนอกที่อยู่บนผิวของบัตรอิเล็กทรอนิกส์เท่านั้น ไม่ได้ทำให้ข้อมูลซึ่งอยู่ในบัตรอิเล็กทรอนิกส์ต้นฉบับถูกดึงออกมาด้วย ต่างจากการทำสำเนาข้อมูล (Data backup) ที่เป็นการนำข้อมูลทั้งหมดในแหล่งบันทึกออกมาทำซ้ำแล้วบรรจุอยู่ในแหล่งบันทึกอีกแหล่งหนึ่ง

จึงสรุปได้ว่า หากเกิดการนำบัตรอิเล็กทรอนิกส์มาถ่ายสำเนา จะเป็นความผิดฐานปลอมเอกสารได้เฉพาะตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น ที่ปรากฏอยู่บนผิวของบัตรอิเล็กทรอนิกส์เท่านั้น แต่ไม่รวมไปถึงข้อมูลซึ่งอยู่ในบัตรอิเล็กทรอนิกส์ด้วย กรณีดังกล่าวไม่ถือว่าเป็นการดึงข้อมูลจากแหล่งบันทึกข้อมูลในบัตรอิเล็กทรอนิกส์และไม่อาจนำความผิดฐานปลอมเอกสารมาปรับใช้ได้

3.4.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายที่มีการนำอนุสัญญาว่าด้วยอาชญากรรมไซเบอร์ (Convention on Cybercrime) ของกลุ่มสหภาพยุโรปมาเป็นแม่แบบในการยกร่าง แม้ว่าประเทศไทยจะไม่ได้เป็นสมาชิกของกลุ่มสหภาพยุโรปทั้งไม่ได้ลงชื่อและไม่ได้ให้สัตยาบันแก่อนุสัญญาดังกล่าวเลยก็ตาม แต่ผู้ร่างก็ได้เล็งเห็นว่าระบบคอมพิวเตอร์เป็นส่วนสำคัญในการประกอบกิจการและการดำรงชีวิตของมนุษย์ การกระทำการใดๆ ต่อระบบคอมพิวเตอร์และข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์ ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน จึงมีการร่างพระราชบัญญัติฉบับนี้ขึ้นตามอนุสัญญาดังกล่าวและได้กำหนดโทษทางอาญาแก่การกระทำผิดอันเกี่ยวกับระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ไว้ด้วย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงนับเป็นกฎหมายที่สำคัญซึ่งจะต้องนำมาพิจารณาว่า จะนำมาปรับใช้กับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้หรือไม่ เพียงใด

เมื่อพิจารณาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แล้วพบว่า พระราชบัญญัติดังกล่าวได้บัญญัติการกระทำความผิดต่างๆ โดยมีวัตถุแห่งการกระทำแบ่งได้ออกเป็น 2 ประเภทคือ การกระทำความผิดที่มีวัตถุแห่งการกระทำเป็นระบบคอมพิวเตอร์และการกระทำความผิดที่มีวัตถุแห่งการกระทำเป็นข้อมูลคอมพิวเตอร์ ดังนั้นจึงจำเป็นต้องพิจารณาเสียก่อนว่าวัตถุแห่งการกระทำทั้ง 2 ประการดังกล่าวนั้นหมายถึงอะไรและจะมีความหมายครอบคลุมถึงวัตถุแห่งการกระทำในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้หรือไม่

3.4.2.1 นิยามของคำว่าระบบคอมพิวเตอร์

แม้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะมิได้บัญญัติคำว่าคอมพิวเตอร์ไว้ดังเช่นในอนุสัญญาว่าด้วยอาชญากรรมไซเบอร์อันเป็นกฎหมายแม่แบบ แต่ก็ได้บัญญัตินิยามของคำว่า ระบบคอมพิวเตอร์ ไว้ในมาตรา 3 ดังนี้

มาตรา 3 บัญญัติว่า “ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ความหมายของระบบคอมพิวเตอร์ได้มีการอธิบายขยายความไว้ในเอกสารที่ใช้ประกอบการนำเสนอร่างกฎหมายฉบับนี้ไว้ว่า ระบบคอมพิวเตอร์ ได้แก่ ฮาร์ดแวร์ (Hardware) และซอฟแวร์ (Software) ที่พัฒนาขึ้นเพื่อใช้ประมวลผลข้อมูลดิจิทัล (Digital Data) ซึ่งประกอบไปด้วยตัวเครื่องคอมพิวเตอร์และอุปกรณ์รอบข้าง (Peripheral) ในการป้อนหรือรับข้อมูล (Input) หรือนำออกหรือแสดงข้อมูล (Output) และเก็บหรือบันทึกข้อมูล (Store and Recode) ดังนั้น ระบบคอมพิวเตอร์จึงเป็นอุปกรณ์เพียงเครื่องเดียวหรือหลายเครื่องอันมีลักษณะเป็นชุดเชื่อมต่อกันก็ได้ โดยเป็นการเชื่อมต่อผ่านระบบเครือข่าย (Network) ก็ได้และมีลักษณะการทำงานโดยอัตโนมัติตามคำสั่งโปรแกรมที่มีการกำหนดไว้ เช่น ระบบแลน (LAN) หรือ ระบบแวน (WAN) ที่ติดตั้งภายในอาคาร โดยไม่มีการแทรกแซงโดยตรงจากมนุษย์[128]

แม้จะได้มีคำอธิบายดังกล่าวของสำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีผู้เสนอร่างกฎหมาย แต่ในมุมมองของนักกฎหมายหลายท่านนั้น แม้จะเป็น

[128] มานิตย์ จุมปา, คำอธิบายกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์, พิมพ์ครั้งที่ 2 (กรุงเทพฯ: วิญญูชน, 2554), หน้า 50.

คอมพิวเตอร์ที่มีองค์ประกอบครบถ้วนซึ่งหมายถึงมีฮาร์ดแวร์และซอฟแวร์ก็ยังไม่เข้าความหมายของระบบคอมพิวเตอร์ เพราะโดยเจตนารมณ์แห่งพระราชบัญญัติคอมพิวเตอร์นั้นบัญญัติขึ้นมาเพื่อคุ้มครองสังคมที่ใช้คอมพิวเตอร์ที่มีลักษณะเป็นชุดเชื่อมต่อกัน ดังนั้นการใช้งานคอมพิวเตอร์เครื่องเดี่ยวๆ โดยลำพังที่ไม่ได้เชื่อมต่อกับโครงข่ายคอมพิวเตอร์จะไม่อยู่ในความหมายของระบบคอมพิวเตอร์ เช่น นายดำใช้คอมพิวเตอร์พิมพ์งานแต่อย่างเดียวและไม่ได้เชื่อมต่อระบบใดๆ[129] รวมถึงกรณีนายดำได้ต่อคอมพิวเตอร์เข้าระบบเครือข่ายแลน (LAN) แต่ใช้ระบบดังกล่าวเพียงลำพังโดยไม่มีคนอื่นมาร่วมใช้ด้วยและไม่ติดต่อกับระบบภายนอกเลย[130]

จากความเห็นดังกล่าว หากสิ่งใดก็ตามที่ไม่เข้าลักษณะของคอมพิวเตอร์ ก็ไม่ต้องไปพิจารณาต่อว่าเป็นระบบคอมพิวเตอร์หรือไม่ เพราะตัวมันเองไม่ใช่คอมพิวเตอร์ตั้งแต่แรกแล้ว ดังนั้นการจะวินิจฉัยความรับผิดในพระราชบัญญัตินี้จะต้องทำการวินิจฉัยเสียก่อนว่าวัตถุแห่งการกระทำนั้นเป็นคอมพิวเตอร์หรือไม่ ซึ่งสิ่งใดก็ตามจะเป็นคอมพิวเตอร์ได้นั้นต้องพิจารณาถึงองค์ประกอบภายในสิ่งนั้นว่ามีองค์ประกอบดังนี้ครบหรือไม่[131] คือ

(1) องค์ประกอบด้านฮาร์ดแวร์ (Hardware) หมายถึง อุปกรณ์ต่างๆ ที่เป็นตัวเครื่องคอมพิวเตอร์ เช่น หน่วยประมวลผลกลาง (Central Processing Unit : CPU) หน่วยความจำภายใน (Memory) อันได้แก่ หน่วยความจำชั่วคราว (Random Access Memory : RAM) หน่วยความจำถาวร (Read Only Memory : ROM) หน่วยความจำสำรอง เช่น ฮาร์ดดิสก์ (Hard Disk) แผ่นดิสก์ (Diskett) แผ่นซีดี (CD - Rom) รวมไปถึง แถบแม่เหล็ก (Magnetic Stripe) หรือชิป (Chip) ก็เป็นหน่วยความจำสำรองเช่นเดียวกัน[132]

(2) องค์ประกอบด้านซอฟต์แวร์ (Software) หมายถึง โปรแกรมชุดคำสั่งที่เขียนให้เครื่องคอมพิวเตอร์ปฏิบัติตาม[133]

ซึ่งจากองค์ประกอบของการเป็นคอมพิวเตอร์และนิยามของระบบคอมพิวเตอร์ในมาตรา 3 ดังกล่าว สามารถนำมาวินิจฉัยในเบื้องต้นต่อวัตถุแห่งการกระทำที่เป็นบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญาได้ดังนี้

---

[129] เรื่องเดียวกัน, หน้า 51.

[130] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, หน้า 115.

[131] เรื่องเดียวกัน, หน้า 118.

[132] เรื่องเดียวกัน, หน้า 3 - 8.

[133] เรื่องเดียวกัน.

3.4.2.1.1 เอกสาร ซึ่งบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ก)

บัตรอิเล็กทรอนิกส์ที่เป็นเอกสาร แม้จะได้มีการบันทึกข้อมูลหรือรหัสไว้ด้วยวิธีการทางอิเล็กทรอนิกส์ แต่เนื่องจากเอกสารนั้น คือ กระดาษหรือวัตถุอื่นใดที่ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแบบอย่างอื่น ด้วยวิธีการพิมพ์หรือถ่ายภาพ ตามประมวลกฎหมายอาญามาตรา 1(7) เพียงเท่านั้น จึงมิได้เป็นคอมพิวเตอร์ตั้งแต่แรก ทั้งแถบแม่เหล็ก (Magnetic Stripe) หรือชิป (Chip) ในเอกสารนั้นก็เป็นเพียงหน่วยความจำสำรองอันเป็นองค์ประกอบหนึ่งของคอมพิวเตอร์เท่านั้นจึงไม่ใช่เครื่องคอมพิวเตอร์ เมื่อไม่ใช่คอมพิวเตอร์ตั้งแต่แรกจึงไม่ต้องวินิจฉัยอีกต่อไปว่าได้มีการเชื่อมต่อโครงข่ายอันเป็นระบบคอมพิวเตอร์หรือไม่

3.4.2.1.2 วัตถุอื่นใด ซึ่งบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ก)

บัตรอิเล็กทรอนิกส์ที่เป็นวัตถุอื่นใดที่พบเห็นได้ทั่วไป เช่น เหรียญรถไฟฟ้ามหานคร โดยปรกติแล้วย่อมไม่มีองค์ประกอบของคอมพิวเตอร์ครบถ้วนจึงไม่ใช่คอมพิวเตอร์ ทั้งแหล่งบันทึกข้อมูลในวัตถุอื่นใดนั้นก็เป็นเพียงหน่วยความจำสำรองอันเป็นองค์ประกอบหนึ่งของคอมพิวเตอร์เท่านั้นจึงไม่ใช่เครื่องคอมพิวเตอร์ เว้นแต่ในอนาคตวัตถุอื่นใดที่ผู้ออกให้แก่ผู้มีสิทธิใช้นั้นจะเป็นคอมพิวเตอร์ด้วยในตัวเองและมีการเชื่อมต่อโครงข่ายอันเป็นระบบแก่วัตถุอื่นใดนั้นด้วยซึ่งต้องอาศัยการพัฒนาทางเทคโนโลยีต่อไป เช่น อุปกรณ์อิเล็กทรอนิกส์ติดตามตัว (Electronic Monitoring : EM)[134]

3.4.2.1.3 ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใด ๆ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ตามมาตรา 1(14)(ข)

การที่มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้นั้น แสดงให้เห็นว่าข้อมูลเหล่านั้นต้องได้จัดเก็บไว้ในหน่วยความจำภายในของคอมพิวเตอร์เครื่องใดเครื่องหนึ่งไว้แล้ว เช่นเก็บ

---

[134] สำนักงานเลขาธิการสภาผู้แทนราษฎร, "รายงานของคณะกรรมาธิการขับเคลื่อนการปฏิรูปประเทศด้านกฎหมายและกระบวนการยุติธรรม สภาขับเคลื่อนประเทศ เรื่อง การใช้อุปกรณ์อิเล็กทรอนิกส์ติดตามตัวในกระบวนการยุติธรรมทางอาญา" [ออนไลน์], เข้าถึงเมื่อ 29 กรกฎาคม 2563. แหล่งที่มา: https://library2.parliament.go.th/giventake/content_nrsa2558/d111559-01.pdf.

ไว้ในคอมพิวเตอร์ของธนาคารพาณิชย์ ในคอมพิวเตอร์ของโรงแรมหรือหอพัก ซึ่งโดยลักษณะทั่วไปแล้วคอมพิวเตอร์ที่ได้เก็บข้อมูลเหล่านี้ไว้มักมีการเชื่อมต่อกับโครงข่ายคอมพิวเตอร์อื่นๆ ภายในหรือภายนอกอยู่แล้วเพื่อใช้งาน เช่น การใช้หมายเลขบัญชีและรหัสของบัตรเครดิตที่ไม่ได้มีการออกบัตรให้เพื่อซื้อสินค้าออนไลน์ การกดรหัสลงเวลางาน หรือการกดรหัสเปิดประตูห้องพักที่ต้องกดผ่านเครื่องคอมพิวเตอร์ ส่งผลให้การทำความผิดใดๆ แก่ข้อมูลดังกล่าว เช่น การดึงข้อมูล ผู้กระทำจำต้องทำการเข้าถึงระบบคอมพิวเตอร์นั้นๆ เสียก่อน อันมีกำหนดเป็นความผิดไว้ในมาตรา 5 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

3.4.2.1.4 ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใด ๆ และได้มีการออกเอกสารหรือวัตถุอื่นใดให้

การที่ได้มีการออกเอกสารหรือวัตถุอื่นใดให้นั้น ส่งผลให้ข้อมูลเหล่านี้มักจะจัดเก็บอยู่ในแหล่งบันทึกความจำที่ติดมากับเอกสารหรือวัตถุอื่นใดนั้น เช่น แถบแม่เหล็ก (Magnetic Stripe) หรือชิป (Chip) ซึ่งถือว่าเป็นเพียงหน่วยความจำสำรองอันเป็นองค์ประกอบหนึ่งของคอมพิวเตอร์เท่านั้นจึงไม่ใช่เครื่องคอมพิวเตอร์ ส่งผลให้การทำใดๆ แก่ข้อมูลในแหล่งบันทึกความจำในเอกสารหรือวัตถุอื่นใดดังกล่าว ไม่ใช่การกระทำกับระบบคอมพิวเตอร์ เว้นแต่ข้อมูลเหล่านั้นจะได้มีการคัดลอกลงในระบบคอมพิวเตอร์ไว้แยกต่างหากจากกันด้วย แต่แม้จะได้คัดลอกลงในระบบคอมพิวเตอร์แล้ว การกระทำที่จะเป็นความผิดได้นั้นก็ต้องกระทำต่อข้อมูลที่ได้คัดลอกซึ่งอยู่ในระบบคอมพิวเตอร์นั้นเท่านั้น ไม่ใช่กระทำต่อข้อมูลในแหล่งบันทึกของเอกสารหรือวัตถุอื่นใดที่มีการออกให้ เพราะถือว่าไม่ใช่ระบบคอมพิวเตอร์ตามที่ได้กล่าวมาแล้วข้างต้น

3.4.2.1.5 สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ ตามมาตรา 1(14)(ค)

เนื่องจากองค์ประกอบทางชีวภาพของมนุษย์ไม่ใช่คอมพิวเตอร์ จึงไม่ต้องพิจารณาต่อว่าการกระทำต่อสิ่งอื่นใดเหล่านี้จะต้องกระทำต่อระบบคอมพิวเตอร์หรือไม่

ตารางที่ 4 วัตถุแห่งการกระทำที่เป็นบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญากับการกระทำต่อระบบคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

วัตถุแห่งการกระทำตามประมวลกฎหมายอาญา	การกระทำต่อระบบคอมพิวเตอร์ ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์	
	ต้องกระทำต่อระบบคอมพิวเตอร์เสียก่อน	ไม่ใช่การกระทำต่อระบบคอมพิวเตอร์
เอกสาร ซึ่งบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ก)		/
วัตถุอื่นใด ซึ่งบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ก)		/
ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ตามมาตรา 1(14)(ข)	/	
ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ และได้มีการออกเอกสารหรือวัตถุอื่นใดให้		/

วัตถุแห่งการกระทำตามประมวลกฎหมายอาญา	การกระทำต่อระบบคอมพิวเตอร์ ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์	
	ต้องกระทำต่อระบบคอมพิวเตอร์เสียก่อน	ไม่ใช่การกระทำต่อระบบคอมพิวเตอร์
สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของตามมาตรา 1(14)(ค)		/

จากองค์ประกอบของการเป็นคอมพิวเตอร์และนิยามของระบบคอมพิวเตอร์ในมาตรา 3 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เมื่อนำมาวิเคราะห์กับวัตถุแห่งการกระทำที่เป็นบัตรอิเล็กทรอนิกส์ตามคำนิยามในมาตรา 1(14) ของประมวลกฎหมายอาญาแล้ว จึงสรุปได้ดังนี้

(ก) กระทำความผิดที่มีวัตถุแห่งการกระทำเป็นข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ตามมาตรา 1(14)(ข) แห่งประมวลกฎหมายอาญา ผู้กระทำความผิดต้องเข้าถึงระบบคอมพิวเตอร์เสียก่อนจึงจะกระทำความผิดแก่ข้อมูลเหล่านั้นได้ ตัวอย่างเช่น กรณีผู้กระทำความผิดที่ต้องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ประเภทดังกล่าว โดยการติดตั้งมัลแวร์หรือไวรัสคอมพิวเตอร์ (Malware or Virus Computer) ให้ทำการเข้าไปดึงข้อมูลบัตรอิเล็กทรอนิกส์ในระบบคอมพิวเตอร์ แม้ผู้กระทำจะไม่ต้องรับผิดตามประมวลกฎหมายอาญาเพราะไม่มีบทบัญญัติกำหนดให้การกระทำดังกล่าวเป็นความผิด แต่ผู้กระทำอาจต้องรับผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในบทบัญญัติที่กำหนดให้การกระทำต่อระบบคอมพิวเตอร์นั้นเป็นความผิด เช่น ความผิดฐานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง ตามมาตรา 5 หรือฐานกระทำโดยมิชอบเพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ ตามมาตรา 8

(ข) กระทำความผิดที่มีวัตถุแห่งการกระทำเป็นบัตรอิเล็กทรอนิกส์ในลักษณะอื่นๆ นอกเหนือจาก (ก) นั้น ไม่ใช่การกระทำต่อระบบคอมพิวเตอร์ด้วย ดังนั้นไม่ว่าการกระทำใดๆ ที่เกี่ยวกับบัตรอิเล็กทรอนิกส์ในลักษณะอื่นๆ อันผู้กระทำจะมีความผิดตามประมวลกฎหมายอาญาหรือไม่ก็ตาม ผู้กระทำก็ไม่มีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในบทบัญญัติที่กำหนดให้การกระทำต่อระบบคอมพิวเตอร์นั้นเป็นความผิด ตัวเอย่างเช่น กรณีผู้กระทำความผิดที่ดึงข้อมูลจากแหล่งบันทึกความจำในบัตรอิเล็กทรอนิกส์ที่เป็นเอกสารโดยใช้เครื่องสกิมเมอร์ ผู้กระทำจะมีความผิดเพียงฐานมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง ตามมาตรา 269/2 เพียงมาตราเดียว แต่ผู้กระทำจะไม่มีความผิดฐานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง ตามมาตรา 5 เพราะแหล่งบันทึกความจำในบัตรอิเล็กทรอนิกส์เป็นเพียงหน่วยความจำสำรองอันเป็นองค์ประกอบหนึ่งของคอมพิวเตอร์จึงไม่ใช่คอมพิวเตอร์และไม่ใช่ระบบคอมพิวเตอร์นั่นเอง

ดังนั้นในการกระทำความผิดที่มีวัตถุแห่งการกระทำเป็นระบบคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะสามารถนำมาปรับใช้กับปัญหาการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้เพียงแค่กรณีบัตรอิเล็กทรอนิกส์ที่มีลักษณะเป็นข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ตามมาตรา 1(14)(ข) ของประมวลกฎหมายอาญาเท่านั้น ซึ่งผู้กระทำการดึงข้อมูลดังกล่าวอาจมีความผิด เช่น ความผิดฐานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง ตามมาตรา 5 หรือฐานกระทำโดยมิชอบเพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ ตามมาตรา 8

3.4.2.2 นิยามของคำว่าข้อมูลคอมพิวเตอร์

เนื่องจากการกระทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นการกระทำโดยมีวัตถุแห่งการกระทำเป็นข้อมูลของบัตรอิเล็กทรอนิกส์ ซึ่งจำต้องพิจารณาว่าจะสามารถนำการกระทำความผิดที่มีวัตถุแห่งการกระทำเป็นข้อมูลคอมพิวเตอร์ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาปรับใช้แก่กรณีดังกล่าวได้หรือไม่ เพียงใด

ข้อมูล (Data) พจนานุกรมฉบับราชบัณฑิตยสถานให้ความหมายว่า “ข้อเท็จจริงหรือสิ่งที่ถือหรือยอมรับว่าเป็นข้อเท็จจริง สำหรับใช้เป็นหลักอนุมานหาความจริงหรือการคำนวณ”[135] การให้ความหมายลักษณะนี้เป็นลักษณะทั่วไป แตกต่างจากข้อมูล (Digital Data) ที่อยู่ในลักษณะของข้อมูลอิเล็กทรอนิกส์ ใน พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ที่เจาะจงไปว่าข้อมูลอิเล็กทรอนิกส์ ต้องเป็น เรื่องราวหรือข้อเท็จจริง ที่เป็นตัวอักษร ตัวเลข เสียง หรือภาพ[136] ที่ได้สร้างขึ้น ส่ง รับ เก็บรักษา หรือประมวลผลด้วย วิธีการทางอิเล็กทรอนิกส์[137] โดยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า วิธีการทางแสง ทางแม่เหล็กไฟฟ้า[138] เป็นต้น นั่นหมายถึง ข้อมูลต่างๆ ที่เป็นข้อเท็จจริง (Information) โดยลักษณะโดยทั่วไปเป็นสิ่งที่ไม่มีรูปร่าง ไม่มีสสาร (Non - substance) จับต้องไม่ได้และจะเป็นข้อมูลอิเล็กทรอนิกส์ได้ต่อเมื่อมีการนำเข้าสู่กระบวนการทางอิเล็กทรอนิกส์ให้สร้างขึ้นใหม่โดยอาจมีการส่ง รับ หรือเก็บรักษาไว้ด้วยวิธีการทางอิเล็กทรอนิกส์ ให้เปลี่ยนจากภาษามนุษย์เป็นภาษาเครื่อง อันเป็นการเรียงกันของเลขฐานสอง คือ เลข 0 และ 1 เท่านั้น[139] เช่น วันเดือนปีเกิดของบุคคล หรือรูปร่างลักษณะของบุคคล เรื่องราวต่างๆ ของบุคคลนับว่าเป็นข้อมูล แต่เมื่อมีการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งเป็นการสร้างขึ้นใหม่ด้วยวิธีการทางอิเล็กทรอนิกส์ ข้อมูลนั้นจึงกลายสภาพเป็นข้อมูลอิเล็กทรอนิกส์ ดังนั้นจึงสรุปได้ว่า ข้อมูลอิเล็กทรอนิกส์ คือข้อมูลที่ได้มีการสร้างใหม่ด้วยวิธีการทางอิเล็กทรอนิกส์ นั่นเอง

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้บัญญัตินิยามของคำว่า คำว่าข้อมูลคอมพิวเตอร์ ไว้ในมาตรา 3 ดังนี้

---

[135] สำนักงานราชบัณฑิตยสภา, พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554 [ออนไลน์], 29 กรกฎาคม 2563. แหล่งที่มา http://www.royin.go.th/dictionary/index.php.

[136] พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4 “ข้อความ” หมายความว่า เรื่องราวหรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ

[137] พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4 “ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

[138] พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4 “อิเล็กทรอนิกส์” หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่างๆ เช่นว่านั้น

[139] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, พิมพ์ครั้งที่ 1 (กรุงเทพฯ: กรุงสยาม พับลิชชิ่ง, 2559), หน้า 114 - 115.

มาตรา 3 บัญญัติว่า “ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

เมื่อนิยามของคำว่าข้อมูลคอมพิวเตอร์ ให้รวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ในมาตรา 4 ด้วย ซึ่งบัญญัติว่า

“ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

ดังนั้นจึงกล่าวได้ว่านิยามของคำว่า ข้อมูลคอมพิวเตอร์ นั้น สามารถแยกออกได้เป็น 2 ประเภทคือ

(ก) ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้

ตัวอย่างของข้อมูลคอมพิวเตอร์ชนิดนี้ ได้มีการให้ไว้ในเอกสารที่ใช้ประกอบการนำเสนอร่างกฎหมาย ไว้ว่า เช่น ข้อมูลที่เป็นรหัสผ่าน หรือลายมือชื่ออิเล็กทรอนิกส์ และเนื่องจากลักษณะการใช้งาน ข้อมูลนี้ต้องเป็นข้อมูลในรูปแบบดิจิทัล (Digital Data) ที่อยู่ในลักษณะข้อมูลอิเล็กทรอนิกส์เท่านั้น ไม่ใช่ข้อมูลทั่วๆ ไป (Data)[140] ที่ยังไม่ได้มีการสร้างขึ้นใหม่ด้วยวิธีการทางอิเล็กทรอนิกส์ และเฉพาะข้อมูลที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้เท่านั้นจึงจะได้รับความคุ้มครอง

(ข) ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์

ข้อมูลคอมพิวเตอร์ประเภทดังกล่าวเกิดจากการแก้ไขเพิ่มเติมร่างกฎหมายที่ได้มีการเสนอเข้าสภานิติบัญญัติแห่งชาติ เพื่อให้กฎหมายมีความครอบคลุมมากขึ้น ข้อมูลเหล่านี้ไม่ได้อยู่ในระบบคอมพิวเตอร์ดังเช่นประเภท (ก) แต่เป็นข้อมูลที่อยู่นอกระบบคอมพิวเตอร์ที่ถูกจัดเก็บในสื่อรูปแบบอื่นๆ เช่น ในแผ่นดิสก์ (Diskett) แผ่นซีดี (CD - Rom) ฮาร์ดดิสแบบพกพา (External hard disk) หรือแฟลชไดร์ฟ (USB flash drive) แต่ก็จำกัดเฉพาะเมื่อได้มีการเชื่อมต่อข้อมูลเหล่านี้เข้ากับระบบคอมพิวเตอร์เท่านั้น เช่น เมื่อมีการนำมาเปิดใช้ เปิดอ่านผ่านระบบคอมพิวเตอร์ก็จะกลายเป็น

---

[140] มานิตย์ จุมปา, คำอธิบายกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์, หน้า 52.

ข้อมูลคอมพิวเตอร์ได้[141] หากยังไม่มีการเชื่อมต่อกับระบบคอมพิวเตอร์ ข้อมูลดังกล่าวก็ไม่อยู่ในความหมายของข้อมูลคอมพิวเตอร์[142] และต้องพิจารณาด้วยว่าผู้กระทำได้ใช้อุปกรณ์ที่ครบองค์ประกอบของการเป็นคอมพิวเตอร์หรือไม่[143] ถ้าหากอุปกรณ์นั้นไม่ใช่คอมพิวเตอร์เสียแล้ว แม้ว่าจะมีข้อมูลในรูปแบบดิจิทัล (Digital Data) บันทึกไว้ในอุปกรณ์นั้นก็ตาม ก็ไม่อาจถือว่าเป็นข้อมูลคอมพิวเตอร์ได้[144]

จากนิยามของคำว่าข้อมูลคอมพิวเตอร์ทั้งสองประการข้างต้น สามารถนำมาวินิจฉัยในเบื้องต้นต่อวัตถุแห่งการกระทำที่เป็นบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญาได้ดังนี้

3.4.2.2.1 เอกสาร ซึ่งบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ก)

ลักษณะของเอกสารนั้นไม่ใช่ข้อมูล[145] เอกสารจึงไม่ใช่ข้อมูลคอมพิวเตอร์โดยสภาพ และแม้ว่าจะได้มีข้อมูลในรูปแบบดิจิทัล (Digital) บันทึกไว้ในแหล่งบันทึกความจำสำรองในเอกสารดังกล่าว เช่น เป็นข้อมูลที่บันทึกอยู่ในแถบแม่เหล็ก (Magnetic Stripe) หรือชิป (Chip) และเนื่องจากการเป็นเอกสารนั้นขาดองค์ประกอบของการเป็นคอมพิวเตอร์ตั้งแต่แรก ดังนั้นหากมีการดึงข้อมูลออกจากเอกสารที่เป็นบัตรอิเล็กทรอนิกส์ดังกล่าวโดยตรง ก็ไม่สามารถปรับใช้ฐานความผิดอันเกี่ยวกับข้อมูลคอมพิวเตอร์ตามพระราชบัญญัตินี้ได้

3.4.2.2.2 วัตถุอื่นใด ซึ่งบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ก)

บัตรอิเล็กทรอนิกส์ที่เป็นวัตถุอื่นใด แม้ว่าจะได้มีข้อมูลในรูปแบบดิจิทัล (Digital) บันทึกไว้ในแหล่งบันทึกความจำสำรองในวัตถุอื่นใดนั้นก็ตาม แต่เนื่องจากบัตรประเภทดังกล่าวที่พบเห็นได้ทั่วไปโดยปรกติแล้วย่อมไม่มีองค์ประกอบของคอมพิวเตอร์ครบถ้วนจึงไม่ใช่

---

[141] สุพิศ ปราณีตพลกรัง, กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์, พิมพ์ครั้งที่ 1 (กรุงเทพฯ: นิติธรรม , 2560), หน้า 17.

[142] เรื่องเดียวกัน, หน้า 53.

[143] ดูหัวข้อที่ 3.4.2.1 ในส่วนอธิบายการเป็นเครื่องคอมพิวเตอร์

[144] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, หน้า 117-118.

[145] โปรดดูหัวข้อที่ 3.4.1.2.1 ความหมายของคำว่าเอกสาร

คอมพิวเตอร์ตั้งแต่แรก ข้อมูลดังกล่าวจึงไม่ใช่ข้อมูลคอมพิวเตอร์ด้วย เว้นแต่ในอนาคตวัตถุอื่นใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้นั้นจะเป็นคอมพิวเตอร์ที่มีการเชื่อมต่อเป็นระบบคอมพิวเตอร์ซึ่งจะทำให้ข้อมูลที่บันทึกอยู่ในวัตถุอื่นใดนั้นก็จะกลายเป็นข้อมูลคอมพิวเตอร์ด้วย

3.4.2.2.3 ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใด ๆ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ตามมาตรา 1(14)(ข)

การที่มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้นั้น แสดงให้เห็นว่าข้อมูลเหล่านั้นต้องได้จัดเก็บไว้ในหน่วยความจำภายในของคอมพิวเตอร์เครื่องใดเครื่องหนึ่งไว้แล้วซึ่งโดยลักษณะทั่วไปแล้วคอมพิวเตอร์ที่ได้เก็บข้อมูลเหล่านี้ไว้มักมีการเชื่อมต่อกับโครงข่ายคอมพิวเตอร์อื่นๆ เป็นระบบคอมพิวเตอร์ไว้พร้อมใช้งานอยู่แล้ว ทำให้ข้อมูลเหล่านี้อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้แล้ว ข้อมูลดังกล่าวจึงมีลักษณะเป็นข้อมูลคอมพิวเตอร์ในตัวเอง ซึ่งหากมีการกระทำผิดกับบัตรอิเล็กทรอนิกส์ประเภทนี้ ผู้กระทำก็อาจจะมีความผิดเกี่ยวกับข้อมูลคอมพิวเตอร์ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ด้วย เช่น ฐานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง ตามมาตรา 7

3.4.2.2.4 ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใด ๆ และได้มีการออกเอกสารหรือวัตถุอื่นใดให้

การที่ได้มีการออกเอกสารหรือวัตถุอื่นใดให้นั้น ส่งผลให้ข้อมูลเหล่านี้มักจะจัดเก็บอยู่ในแหล่งบันทึกความจำที่ติดมากับเอกสารหรือวัตถุอื่นใดนั้น เช่น แถบแม่เหล็ก (Magnetic Stripe) หรือชิป (Chip) ซึ่งเป็นข้อมูลที่อยู่นอกระบบคอมพิวเตอร์ที่ถูกจัดเก็บในสื่อรูปแบบอื่นๆ ทำนองเดียวกันกับข้อมูลที่จัดเก็บในแผ่นดิสก์ (Diskett) แผ่นซีดี (CD - Rom) ฮาร์ดดิสแบบพกพา (External hard disk) แฟลชไดร์ฟ (USB flash drive) เป็นต้น ซึ่งหากเกิดการดึงข้อมูลออกจากบัตรอิเล็กทรอนิกส์ประเภทนี้โดยตรงโดยที่ไม่ได้ดึงจากการเชื่อมต่อข้อมูลประเภทดังกล่าวกับระบบคอมพิวเตอร์แล้ว ข้อมูลดังกล่าวจะไม่เป็นข้อมูลคอมพิวเตอร์ จึงไม่อาจปรับใช้ฐานความผิดอันเกี่ยวกับข้อมูลคอมพิวเตอร์ตามพระราชบัญญัตินี้ได้ เช่น การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์โดยใช้เครื่องสกิมเมอร์นั้นเป็นการดึงข้อมูลจากแหล่งบันทึกความจำสำรองที่เป็นแถบแม่เหล็ก (Magnetic

Stripe) หรือชิป (Chip) ของบัตรอิเล็กทรอนิกส์โดยตรง[146] ผู้กระทำจึงไม่ได้กระทำต่อข้อมูลคอมพิวเตอร์ จึงจะลงโทษในความผิดฐานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง ตามมาตรา 7 มิได้ เว้นแต่ข้อมูลเหล่านั้นจะได้มีการคัดลอกลงในระบบคอมพิวเตอร์ไว้แยกต่างหากจากกันด้วย ข้อมูลดังกล่าวจึงจะเป็นข้อมูลคอมพิวเตอร์ แต่การกระทำที่จะเป็นความผิดได้นั้นก็ต้องกระทำต่อข้อมูลที่ได้คัดลอกซึ่งอยู่ในระบบคอมพิวเตอร์นั้นเท่านั้น ไม่ใช่กระทำต่อข้อมูลในแหล่งบันทึกของเอกสารหรือวัตถุอื่นใดที่มีการออกให้เพราะถือว่าไม่ใช่ข้อมูลคอมพิวเตอร์ตามที่ได้กล่าวมาแล้วข้างต้น

3.4.2.2.5 สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ ตามมาตรา 1(14)(ค)

เนื่องจากองค์ประกอบทางชีวภาพของมนุษย์ไม่ใช่คอมพิวเตอร์ จึงไม่ต้องพิจารณาต่อว่าการกระทำต่อสิ่งอื่นใดเหล่านี้จะต้องกระทำต่อข้อมูลคอมพิวเตอร์หรือไม่

[146] Deenamtang, “การป้องกัน การ Skimming ขโมยข้อมูล บัตร ATM หรือ บัตร Credit” [ออนไลน์], เข้าถึงเมื่อ 25 กรกฎาคม 2563. แหล่งที่มา https://www.deenamtang.com/14928366/การป้องกัน-การ-skimming-ขโมยข้อมูล-บัตร-atm-หรือ-บัตร-credit.

ตารางที่ 5 วัตถุแห่งการกระทำที่เป็นบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญากับการกระทำต่อข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

วัตถุแห่งการกระทำตามประมวลกฎหมายอาญา	การกระทำต่อข้อมูลคอมพิวเตอร์ ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์	
	เป็นการกระทำต่อข้อมูลคอมพิวเตอร์	ไม่ใช่การกระทำต่อข้อมูลคอมพิวเตอร์
เอกสาร ซึ่งบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ก)		/
วัตถุอื่นใด ซึ่งบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ก)		/
ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ตามมาตรา 1(14)(ข)	/	
ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ และได้มีการออกเอกสารหรือวัตถุอื่นใดให้		/

วัตถุแห่งการกระทำตามประมวลกฎหมายอาญา	การกระทำต่อข้อมูลคอมพิวเตอร์ ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์	
	เป็นการกระทำต่อข้อมูลคอมพิวเตอร์	ไม่ใช่การกระทำต่อข้อมูลคอมพิวเตอร์
สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ ตามมาตรา 1(14)(ค)		/

จากนิยามของข้อมูลคอมพิวเตอร์ในมาตรา 3 ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ประกอบกับนิยามของข้อมูลอิเล็กทรอนิกส์ ในมาตรา 4 ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 เมื่อนำมาวิเคราะห์กับวัตถุแห่งการกระทำที่เป็นบัตรอิเล็กทรอนิกส์ตามคำนิยามในมาตรา 1(14) ของประมวลกฎหมายอาญาแล้ว จึงสรุปได้ดังนี้

(ก) กระทำความผิดที่มีวัตถุแห่งการกระทำเป็นข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ตามมาตรา 1(14)(ข) แห่งประมวลกฎหมายอาญา ถือเป็นการกระทำความผิดต่อข้อมูลคอมพิวเตอร์ด้วย ตัวอย่างเช่น กรณีผู้กระทำความผิดที่ต้องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ประเภทดังกล่าว โดยการติดตั้งมัลแวร์หรือไวรัสคอมพิวเตอร์ (Malware or Virus Computer) เข้าไปในระบบคอมพิวเตอร์ ให้ทำการเข้าไปดึงข้อมูลบัตรอิเล็กทรอนิกส์ แม้ผู้กระทำจะไม่ต้องรับผิดตามประมวลกฎหมายอาญาเพราะไม่มีบทบัญญัติกำหนดให้การกระทำดังกล่าวเป็นความผิด แต่ผู้กระทำอาจต้องรับผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในบทบัญญัติที่กำหนดให้การกระทำต่อข้อมูลคอมพิวเตอร์นั้นเป็นความผิด เช่น ความผิดฐานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง ตามมาตรา 7 หรือฐานกระทำโดยมิชอบเพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ ตามมาตรา 8

(ข) กระทำความผิดที่มีวัตถุแห่งการกระทำเป็นบัตรอิเล็กทรอนิกส์ในลักษณะอื่นๆ นอกเหนือจาก (ก) นั้น ไม่ใช่การกระทำต่อข้อมูลคอมพิวเตอร์ ผู้กระทำจึงไม่มีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในบทบัญญัติที่กำหนดให้การกระทำต่อข้อมูลคอมพิวเตอร์นั้นเป็นความผิด ตัวอย่างเช่น กรณีผู้กระทำความผิดที่ดึงข้อมูลจากแหล่งบันทึกความจำในบัตรอิเล็กทรอนิกส์ที่เป็นเอกสารโดยใช้เครื่องสกิมเมอร์ ผู้กระทำจะมีความผิดเพียงฐานมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง ตามมาตรา 269/2 เพียงมาตราเดียว แต่ผู้กระทำจะไม่มีความผิดฐานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงตามมาตรา 7 เพราะการดึงข้อมูลจากหน่วยความจำของบัตรอิเล็กทรอนิกส์โดยใช้เครื่องสกิมเมอร์เป็นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์โดยตรง ซึ่งข้อมูลดังกล่าวไม่ถือเป็นข้อมูลคอมพิวเตอร์

ดังนั้นในการกระทำความผิดที่มีวัตถุแห่งการกระทำเป็นข้อมูลคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะสามารถนำมาปรับใช้กับปัญหาการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้เพียงแค่กรณีบัตรอิเล็กทรอนิกส์ที่มีลักษณะเป็นข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ตามมาตรา 1(14)(ข) ของประมวลกฎหมายอาญาเท่านั้น เช่น ผู้กระทำความผิดต้องรับโทษฐานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงตามมาตรา 7 หรือฐานกระทำโดยมิชอบเพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ ตามมาตรา 8

ตารางที่ 6 สรุปอุปสรรคในการนำบทบัญญัติอื่นที่มีลักษณะใกล้เคียงมาบังคับใช้แทนกับเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

(โดยที่ / คือ สามารถนำมาใช้บังคับได้ , X คือ ไม่สามารถนำมาใช้บังคับได้)

ประเภทของบัตรอิเล็กทรอนิกส์	บทบัญญัติอื่นที่นำมาใช้ได้กับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์				
	ประมวลกฎหมายอาญา		พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550		
	ความผิดฐานลักทรัพย์	ความผิดฐานปลอมเอกสาร	ฐานความผิดที่มีวัตถุแห่งการกระทำเป็นระบบคอมพิวเตอร์	ฐานความผิดที่มีวัตถุแห่งการกระทำเป็นข้อมูลคอมพิวเตอร์	ฐานดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ มาตรา 8
เอกสาร ซึ่งบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ตามมาตรา 1(14)(ก)	X *คุ้มครองเฉพาะตัวเอกสาร ไม่รวมข้อมูลในบัตร	/ *คุ้มครองเฉพาะข้อมูลบนผิวของบัตร ไม่รวมข้อมูลแหล่งบันทึกของบัตร	X	X	X

ประเภทของบัตรอิเล็กทรอนิกส์	บทบัญญัติอื่นที่นำมาใช้ได้กับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์				
	ประมวลกฎหมายอาญา		พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550		
	ความผิดฐานลักทรัพย์	ความผิดฐานปลอมเอกสาร	ฐานความผิดที่มีวัตถุแห่งการกระทำเป็นระบบคอมพิวเตอร์	ฐานความผิดที่มีวัตถุแห่งการกระทำเป็นข้อมูลคอมพิวเตอร์	ฐานดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ มาตรา 8
วัตถุอื่นใด ซึ่งบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ตามมาตรา 1(14)(ก)	X *คุ้มครองเฉพาะตัววัตถุอื่นใดไม่รวมข้อมูลในบัตร	X *วัตถุอื่นใด ไม่ใช่เอกสาร	X	X	X
ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใด ๆ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ตามมาตรา 1(14)(ข)	X *ข้อมูลไม่ใช่ทรัพย์และไม่มีการเอาไป	X *ข้อมูลไม่ใช่เอกสาร	/	/	/

ประเภทของบัตรอิเล็กทรอนิกส์	บทบัญญัติอื่นที่นำมาใช้ได้กับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์				
	ประมวลกฎหมายอาญา		พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550		
	ความผิดฐานลักทรัพย์	ความผิดฐานปลอมเอกสาร	ฐานความผิดที่มีวัตถุแห่งการกระทำเป็นระบบคอมพิวเตอร์	ฐานความผิดที่มีวัตถุแห่งการกระทำเป็นข้อมูลคอมพิวเตอร์	ฐานดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ มาตรา 8
ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใด ๆ และ<u>ได้มีการออกเอกสารหรือวัตถุอื่นใดให้</u>	X *ข้อมูลไม่ใช่ทรัพย์และไม่มีการเอาไป	X *ข้อมูลไม่ใช่เอกสาร	X	X	/ *เฉพาะการดักรับข้อมูลที่ส่งผ่านในระบบคอมพิวเตอร์เท่านั้น
สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ค)	X	X	X	X	/ *เฉพาะการดักรับข้อมูลที่ส่งผ่านในระบบคอมพิวเตอร์เท่านั้น

บทที่ 4
กฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ

การยืนยันตัวตนของบุคคล (Identity Verification) โดยการใช้ข้อมูลเป็นสิ่งที่เกิดขึ้นและได้รับการพัฒนามาอย่างยาวนานพร้อมกับพัฒนาการทางเทคโนโลยีของมนุษย์ เริ่มตั้งแต่การใช้รอยสัก (Tattoos) ในยุโรปและอียิปต์โบราณ เมื่อเริ่มมีการประดิษฐ์ตัวอักษรขึ้น อาณาจักรโรมันก็เริ่มคิดค้นการบันทึกข้อมูลของประชากรของตนลงในเอกสารต่างๆ เช่น สูติบัตร โฉนดที่ดินและทะเบียนราษฎร์ ต่อมาใน ค.ศ. 1829 เซอร์ รอเบิร์ต พีล (Sir Robert Peel) นายกรัฐมนตรีสหราชอาณาจักรได้ปฏิรูปกฎหมายอาญาของสหราชอาณาจักรให้สามารถนำตัวเลขมาใช้ในการอ้างอิงกับบุคคลได้อันเป็นฐานข้อมูลที่ทันสมัยและทำให้กำเนิดบัตรประจำตัวประชาชนขึ้นตามมา จนกระทั่ง ค.ศ. 1977 ได้เริ่มมีการบันทึกข้อมูลในรูปแบบดิจิตัลซึ่งเป็นที่มาของการเกิดบัตรสมาร์ทการ์ด (Smart Card) ขึ้น โดยมีวัตถุประสงค์ในการใช้เก็บบันทึกข้อมูลของบุคคลต่างๆ ไว้ในแหล่งเดียว ไม่ว่าจะเป็นหมายเลขบัตรประชาชน วันเดือนปีเกิด หรือหมายเลขธุรกรรมทางการเงินของบุคคล เป็นต้น และที่สุดใน ค.ศ. 2004 ซึ่งเริ่มมีการใช้เอกลักษณ์ทางชีวภาพของบุคคลมาใช้ในการยืนยันตัวตนของบุคคลมาจนถึงปัจจุบัน[1]

บัตรอิเล็กทรอนิกส์ จึงนับว่าเป็นผลจากการพัฒนาของเทคโนโลยีในการเก็บข้อมูลของมนุษย์ที่ใช้ยืนยันตัวตนของบุคคลซึ่งช่วยอำนวยความสะดวกในชีวิตประจำวันและมีรูปแบบการใช้งานที่หลากหลายซึ่งโดยส่วนใหญ่แล้วมักจะอยู่ในรูปแบบของข้อมูลดิจิตัลหรือข้อมูลอิเล็กทรอนิกส์ในแหล่งบันทึกต่างๆ ไม่ว่าจะเป็นแหล่งบันทึกข้อมูลประเภทแถบแม่เหล็ก (Magnetic stripe) หรือชิป (Chip) บนบัตรพลาสติกหรือในคอมพิวเตอร์ และด้วยคุณประโยชน์ที่มหาศาลนี้เองจึงเป็นที่มาให้อาชญากรพัฒนาเทคโนโลยีที่ใช้ในการดึงข้อมูลของบัตรเหล่านั้นเพื่อให้ได้มาซึ่งข้อมูลอันนำไปใช้แสวงหาผลประโยชน์อื่นๆ ต่อไป ซึ่งในประเทศที่มีการใช้งานบัตรอิเล็กทรอนิกส์อย่างแพร่หลายก็ต้องเผชิญกับอาชญากรรมการดึงข้อมูลจากบัตรด้วยกันอย่างมาก เช่น สหรัฐอเมริกา สหราชอาณาจักรและเครือรัฐออสเตรเลีย คือประเทศที่ติดสิบอันดับแรกของโลก[2] ที่พบการกระทำความผิดเกี่ยวกับการฉ้อโกงบัตร

[1] Trulioo.com, "100,000 Years of Identity Verification: An Infographic History" [Online], Accessed: 25 October 2020. Available from: https://www.trulioo.com/blog/infographic-the-history-of-id-verification.

[2] สถิติใน ค.ศ. 2016

มากที่สุด[3] นอกจากนั้นสาธารณรัฐฟิลิปปินส์ ยังเป็นอีกประเทศหนึ่งที่เกิดการกระทำความผิดและมีความสูญเสียทางการเงินจากอาชญากรรมดังกล่าว[4] เป็นจำนวนมาก[5] การกระทำความผิดที่เกิดขึ้นนี้ทำให้ความเชื่อใจในการใช้บัตรของสาธารณะชนลดลงเป็นอย่างมากอันส่งผลกระทบต่อการใช้งานข้อมูลเหล่านั้นกับระบบอื่นๆ ในประเทศ[6] ประเทศเหล่านี้จึงได้บัญญัติกฎหมายขึ้นเพื่อกำหนดความผิดในการดึงข้อมูลบัตรในรูปแบบต่างๆ ขึ้น เพื่อป้องกันและปราบการการกระทำความผิดที่เกิดขึ้นและเพื่อให้กฎหมายมีความทันสมัยครอบคลุมกับลักษณะความผิดที่เกิดขึ้นอีกด้วย

ในบทที่ 4 นี้จะกล่าวถึงบทบัญญัติต่างๆ ที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ที่ได้กำหนดไว้ในกฎหมายของต่างประเทศ อันได้แก่ สหรัฐอเมริกา สหราชอาณาจักร สาธารณรัฐฟิลิปปินส์ และเครือรัฐออสเตรเลีย ตลอดจนคำพิพากษาที่เกี่ยวข้องของศาลในประเทศดังกล่าว ซึ่งมีลักษณะที่แตกต่างกับบทบัญญัติกฎหมายของประเทศไทยหลายประการ จึงต้องทำการศึกษาถึงหลักการและลักษณะของบทบัญญัติที่เกี่ยวข้องกับการดึงข้อมูลบัตรในกฎหมายของต่างประเทศเหล่านี้ เพื่อค้นหาแนวทางในการนำมาปรับใช้และแก้ไขปัญหาในการบังคับใช้กฎหมายอันเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในประเทศไทยต่อไป

4.1 สหรัฐอเมริกา

ในเรื่องการดึงข้อมูลจากบัตรนี้แม้จะได้มีบทบัญญัติอันสามารถเอาผิดแก่ผู้กระทำได้ทั้งในกฎหมายของรัฐบาลกลางสหรัฐและกฎหมายที่หลายมลรัฐได้ตราขึ้นเป็นของตนเอง แต่คดีที่เกิดขึ้นนั้นโดยส่วนใหญ่แล้วจะเป็นการดำเนินการโดยหน่วยงานของรัฐบาลกลางและใช้กฎหมายของรัฐบาล

[3] Ben Knieff, "2016 Global Consumer Card Fraud: Where Card Fraud Is Coming From" [Online], Accessed: 25 October 2020. Available from: https://www.paymentscardsandmobile.com/wp-content/uploads/2016/07/2016-Global-Consumer-Card-Fraud-Where-Card-Fraud-Is-Coming-From.pdf.

[4] สูญเสียไปทั้งสิ้นประมาณ 506,850,866 เปโซฟิลิปปินส์ (ประมาณ 327,236,939 บาทไทย) และมีผู้ได้รับผลกระทบจากการกระทำความผิดถึง 80,000 ราย ใน ค.ศ. 2016

[5] Philip C. Tubeza, "P507m Lost to Credit Card Fraud in 2016" [Online], Accessed: 25 October 2020. Available from: https://newsinfo.inquirer.net/882963/p507m-lost-to-credit-card-fraud-in-2016.

[6] David S. Wall, "Future Identities: Changing Identities in the Uk – the Next 10 Years" [Online], Accessed: 25 October 2020. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/275784/13-521-identity-related-crime-uk.pdf.

กลางเป็นหลักในการดำเนินคดี[7] ดังนั้นในหัวข้อนี้ ผู้วิจัยจึงเลือกกฎหมายของรัฐบาลกลางของสหรัฐอเมริกาเป็นหลักในการศึกษาวิจัย

บทบัญญัติที่กำหนดความผิดทางอาญาของสหรัฐอเมริกานั้นได้รับการบัญญัติรวมอยู่ในรัฐบัญญัติของสหรัฐอเมริกา (The United States Code) ซึ่งได้รับการตีพิมพ์ครั้งแรกในปี 1926 และเผยแพร่โดยสำนักงานที่ปรึกษาการปรับปรุงแก้ไขกฎหมายของสภาผู้แทนราษฎรแห่งสหรัฐอเมริกา (Office of the Law Revision Counsel of the U.S. House of Representatives) อันเป็นการรวบรวมและประมวลกฎหมายที่ใช้เป็นการทั่วไปและถาวร (General and permanent laws) ของรัฐบาลกลางแห่งสหรัฐอเมริกา โดยบทบัญญัติที่เกี่ยวข้องกับการดึงข้อมูลบัตรนั้น อยู่ในหัวข้อที่ 18 อาชญากรรมและกระบวนการยุติธรรมทางอาญา (Title 18. CRIMES AND CRIMINAL PROCEDURE) ส่วนที่ 1 อาชญากรรม (Part I. CRIMES) บทที่ 47 การฉ้อโกงและรายงานที่เป็นเท็จ (FRAUD AND FALSE STATEMENTS) ซึ่งกำหนดไว้ดังต่อไปนี้

4.1.1 การฉ้อโกงและการกระทำที่เกี่ยวข้องกับเอกสารระบุตัวตน ลักษณะเฉพาะที่แท้จริงและข้อมูล (Fraud and related activity in connection with identification documents, authentication features, and information)

การฉ้อโกงและการกระทำที่เกี่ยวข้องกับเอกสารระบุตัวตน ลักษณะเฉพาะที่แท้จริงและข้อมูล (Fraud and related activity in connection with identification documents, authentication features, and information) บัญญัติอยู่ในมาตรา 1028 (18 U.S.C. § 1028) ซึ่งพัฒนามาจากพระราชบัญญัติข้อสันนิษฐานในการขัดขวางและการโจรกรรมข้อมูลส่วนบุคคล ค.ศ. 1998 (Identity Theft and Assumption Deterrence Act 1998) อันเป็นบทบัญญัติที่เอาผิดกับการโจรกรรมข้อมูลส่วนบุคคล (Identity theft) ในรูปแบบต่างๆ โดยการกระทำการฉ้อโกงหรือหลอกลวงเพื่อให้ตนเองได้ไปซึ่งข้อมูลส่วนบุคคลของผู้อื่นโดยผิดกฎหมายและนำข้อมูลที่ได้มานั้นไปแสวงหาประโยชน์ต่อไป[8]

---

[7] Arkady Bukh, "Skimming" [Online], Accessed: 22 October 2020. Available from: https://nyccriminallawyer.com/fraud-charge/credit-card-fraud-charge/skimming/.

[8] FindLaw, "Identity Theft" [Online], Accessed: 22 October 2020. Available from: https://criminal.findlaw.com/criminal-charges/identity-theft.html.

ในมาตราดังกล่าวมีการกระทำความผิดที่เกี่ยวข้องกับการดึงข้อมูลบัตร ได้บัญญัติอยู่ในอนุมาตรา (a)(7) ซึ่งบัญญัติว่า

มาตรา 1028 (a)(7) บัญญัติว่า “ผู้ใด (Whoever) ในกรณีที่อธิบายไว้ในอนุมาตรา (c) ของมาตรานี้ โดยเจตนา โอน (Transfers) ครอบครอง (Possesses) หรือใช้ (Uses) โดยไม่มีอำนาจตามกฎหมายซึ่ง สิ่งที่อ้างอิงในการระบุตัวตน (A means of identification) ของผู้อื่น ด้วยเจตนาที่จะกระทำหรือช่วยเหลือหรือสนับสนุนหรือเกี่ยวข้องกับการกระทำที่ผิดกฎหมายใดๆ ที่ถือเป็นการละเมิดต่อกฎหมายของรัฐบาลกลาง หรือก่อให้เกิดความผิดอาญาร้ายแรงภายใต้กฎหมายของมลรัฐหรือท้องถิ่น... จะต้องรับโทษตามที่ระบุไว้ในอนุมาตรา (b)”

ในกรณีที่อธิบายไว้ในอนุมาตรา (c) เฉพาะที่ใช้กับมาตรานี้หมายถึง การนั้นได้ส่งผลต่อการพาณิชย์ระหว่างรัฐหรือต่างประเทศ รวมถึงการโอนเอกสารนั้นทางอิเล็กทรอนิกส์ หรือทางเมล์ (Mail)[9] อนึ่งการกระทำความผิดโดยผ่านระบบอินเตอร์เน็ตก็ถือว่าได้ส่งผลต่อการพาณิชย์ระหว่างรัฐหรือต่างประเทศแล้ว[10] การกำหนดลักษณะนี้ก็เพื่อให้สามารถปรับใช้กฎหมายในระดับรัฐบาลกลางแก่การกระทำความผิดของผู้กระทำได้

การกระทำความผิดตามมาตรานี้ที่เกี่ยวข้องกับการดึงข้อมูลบัตรคือการ โอน (Transfers) อันหมายรวมถึง การเลือก (Selecting) และการวาง (Placing) หรือกำกับ (Directing) ตำแหน่งบนตำแหน่งทางออนไลน์ที่ทำให้ผู้อื่นสามารถใช้ได้[11] และยังหมายถึงการดึงข้อมูลอีกด้วย ดังตัวอย่างในคดี U. S. v. Amry (2003) นาย Mohamed Amry อดีตลูกจ้างของ Bally's Health Club ในเมืองเคมบริดจ์ (Cambridge) รัฐแมสซาชูเซตส์ (Massachusetts) ได้ใช้เครื่องสกิมเมอร์ในการดึงข้อมูลบัตรเครดิตของสมาชิก ทำให้ได้รับ (Obtain) ข้อมูลเกี่ยวกับชื่อ หมายเลขประกันสังคม และข้อมูลบัตรเครดิต ไปอย่างน้อย 30 คน ให้แก่นาย Abdelghani Meskini ผู้สมรู้ร่วมคิดในการนำข้อมูลดังกล่าวไปเปิดบัญชีธนาคารในเมืองนิวยอร์ค (New York)[12] และในคดี U. S. v. Fergerson[13]

---

[9] Subsection (c)(3) of section 1028 of United States Code

[10] United States v. Lopez (1995), United States v. MacEwan (2006)

[11] Subsection (d)(10) of section 1028 of United States Code

[12] ซึ่งนอกจากความผิดตามมาตรานี้แล้ว นาย Mohamed Amry ยังมีความผิดฐานฉ้อโกงธนาคาร ตามมาตรา 1344 ฐานสมรู้ร่วมคิดกันกระทำการฉ้อโกงอุปกรณ์ในการเข้าถึง ตามมาตรา 1029 อีกด้วย

[13] HOUSE OF REPRESENTATIVES, "Identity Theft Penalty Enhancement Act" [Online], Accessed: 20 October 2020. Available from: https://www.govinfo.gov/content/pkg/CRPT-108hrpt528/html/CRPT-108hrpt528.html.

นาง Diana Fergerson ได้ทำการขโมยข้อมูลส่วนบุคคลและนำไปใช้ในการรับประโยชน์ประกันสังคม กว่า 45,000 ดอลลาร์สหรัฐและใช้สร้างเครดิตให้แก่ตนเอง นาง Fergerson ได้ให้การรับสารภาพและถูกลงโทษในหลายหารวมถึงความผิดตามมาตรานี้ด้วย

วัตถุแห่งการกระทำความผิดตามมาตรานี้คือ สิ่งที่อ้างอิงในการระบุตัวตน (A means of identification) ซึ่งอนุมาตรา (d) ให้นำนิยามว่าหมายถึง[14] ชื่อหรือหมายเลขใดๆ ที่อาจใช้โดยลำพังหรือร่วมกับข้อมูลอื่นๆ ในการระบุตัวตนของบุคคลโดยเฉพาะเจาะจง ซึ่งรวมถึง

(A) ชื่อ หมายเลขประกันสังคม วันเดือนปีเกิด ใบอนุญาตขับขี่หรือหมายเลขขับขี่ เลขทะเบียนคนต่างด้าว หมายเลขพาสปอร์ต เลขประจำตัวผู้เสียภาษี

(B) เอกลักษณ์ข้อมูลทางชีวภาพ (Biometric data) เช่น ลายพิมพ์นิ้วมือ พิมพ์เสียง (Voice print) ภาพเรตินา (Retina) หรือม่านตา (Iris) หรือเอกลักษณ์ที่แสดงออกทางกายภาพ

(C) เอกลักษณ์ที่เป็น หมายเลขระบุตัวตนทางอิเล็กทรอนิกส์ ที่อยู่ หมายเลขเส้นทาง (Routing code)[15]

(D) ข้อมูลที่ใช้ระบุตัวตนในการสื่อสารโทรคมนาคม หรืออุปกรณ์ในการเข้าถึง (ตามที่กำหนดไว้ในมาตรา 1029(e)[16])

สิ่งที่อ้างอิงในการระบุตัวตนของบุคคลดังที่ได้กำหนดไว้ตามมาตรานี้อยู่ในลักษณะเป็นข้อมูลส่วนบุคคลซึ่งสามารถนำไปใช้ในการออกบัตรใดๆ ต่อไปได้ และเมื่อได้มีการออกบัตรแล้ว ข้อมูลดังกล่าวก็ย่อมเป็นข้อมูลของบัตรที่ได้รับความคุ้มครองตามมาตรานี้ จากการกระทำการโอน (Transfers) ครอบครอง (Possesses) หรือใช้ (Uses) โดยไม่มีอำนาจตามกฎหมาย ซึ่งย่อมรวมถึงการดึงข้อมูลด้วยตามตัวอย่างคดีที่ได้กล่าวไปแล้ว ดังนั้น หากผู้ใดได้ดึงข้อมูลบัตรที่ประกอบด้วย

---

[14] Subsection (d)(7) of section 1028 of United States Code

[15] Routing Number หรือ Routing Transit Number (RTN) หรือ ABA Number คือตัวเลขรหัสธนาคารหรือสถาบันการเงิน 9 หลัก กำหนดโดย American Bankers' Association ใช้สำหรับระบุการส่งคำสั่งโอนเงินจากธนาคารผู้ส่งไปยังธนาคารผู้รับผ่านระบบ US ACH ภายในประเทศสหรัฐอเมริกา และเป็นชุดตัวเลขสำหรับโอนเงินภายในสาขาของธนาคาร เพื่ออำนวยความสะดวกในการโอนตัวเลขที่มีค่าเงินกันไปมา

[16] หมายความว่า "ใดๆ ก็ตามที่เป็น บัตร (Card) ป้าย (Plate) รหัส (Code) หมายเลขบัญชี (Account number) หมายเลขอิเล็กทรอนิกส์ (Electronic serial number) หมายเลขประจำตัวมือถือ (Mobile identification number) หมายเลขประชาชน (Personal identification number) หรือ บริการ อุปกรณ์ เครื่องมือที่ใช้ในการระบุตัวตนในการโทรคมนาคม หรือวิธีการอื่นในการเข้าถึงบัญชี ที่สามารถใช้โดยลำพังหรือร่วมกับอุปกรณ์ในการเข้าถึงอื่น ในการรับเงิน สินค้า บริการ หรือสิ่งมีค่าอื่นใด หรือสามารถใช้ในการโอนเงินที่นอกเหนือจากการใช้วิธีทางเอกสาร

ข้อมูลส่วนบุคคลดังกล่าว ไม่ว่าจะเป็นบัตรที่ได้มีการออกเอกสารหรือวัตถุอื่นใดให้หรือไม่ก็ตาม ก็ย่อมจะเป็นการกระทำความผิดตามมาตรานี้ แต่อย่างไรก็ตามผู้กระทำนั้นต้องมีเจตนาที่จะกระทำหรือช่วยเหลือหรือสนับสนุนหรือเกี่ยวข้องกับการกระทำที่ผิดกฎหมายด้วยจึงจะเป็นความผิดตามมาตรานี้ ซึ่งโดยปกติแล้วการกระทำความผิดในมาตรานี้ย่อมเกี่ยวข้องกับการกระทำความผิดอื่นๆ ด้วย[17] ซึ่งถือว่าผู้กระทำมีเจตนาตามมาตรานี้แล้ว

บทลงโทษตามมาตรานี้บัญญัติอยู่ในอนุมาตรา (b) ซึ่งมีกำหนดไว้ห้าระดับด้วยกันคือ

(ก) อัตราโทษจำคุกไม่เกิน 5 ปีหรือปรับหรือทำจำทั้งปรับ

(ข) อัตราโทษจำคุกไม่เกิน 15 ปีหรือปรับหรือทำจำทั้งปรับ ถ้าการกระทำผิดนั้นเป็นผลให้ผู้กระทำความผิดได้รับสิ่งใดก็ตามที่มีมูลค่ารวมกันตั้งแต่ 1,000 ดอลลาร์สหรัฐ[18] ภายในระยะเวลา 1 ปี

(ค) อัตราโทษจำคุกไม่เกิน 20 ปีหรือปรับหรือทำจำทั้งปรับ ถ้าเป็นการอำนวยความสะดวกในการก่ออาชญากรรมค้ายาเสพติด หรือเกี่ยวข้องกับอาชญากรรมเกี่ยวกับความรุนแรง หรือเป็นกรณีการกระทำความผิดซ้ำ

(ง) อัตราโทษจำคุกไม่เกิน 30 ปีหรือปรับหรือทำจำทั้งปรับ ถ้าเป็นการกระทำเพื่อสนับสนุนการก่อการร้ายภายในประเทศหรือการก่อการร้ายข้ามชาติ

(จ) ริบทรัพย์สินใดๆ ที่เป็นของผู้กระทำความผิดที่ได้ใช้หรือมีไว้เพื่อจะใช้ในการกระทำความผิด ให้ตกเป็นของสหรัฐ

4.1.2 การฉ้อโกงและการกระทำที่เกี่ยวข้องกับอุปกรณ์ในการเข้าถึง (Fraud and related activity in connection with access devices)

การฉ้อโกงและการกระทำที่เกี่ยวข้องกับอุปกรณ์ในการเข้าถึง (Fraud and related activity in connection with access devices) บัญญัติอยู่ในมาตรา 1029 (18 U.S.C. § 1029) อันพัฒนามาจากพระราชบัญญัติการฉ้อโกงบัตรเครดิต ค.ศ. 1984 (Credit Card Fraud Act of 1984) ซึ่งเอา

---

[17] เช่น เกี่ยวข้องกับการฉ้อโกงข้อมูลส่วนบุคคล ตามมาตรา 1028 หรืออาชญากรรมบัตรเครดิต ตามมาตรา 1029 หรืออาชญากรรมคอมพิวเตอร์ ตามมาตรา 1030 หรืออาชญากรรมเมล์ ตามมาตรา 1341 หรืออาชญากรรมโทรเลข ตามมาตรา 1343 หรือการฉ้อโกงสถาบันการเงิน ตามมาตรา 1344

[18] ประมาณ 31,180 บาท (อัตราแลกเปลี่ยน ณ วันที่ 21 ตุลาคม 2563)

ผิดกับการฉ้อโกงหรือการปลอมแปลงบัตรในความหมายของการเป็นอุปกรณ์ในการเข้าถึง (access devices) เพื่อให้ครอบคลุมกับรูปแบบของการกระทำความผิดต่างๆ ที่เกิดขึ้น[19]

ในมาตราดังกล่าวมีการกระทำความผิดที่เกี่ยวข้องกับการดึงข้อมูลบัตร ได้บัญญัติอยู่ในอนุมาตรา (a)(1) ซึ่งบัญญัติว่า

มาตรา 1029 (a)(1) บัญญัติว่า “ผู้ใด (Whoever) โดยรู้สำนึก (Knowingly) และมีเจตนาที่จะฉ้อโกง ผลิต (Produce) ใช้ หรือเคลื่อนย้าย (Traffics in) อุปกรณ์ในการเข้าถึงปลอม (Counterfeit access devices) อย่างน้อยหนึ่งชิ้น... หากความผิดนั้นส่งผลกระทบต่อการพาณิชย์ระหว่างรัฐหรือการพาณิชย์ต่างประเทศ (Interstate or foreign commerce) จะต้องรับโทษตามที่ระบุไว้ในอนุมาตรา (c)”

วัตถุแห่งการกระทำความผิดตามมาตรานี้คือ อุปกรณ์ในการเข้าถึงปลอม (Counterfeit access devices) ซึ่งอนุมาตรา (e) ให้คำนิยามไว้ว่าหมายถึง “อุปกรณ์ในการเข้าถึงที่ได้ทำปลอมขึ้น[20] หรือส่วนประกอบที่สามารถระบุได้ (Identifiable component) ของอุปกรณ์ในการเข้าถึง”[21] ดังนั้นจึงจำต้องพิจารณาคำว่า อุปกรณ์ในการเข้าถึง (Access devices) ประกอบด้วย ซึ่งหมายความว่า “ใดๆ ก็ตามที่เป็น บัตร (Card) ป้าย (Plate) รหัส (Code) หมายเลขบัญชี (Account number) หมายเลขอิเล็กทรอนิกส์ (Electronic serial number) หมายเลขประจำตัวมือถือ (Mobile identification number) หมายเลขประชาชน (Personal identification number) หรือ บริการ อุปกรณ์ เครื่องมือที่ใช้ในการระบุตัวตนในการโทรคมนาคม หรือ วิธีการอื่นในการเข้าถึงบัญชี ที่สามารถใช้โดยลำพังหรือร่วมกับอุปกรณ์ในการเข้าถึงอื่น ในการรับเงิน สินค้า บริการ หรือสิ่งมีค่าอื่นใด หรือสามารถใช้ในการโอนเงินที่นอกเหนือจากการใช้วิธีทางเอกสาร”[22] ดังนั้นคำว่า อุปกรณ์ในการเข้าถึงปลอม ตามมาตรานี้จึงหมายถึง

[19] Eisner Gorin LLP, "Credit Card Fraud" [Online], Accessed: 22 October 2020. Available from: https://www.thefederalcriminalattorneys.com/fraud-crimes/federal-credit-card-fraud/.

[20] ด้วยวิธีการประดิษฐ์ขึ้น (Fictitious) เปลี่ยนแปลง (Altered) หรือสร้างขึ้น (Forged)

[21] Subsection (e)(2) of section 1029 of United States Code

[22] Subsection (e)(1) of section 1029 of United States Code

(ก) บัตร รหัส หมายเลขใดๆ เป็นต้น ที่เป็นของปลอม เช่น บัตรปลอม รหัสปลอม หมายเลขปลอม

(ข) บัตร รหัส หมายเลขใดๆ เป็นต้น ที่เป็นส่วนประกอบของบัตร รหัส หรือหมายเลขนั้นๆ ที่แท้จริง ซึ่งในความหมายนี้จึงหมายถึง ข้อมูลของบัตรใดๆ ในฐานะที่ข้อมูลนั้นเป็นส่วนประกอบของบัตรที่ได้มีการออกเอกสารหรือวัตถุอื่นใดให้ (Physical Cards) หรือเป็นส่วนประกอบของรหัสบัตรที่มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ (Virtual Cards) ตัวอย่างในคดี UNITED STATES v. BARSUMYAN (2008)[23] นาย Aram Barsumyan ได้ตกลงกับพนักงานโรงแรมคนหนึ่งให้ใช้เครื่องสกิมเมอร์ดึงข้อมูลบัตรเครดิตของลูกค้าที่มาพักในโรงแรมเพื่อแลกกับบัตรปลอมที่ตนจะทำขึ้นแล้วนำมาให้พนักงานนั้นเพื่อนำบัตรปลอมไปใช้ต่อไป นาย Barsumyan ถูกจับและถูกศาลตัดสินตามมาตรานี้ เพราะถือว่าข้อมูลบัตรเครดิตที่ได้ดึงมานั้นเข้าลักษณะการเป็นอุปกรณ์ในการเข้าถึงปลอมอันเป็นวัตถุแห่งการกระทำความผิดตามมาตรานี้แล้ว

การกระทำการเคลื่อนย้าย (Traffics in) นั้นอนุมาตรา (e) ให้คำนิยามไว้ว่าหมายถึง “โอน (Transfer) หรือได้รับ (Obtain) ไว้ในการควบคุม โดยมีเจตนาจะโอนหรือกำจัดทิ้ง”[24] ส่วนคำว่าผลิต (Produce) ยังให้ความหมายถึง ทำซ้ำ (Duplicate)[25] อีกด้วย และเมื่อพิจารณาจากคดี UNITED STATES v. BARSUMYAN ข้างต้นที่เป็นการดึงข้อมูลจากบัตรเครดิตกับคำนิยามดังกล่าว จึงอาจกล่าวได้ว่า การดึงไม่ว่าด้วยวิธีการใด ย่อมอยู่ในความหมายของการโอน ได้รับหรือทำซ้ำ อันเป็นการกระทำดังที่ได้กำหนดไว้ในมาตรานี้

ดังนั้น หากผู้ใดได้ทำการดึงข้อมูลของบัตร ไม่ว่าบัตรนั้นจะได้มีการออกเอกสารหรือวัตถุอื่นใดให้หรือไม่ก็ตาม ก็จะเป็นการโอน ได้รับหรือทำซ้ำอุปกรณ์ในการเข้าถึงปลอม อันเป็นความผิดตามมาตรานี้ อย่างไรก็ตามข้อมูลในบัตรที่จะเป็นวัตถุแห่งการกระทำความผิดตามมาตรานี้ได้นั้น จะต้องเป็นข้อมูลของบัตรที่มีวัตถุประสงค์ในการใช้ในการรับเงิน สินค้า บริการ หรือสิ่งมีค่าอื่นใด หรือสามารถใช้ในการโอนเงินที่นอกเหนือจากการใช้วิธีทางเอกสารโดยทั่วไปด้วย เช่น บัตรเอทีเอ็ม บัตรเครดิต บัตรเดบิต บัตรเงินสด บัตรเติมเงิน บัตรรถไฟฟ้า หรือบัตรกำนัล และผู้กระทำจะต้องรู้สำนึกและมีเจตนาที่จะฉ้อโกงด้วย ซึ่งหมายความว่า ผู้กระทำตระหนักรู้ถึงผลธรรมดาที่จะเกิดขึ้นจากการ

---

[23] Findlaw, "United States V. Barsumyan" [Online], Accessed: 20 October 2020. Available from: https://caselaw.findlaw.com/us-9th-circuit/1410201.html#footnote_ref_3.

[24] Subsection (e)(5) of section 1029 of United States Code

[25] Subsection (e)(4) of section 1029 of United States Code

กระทำของตนและตั้งใจว่าจะเกิดผลนั้นขึ้นด้วย คือ รู้ว่ามีคนที่กำลังจะถูกฉ้อโกงอยู่และตนตั้งใจว่าจะให้คนนั้นถูกฉ้อโกงจากการกระทำของตน[26]

บทลงโทษตามมาตรานี้บัญญัติอยู่ในมาตราอนุมาตรา (c) ซึ่งมีอัตราโทษจำคุกไม่เกิน 10 ปี หรือปรับหรือทำจำทั้งปรับ[27] หรือ หากเป็นกรณีการกระทำความผิดซ้ำ[28] จะมีอัตราจำคุกไม่เกิน 20 ปี หรือปรับหรือทำจำทั้งปรับ

4.1.3 การฉ้อโกงและการกระทำที่เกี่ยวข้องกับคอมพิวเตอร์ (Fraud and related activity in connection with computers)

การฉ้อโกงและการกระทำที่เกี่ยวข้องกับคอมพิวเตอร์ (Fraud and related activity in connection with computers) บัญญัติอยู่ในมาตรา 1030 (18 U.S.C. § 1030) อันพัฒนามาจากพระราชบัญญัติการละเมิดและการฉ้อโกงทางคอมพิวเตอร์ ค.ศ. 1986 (The Computer Fraud and Abuse Act 1986) ซึ่งเอาผิดกับการกระทำที่เกี่ยวข้องในการเข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือเกินกว่าที่ได้รับอนุญาตอันกระทบต่อคอมพิวเตอร์ของรัฐบาลกลาง สถาบันการเงินหรือคอมพิวเตอร์ที่เชื่อมต่อกับระบบอินเตอร์เน็ต[29]

ในมาตราดังกล่าวมีการกระทำความผิดที่เกี่ยวข้องกับการดึงข้อมูลบัตร ได้บัญญัติอยู่ในอนุมาตรา (a)(2) ซึ่งบัญญัติว่า

มาตรา 1030 (a)(2) บัญญัติว่า “ผู้ใด (Whoever) โดยเจตนา เข้าถึง (Accesses) คอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือเกินกว่าที่ได้รับอนุญาตและด้วยการกระทำดังกล่าวจึงได้รับ (Obtain) (A) ข้อมูลที่เป็นบันทึกทางการเงินของสถาบันการเงินหรือของผู้ออกบัตร หรือที่เป็นข้อมูล

---

[26] Charles Doyle, "Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws" [Online], Accessed: 20 October 2020. Available from: https://www.everycrsreport.com/files/20141015_97-1025_31056cd16cc55cc39047e24e327a15875045157f.pdf.

[27] อัตราค่าปรับขึ้นอยู่กับความผิดอาญาว่าเป็นความผิดลหุโทษ (Misdemeanor) หรือความผิดร้ายแรง (Felony) โดยหากเป็นการกระทำความผิดของปัจเจกชน ค่าปรับความผิดลหุโทษจะอยู่ที่ 5,000 ถึง 250,000 ดอลลาร์สหรัฐ ส่วนค่าปรับความผิดร้ายแรงจะไม่เกิน 250,000 ดอลลาร์สหรัฐ ตามมาตรา 3571 ในรัฐบัญญัติสหรัฐอเมริกา (United States Code)

[28] ผู้กระทำผิดได้ถูกตัดสินให้รับผิดในความผิดใดๆ ดังที่ได้กำหนดในมาตรานี้อันเป็นการกระทำความผิดซ้ำในมาตราเดียวกัน

[29] Charles Doyle, "Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws" [Online], Accessed: 20 October 2020. Available from: https://fas.org/sgp/crs/misc/RS20830.pdf.

ขององค์การเกี่ยวกับการรายงานผู้บริโภค หรือ (B) ข้อมูลของกระทรวงหรือองค์กรใดๆ ของสหรัฐอเมริกา หรือ (C) ข้อมูลจากเครื่องคอมพิวเตอร์ใดๆ ที่มีการป้องกัน... จะต้องได้รับโทษตามที่บัญญัติไว้ในอนุมาตรา (c)"

การกระทำตามมาตรานี้คือการ เข้าถึง (Accesses) คอมพิวเตอร์และด้วยการเข้าถึงคอมพิวเตอร์นั้นจึงได้รับ (Obtain) ข้อมูล ดังนั้นการกระทำตามมาตรานี้จึงประกอบไปด้วยสองกรรม คือ ต้องมีการเข้าถึงและมีการได้รับ จึงจะครบองค์ประกอบความผิดตามมาตรานี้ โดยคำว่า เข้าถึงนั้นไม่มีการบัญญัติคำนิยามไว้ในมาตรานี้และศาลของสหรัฐอเมริกาก็ยังไม่มีคำอธิบายที่แน่นอนว่าหมายความว่าอย่างไร[30] แต่โดยลักษณะของการกระทำแล้วย่อมเป็นการบุกรุกคอมพิวเตอร์ (Computer trespassing) โดยวิธีการต่าง เช่น การแฮก (Hacking)[31] ส่วนคำว่าได้รับ นั้นแม้จะมิได้บัญญัติคำนิยามไว้เช่นเดียวกัน แต่รัฐสภาสหรัฐ (United States Congress) ได้กล่าวว่านอกจากจะหมายถึงการคัดลอก (Copied) หรือการขนส่ง (Transported) แล้ว เพียงแต่การอ่าน (Reading) ก็ถือว่าเป็นการได้รับไปแล้ว เพราะในสภาพแวดล้อมทางอิเล็กทรอนิกส์นั้น ข้อมูลสามารถที่จะถูกขโมยไปได้โดยที่ต้นฉบับของข้อมูลนั้นยังคงอยู่ครบถ้วน[32] ดังนั้นคำว่า ได้รับ ในทางอิเล็กทรอนิกส์นั้นจึงมีความหมายที่กว้างกว่าการได้รับสิ่งของทั่วๆ ไปที่จะมีการเพิ่มขึ้นทางฝั่งผู้ได้รับและจะต้องมีการสูญเสียไปจากแหล่งที่มีอยู่เดิม

ข้อมูลอันเป็นวัตถุแห่งการกระทำความผิดตามมาตรานี้ หมายความว่า เป็นข้อมูลในรูปแบบอิเล็กทรอนิกส์ซึ่งเก็บไว้ในรูปแบบอันจับต้องมิได้ (Intangible form)[33] กำหนดไว้สามประเภท อันได้แก่

(A) ข้อมูลที่เป็นบันทึกทางการเงินของสถาบันการเงินหรือของผู้ออกบัตร หรือที่เป็นข้อมูลขององค์การเกี่ยวกับการรายงานผู้บริโภค หมายถึง ข้อมูลจากบันทึกที่สถาบันทางการเงินจัดทำขึ้นซึ่ง

---

[30] พิญดา เลิศกิตติกุล, "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2550), หน้า 88.

[31] Charles Doyle, " Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws" [Online], Accessed: 20 October 2020. Available from: https://fas.org/sgp/crs/misc/RS20830.pdf.

[32] Charles Doyle, "Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws" [Online], Accessed: 20 October 2020. Available from: https://www.everycrsreport.com/files/20141015_97-1025_31056cd16cc55cc39047e24e327a15875045157f.pdf.

[33] Ibid.

เกี่ยวข้องกับความสัมพันธ์ระหว่างลูกค้ากับสถาบันทางการเงิน[34] หรือข้อมูลเครดิตและข้อมูลอื่นๆ ของผู้บริโภคขององค์การเกี่ยวกับการรายงานผู้บริโภค[35] เช่น ข้อมูลทางการเงินของบุคคล (personal financial information) ที่ได้เก็บไว้ในไฟล์ในเครื่องคอมพิวเตอร์[36]

(B) ข้อมูลของกระทรวงหรือองค์กรใดๆ ของสหรัฐอเมริกา หมายถึง ข้อมูลของฝ่ายนิติบัญญัติ ฝ่ายตุลาการ[37] หรือกระทรวงต่างๆ ของสหรัฐอเมริกา[38] เช่น กระทรวงแรงงาน กระทรวงการต่างประเทศ กระทรวงความกลาโหม

(C) ข้อมูลจากเครื่องคอมพิวเตอร์ใดๆ ที่มีการป้องกัน หมายถึง[39] ข้อมูลจากเครื่องคอมพิวเตอร์สำหรับการใช้งานของสถาบันการเงินหรือรัฐบาลสหรัฐโดยเฉพาะ หรือจากเครื่องคอมพิวเตอร์อื่นที่การกระทำผิดนี้จะส่งผลต่อการใช้งานของสถาบันการเงินหรือรัฐบาลสหรัฐ เช่น ธนาคารพาณิชย์ บริษัทเครดิตยูเนี่ยน[40] หรือจากเครื่องคอมพิวเตอร์ที่ใช้แล้วจะส่งผลต่อการพาณิชย์หรือการสื่อสารระหว่างรัฐหรือต่างประเทศ ซึ่งหมายถึง เป็นข้อมูลจากเครื่องคอมพิวเตอร์ใดๆ ที่ดำเนินธุรกรรมทางการเงินผ่านระบบอินเตอร์เน็ตได้ ก็ถือว่าส่งผลต่อการพาณิชย์หรือการสื่อสารระหว่างรัฐหรือต่างประเทศแล้ว[41]

กล่าวโดยสรุปคือมาตรานี้ เอาผิดกับการกระทำการเข้าถึง (Accesses) โดยไม่ได้รับอนุญาต อันเป็นการบุกรุกเครื่องคอมพิวเตอร์โดยใช้วิธีการต่างๆ เช่น การแฮก (Hacking) และด้วยการเข้าถึงนั้นผู้กระทำได้กระทำการได้รับ (Obtain) เช่น การคัดลอก (Copied) การขนส่ง (Transported) หรือเพียงแต่การอ่าน (Reading) ข้อมูลใดๆ ที่กำหนดไว้สามประเภท เช่น ข้อมูลทางการเงินของบุคคล ของสถาบันการเงิน ข้อมูลของกระทรวงหรือองค์กรต่างๆ ของสหรัฐ ข้อมูลที่บุคคลใช้ดำเนินธุรกรรม

[34] Subsection (e)(5) of section 1030 of United States Code

[35] Subsection (a)(3) of section 1681 of United States Code

[36] Charles Doyle, Cybercrime: “An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws” [Online], Accessed: 20 October 2020. Available from: https://www.everycrsreport.com/files/20141015_97-1025_31056cd16cc55cc39047e24e327a15875045157f.pdf.

[37] Subsection (e)(7) of section 1681 of United States Code

[38] Section 5 of section 101 of United States Code

[39] Subsection (e)(2) of section 1030 of United States Code

[40] Meaning of “financial institution” in section 1030(e)(4) of United States Code

[41] Charles Doyle, Cybercrime: “An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal” Laws [Online], Accessed: 20 October 2020. Available from: https://www.everycrsreport.com/files/20141015_97-1025_31056cd16cc55cc39047e24e327a15875045157f.pdf.

ทางการเงินผ่านระบบอินเตอร์เน็ต และต้องเป็นข้อมูลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ที่อยู่ในเครื่องคอมพิวเตอร์ด้วย

เนื่องจากคำนิยามของคำว่า คอมพิวเตอร์ ดังที่กำหนดไว้ในอนุมาตรา (e)(1) นั้นมิได้บัญญัติให้รวมถึงอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ด้วย (Computer storage device)[42] ดังนั้น บัตรใดๆ ที่มีการออกเอกสารหรือวัตถุอื่นใดให้ซึ่งเป็นอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์รูปแบบหนึ่งจึงมิใช่คอมพิวเตอร์ อันส่งผลให้ข้อมูลในบัตรรูปแบบดังกล่าวจะไม่ได้รับความคุ้มครองจากการกระทำความผิดจากการดึงข้อมูลตามมาตรานี้ ดังนั้นมาตราดังกล่าวจึงสามารถใช้ได้แก่ข้อมูลบัตรประเภทที่มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ซึ่งข้อมูลบัตรนั้นจำต้องได้บันทึกอยู่ในคอมพิวเตอร์เท่านั้น เช่น รหัสบัตรเครดิต รหัสประจำตัว ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการใช้งานระบบคอมพิวเตอร์ในกระทรวงหรือหน่วยงานต่างๆ

บทลงโทษตามมาตรานี้บัญญัติอยู่ในอนุมาตรา (c)(2) ซึ่งมีกำหนดไว้สามระดับด้วยกันคือ

(ก) อัตราโทษจำคุกไม่เกิน 1 ปีหรือปรับหรือทำจำทั้งปรับ

(ข) อัตราโทษจำคุกไม่เกิน 5 ปีหรือปรับหรือทำจำทั้งปรับ ถ้าเป็นการกระทำเพื่อแสวงหาประโยชน์ทางการพาณิชย์หรือประโยชน์ทางการเงิน หรือ เป็นการกระทำเพื่อความก้าวหน้าในการกระทำความผิดอาญาอื่นๆ หรือฝ่าฝืนรัฐธรรมนูญของสหรัฐอเมริกาหรือกฎหมายของมลรัฐใดๆ หรือมูลค่าของข้อมูลที่ผู้กระทำความผิดได้รับนั้นมากกว่า 5,000 ดอลลาร์สหรัฐ[43]

(ค) หากเป็นกรณีการกระทำความผิดซ้ำ จะมีอัตราจำคุกไม่เกิน 10 ปีหรือปรับหรือทำจำทั้งปรับ

ข้อสังเกต หากการดึงข้อมูลอันเป็นวัตถุแห่งการกระทำความผิดตามมาตรา 1029(a)(1) และมาตรา 1030(a)(2) นั้น เข้าลักษณะการเป็น สิ่งที่อ้างอิงในการระบุตัวตน (A means of identification) ตามคำนิยามดังที่กำหนดไว้ในมาตรา 1028 ด้วยแล้ว ผู้กระทำย่อมต้องรับผิดตามมาตรา 1028A อีกกระทงหนึ่งด้วย ซึ่งมีอัตราโทษจำคุก 2 ปี

---

[42] คำว่า “คอมพิวเตอร์” หมายถึง อุปกรณ์ที่เกี่ยวกับอิเล็กทรอนิกส์ แม่เหล็กไฟฟ้า การมองเห็น เคมีไฟฟ้า หรืออุปกรณ์ประมวลผลข้อมูลด้วยความเร็วสูงอื่นๆ ที่ทำหน้าที่ทางตรรกะ เลขคณิตหรือการจัดเก็บข้อมูล และรวมถึงสถานที่ที่ใช้ในการจัดเก็บข้อมูลหรือใช้ในการติดต่อสื่อสารที่เกี่ยวข้องโดยตรงหรือทำหน้าที่เชื่อมต่ออุปกรณ์เหล่านั้นเข้าด้วยกัน แต่คำนิยามนี้ไม่รวมถึงเครื่องพิมพ์ดีดหรือเครื่องเรียงพิมพ์อัตโนมัติ เครื่องคิดเลขแบบพกพาหรืออุปกรณ์อื่นที่ลักษณะคล้ายกัน

[43] ประมาณ 155,902 บาท (อัตราแลกเปลี่ยน ณ วันที่ 21 ตุลาคม 2563)

ตารางที่ 7 เปรียบเทียบบทบัญญัติของกฎหมายสหรัฐอเมริกาที่เกี่ยวข้องกับการดึงข้อมูลจากบัตร

บทบัญญัติ	การกระทำ	วัตถุแห่งการกระทำ	เจตนา	โทษ
มาตรา 1028(a)(7)	โอน (Transfers) (หมายถึงการดึงด้วย) โดยไม่มีอำนาจตามกฎหมาย	สิ่งที่อ้างอิงในการระบุตัวตน (A means of identification) ของผู้อื่น	เจตนาที่จะกระทำหรือช่วยเหลือหรือสนับสนุนหรือเกี่ยวข้องกับการกระทำที่ผิดกฎหมายใดๆ ที่ถือเป็นการละเมิดต่อกฎหมายของรัฐบาลกลาง หรือก่อให้เกิดความผิดอาญาร้ายแรงภายใต้กฎหมายของมลรัฐหรือท้องถิ่น	จำคุกไม่เกิน 5 ปี ถึง 30 ปี ขึ้นอยู่กับลักษณะของการกระทำความผิด หรือปรับหรือทั้งจำทั้งปรับ และริบทรัพย์สินใดๆ ที่เป็นของผู้กระทำความผิดที่ได้ใช้หรือมีไว้เพื่อจะใช้ในการกระทำความผิด ให้ตกเป็นของสหรัฐด้วย
มาตรา 1029(a)(1)	ผลิต (Produce) ใช้หรือเคลื่อนย้าย (Traffics in) (หมายถึงได้รับ (Obtain) หรือทำซ้ำ (Duplicate) ด้วย)	อุปกรณ์ในการเข้าถึงปลอม (Counterfeit access devices) (หมายถึงข้อมูลของบัตรใดๆ ที่มีวัตถุประสงค์ในการใช้ทำธุรกรรมทางการเงิน)	เจตนาที่จะฉ้อโกง	จำคุกไม่เกิน 10 ปี หรือไม่เกิน 20 ปี ในกรณีการกระทำความผิดซ้ำ หรือปรับหรือทั้งจำทั้งปรับ

บทบัญญัติ	การกระทำ	วัตถุแห่งการกระทำ	เจตนา	โทษ
มาตรา 1030(a)(2)	เข้าถึง (Accesses) คอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือเกินกว่าที่ได้รับอนุญาตและด้วยการกระทำดังกล่าวจึงได้รับ (Obtain)	ข้อมูลในรูปแบบอิเล็กทรอนิกส์ที่อยู่ในคอมพิวเตอร์ที่ได้กำหนดไว้สามประเภท	เจตนาธรรมดา	จำคุกไม่เกิน 1 ปี ถึง 5 ปี ขึ้นอยู่กับลักษณะของการกระทำความผิดหรือไม่เกิน 10 ปี ในกรณีการกระทำความผิดซ้ำ หรือปรับหรือทั้งจำทั้งปรับ

ข้อสังเกต นอกจากรัฐบัญญัติของสหรัฐอเมริกา (The United States Code) ที่ได้กล่าวมาซึ่งเป็นกฎหมายของรัฐบาลกลางแห่งสหรัฐแล้ว มลรัฐต่างๆ ก็มีบทบัญญัติกฎหมายเป็นของตนเองเพื่อเอาผิดกับการกระทำในลักษณะการดึงข้อมูลบัตรด้วย ดังตัวอย่างในตารางต่อไปนี้

ตารางที่ 8 เปรียบเทียบบทบัญญัติของกฎหมายมลรัฐในสหรัฐอเมริกาที่เกี่ยวข้องกับการดึงข้อมูลจากบัตร

มลรัฐ	บทบัญญัติ	การกระทำความผิด	โทษ
Arizona	Revised Statutes Title 13 § 13-2110	มันเป็นการกระทำผิดกฎหมาย หากบุคคลใช้อุปกรณ์ในการสแกน (scanning device) หรือเครื่องถ่ายรหัส (reencoder) โดยไม่ได้รับอนุญาตจากผู้ถือบัตรเครดิต ซึ่งข้อมูล (information) ของบัตรนั้นได้ถูกสแกนหรือเข้ารหัสด้วยเจตนาจะฉ้อโกงผู้ถือบัตร ผู้ออกบัตรหรือผู้ค้า	จำคุกตั้งแต่ 1 ปี 6 เดือน จนถึง 3 ปี

มลรัฐ	บทบัญญัติ	การกระทำความผิด	โทษ
California	Penal Code – PEN § 484e(d)	บุคคลใด ได้มา (acquires) หรือเก็บรักษา (retains possession) ข้อมูลบัตรในการเข้าถึงบัญชี (access card account information) โดยรู้ว่าบัตรนั้นได้ออกให้ผู้อื่นใช้ โดยไม่ได้รับความยินยอมจากผู้ถือบัตรหรือผู้ออกบัตร ด้วยเจตนาจะใช้ในทางทุจริต จะมีความผิดฐานโจรกรรม	จำคุกไม่เกิน 1 ปี
Delaware	Code Title 11 § 854	บุคคลจะกระทำความผิดฐานโจรกรรมข้อมูลเมื่อบุคคลนั้นจงใจหรือประมาท ได้รับ (obtain) ผลิต ครอบครอง ใช้ ขาย ให้หรือโอน ข้อมูลที่ระบุตัวบุคคล (personal identifying information) ซึ่งเป็นของหรือเกี่ยวข้องกับบุคคลอื่นโดยมิได้รับอนุญาตจากบุคคลนั้น โดยเจตนาจะใช้ข้อมูลเพื่อกระทำหรือสนับสนุนอาชญากรรมใดๆ	จำคุกไม่เกิน 8 ปี
	Code Title 11 § 903A(a)	บุคคลใด จงใจและโดยเจตนาที่จะฉ้อโกง ครอบครองหรือใช้อุปกรณ์สแกน (scanning device) เพื่อเข้าถึง อ่าน ได้รับ (obtain) จดจำ หรือจัดเก็บ ไม่ว่าชั่วคราวหรือถาวร ซึ่งข้อมูล (information) ที่ได้เข้ารหัสบนชิปคอมพิวเตอร์หรือแถบแม่เหล็กหรือแถบของบัตรชำระเงินโดยไม่ได้รับอนุญาตจากผู้สิทธิใช้บัตรชำระเงิน	จำคุกไม่เกิน 8 ปี
	Code Title 11 § 935	คัดลอก (copy) รับ (Take) ได้รับ (receives) ข้อมูล ไม่ว่าอยู่ในคอมพิวเตอร์ ระหว่างการสื่อสารของคอมพิวเตอร์ ผลิตหรือใช้โดยคอมพิวเตอร์	จำคุกไม่เกิน 1 ปีถึงไม่เกิน 8 ปี

มลรัฐ	บทบัญญัติ	การกระทำความผิด	โทษ
Florida	Statutes Title XLVI § 817.625(2)(a)	บุคคลใดก็ตามที่ใช้อุปกรณ์สแกน (scanning device) เพื่อเข้าถึง อ่าน ได้รับ (obtain) จดจำ หรือจัดเก็บ ไม่ว่าชั่วคราวหรือถาวร ซึ่งข้อมูล (information) ที่ได้เข้ารหัสบนแถบแม่เหล็กหรือแถบของบัตรชำระเงิน โดยไม่ได้รับอนุญาตจากผู้มีสิทธิใช้บัตรชำระเงินนั้น และมีเจตนาเพื่อฉ้อโกงผู้นั้น ผู้ออกบัตรชำระเงินให้หรือผู้ค้า	จำคุกไม่เกิน 5 ปีหรือปรับไม่เกิน 5,000 ดอลลาร์สหรัฐ
Illinois	Statutes Chapter 720 §16-6(c)(1)	บุคคลจะกระทำความผิดในการใช้อุปกรณ์สแกนเพื่อการฉ้อโกงเมื่อบุคคลนั้นโดยรู้สำนึก ใช้อุปกรณ์ในการสแกน (scanning device) ในการเข้าถึง (access) อ่าน (read) ได้รับ (obtain) จดจำ (memorize) หรือเก็บ (store) ไม่ว่าชั่วคราวหรือถาวร ซึ่งข้อมูล (information) ที่เข้ารหัสไว้ในแถบแม่เหล็กหรือแถบของบัตรชำระเงิน โดยไม่ได้รับอนุญาตจากผู้มีสิทธิใช้บัตรชำระเงินและมีเจตนาจะฉ้อโกงผู้นั้น ผู้ออกบัตรชำระเงินให้หรือผู้ค้า	จำคุกตั้งแต่ 1 ปีถึง 3 ปีหรือปรับไม่เกิน 25,000 ดอลลาร์สหรัฐ
	Statutes Chapter 720 § §16-30(3)	บุคคลจะกระทำการโจรกรรมข้อมูลส่วนบุคคลเมื่อเขาโดยรู้สำนึก ได้รับ (obtains) บันทึก (records) ครอบครอง ขาย โอน (transfers) ซื้อหรือผลิตข้อมูลประจำตัวบุคคล (personal identification information) ของบุคคลอื่นด้วยเจตนาที่จะก่ออาชญากรรมใดๆ	จำคุกตั้งแต่ 2 ปีถึง 5 ปีหรือปรับไม่เกิน 25,000 ดอลลาร์สหรัฐ

มลรัฐ	บทบัญญัติ	การกระทำความผิด	โทษ
Kentucky	Revised Statutes Title XL. § 434.675(1)	ห้ามมิให้บุคคลใดใช้อุปกรณ์สแกน (scanning device) เพื่อเข้าถึง อ่าน ได้รับ (obtain) จดจำ หรือจัดเก็บ ไม่ว่าชั่วคราวหรือถาวร ซึ่งข้อมูล (information) ที่ได้เข้ารหัสบนแถบแม่เหล็กหรือแถบของบัตรชำระเงินโดยมีเจตนาที่จะฉ้อโกงผู้ที่ได้รับอนุญาตให้ใช้ ผู้ออกบัตรชำระเงินให้หรือผู้ค้า	จำคุกตั้งแต่ 1 ปีถึง 5 ปี
Nevada	Revised Statutes Title 15 § 205.605 1(a)	บุคคลจะต้องไม่ใช้อุปกรณ์ในการสแกน (scanning device) ในการเข้าถึง (access) อ่าน (read) ได้รับ (obtain) จดจำ (memorize) หรือเก็บ (store) ไม่ว่าชั่วคราวหรือถาวร ซึ่งข้อมูล (information) ที่เข้ารหัสไว้ในแถบแม่เหล็กหรือแถบของบัตรชำระเงิน โดยไม่ได้รับอนุญาตจากผู้มีสิทธิใช้บัตรชำระเงินและมีเจตนาจะฉ้อโกงผู้นั้น ผู้ออกบัตรชำระเงินหรือผู้อื่น	จำคุกตั้งแต่ 1 ปีถึง 5 ปี และอาจปรับไม่เกิน 10,000 ดอลลาร์สหรัฐ
Texas	Penal Code § 31.17(b)(1)	ได้รับ (obtains) ใบสั่งซื้อทางการเงินหรือข้อมูลบัตรชำระเงิน (payment card information) ของผู้อื่นโดยใช้อุปกรณ์อิเล็กทรอนิกส์ ภาพถ่าย ถ่ายภาพ บันทึกภาพ หรืออุปกรณ์อื่นๆ ซึ่งสามารถเข้าถึง อ่าน บันทึก จับภาพ คัดลอก ถ่ายภาพ สแกน ทำซ้ำหรือจัดเก็บในลักษณะใดๆ	จำคุกไม่เกิน 180 วันหรือปรับไม่เกิน 2,000 ดอลลาร์สหรัฐ หรือทั้งจำทั้งปรับ

มลรัฐ	บทบัญญัติ	การกระทำความผิด	โทษ
Maine	Revised Statutes Title 17-A § 905-B	บุคคลจะมีความผิด ถ้าหากจงใจใช้อุปกรณ์ในการสแกน (scanning device) หรือเครื่องถ่ายรหัส (reencoder) โดยไม่ได้รับอนุญาตจากผู้มีสิทธิใช้บัตรชำระเงิน ซึ่งข้อมูลบัตร (card information) นั้นได้ถูกสแกนหรือเข้ารหัสด้วยเจตนาจะฉ้อโกงหรือหลอกลวงผู้มีสิทธิใช้บัตรชำระเงิน ผู้ออกบัตรชำระเงินให้หรือผู้อื่น	จำคุกไม่เกิน 1 ปีหรือปรับไม่เกิน 2,000 ดอลลาร์สหรัฐ
Wisconsin	Statutes Crimes § 943.202(b)2	บุคคลจะมีความผิด ถ้าใช้หรือพยายามจะใช้เครื่องถ่ายรหัส (reencoder) หรืออุปกรณ์ในการสแกน (scanning device) กับข้อมูลระบุตัวบุคคลใดๆ (personal identifying information) หรือใช้ในการเข้าถึง (access) ข้อมูลที่ได้เข้ารหัสไว้ในบัตรเครดิตโดยไม่ได้รับอนุญาตจากผู้มีสิทธิใช้บัตรเครดิต	จำคุกไม่เกิน 6 ปีหรือปรับไม่เกิน 10,000 ดอลลาร์สหรัฐหรือทั้งจำทั้งปรับ

ในคดีที่เกิดขึ้นนั้น หน่วยงานของรัฐบาลกลางและมลรัฐจะเป็นผู้ตัดสินใจว่าผู้กระทำความผิดควรที่จะต้องถูกดำเนินคดีโดยอาศัยกฎหมายในระดับรัฐบาลกลางหรือระดับมลรัฐ ซึ่งโดยทั่วไปแล้วการกระทำความผิดที่เกิดผลกระทบที่สำคัญต่อสหรัฐอเมริกานั้นมักจะใช้กฎหมายในระดับรัฐบาลกลางในการดำเนินคดีมากกว่ากฎหมายในระดับมลรัฐ แต่ไม่ว่าจะใช้กฎหมายในระดับใดก็ตามผู้กระทำความผิดก็มักจะถูกลงโทษด้วยการจำคุกเป็นระยะเวลานานและต้องชดใช้ค่าปรับมหาศาลจากการกระทำความผิดในการดึงข้อมูลบัตรเสมอ[44]

ดังนั้นในเรื่องการดึงข้อมูลจากบัตรนี้สามารถปรับใช้กฎหมายของสหรัฐอเมริกาไม่ว่าจะเป็นกฎหมายของรัฐบาลกลางสหรัฐหรือกฎหมายของบางมลรัฐที่ได้บัญญัติขึ้นเองดังที่ได้ยกตัวอย่างมาแล้ว เพื่อลงโทษแก่ผู้กระทำความผิดได้ โดยรัฐบัญญัติของสหรัฐอเมริกา (The United States Code) ในฐานะของกฎหมายแห่งรัฐบาลกลางสหรัฐที่ได้รวบรวมและประมวลการกระทำความผิดทาง

[44] Arkady Bukh, "Credit Card Fraud" [Online], Accessed: 24 October 2020. Available from: https://nyccriminallawyer.com/fraud-charge/credit-card-fraud-charge/.

อาญาไว้จึงมีส่วนสำคัญในการบังคับใช้กับการกระทำความผิดในเรื่องการดึงข้อมูลนี้ โดยได้แบ่งการกระทำความผิดนี้ออกเป็นสามประเภทใหญ่ๆ ตามลักษณะของข้อมูลบัตรอันเป็นวัตถุแห่งการกระทำความผิด ประเภทแรกตามมาตรา 1028(a)(7) คือการโจรกรรมข้อมูลส่วนบุคคล (Identity theft) อันเป็นการดึงข้อมูลบัตรที่มีลักษณะเป็นข้อมูลส่วนบุคคล ตามนิยามของคำว่า “สิ่งที่อ้างอิงในการระบุตัวตน (A means of identification) ของผู้อื่น” ซึ่งเป็นข้อมูลบัตรที่เกี่ยวข้องกับการระบุตัวตนของบุคคลโดยเฉพาะเจาะจง ไม่ว่าจะเป็นชื่อ ที่อยู่ วันเดือนปีเกิด หมายเลขต่างๆ ของบุคคล เช่น หมายเลขประกันสังคม หมายเลขพาสปอร์ต รวมถึงเอกลักษณ์ข้อมูลทางชีวภาพและอุปกรณ์ในการเข้าถึง (Access device)[45] ที่บุคคลนั้นใช้ในการทำธุรกรรมทางการเงินด้วย ประเภทที่สองตามมาตรา 1029(a)(1) คือการดึงข้อมูลบัตรที่มีลักษณะเป็นข้อมูลที่มีวัตถุประสงค์เพื่อใช้ในการรับเงิน สินค้า บริการ หรือสิ่งมีค่าอื่นใด หรือสามารถใช้ในการโอนเงินที่นอกเหนือจากการใช้วิธีทางเอกสาร เช่น บัตร รหัส หมายเลขใดๆ ของบัตรเอทีเอ็ม บัตรเครดิต บัตรเดบิต บัตรเงินสด บัตรเติมเงิน บัตรรถไฟฟ้า บัตรกำนัล ซึ่งกฎหมายของสหรัฐได้บัญญัติให้ข้อมูลเหล่านี้เป็น “อุปกรณ์ในการเข้าถึง” (Access device) ประเภทที่สามตามมาตรา 1030(a)(2) คือการดึงข้อมูลบัตรที่มีลักษณะเป็นข้อมูลอิเล็กทรอนิกส์ที่อยู่ในคอมพิวเตอร์และเป็นข้อมูลตามที่มาตราดังกล่าวได้กำหนดไว้ เช่น ข้อมูลที่เป็นบันทึกทางการเงินของสถาบันการเงินหรือของผู้ออกบัตร ข้อมูลของกระทรวงหรือองค์กรใดๆ ของสหรัฐอเมริกา หรือข้อมูลจากเครื่องคอมพิวเตอร์ใดๆ ที่มีการป้องกัน ทั้งนี้ข้อมูลบัตรที่ผู้กระทำความผิดได้ดึงไปนั้นโดยส่วนใหญ่แล้วมักจะเข้าลักษณะของข้อมูลตั้งแต่สองประเภทขึ้นไปอันทำให้ผู้กระทำต้องรับผิดหลายกระทง[46] และต้องรับผิดมากขึ้นอันเป็นความผิดเกี่ยวเนื่องกันตามมาตรา 1028A อีกด้วย เช่น การดึงข้อมูลบัตรเครดิตที่มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ในเครื่องคอมพิวเตอร์ที่มีการป้องกันนอกจากจะเป็นความผิดตามมาตรา 1029(a)(1) แล้ว ยังเป็นการดึงข้อมูลส่วนบุคคลในฐานะที่บัตรเอทีเอ็มเป็นสิ่งที่อ้างอิงในการระบุตัวตน ตามมาตรา 1028(a)(7) และเป็นการเข้าถึงคอมพิวเตอร์และได้มาซึ่งข้อมูลทางการเงินของบุคคลของสถาบันการเงิน ตามมาตรา 1030(a)(2) อีกด้วย เมื่อบวกโทษเหล่านั้นเข้าด้วยกันแล้วย่อมทำให้ผู้กระทำต้องรับผิดด้วยการถูกจำคุกเป็นระยะเวลานานและเสียค่าปรับอย่างสูงแทบทั้งสิ้น

การบัญญัติกฎหมายดังที่กล่าวมา ย่อมแสดงให้เห็นว่าสหรัฐอเมริกาและมลรัฐต่างๆ ได้เล็งเห็นปัญหาจากการกระทำความผิดในลักษณะการดึงข้อมูลและมีความจริงจังในการแก้ปัญหาดังกล่าว ซึ่งแม้ว่ารัฐบาลกลางจะได้มีบทบัญญัติอันเอาผิดแก่การกระทำในลักษณะนี้โดยละเอียดอยู่

---

[45] ตามคำนิยามในมาตรา 1029(e)

[46] Arkady Bukh, “CREDIT CARD FRAUD” [Online], Accessed: 24 October 2020. Available from: https://nyccriminallawyer.com/fraud-charge/credit-card-fraud-charge/.

แล้ว แต่มลรัฐต่างๆ ก็ยังได้บัญญัติกฎหมายขึ้นเป็นของตนเองเพื่อใช้ในการแก้ปัญหานี้อีกด้วย สหรัฐอเมริกาจึงนับว่าเป็นประเทศที่มีกฎหมายอันเอาผิดแก่การดึงข้อมูลจากบัตรได้อย่างครอบคลุมและมีประสิทธิภาพประเทศหนึ่ง

4.2 สหราชอาณาจักร

4.2.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990)

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) หรือในชื่อเต็มคือพระราชบัญญัติจัดให้มีการรักษาข้อมูลคอมพิวเตอร์จากการเข้าถึงหรือแก้ไขโดยมิได้รับอนุญาตและเพื่อวัตถุประสงค์อื่นที่เกี่ยวข้อง (An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes) เป็นกฎหมายของสหราชอาณาจักร ซึ่งได้ประกาศใช้เมื่อวันที่ 29 สิงหาคม 2533 จากความล้มเหลวในการฟ้องร้องที่ไม่สามารถเอาผิดโดยเฉพาะเจาะจงกับการแฮกเข้าไปในคอมพิวเตอร์ของบริษัท บริติช เทเลคอม (British Telecom) โดยสภาขุนนางแห่งอังกฤษ (House of Lords) ได้วางหลักว่ากฎหมายที่มีอยู่ในขณะนั้นไม่ได้ระบุให้เอาผิดกับการกระทำลักษณะดังกล่าวได้[47] อันทำให้เกิดอาชญากรรมทางคอมพิวเตอร์ที่สร้างความเสียหายให้แก่ประเทศเป็นจำนวนมาก[48] จนเป็นที่มาของการบัญญัติกฎหมายฉบับนี้ขึ้นจากร่างกฎหมายของสมาชิกส่วนตัว (Private member's bill) ของสภานิติบัญญัติ ที่เสนอโดย ไมเคิล โคลวิน (Michael Colvin)[49] เพื่อดำเนินการกับการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ เช่น การแฮก (Hacking) การเข้าถึงระบบคอมพิวเตอร์ในระบบแลน (Lan) หรือในเครือข่าย (Networks) โดยการใช้โปรแกรมมัลแวร์ (Malware)

---

[47] R v Gold & Schifreen (1988)

[48] Hansard, "Computer Misuse Bill" [Online], Accessed: 16 October 2020. Available from: https://api.parliament.uk/historic-hansard/commons/1990/feb/09/computer-misuse-bill.

[49] Ibid.

พระราชบัญญัติฉบับนี้มีบทบัญญัติที่เกี่ยวข้องต่อการศึกษาวิจัยในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ดังต่อไปนี้

4.2.1.1 การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต

การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Unauthorised access to computer material) อยู่ในมาตรา 1 ซึ่งบัญญัติว่า

มาตรา 1 บัญญัติว่า “(1) บุคคล (A person) จะมีความผิดหาก (a) ทำให้เครื่องคอมพิวเตอร์กระทำการใดๆ (Perform any function) ด้วยเจตนาเพื่อจะได้รับการเข้าถึง (Access) โปรแกรม (Program) หรือข้อมูล (Data) ใดๆ ที่อยู่ในเครื่องคอมพิวเตอร์ (b) โดยไม่ได้รับอนุญาต (c) และในขณะนั้นเขารู้ว่าการทำเช่นนั้นจะเป็นเหตุให้เครื่องคอมพิวเตอร์กระทำการดังกล่าว”

ลักษณะของการกระทำความผิดที่เกี่ยวข้องกับการดึงข้อมูลจากบัตร ก็คือการทำให้เครื่องคอมพิวเตอร์กระทำการใดๆ (Causes a computer to perform any function) โดยไม่ได้รับอนุญาต ซึ่งมาตรา 17(2)(b) บัญญัติให้รวมถึง “การคัดลอก (Copies) หรือเคลื่อนย้าย (moves) ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ไปยังที่อื่นภายในเครื่องคอมพิวเตอร์หรือจากเครื่องคอมพิวเตอร์ไปยังอุปกรณ์ในการจัดเก็บข้อมูล (Storage medium) ใดๆ ก็ตาม” ด้วย อีกทั้งยังถือว่าผู้กระทำได้มีเจตนาเพื่อจะได้รับการเข้าถึงข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์แล้ว นอกจากนี้มาตรา 17(6) ยังบัญญัติให้ “ข้อมูลที่อยู่ในอุปกรณ์ในการจัดเก็บข้อมูล (Storage medium) ในขณะเวลาที่อุปกรณ์นั้นได้เชื่อมต่อและรับรู้โดยเครื่องคอมพิวเตอร์แล้ว” เป็นข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ตามมาตรานี้อีกด้วย ดังนั้นจึงสามารถแบ่งลักษณะของการกระทำความผิดตามมาตรานี้ได้ออกเป็น 2 กรณีคือ

(ก) การคัดลอกหรือเคลื่อนย้าย ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ไปยังที่อื่นภายในเครื่องคอมพิวเตอร์หรือจากเครื่องคอมพิวเตอร์ไปยังอุปกรณ์ในการจัดเก็บข้อมูล

กรณีแรก เป็นกรณีที่ใช้กับบัตรที่ผู้ออกมิได้ออกตัวบัตรให้แก่ผู้มีสิทธิใช้ เช่น ผู้ออกได้ออกให้เพียงรหัสบัตร ตัวเลข หมายเลขบัญชี ซึ่งข้อมูลบัตรเหล่านี้จะต้องถูกจัดเก็บอยู่เครื่องคอมพิวเตอร์ของผู้ออกให้หรือในขณะที่ผู้มีสิทธิใช้ได้กรอกลงไปในเครื่องคอมพิวเตอร์ ดังนั้นข้อมูลบัตรดังกล่าวจะถูกดึงได้ก็เพียงแต่วิธีการคัดลอกหรือเคลื่อนย้ายข้อมูลจากเครื่องคอมพิวเตอร์นั้นไปยังเครื่องคอมพิวเตอร์เครื่องอื่นหรือได้บันทึกข้อมูลนั้นลงในอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลอื่น เช่น การคัดลอกข้อมูลลงในแฟลชไดร์ฟ (Flash Drive) หรือแผ่นซีดี (CD Rom)

(ข) การคัดลอก หรือเคลื่อนย้าย ข้อมูลที่อยู่ในอุปกรณ์ในการจัดเก็บข้อมูล ในขณะเวลาที่อุปกรณ์นั้นได้เชื่อมต่อและรับรู้โดยเครื่องคอมพิวเตอร์แล้ว

กรณีที่สอง เป็นกรณีที่ใช้กับบัตรที่มีการออกเป็นตัวบัตรที่เป็นเอกสารหรือวัตถุอื่นใดให้ แม้พระราชบัญญัติฉบับนี้จะไม่ได้ให้คำนิยามของคำว่าอุปกรณ์ในการจัดเก็บข้อมูล (Storage medium) ไว้ แต่โดยทั่วไปแล้วย่อมหมายถึงอุปกรณ์ที่ใช้ในการเก็บหรือรับข้อมูลอิเล็กทรอนิกส์ ซึ่งมีหลายประเภท เริ่มตั้งแต่ เทปเจาะรู (Paper tape) ฟลอปปีดิสก์ หรือ ดิสเกตต์ (Floppy disk or diskette) ที่ใช้เทคโนโลยีแถบแม่เหล็ก (Magnetic) ไปจนถึงการใช้ชิป (Chip) เป็นต้น[50] ดังนั้นบัตรที่มีการออกเอกสารหรือวัตถุอื่นใดให้ตามสภาพของบัตรซึ่งได้บรรจุข้อมูลอยู่ในแหล่งบันทึกในบัตรที่เป็นแผ่นแม่เหล็กหรือชิป โดยทั่วไปจึงถือว่าเป็นอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลประเภทหนึ่งด้วย แต่จะเป็นการกระทำความผิดตามมาตรานี้ได้ก็ต่อเมื่อได้กระทำการคัดลอกหรือเคลื่อนย้ายข้อมูลในบัตรในขณะที่บัตรใบนั้นได้เชื่อมต่อและรับรู้ (Regarded) โดยคอมพิวเตอร์แล้ว เช่น การใช้เครื่องสกิมเมอร์คัดลอกข้อมูลในบัตรเอทีเอ็มในขณะที่บัตรเอทีเอ็มนั้นได้เสียบใช้งานอยู่ภายในเครื่องจ่ายเงินอัตโนมัติซึ่งได้อ่านและประมวลผลข้อมูลของบัตรใบนั้นอยู่อันเป็นการรับรู้โดยเครื่องคอมพิวเตอร์แล้ว ซึ่งหากบัตรใบนั้นมิได้เชื่อมต่อและรับรู้โดยเครื่องคอมพิวเตอร์แล้วเกิดการดึงข้อมูลจากบัตรใบนั้นขึ้น แม้บัตรจะเป็นอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลก็ตาม แต่ก็ไม่ใช่การทำให้เครื่องคอมพิวเตอร์กระทำการใดๆ อันเป็นการกระทำความผิดตามมาตรานี้

การกระทำความผิดตามมาตรานี้ผู้กระทำต้องมีเจตนา “เพื่อจะได้รับการเข้าถึงข้อมูลใดๆ ที่อยู่ในเครื่องคอมพิวเตอร์” ด้วย โดยไม่จำเป็นต้องเฉพาะเจาะจงว่าจะเข้าถึงข้อมูลใดประเภทใดหรืออยู่ในเครื่องคอมพิวเตอร์เครื่องใด[51] เพียงแต่ผู้กระทำรู้ว่าการนั้นจะเป็นการเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์ก็เพียงพอแล้ว เช่นในกรณีการใช้เครื่องสกิมเมอร์ดึงข้อมูลในบัตร ผู้กระทำไม่จำต้องรู้ว่าข้อมูลนั้นประกอบด้วยข้อมูลอะไรบ้าง จะบันทึกในแถบแม่เหล็กหรือในชิปของบัตร หรือจะมีบัตรใบไหนบ้างที่มาใช้งานกับเครื่องจ่ายเงินอัตโนมัติที่ตนได้ติดตั้งเครื่องสกิมเมอร์ไว้

ดังนั้นบทบัญญัติตามมาตรา 1 นี้จึงเอาผิดกับการกระทำการดึงข้อมูลบัตรที่มีเครื่องคอมพิวเตอร์เข้ามาเกี่ยวข้องด้วยเท่านั้น ไม่ว่าจะเป็นข้อมูลบัตรที่อยู่ในเครื่องคอมพิวเตอร์โดยสภาพหรือที่อยู่ในตัวบัตรในขณะที่บัตรนั้นได้เชื่อมและรับรู้โดยเครื่องคอมพิวเตอร์แล้ว ซึ่งหากเป็นการดึงข้อมูลที่ไม่มีเครื่องคอมพิวเตอร์มาเกี่ยวข้องด้วยก็มิอาจใช้มาตรานี้ในการลงโทษผู้กระทำได้ ดังนั้นพระราชบัญญัติฉบับนี้จึงได้บัญญัติมาตรา 3A ขึ้นอีกเพื่อให้ครอบคลุมถึงการกระทำความผิดทั้งหมดดังจะกล่าวต่อไป

---

[50] Margaret Rouse, "Storage Medium (Storage Media)" [Online], Accessed: 16 October 2020. Available from: https://searchstorage.techtarget.com/definition/storage-medium.

[51] Section 1(2) of Computer Misuse Act 1990

4.2.1.2 การทำ จัดหาหรือได้รับสิ่งของเพื่อใช้ในการกระทำความผิดทางคอมพิวเตอร์

การทำ จัดหาหรือได้รับสิ่งของเพื่อใช้ในการกระทำความผิดทางคอมพิวเตอร์ (Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA) อยู่ในมาตรา 3A แต่เฉพาะที่เกี่ยวข้องกับการดึงข้อมูลบัตรนั้นบัญญัติอยู่ในอนุมาตรา 3 ที่บัญญัติขึ้นมาโดยเฉพาะเพื่อรับมือกับอาชญากรรมที่เป็นการโจมตีระบบข้อมูล (Attacks against information systems) ตามคำสั่งของรัฐสภาและสภายุโรป (THE EUROPEAN PARLIAMENT AND OF THE COUNCIL)[52] ซึ่งบัญญัติว่า

มาตรา 3A(3) บัญญัติว่า “บุคคล (A person) จะมีความผิดหากเขาได้รับ (Obtains) สิ่งของ (Article) ใดๆ (a) โดยเจตนา หรือ (b) เล็งเห็นว่าเป็นการทำเพื่อใช้หรือช่วยเหลือในการกระทำความผิดที่กำหนดไว้ในมาตรา 1 มาตรา 3 หรือมาตรา 3ZA”

โดยคำว่า สิ่งของ (Article) นั้นอนุมาตรา 4[53] ให้คำนิยามว่ารวมถึง “ข้อมูล (Data) หรือโปรแกรมใดๆ ก็ตามที่อยู่ในรูปแบบอิเล็กทรอนิกส์ (Electronic Form)” ซึ่งในบันทึกคำอธิบาย (Explanatory Notes) ของพระราชบัญญัติอาชญากรรมร้ายแรง ค.ศ. 2015 (Serious Crime Act 2015) อันเป็นกฎหมายที่กำหนดให้มีการบัญญัติอนุมาตรา 3 นี้เพิ่มเติม ได้ยกตัวอย่างข้อมูลในรูปแบบอิเล็กทรอนิกส์ไว้ เช่น รหัสผ่านคอมพิวเตอร์ รหัสการเข้าถึง (access code) หรือข้อมูลในรูปแบบที่คล้ายกันอันมีไว้เพื่อใช้ในการเข้าถึงเครื่องคอมพิวเตอร์[54]

มาตรานี้เป็นบทบัญญัติที่บัญญัติขึ้นมาเฉพาะเพื่อใช้กับการกระทำความผิดแก่การได้รับ (Obtains) ข้อมูลใดๆ ก็ตามที่อยู่ในรูปแบบอิเล็กทรอนิกส์ ซึ่งข้อมูลของบัตรที่มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ที่อยู่ในคอมพิวเตอร์หรือข้อมูลของบัตรที่ได้มีการออกเอกสารหรือวัตถุอื่นใดให้ที่ได้บันทึกไว้ในแหล่งบันทึกข้อมูลของบัตร เช่น ในแถบแม่เหล็กหรือในชิปของบัตรใบนั้น ก็ย่อมเป็นข้อมูลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ทั้งสิ้นและย่อมที่จะได้รับความคุ้มครองตามมาตรานี้หากไม่สามารถใช้มาตรา 1 ดังที่กล่าวมาแล้วในการลงโทษผู้กระทำได้ เช่น ในกรณีที่ผู้กระทำได้ใช้เครื่อง

---

[52] Official Journal of the European Union, "Directive 2013/40/Eu of the European Parliament and of the Council" [Online], Accessed: 16 October 2020. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF.

[53] Subsection 4 of section 3A of Computer Misuse Act 1990

[54] Legislation.gov.uk, "Serious Crime Act 2015 Explanatory Notes" [Online], Accessed: 16 October 2020. Available from: from: https://www.legislation.gov.uk/ukpga/2015/9/notes/division/3/2/2/2.

สกิมเมอร์แบบพกพก (Handheld Skimmer) ในการดึงข้อมูลบัตรซึ่งโดยสภาพบัตรนั้นไม่ได้เชื่อมต่อกับเครื่องคอมพิวเตอร์ในขณะนั้น จึงไม่อาจปรับใช้มาตรา 1 แก่การกระทำดังกล่าวได้ แต่ข้อมูลในบัตรที่อยู่ในรูปแบบอิเล็กทรอนิกส์ก็ยังเป็นสิ่งของ (Article) ซึ่งการที่ผู้กระทำได้รับ (Obtains) ข้อมูลจากการดึงนั้นย่อมเป็นความผิดตามมาตรานี้ อันเป็นการบัญญัติกฎหมายขึ้นเพื่อให้ครอบคลุมการกระทำความผิดในเรื่องการดึงข้อมูลจากบัตรทั้งหมด

การกระทำความผิดตามมาตรานี้ผู้กระทำต้องมีเจตนาหรือเล็งเห็นว่าเป็นการทำเพื่อจะใช้หรือช่วยเหลือในการกระทำความผิดที่กำหนดไว้ในมาตรา 1 มาตรา 3 หรือมาตรา 3ZA อันหมายความว่าจะนำข้อมูลที่ได้มานั้นไปกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ต่อไปจึงจะเป็นความผิดตามมาตรานี้ได้ เช่น จะนำข้อมูลนั้นไปใช้ในการเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาตตามมาตรา 1 หรือจะนำไปใช้ในการทำให้เครื่องคอมพิวเตอร์เสียหายโดยไม่ได้รับอนุญาตตามมาตรา 3 หรือจะนำไปใช้ในการทำความเสียหายร้ายแรงอันเกี่ยวกับคอมพิวเตอร์โดยไม่ได้รับอนุญาตตามมาตรา 3ZA และเป็นสิ่งที่จำเป็นอย่างยิ่งที่โจทก์จะต้องมีการพิสูจน์ในชั้นศาล มิใช่เป็นเพียงการกระทำการดึงข้อมูลแต่เพียงอย่างเดียว[55]

การกระทำความผิดไม่ว่าจะเป็นการเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาตที่บัญญัติไว้ใน มาตรา 1 หรือการได้รับสิ่งของเพื่อใช้ในการกระทำความผิดทางคอมพิวเตอร์ ในมาตรา 3A(3) ก็ต่างมีอัตราโทษที่เท่ากันคือ หากเป็นคดีอาญาสามัญ (Summary Offences) จะมีอัตราโทษจำคุกไม่เกิน 12 เดือนหรือปรับ[56] ไม่เกิน 5,000 ปอนด์สเตอร์ลิง[57] หรือทั้งจำทั้งปรับ แต่หากเป็นคดีอาญาอุกฉกรรจ์ (Indictable Offences) จะมีอัตราโทษจำคุกไม่เกิน 2 ปีหรือปรับ (ไม่มีจำนวนจำกัด) หรือทั้งจำทั้งปรับ

4.2.2 พระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006 (The Fraud Act 2006)

พระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006 (The Fraud Act 2006) หรือในชื่อเต็มคือ พระราชบัญญัติจัดให้มีและเกี่ยวข้องกับความรับผิดทางอาญาจากการฉ้อโกงและการได้รับการบริการโดยมิชอบ (An Act to make provision for, and in connection with, criminal liability for

---

[55] The Crown Prosecution Service, "Computer Misuse Act" [Online], Accessed: 16 October 2020. Available from: https://www.cps.gov.uk/legal-guidance/computer-misuse-act.

[56] Legislation.gov.uk, "Criminal Justice Act 1982" [Online], Accessed: 15 October 2020. Available from: https://www.legislation.gov.uk/ukpga/1982/48/section/37.

[57] ประมาณ 202,832 บาท (อัตราแลกเปลี่ยน ณ วันที่ 15 ตุลาคม 2563)

fraud and obtaining services dishonestly) เป็นกฎหมายของสหราชอาณาจักร ซึ่งได้ประกาศใช้เมื่อวันที่ 15 มกราคม 2550 จากรายงานของคณะกรรมาธิการกฎหมาย (The Law Commission) เรื่องการปฏิรูปกฎหมายฉ้อโกงในเดือนพฤษภาคม 2547 ที่ให้มีการบัญญัติกฎหมายเพื่อใช้รับมืออาชญากรรมการฉ้อโกง[58] ซึ่งเป็นพระราชบัญญัติที่กำหนดความผิดทั่วไปเกี่ยวกับการฉ้อโกง เช่น การฉ้อโกงโดยการแสดงเท็จ การฉ้อโกงโดยการไม่เปิดเผยข้อมูล หรือการฉ้อโกงโดยการใช้ตำแหน่งในทางที่ผิด ทั้งได้บัญญัติความผิดขึ้นใหม่อันเป็นการเฉพาะเกี่ยวกับการได้มา (Obtain) ซึ่งทรัพย์สินโดยการหลอกลวง การได้มาซึ่งความได้เปรียบทางการเงินและความผิดอื่นๆ เพื่อใช้แทนพระราชบัญญัติโจรกรรม ค.ศ. 1978 (Theft Act 1978) ที่เป็นที่วิจารณ์อย่างมากถึงความซับซ้อนและความยากลำบากในการพิสูจน์ต่อศาล[59] และพระราชบัญญัติฉบับนี้ยังเป็นหนึ่งในสามพระราชบัญญัติของสหราชอาณาจักร[60] ในการลงโทษแก่การกระทำความผิดในลักษณะการโจรกรรมเอกลักษณ์บุคคล[61] (Identity Theft) ที่เกิดขึ้นมากจากการพัฒนาทางเทคโนโลยีในการเข้าถึงข้อมูลต่างๆ อันทำให้ข้อมูลส่วนบุคคลนั้นถูกอาชญากรนำไปใช้โดยปราศจากความยินยอมจากเจ้าของข้อมูลดังกล่าวเพื่อไปแสวงหาประโยชน์อื่นๆ ต่อไป เช่น การนำข้อมูลส่วนบุคคลนั้นไปเปิดบัญชีหรือใช้สั่งสินค้าออนไลน์[62] รวมถึงอาชญากรรมการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ด้วย[63]

ในส่วนของเรื่องการดึงข้อมูลจากบัตรนั้น พระราชบัญญัติฉบับนี้ส่วนใหญ่จะใช้บังคับการฉ้อโกงที่เกิดขึ้นภายหลังจากที่ผู้กระทำความผิดได้รับข้อมูลจากบัตรมาแล้ว และนำข้อมูลที่ได้มานั้นไป

---

[58] legislation.gov.uk, "Fraud Act 2006 Background" [Online], Accessed: 15 October 2020. Available from: https://www.legislation.gov.uk/ukpga/2006/35/notes/division/3.

[59] Wikipedia, "Fraud Act 2006" [Online], Accessed: 15 October 2020. Available from: https://en.wikipedia.org/wiki/Fraud_Act_2006.

[60] นอกจากพระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006 (The Fraud Act 2006) แล้ว สหราชอาณาจักรยังมีพระราชบัญญัติเอกสารประจำตัวบุคคล ค.ศ. 2010 (The Identity Documents Act 2010) และพระราชบัญญัติการปลอมและแปลง ค.ศ. 1981 (The Forgery and Counterfeiting Act 1981) ในการเอาผิดกับการโจรกรรมเอกลักษณ์บุคคลด้วย

[61] David S. Wall, “Future Identities: Changing identities in the UK – the next 10 years” [Online], Accessed: 15 October 2020. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/275784/13-521-identity-related-crime-uk.pdf.

[62] คณะนิติศาสตร์ มหาลัยสงขลานครินทร์, "การโจรกรรมเอกลักษณ์บุคคล (Identity Theft)" [ออนไลน์], เข้าถึงเมื่อ 15 ตุลาคม 2563. แหล่งที่มา: https://www.bangkokbiznews.com/blog/detail/646271.

[63] Julia Kagan, "Skimming" [Online], Accessed: 15 October 2020. Available from: https://www.investopedia.com/terms/s/skimming.asp.

ฉ้อโกงโดยการทำให้เข้าใจผิด (Misleading)[64] แก่บุคคลอื่นหรือเครื่องมืออัตโนมัติใดๆ[65] เช่น เครื่องจ่ายเงินอัตโนมัติ ตัวอย่างเช่น การนำข้อมูลที่ได้มาไปทำบัตรปลอมหรือนำไปใช้แสวงหาประโยชน์ใดๆ โดยการแสดงเท็จว่าตนเป็นเจ้าของข้อมูลบัตรนั้นโดยเจตนาให้ได้รับ (Gain) เงินหรือทรัพย์สิน ย่อมเป็นการฉ้อโกงโดยการแสดงเท็จซึ่งเป็นความผิดตามพระราชบัญญัตินี้[66] การดึงข้อมูลจากบัตรแม้ว่าจะไม่ใช่รูปแบบในการกระทำความผิดที่เป็นการฉ้อโกงดังที่พระราชบัญญัติฉบับนี้ได้กำหนดไว้ แต่ก็นับว่าเป็นกระบวนการเริ่มต้นที่สำคัญในการพัฒนาไปสู่การกระทำความผิดในเรื่องฉ้อโกง พระราชบัญญัติฉบับนี้จึงกำหนดให้มีการกระทำผิดต่อการครอบครองสิ่งของเพื่อใช้ในการฉ้อโกง อยู่ในมาตรา 6 ซึ่งเกี่ยวข้องต่อการศึกษาวิจัยในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ อันบัญญัติไว้ดังนี้

มาตรา 6 บัญญัติว่า “บุคคล (A person) จะมีความผิดหากมีสิ่งของ (Article) ใดๆ ไว้ในครอบครอง (Possession) หรือควบคุม (Control) เพื่อใช้ในการดำเนินการหรือเกี่ยวข้องในการฉ้อโกงใดๆ”

โดยคำว่า สิ่งของ (Article) นั้น มาตรา 8 ให้คำนิยามว่ารวมถึง “ข้อมูล (Data) หรือโปรแกรมใดๆ ก็ตามที่อยู่ในรูปแบบอิเล็กทรอนิกส์ (Electronic Form)” ซึ่งในบันทึกคำอธิบาย (Explanatory Notes) ของพระราชบัญญัติฉบับนี้ ได้ยกตัวอย่างเช่น คดีที่ใช้ข้อมูลบัตรเครดิตของบุคคลอื่นที่อยู่ในไฟล์ (Files) ในเครื่องคอมพิวเตอร์เป็นเครื่องมือในการฉ้อโกง[67]

มาตรานี้เป็นเรื่องการครอบครองหรือควบคุมสิ่งของโดยที่จะนำไปใช้หรือเป็นสิ่งของที่เกี่ยวข้องในการจะนำไปใช้ในการฉ้อโกงใดๆ ต่อไปให้เป็นความผิด โดยเป็นการร่างกฎหมายโดยอาศัยคำจากพระราชบัญญัติโจรกรรม ค.ศ. 1968 (Theft Act 1968) ซึ่งเอาผิดบุคคลที่พร้อม (Go equipped) จะกระทำความผิดในการลักทรัพย์ การครอบครองหรือควบคุมสิ่งของดังกล่าวก็เสมือนการพร้อมที่จะกระทำความผิดต่อไปนั่นเอง จึงได้บัญญัติให้การกระทำดังกล่าวเป็นความผิดด้วยแม้

---

[64] มาตรา 2 อนุมาตรา 2(a) ใน The Fraud Act 2006

[65] Legislation.gov.uk, "Fraud Act 2006 Explanatory Notes" [Online], Accessed: 15 October 2020. Available from: https://www.legislation.gov.uk/ukpga/2006/35/notes/division/5/2.

[66] มาตรา 2 ของ The Fraud Act 2006

[67] Legislation.gov.uk, "Fraud Act 2006 Explanatory Notes" [Online], Accessed: 15 October 2020. Available from: https://www.legislation.gov.uk/ukpga/2006/35/notes/division/5/8.

การกระทำดังกล่าวจะไม่ใช่การฉ้อโกงก็ตาม[68] อย่างไรก็ตามพระราชบัญญัติฉบับนี้มิได้ให้คำนิยามว่าครอบครองหรือควบคุมไว้ แต่มีความเห็นคำว่าครอบครองนั้นไม่จำเป็นต้องเคร่งครัดว่าต้องเป็นการครอบครองโดยกายภาพเท่านั้น[69] ยังรวมการครอบครองซอฟแวร์ (Software) หรือวัตถุที่ (Material) ที่ไม่มีรูปร่างที่อยู่ในแหล่งบันทึกข้อมูลคอมพิวเตอร์ด้วยและแม้ว่าข้อมูลนั้นจะถูกลบไปแล้วก็ตามก็ยังเป็นการครอบครองอยู่[70]

การกระทำความผิดตามมาตรานี้สามารถนำมาใช้กับการกระทำความผิดในลักษณะการดึงข้อมูลออกมาจากบัตรได้ ไม่ว่าจะเป็นข้อมูลที่อยู่ภายในแหล่งบันทึกของบัตรหรือบนบัตรในลักษณะที่พิมพ์ออกมาจากคอมพิวเตอร์ (Hard Copy) ซึ่งเป็นบัตรที่มีการออกเอกสารหรือวัตถุอื่นใดให้ หรือเป็นข้อมูลบัตรที่มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ก็ตาม ข้อมูลบัตรเหล่านี้ก็ล้วนเป็นข้อมูลอิเล็กทรอนิกส์ ในความหมายของการเป็นสิ่งของ (Article) ที่เป็นวัตถุแห่งการกระทำความผิดตามมาตรานี้ ซึ่ง ณ เวลาที่ผู้กระทำความผิดประสบความสำเร็จในการได้รับ (Obtaining) ข้อมูลบัตรนั้นจากการกระทำการดึงข้อมูลจากบัตรด้วยวิธีการต่างๆ แล้ว ก็ถือว่า ณ เวลานั้นผู้กระทำได้มีสิ่งของใดๆ ไว้ในการครอบครองหรือควบคุมซึ่งเป็นความผิดตามมาตรานี้ทันที[71]

อย่างไรก็ตามการกระทำความผิดตามมาตรานี้ ผู้กระทำจะต้องครอบครองหรือควบคุมข้อมูลนั้นโดยมีเจตนาเพื่อจะใช้ในการดำเนินการหรือเกี่ยวข้องในการฉ้อโกงใดๆ ต่อไปในอนาคตด้วย ซึ่งไม่จำต้องพิสูจน์โดยเฉพาะเจาะจงว่าผู้กระทำนั้นจะไปใช้ในการฉ้อโกงแบบใด เพียงแต่พิสูจน์ว่ามีเจตนาที่จะนำไปฉ้อโกงต่อไปก็เพียงพอแล้ว[72]

---

[68] Legislation.gov.uk, "Fraud Act 2006 Explanatory Notes" [Online], Accessed: 15 October 2020. Available from: https://www.legislation.gov.uk/ukpga/2006/35/notes/division/5/6..

[69] The Crown Prosecution Service, "The Fraud Act 2006" [Online], Accessed: 15 October 2020. Available from: https://www.cps.gov.uk/legal-guidance/fraud-act-2006.

[70] R v ROSS WARWICK PORTER (2006)

[71] The Crown Prosecution Service, “The Fraud Act 2006” [Online], Accessed: 15 October 2020. Available from: https://www.cps.gov.uk/legal-guidance/fraud-act-2006.

[72] Legislation.gov.uk, “Fraud Act 2006 Explanatory Notes” [Online], Accessed: 15 October 2020. Available from: https://www.legislation.gov.uk/ukpga/2006/35/notes/division/5/6.

การกระทำความผิดตามมาตรานี้หากเป็นคดีอาญาสามัญ (Summary Offences) จะมีอัตราโทษจำคุกไม่เกิน 12 เดือนหรือปรับ[73] ไม่เกิน 5,000 ปอนด์สเตอร์ลิง[74] หรือทั้งจำทั้งปรับ แต่หากเป็นคดีอาญาอุกฉกรรจ์ (Indictable Offences) จะมีอัตราโทษจำคุกไม่เกิน 5 ปีหรือปรับ (ไม่มีจำนวนจำกัด) หรือทั้งจำทั้งปรับ

4.2.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018 (Data Protection Act 2018)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018 (Data Protection Act 2018) หรือในชื่อเต็มคือพระราชบัญญัติจัดระเบียบปฏิบัติในการประมวลผลข้อมูลที่เกี่ยวข้องกับบุคคล จัดความเกี่ยวพันในการทำหน้าที่ของกรรมาธิการข้อมูลภายใต้ระเบียบปฏิบัติที่เกี่ยวกับข้อมูล จัดข้อกำหนดในทางปฏิบัติสำหรับการตลาดทางตรงและเพื่อวัตถุประสงค์อื่นที่เกี่ยวข้อง (An Act to make provision for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner's functions under certain regulations relating to information; to make provision for a direct marketing code of practice; and for connected purposes) เป็นกฎหมายของสหราชอาณาจักร ซึ่งได้ประกาศใช้เมื่อวันที่ 25 พฤษภาคม 2561 จากคำสั่งการคุ้มครองข้อมูลของสหภาพยุโรป ค.ศ. 1995 (EU Data Protection Directive 1995) ที่ให้ประเทศสมาชิกมีบทบัญญัติที่เกี่ยวข้องในการป้องกันข้อมูลทั้งในการประมวลผลและการเคลื่อนย้ายข้อมูลต่างๆ จึงทำให้สหราชอาณาจักรจำต้องปรับปรุงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1984 (Data Protection Act 1984) ที่มีอยู่เดิมให้สอดคล้องกับสหภาพยุโรป[75] และต่อมาได้นำกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation : GDPR) มาเป็นต้นแบบในการพัฒนาพระราชบัญญัติฉบับนี้ เพื่อให้สหราชอาณาจักรมีกฎหมายไปในแนวทางเดียวกับประเทศอื่นๆ ในยุโรป ณ เวลาที่ตนเอง

[73] Legislation.gov.uk, "Criminal Justice Act 1982" [Online], Accessed: 15 October 2020. Available from: https://www.legislation.gov.uk/ukpga/1982/48/section/37.

[74] ประมาณ 202,832 บาท (อัตราแลกเปลี่ยน ณ วันที่ 15 ตุลาคม 2563)

[75] Legislation.gov.uk, "Data Protection Act 2018 Legal Background" [Online], Accessed: 17 October 2020. Available from: https://www.legislation.gov.uk/ukpga/2018/12/notes/division/4/index.htm.

ออกจากสหภาพยุโรปแล้ว[76] ซึ่งพระราชบัญญัติฉบับนี้ได้บัญญัติขึ้นเพื่อสร้างมาตรฐานใหม่ในการปกป้องข้อมูลส่วนบุคคล[77] ทำให้ประชาชนสามารถควบคุมการใช้ข้อมูลของตนจากการละเมิดขององค์กรภาครัฐและภาคเอกชนต่างๆ ซึ่งถือว่าเป็นสิทธิขั้นพื้นฐานได้มากขึ้น และเพื่อส่งเสริมการคุ้มครองข้อมูลส่วนบุคคลของภาคธุรกิจให้เทียบเท่ากับมาตรฐานสากล[78]

พระราชบัญญัติฉบับนี้มีบทบัญญัติที่เกี่ยวข้องต่อการศึกษาวิจัยในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ อยู่ในมาตรา 170 อันเป็นการได้รับข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย ซึ่งเป็นบทบัญญัติที่พัฒนามาจากมาตรา 55 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998 (Data Protection Act 1998) เพื่อให้มีความสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR)[79] ซึ่งบัญญัติไว้ดังนี้

มาตรา 170 บัญญัติว่า “(1) มันเป็นการกระทำความผิดสำหรับบุคคล (A person) โดยเจตนาหรือประมาท (a) แก่การได้รับ (Obtain) หรือเปิดเผย (Disclose) ข้อมูลส่วนบุคคล (Personal data) โดยมิได้รับความยินยอมจากผู้ควบคุม (Controller)”

คำว่า ผู้ควบคุม (Controller) นั้นมาตรา 32 ให้คำนิยามว่าหมายถึง หน่วยงานที่มีอำนาจซึ่งโดยลำพังหรือร่วมกับหน่วยงานอื่นในการกำหนดเป้าหมายและวิธีในการประมวลผล (Processing) ข้อมูลส่วนบุคคล ส่วนในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) ให้คำนิยามไว้ว่าหมายถึง บุคคลธรรมดาหรือตามกฎหมาย หน่วยงานสาธารณะ หน่วยงานอื่นๆ โดยลำพังหรือร่วมกับผู้อื่น ซึ่งได้กำหนดเป้าหมายและวิธีในการประมวลผลข้อมูลส่วนบุคคล หรือในกรณีที่เป้าหมายและวิธีนั้นถูกกำหนดโดยสหภาพ (Union) หรือประเทศสมาชิก (Member State) ผู้ควบคุมคือผู้ที่ถูกกำหนดโดยกฎหมายของสหภาพหรือประเทศสมาชิกนั้น[80] ดังนั้นจึงหมายถึง หน่วยงานต่างๆ ทุก

---

[76] Robin Hopkins, "The Data Protection Bill: A Brief Overview What Does the Data Protection Bill Do?" [Online], Accessed: 17 October 2020. Available from: https://uk.practicallaw.thomsonreuters.com/w-010-5346?transitionType=Default&contextData=(sc.Default)&firstPage=true.

[77] Legislation.gov.uk, "Data Protection Act 2018 Overview of the Act" [Online], Accessed: 17 October 2020. Available from: https://www.legislation.gov.uk/ukpga/2018/12/notes/division/2/index.htm.

[78] กรุงเทพธุรกิจออนไลน์, "'ข้อมูลส่วนบุคคล' สำคัญแค่ไหน ตามกฎหมาย GDPR ยุโรป" [ออนไลน์]. แหล่งที่มา: https://www.bangkokbiznews.com/news/detail/882376.

[79] อย่างไรก็ตาม บทบัญญัติตามพระราชบัญญัติฉบับใหม่นี้ก็เป็นเพียงการเพิ่มเติมโดยเล็กน้อยเท่านั้น คือ การเพิ่มคำว่า ผู้ควบคุม (Controller) และเพิ่มความผิดใหม่บางลักษณะในมาตรา 170 ดังกล่าว เพื่อรับมือกับอาชญากรรมในปัจจุบัน เช่น การดึงข้อมูลไปแล้วยังเก็บรักษาข้อมูลนั้นไว้โดยไม่ได้รับความยอนยอมจากผู้ควบคุม ตามมาตรา 170(1)(c)

[80] Article 4(7) of General Data Protection Regulation

หน่วยงาน ไม่ว่าภาครัฐ ภาคเอกชน หรือภาคธุรกิจที่มีการดำเนินการเกี่ยวกับการเก็บข้อมูลส่วนบุคคล หรือการให้บริการออนไลน์แก่บุคคลต่างๆ[81] ในสหราชอาณาจักรย่อมเป็น “ผู้ควบคุม” ในความหมายของมาตรานี้ ตัวอย่างเช่น แพทย์ที่ใช้ระบบอัตโนมัติในการเรียกคิวผู้ป่วยโดยระบบนั้นได้แสดงชื่อและหมายเลขห้องที่ผู้ป่วยจะเข้าทำการรักษา ข้อมูลส่วนบุคคลของลูกค้าที่ฝ่ายบัญชีของบริษัทรวบรวมไว้[82] ข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของธนาคาร[83] ในกรณีเหล่านี้ แพทย์ ฝ่ายบัญชีและธนาคาร คือ ผู้ควบคุม ตามมาตรานี้

ส่วนคำว่า ข้อมูลส่วนบุคคล (Personal data) นั้นมาตรา 3(2) ให้คำนิยามว่าหมายถึง ข้อมูลใดๆ ที่เกี่ยวข้องกับบุคคลที่มีชีวิตที่ระบุตัวตนได้ ส่วนในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) ให้คำนิยามไว้ว่าหมายถึง ข้อมูลใดๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัวตนได้ ทั้งทางตรงหรือทางอ้อม เช่น ชื่อ หมายเลขประจำตัว ตำแหน่งที่อยู่ ข้อมูลที่ระบุทางออนไลน์ ปัจจัยที่เกี่ยวกับสรีระวิทยา ลักษณะทางพันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรมหรือสังคมของบุคคลผู้นั้น[84]

การกระทำความผิดตามมาตรานี้ที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรคือ การได้รับ (Obtain) ข้อมูลส่วนบุคคลโดยมิได้รับความยินยอมที่เป็นคำสั่งหรือการยืนยันที่ชัดเจน[85] จากผู้ควบคุม[86] โดยที่ไม่ได้จำกัดว่าข้อมูลนั้นจะอยู่ในรูปลักษณะใด จึงหมายความว่า ข้อมูลส่วนบุคคลทั้งทางตรงหรือทางอ้อมที่อยู่ในรูปแบบอิเล็กทรอนิกส์หรือไม่ก็ย่อมจะเป็นวัตถุแห่งการกระทำความผิดตามมาตรานี้ทั้งสิ้น

ดังนั้น ข้อมูลในบัตรไม่ว่าจะมีการออกเอกสารหรือวัตถุอื่นใดให้หรือไม่ และไม่ว่าจะได้บันทึกอยู่ในเครื่องคอมพิวเตอร์ ในแหล่งบันทึกของบัตร หรือบนพื้นผิวของบัตรใบนั้น ย่อมมีลักษณะเป็น

---

[81] กรุงเทพธุรกิจออนไลน์, “'ข้อมูลส่วนบุคคล' สำคัญแค่ไหน ตามกฎหมาย GDPR ยุโรป” [ออนไลน์], เข้าถึงเมื่อ 17 ตุลาคม 2563. แหล่งที่มา https://www.bangkokbiznews.com/news/detail/882376.

[82] Information Commisoner’s Office, "What Are ‘Controllers’ and ‘Processors’?" [Online], Accessed: 17 October 2020. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/.

[83] Office of the Attorney General, "S.I. No. 537/2019 - Data Protection Act 2018 (Section 60(6)) (Central Bank of Ireland) Regulations 2019" [Online], Accessed: 17 October 2020. Available from: http://www.irishstatutebook.ie/eli/2019/si/537/made/en/print.

[84] Article 4(1) of General Data Protection Regulation

[85] Meaning of ‘consent’ in Article 4(1) of General Data Protection Regulation

[86] ในกรณีที่มีผู้ควบคุมข้อมูลนั้นหลายหน่วยงาน การได้รับความยินยอมเพียงแต่หน่วยงานเดียวก็เพียงพอแล้ว ตามมาตรา 170(7)(b)

ข้อมูลส่วนบุคคลตามมาตรานี้ ซึ่งหากผู้ใดได้กระทำการดึงข้อมูลบัตรที่เป็นข้อมูลส่วนบุคคลเหล่านั้นไปจากหน่วยงานไม่ว่าภาครัฐหรือภาคเอกชนที่ควบคุมดูแลข้อมูลนั้นอยู่ อันเป็นการได้รับข้อมูล (Obtain) ไปโดยมิได้รับความยินยอมจากหน่วยงานซึ่งเป็นผู้ควบคุมนั้น การกระทำการดึงข้อมูลบัตรดังกล่าวย่อมเป็นการกระทำความผิดตามมาตรานี้ ซึ่งนอกจากผู้กระทำจะกระทำโดยมีเจตนาแล้ว มาตรานี้ยังรวมถึงการดึงข้อมูลบัตรจากการกระทำโดยประมาทอีกด้วย

บทลงโทษตามมาตรานี้บัญญัติอยู่ในมาตรา 169(2) ซึ่งหากเป็นคดีอาญาสามัญ (Summary Offences) ในประเทศอังกฤษและเวลส์ จะมีอัตราโทษจำคุกไม่เกิน 12 เดือนหรือปรับ (ไม่มีจำนวนจำกัด) ส่วนในประเทศสกอตแลนด์และไอร์แลนเหนือ จะมีอัตราโทษจำคุกไม่เกิน 12 เดือนหรือปรับ[87] ไม่เกิน 5,000 ปอนด์สเตอร์ลิง[88] แต่หากเป็นคดีอาญาอุกฉกรรจ์ (Indictable Offences) จะมีอัตราโทษจำคุกไม่เกิน 5 ปีหรือปรับ (ไม่มีจำนวนจำกัด)

[87] Legislation.gov.uk, “Criminal Justice Act 1982” [Online], Accessed: 15 October 2020. Available from: https://www.legislation.gov.uk/ukpga/1982/48/section/37.

[88] ประมาณ 202,832 บาท (อัตราแลกเปลี่ยน ณ วันที่ 15 ตุลาคม 2563)

ตารางที่ 9 เปรียบเทียบบทบัญญัติของกฎหมายสหราชอาณาจักรที่เกี่ยวข้องกับการดึงข้อมูลจากบัตร

บทบัญญัติ	การกระทำ	วัตถุแห่งการกระทำ	เจตนา	โทษ	
				Summary Offences	Indictable Offences
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990					
มาตรา 1	ทำให้เครื่องคอมพิวเตอร์กระทำการใดๆ (หมายถึง คัดลอก หรือเคลื่อนย้ายข้อมูล) โดยไม่ได้รับอนุญาต	ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ (รวมถึงข้อมูลที่อยู่ในอุปกรณ์ในการจัดเก็บข้อมูล (Storage medium) ในขณะเวลาที่อุปกรณ์นั้นได้เชื่อมต่อและรับรู้โดยเครื่องคอมพิวเตอร์แล้ว)	เพื่อจะได้รับการเข้าถึง (Access) โปรแกรม (Program) หรือข้อมูล (Data) ใดๆ ที่อยู่ในเครื่องคอมพิวเตอร์	จำคุกไม่เกิน 12 เดือน หรือปรับไม่เกิน 5,000 ปอนด์สเตอร์ลิง หรือทั้งจำทั้งปรับ	จำคุกไม่เกิน 2 ปีหรือปรับหรือทั้งจำทั้งปรับ

บทบัญญัติ	การกระทำ	วัตถุแห่งการกระทำ	เจตนา	โทษ	
				Summary Offences	Indictable Offences
มาตรา 3A(3)	ได้รับ (Obtains)	สิ่งของ (Article) (ข้อมูล หรือโปรแกรมใดๆ ก็ตามที่อยู่ในรูปแบบอิเล็กทรอนิกส์)	เพื่อจะใช้หรือช่วยเหลือในการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ต่อไป	จำคุกไม่เกิน 12 เดือน หรือปรับไม่เกิน 5,000 ปอนด์ สเตอร์ลิง หรือทั้งจำทั้งปรับ	จำคุกไม่เกิน 2 ปีหรือปรับหรือทั้งจำทั้งปรับ
พระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006					
มาตรา 6	มีไว้ในครอบครอง (Possession) หรือควบคุม (Control)	สิ่งของ (Article) (ข้อมูล หรือโปรแกรมใดๆ ก็ตามที่อยู่ในรูปแบบอิเล็กทรอนิกส์)	เพื่อจะใช้ในการดำเนินการหรือเกี่ยวข้องในการฉ้อโกงต่อไป	จำคุกไม่เกิน 12 เดือน หรือปรับไม่เกิน 5,000 ปอนด์ สเตอร์ลิง หรือทั้งจำทั้งปรับ	จำคุกไม่เกิน 5 ปีหรือปรับหรือทั้งจำทั้งปรับ

บทบัญญัติ	การกระทำ	วัตถุแห่งการกระทำ	เจตนา	โทษ	
				Summary Offences	Indictable Offences
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018					
มาตรา 170	ได้รับ (Obtain) โดยมิได้รับความยินยอมจากผู้ควบคุม	ข้อมูลส่วนบุคคล (Personal data)	เจตนาธรรมดา	จำคุกไม่เกิน 12 เดือน หรือปรับไม่เกิน 5,000 ปอนด์สเตอร์ลิง (อังกฤษและเวลส์ ปรับไม่มีจำนวนจำกัด)	จำคุกไม่เกิน 5 ปีหรือปรับ (ไม่มีจำนวนจำกัด)

ดังนั้นในเรื่องการดึงข้อมูลจากบัตรนี้ สามารถใช้พระราชบัญญัติทั้งสามฉบับของสหราชอาณาจักรดังที่กล่าวมาแล้วในการลงโทษผู้กระทำความผิดได้ ขึ้นอยู่กับลักษณะของการกระทำความผิดที่เกิดขึ้น โดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) นั้น มุ่งเอาผิดต่อการดึงข้อมูลบัตรที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์และมีเครื่องคอมพิวเตอร์เข้ามาเกี่ยวข้องในการกระทำความผิด ไม่ว่าจะเพื่อเข้าถึงโปรแกรมหรือข้อมูลใดๆ ในเครื่องคอมพิวเตอร์นั้น หรือจะนำข้อมูลบัตรไปใช้หรือช่วยเหลือในการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ต่อไป ส่วนพระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006 (The Fraud Act 2006) แม้จะเอาผิดต่อการดึงข้อมูลบัตรที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์เหมือนกัน แต่ก็ไม่จำต้องมีเครื่องคอมพิวเตอร์เข้ามาเกี่ยวข้องในการกระทำความผิดด้วย เช่น การดึงข้อมูลบัตรโดยใช้เครื่องสกิมเมอร์แบบพกพา (Handheld Skimmer) แต่อย่างไรก็ดี โจทก์นั้นก็จำต้องพิสูจน์ว่าผู้กระทำมีเจตนาที่จะนำข้อมูลบัตรที่ได้มาไปใช้ในการดำเนินการหรือเกี่ยวข้องในการฉ้อโกงใดๆ ต่อไปในอนาคตด้วย ส่วนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018 (Data Protection Act 2018) นั้นจะเอาผิดกับการดึงข้อมูลในทุกรูปแบบ เพราะถือว่าเป็นข้อมูลที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัวตนได้โดยทางตรงหรือทางอ้อม ดังนั้นไม่ว่าข้อมูลบัตรที่อยู่ใน

รูปแบบข้อมูลอิเล็กทรอนิกส์ เช่น ที่อยู่ในเครื่องคอมพิวเตอร์หรือในแถบแม่เหล็กหรือชิปของบัตรที่มีการออกเอกสารหรือวัตถุอื่นใดให้ หรือที่มิได้อยู่ในรูปแบบอิเล็กทรอนิกส์ เช่นข้อมูลที่พิมพ์อยู่บนผิวบัตร ก็ย่อมได้รับความคุ้มครองตามพระราชบัญญัตินี้ด้วยกันทั้งสิ้น

การกระทำผิดที่มีวัตถุแห่งการกระทำเป็นข้อมูลส่วนบุคคลในสหราชอาณาจักรอันรวมถึงการกระทำแก่ข้อมูลในบัตรอิเล็กทรอนิกส์ โดยส่วนใหญ่แล้วจะถูกมองว่าเป็นการโจรกรรมเอกลักษณ์บุคคล (Identity Theft)[89] ทำให้ในการดึงข้อมูลบัตรในบางกรณีนั้น ผู้กระทำอาจจะต้องรับผิดต่อบทบัญญัติที่กำหนดไว้ในพระราชบัญญัติทั้งสามฉบับนี้ก็ได้[90] เช่น ในคดีที่ผู้กระทำการดึงข้อมูลจากบัตรที่กำลังเชื่อมต่อกับเครื่องจ่ายเงินอัตโนมัติโดยใช้เครื่องสกิมเมอร์นั้น การกระทำดังกล่าวย่อมเป็นการเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต ตามมาตรา 1 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 แต่ในขณะเดียวกันการกระทำต่อบัตรใบนั้นยังเป็นอาชญากรรมบัตรเครดิต (Credit Card Fraud) อันเป็นการโจรกรรมเอกลักษณ์บุคคลด้วย[91] เมื่อพิจารณาเจตนาในการกระทำความผิดแล้ว ผู้กระทำนั้นจะต้องนำข้อมูลซึ่งอยู่ในรูปแบบอิเล็กทรอนิกส์ที่ได้รับมาจากการดึงนั้นไปทำการฉ้อโกงใดๆ ต่อไปในอนาคตอย่างแน่แท้ เช่น เอาไปทำบัตรปลอมแล้วนำบัตรปลอมนั้นไปใช้หรือนำไปซื้อขายข้อมูลให้แก่ผู้อื่นอีกต่อไป แม้การกระทำการดึงข้อมูลจะยังไม่ใช่การฉ้อโกง แต่ก็เป็นการครอบครองสิ่งของเพื่อใช้ในการฉ้อโกง ตามมาตรา 6 แห่งพระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006 อีกทั้งการดึงข้อมูลจากบัตรโดยมิได้รับความยินยอมจากธนาคารในฐานะเป็นผู้ควบคุมข้อมูลดังกล่าวอยู่ ยังเป็นการได้รับข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย ตามมาตรา 170 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018 ด้วย

สหราชอาณาจักรจึงนับว่าเป็นประเทศที่มีกฎหมายอันเอาผิดแก่การดึงข้อมูลจากบัตรมาอย่างช้านานและจาการพัฒนากฎหมายโดยการแก้ไขเพิ่มเติมพระราชบัญญัติทั้งสามที่มีอยู่อย่างเสมอให้ทันกับสภาพการกระทำความผิดและให้สอดคล้องกับสหภาพยุโรป ทำให้สามารถใช้พระราชบัญญัติ

---

[89] David S. Wall, “Future Identities: Changing identities in the UK – the next 10 years” [Online], Accessed: 17 October 2020. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/275784/13-521-identity-related-crime-uk.pdf.

[90] The Crown Prosecution Service, “Computer Misuse Act” [Online], Accessed: 17 October 2020. Available from: https://www.cps.gov.uk/legal-guidance/computer-misuse-act.

[91] Experian.com, "Credit Card Fraud: What to Do If You’re a Victim" [Online], Accessed: 17 October 2020. Available from: https://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/credit-card-fraud-what-to-do-if-you-are-a-victim/.

ทั้งสามรับมือกับการกระทำความผิดต่อการดึงข้อมูลได้อย่างครอบคลุมและครบถ้วน อย่างไรก็ดีจากการที่มีพระราชบัญญัติทั้งสามฉบับในการบังคับใช้ทำให้บางคดีนั้นก็มีความเห็นที่แตกต่างกันว่าควรต้องใช้พระราชบัญญัติฉบับใดมาปรับใช้[92] ทำให้ผู้ใช้กฎหมายขาดความเข้าใจและไปใช้กฎหมายเพียงฉบับใดฉบับหนึ่งมากกว่าในการดำเนินคดี[93] และการบัญญัติกฎหมายให้เอาผิดกับการกระทำลักษณะหนึ่งอย่างมากเกินไปก็ทำให้ผู้กระทำเปลี่ยนไปใช้วิธีการอื่นๆ ในการกระทำความผิดมากขึ้น[94]

4.3 สาธารณรัฐฟิลิปปินส์

4.3.1 พระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012 (Cybercrime Prevention Act of 2012)

พระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012 (Cybercrime Prevention Act of 2012) หรือในชื่อเต็มคือพระราชบัญญัติกำหนดนิยามอาชญากรรมไซเบอร์เพื่อป้องกัน สืบสวนสอบสวน ปราบปรามและกำหนดโทษและเพื่อวัตถุประสงค์อื่นๆ (AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES) หรือสาธารณรัฐพระราชบัญญัติที่ 10175 (Republic Act No. 10175) เป็นกฎหมายของสาธารณรัฐฟิลิปปินส์ ซึ่งได้ประกาศใช้เมื่อวันที่ 12 กันยายน 2555 จากการตระหนักถึงความสำคัญของข้อมูลและการสื่อสารในการดำเนินการทางธุรกิจ อุตสาหกรรม และการสื่อสารภายในประเทศ และความสำคัญของการจัดให้มีสภาพแวดล้อมที่เอื้อต่อการพัฒนาทางเทคโนโลยีสารสนเทศและการสื่อสารอย่างรวดเร็ว และทำให้เกิดการแลกเปลี่ยนหรือการส่งมอบข้อมูลได้อย่างอิสระ จึงมีความจำเป็นต้องมีการออกกฎหมายดังกล่าวเพื่อปกป้องและรักษาความสมบูรณ์ของคอมพิวเตอร์ ระบบการสื่อสารในเครือข่ายและฐานข้อมูลดังกล่าว ทั้งการ

---

[92] The Crown Prosecution Service, “Computer Misuse Act” [Online], Accessed: 17 October 2020. Available from: https://www.cps.gov.uk/legal-guidance/computer-misuse-act.

[93] เช่นในประเทศอังกฤษและเวลส์ การกระทำผิดจะถูกฟ้องและตัดสินโดยใช้พระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006 เป็นส่วนใหญ่

[94] Peter Yapp, "The 30-Year-Old Computer Misuse Act Is Not Fit for Purpose" [Online], Accessed: 17 October 2020. Available from: https://www.scl.org/articles/10854-the-30-year-old-computer-misuse-act-is-not-fit-for-purpose.

รักษาความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลที่จัดเก็บไว้ในนั้น จากการใช้งานในทางที่ผิด การละเมิด การเข้าถึงที่ผิดกฎหมายในทุกรูปแบบ ให้ต้องได้รับการลงโทษตามกฎหมาย[95]

พระราชบัญญัติฉบับนี้ได้กำหนดให้การกระทำที่เป็นความผิดทางไซเบอร์ (Cybercrime Offenses) ไว้ในหมวดที่ 2 ว่าด้วยการกระทำที่สามารถลงโทษได้ (Chapter 2 PUNISHABLE ACTS) ในมาตรา 4 (Section 4) ซึ่งมีบทบัญญัติที่เกี่ยวข้องต่อการศึกษาวิจัยในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ดังต่อไปนี้

4.3.1.1 การเข้าถึงโดยผิดกฎหมาย

การเข้าถึงโดยผิดกฎหมาย (Illegal Access) บัญญัติอยู่ในมาตรา 4(a) อันหมวดความผิดต่อการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ โดยบัญญัติไว้ดังนี้

มาตรา 4 (a)(1) บัญญัติว่า “เข้าถึงโดยผิดกฎหมาย คือ การเข้าถึงระบบคอมพิวเตอร์ไม่ว่าทั้งหมดหรือแต่บางส่วนโดยไม่มีสิทธิ”

โดยการเข้าถึง (Access) ตามพระราชบัญญัตินี้ หมายถึง การกระทำที่เป็นการออกคำสั่ง หรือการสื่อสาร การจัดเก็บข้อมูล การดึงข้อมูลมา (Retrieving data from) หรือการใช้ทรัพยากรใดๆ ในระบบคอมพิวเตอร์ (Computer System) หรือเครือข่ายการสื่อสาร (Communication Network)[96] โดยคำจำกัดความของระบบคอมพิวเตอร์ (Computer System) นั้นพระราชบัญญัติฉบับนี้ได้ให้ความหมายว่า หมายถึง อุปกรณ์ใดๆ หรือกลุ่มของอุปกรณ์ที่เชื่อมต่อกันหรือที่เกี่ยวข้องกัน ซึ่งอย่างน้อยชิ้นหนึ่งต้องมีการดำเนินการตามโปรแกรมและประมวลผลข้อมูลโดยอัตโนมัติ และครอบคลุมอุปกรณ์ทุกประเภทที่มีความสามารถในการประมวลผลข้อมูล ซึ่งไม่จำกัดเพียงเครื่องคอมพิวเตอร์และโทรศัพท์มือถือเท่านั้น แต่รวมถึงอุปกรณ์ที่ประกอบไปด้วยฮาร์ดแวร์และซอฟแวร์ และรวมไปถึงส่วนประกอบอินพุต (Input) และเอาต์พุต (Output) และหน่วยเก็บข้อมูล (Storage Components) ซึ่งอยู่โดยลำพังหรือที่เชื่อมต่อในเครือข่ายหรืออุปกรณ์อื่นที่คล้ายกัน และให้รวมถึงอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ด้วย (Computer data storage devices)[97]

---

[95] Section 2 of Republic Act No. 10175

[96] Section 3(a) of Republic Act No. 10175

[97] Section 3(g) of Republic Act No. 10175

แม้ในพระราชบัญญัติดังกล่าวจะไม่ได้ให้ความหมายของคำว่าอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ (Computer data storage devices) เอาไว้ แต่ก็ได้ให้ความหมายคำว่าข้อมูลคอมพิวเตอร์ (Computer Data) เอาไว้ว่าหมายถึง ข้อเท็จจริง ข้อมูล หรือแนวคิดใดๆ ที่สามารถประมวลผลในระบบคอมพิวเตอร์ได้ รวมถึงโปรแกรมที่ทำให้ระบบคอมพิวเตอร์ทำงานได้ ทั้งยังหมายถึงเอกสารอิเล็กทรอนิกส์ ข้อความอิเล็กทรอนิกส์ ไม่ว่าจะได้บรรจุอยู่ในคอมพิวเตอร์ส่วนตัว (Local Computer) หรือระบบออนไลน์ก็ตาม[98] จึงทำให้อุปกรณ์ใดๆ ก็ตามที่มีข้อมูลที่สามารถนำไปประมวลผลในระบบคอมพิวเตอร์ได้ และได้บันทึกข้อมูลดังกล่าวไว้ภายในหน่วยบันทึกข้อมูลของอุปกรณ์นั้นๆ อุปกรณ์ดังกล่าวก็ถือได้ว่าเป็นอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ ในความหมายของพระราชบัญญัติฉบับนี้แล้ว

ผลที่ตามมาจากการที่คำนิยามของพระราชบัญญัติฉบับนี้ที่กำหนดว่าอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ (Computer data storage devices) คือระบบคอมพิวเตอร์ (Computer System) ด้วย คือส่งผลให้หากมีการดึงข้อมูลออกมาจากอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ดังกล่าวแล้ว ย่อมเป็นการเข้าถึง (Access) ระบบคอมพิวเตอร์ไม่ว่าทั้งหมดหรือแต่บางส่วนตามคำนิยามที่ได้กล่าวมาแล้วข้างต้น ซึ่งหากไม่มีสิทธิแล้ว การกระทำดังกล่าวจะเป็นการเข้าถึงโดยผิดกฎหมายอันผู้กระทำย่อมต้องรับผิดตามมาตรา 4 (a)(1) ซึ่งลักษณะของบัตรโดยทั่วไปนั้นย่อมมีแหล่งบันทึกข้อมูลไม่ว่าจะเป็นแถบแม่เหล็กหรือชิปที่ทำหน้าที่จัดเก็บข้อมูลคอมพิวเตอร์ไว้อยู่ด้วย บัตรเหล่านี้ย่อมเข้าความหมายของคำว่าอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ ซึ่งหากมีการดึงข้อมูลออกจากบัตรแล้ว ผู้กระทำย่อมมีความผิดตามมาตรานี้

4.3.1.2 การขโมยข้อมูลประจำตัวที่เกี่ยวข้องกับคอมพิวเตอร์

การขโมยข้อมูลประจำตัวที่เกี่ยวข้องกับคอมพิวเตอร์ (Computer-related Identity Theft) บัญญัติอยู่ในมาตรา 4(b) อันหมวดความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ โดยบัญญัติไว้ดังนี้

มาตรา 4(b)(3) บัญญัติว่า “ขโมยข้อมูลประจำตัวที่เกี่ยวข้องกับคอมพิวเตอร์ (Computer-related Identity Theft) คือ เจตนาเข้ายึดถือ (Acquisition) ใช้ โอน ครอบครอง (Possession) เปลี่ยนแปลงหรือลบ ข้อมูลประจำตัว (Identifying information) ของบุคคลอื่นโดยไม่มีสิทธิ”

---

[98] Section 3(e) of Republic Act No. 10175

คำว่า ข้อมูลประจำตัว (Identifying information) แม้พระราชบัญญัตินี้จะไม่ได้ให้คำนิยามไว้ แต่ในคดี Disini v. Secretary of Justice[99] (ค.ศ. 2014) ศาลฎีกา (Supreme Court) ของสาธารณรัฐฟิลิปปินส์ได้อธิบายว่า “ข้อมูลประจำตัวปกติเกี่ยวกับบุคคล ได้แก่ ชื่อ สัญชาติ ที่อยู่อาศัย หมายเลขติดต่อ สถานที่อยู่ วันเดือนปีเกิด ชื่อคู่สมรสหากมี และข้อมูลอื่นๆ ในลักษณะที่คล้ายกัน ซึ่งกฎหมายจะลงโทษผู้ที่ได้เข้ายึดถือหรือใช้ข้อมูลเหล่านั้นโดยไม่มีสิทธิเนื่องจากเป็นการก่อให้เกิดความเสียหายโดยปริยายแล้ว และการขโมยข้อมูลดังกล่าวต้องมีเจตนาเพื่อกระทำผิดกฎหมายด้วย”

การขโมยข้อมูลประจำตัว (Identity Theft) เป็นการกระทำความผิดที่ผู้กระทำพยายามที่จะขโมยข้อมูลที่เกี่ยวข้องกับบุคคล เช่น ชื่อ หมายเลขติดต่อ ดังที่ศาลฎีกาของสาธารณรัฐฟิลิปปินส์ได้ยกตัวอย่างในคดี Disini v. Secretary of Justice อีกทั้งโดยทั่วไปยังรวมถึงข้อมูลต่างๆ เช่น ข้อมูลบัตรเครดิต เพื่อนำข้อมูลที่ได้นั้นไปกระทำความผิดอื่นๆ ต่อไป เช่น นำไปถอนเงินออกจากบัญชี นำไปขายให้แก่เว็บไซต์ใต้ดิน (Dark Web)[100] ซึ่งการขโมยนั้นมีหลากหลายวิธี เช่น การฟิตชิ่ง (Phishing) การสกิมมิ่ง (Skimming) การแฮกระบบคอมพิวเตอร์ (Hacking) และวิธีการเหล่านี้เป็นวิธีการปกติที่ผู้กระทำผิดใช้ในการดึงข้อมูลจากบัตรด้วย ดังนั้นพระราชบัญญัติฉบับนี้จึงต้องบัญญัติให้การขโมยข้อมูลประจำตัวบุคคลอันเป็นส่วนประกอบของข้อมูลในบัตร ให้เป็นความผิดตามมาตรา 4(b)(3) นี้ด้วยเพื่อให้กฎหมายของสาธารณรัฐฟิลิปปินส์มีบทบัญญัติที่ครอบคลุมกับลักษณะการกระทำความผิดอย่างครบถ้วน

บทกำหนดโทษของพระราชบัญญัตินี้อยู่ในหมวดที่ 3 ว่าด้วยบทลงโทษ (Chapter 3 PENALTIES) ซึ่งบทลงโทษตามมาตรา 4(a)(1) และมาตรา 4(b)(3) นั้นกำหนดไว้ในมาตรา 8 ดังนี้

มาตรา 8 วรรคหนึ่ง “บุคคลใดพบว่าได้กระทำความผิดในบรรดาการกระทำที่สามารถลงโทษได้ ซึ่งได้แจกแจงในมาตรา 4(a) และ 4(b) ตามพระราชบัญญัตินี้ จักต้องถูกลงโทษด้วยการจำคุกในระดับเรือนจำใหญ่ (Prision Mayor) หรือปรับเป็นอย่างน้อย 200,000 เปโซฟิลิปปินส์[101] จนถึงจำนวนที่สมน้ำสมเนื้อกับความเสียหายที่เกิดขึ้น หรือทั้งจำทั้งปรับ”

---

[99] G.R. No. 203335

[100] Jennifer van der Kleut, "Identity Theft: What Is It and How to Avoid It" [Online], Accessed: 10 October 2020. Available from: https://us.norton.com/internetsecurity-id-theft-what-is-identity-theft.html.

[101] ประมาณ 129,797 บาท (อัตราแลกเปลี่ยน ณ วันที่ 5 ตุลาคม 2563)

โดยโทษจำคุกในระดับเรือนจำใหญ่ (Prision Mayor) นั้น ตามกฎหมายอาญาที่ได้แก้ไขใหม่ของสาธารณรัฐฟิลิปปินส์ (AN ACT REVISING THE PENAL CODE AND OTHER PENAL LAWS) คือโทษจำคุกตั้งแต่ 6 ปีกับอีกหนึ่งวันไปจนถึง 12 ปี[102]

หากการกระทำความผิดตามมาตรา 4 (a)(1) เป็นการกระทำต่อโครงสร้างพื้นฐานที่สำคัญของรัฐ (Critical Infrastructure) อันได้แก่ระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ที่มีความสำคัญต่อสาธารณรัฐฟิลิปปินส์มากจนไม่อาจจะให้มีการทำลายหรือรบกวนระบบดังกล่าวได้เพราะอาจทำให้กระทบต่อความมั่นคงหรือเศรษฐกิจของประเทศ[103] ผู้กระทำต้องรับโทษหนักขึ้นตามมาตรา 8 วรรคสามด้วย

มาตรา 8 วรรคสาม “ถ้าการกระทำในมาตรา 4(a) เป็นการกระทำต่อโครงสร้างพื้นฐานที่สำคัญของรัฐ (Critical Infrastructure) จักต้องถูกลงโทษด้วยการจำคุกในระดับการปฏิเสธชั่วคราว (Reclusion temporal) หรือปรับเป็นอย่างน้อย 500,000 เปโซฟิลิปปินส์[104] จนถึงจำนวนที่สมน้ำสมเนื้อกับความเสียหายที่เกิดขึ้น หรือทั้งจำทั้งปรับ”

โดยโทษจำคุกในระดับการปฏิเสธชั่วคราว (Reclusion temporal) นั้น ตามกฎหมายอาญาที่ได้แก้ไขใหม่ของสาธารณรัฐฟิลิปปินส์ (AN ACT REVISING THE PENAL CODE AND OTHER PENAL LAWS) คือโทษจำคุกตั้งแต่ 12 ปีกับอีกหนึ่งวันไปจนถึง 20 ปี[105]

4.3.2 พระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 (Access Devices Regulation Act of 1988)

พระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 (Access Devices Regulation Act of 1998) หรือในชื่อเต็มคือพระราชบัญญัติที่เกี่ยวข้องกับปัญหาและการใช้งานอุปกรณ์ในการเข้าถึงเพื่อกำหนดโทษและวัตถุประสงค์อื่นๆ ในการยับยั้งการฉ้อโกงและการกระทำความผิดอื่นที่เกี่ยวข้อง (AN ACT REGULATING THE ISSUANCE AND USE OF ACCESS DEVICES, PROHIBITING FRAUDULENT ACTS COMMITTED RELATIVE THERETO, PROVIDING PENALTIES AND FOR OTHER PURPOSES) หรือสาธารณรัฐพระราชบัญญัติฉบับที่ 8484 (Republic Act No. 8484) ซึ่งได้

---

[102] Article 27 of AN ACT REVISING THE PENAL CODE AND OTHER PENAL LAWS

[103] Section 3(j) of Republic Act No. 10175

[104] ประมาณ 324,672 บาท (อัตราแลกเปลี่ยน ณ วันที่ 5 ตุลาคม 2563)

[105] Article 27 of AN ACT REVISING THE PENAL CODE AND OTHER PENAL LAWS

ประกาศใช้เมื่อวันที่ 11 กุมภาพันธ์ 2535 เป็นกฎหมายอีกฉบับหนึ่งของสาธารณรัฐฟิลิปปินส์ที่บัญญัติขึ้นมาเพื่อดำเนินคดีแก่การกระทำความผิดเกี่ยวกับองค์กรธนาคารโดยเฉพาะ เพราะสถาบันทางการเงินของสาธารณรัฐฟิลิปปินส์นั้นมีการใช้เทคโนโลยีขั้นสูงในการทำธุรกรรมทางการเงินประกอบกับมีการใช้อุปกรณ์ในการเข้าถึง (Access device) ในการทำธุรกรรมทางการเงินของคนในชาติเป็นจำนวนมากในปี 1998 จึงได้บัญญัติกฎหมายดังกล่าวขึ้น[106] อย่างไรก็ตามด้วยการพัฒนาของเทคโนโลยีหลังจากนั้นทำให้อาชญากรสามารถนำเทคโนโลยีสมัยใหม่มาประยุกต์ใช้เพื่อเข้าถึงข้อมูลที่อยู่ภายในอุปกรณ์ในการเข้าถึง (Access device) และข้อมูลเหล่านี้ได้ถูกนำไปใช้ต่ออันก่อให้เกิดประโยชน์แก่อาชญากรเหล่านั้นเป็นจำนวนมาก การดังกล่าวส่งผลกระทบต่อความไว้วางใจของสาธารณชนต่อองค์กรธนาคารและเป็นอันตรายต่อเศรษฐกิจของสาธารณรัฐฟิลิปปินส์เป็นอย่างมาก[107] สภาคองเกรสด้วยความเห็นชอบประธานาธิบดีดูแตร์เต (Rodrigo Duterte) จึงได้ทำการแก้ไขเพิ่มเติมบทบัญญัติของพระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 ด้วยการออกพระราชบัญญัติกำหนดข้อห้ามเพิ่มเติมและการเพิ่มบทลงโทษสำหรับการละเมิดสาธารณรัฐพระราชบัญญัติฉบับที่ 8484 หรือเรียกอีกอย่างว่า “พระราชบัญญัติควบคุมอุปกรณ์การเข้าถึงปี 1998” (An Act Providing for Additional Prohibitions to and Increasing Penalties for Violations of Republic Act No. 8484, Otherwise Known as the “Access Devices Regulation Act of 1998”) หรือสาธารณรัฐพระราชบัญญัติฉบับที่ 11449 (Republic Act No. 11449) มาบังคับใช้เมื่อวันที่ 28 สิงหาคม 2562 ที่ผ่านมา โดยมีการเพิ่มเติมบทบัญญัติที่มีอยู่เดิมให้ครอบคลุมถึงลักษณะของการกระทำความผิดมากขึ้นและทั้งยังปรับปรุงบทกำหนดโทษโดยการเพิ่มอัตราโทษให้สูงขึ้นกว่าบทบัญญัติเดิมเป็นอย่างมากเพื่อใช้ในการดำเนินการแก่อาชญากรอย่างสาสม ดังนั้นในการศึกษาวิจัยพระราชบัญญัติดังกล่าว ผู้วิจัยจะศึกษาทั้งบทบัญญัติที่มีอยู่ในกฎหมายเดิมและที่แก้ไขเพิ่มเติมและจะเรียกรวมกันไปว่า “พระราชบัญญัติ” โดยจะทำการอ้างอิงไว้ในส่วนท้ายเพื่อให้ทราบว่าเป็นกฎหมายฉบับใด

วัตถุแห่งการกระทำความผิดที่เกี่ยวข้องต่อการศึกษาวิจัยในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ตามพระราชบัญญัตินี้เดิมนั้น[108] กำหนดแค่เพียงอุปกรณ์ในการเข้าถึง (Access Device) ซึ่งมีนิยามกำหนดไว้ดังนี้

---

[106] Section 2 of Republic Act No. 8484

[107] Section 1 of Republic Act No. 11449

[108] Republic Act No. 8484

มาตรา 3(a) อุปกรณ์ในการเข้าถึง (Access Device) หมายถึง “บัตรใดๆ ก็ตาม ป้าย รหัส หมายเลขบัญชี หมายเลขทางอิเล็กทรอนิกส์ หมายเลขประจำตัวบุคคล หรืออุปกรณ์ที่ใช้ในการโทรคมนาคม อุปกรณ์หรือเครื่องมือที่ใช้ในการระบุตัวบุคคล หรือวิธีการอื่นใดก็ตามในการเข้าถึงบัญชีที่สามารถใช้เพื่อให้ได้รับเงิน สินค้า บริการ หรือสิ่งมีค่าอื่นๆ หรือใช้ในการโอนเงินนอกเหนือจากการโอนที่เป็นการดำเนินงานทางเอกสารทั่วไป”

เมื่อพิจารณาบทนิยามดังกล่าวแล้วพบว่าไม่ว่าจะเป็นบัตรในรูปแบบใดก็ตาม รหัส หมายเลขบัญชี หมายเลขบัตรประจำตัวประชาชน เป็นต้น ก็เป็นวัตถุแห่งการกระทำความผิดตามพระราชบัญญัติเดิมได้ทั้งสิ้น แต่อย่างไรก็ตาม สาธารณรัฐฟิลิปปินส์ก็ได้มีการแก้ไขเพิ่มเติมโดยเพิ่มคำนิยามให้มีวัตถุแห่งการกระทำที่มีลักษณะเฉพาะตัวนอกเหนือจากคำว่าอุปกรณ์ในการเข้าถึง โดยการเพิ่มคำนิยามดังนี้

มาตรา 3(b)[109] บัตรชำระเงิน (Payment Card) หมายถึง “บัตรที่ผู้ถือบัตรสามารถใช้และได้รับการยอมรับให้ทำการเบิกถอนเงินสดหรือชำระเงินเพื่อการซื้อสินค้าหรือบริการ การโอนเงินและการทำธุรกรรมอื่นๆ ซึ่งโดยปกติแล้วบัตรชำระเงินจะเชื่อมโยงกับบัญชีเงินฝากหรือบัญชีเครดิตเงินกู้”

นอกจากที่ได้กำหนดคำนิยามของบัตรชำระเงินดังกล่าวแล้ว มาตรา 3(o) ของพระราชบัญญัติดังกล่าว[110] ยังเพิ่มเติมรายละเอียดของคำว่าบัตรชำระเงินเพิ่มขึ้นด้วย ดังนี้

มาตรา 3(o) บัตรชำระเงิน (Payment Card) ให้หมายถึง “บัตรใดๆ ก็ตาม ไม่ว่าจะทำขึ้นด้วยวัสดุใดหรือจะอยู่ในรูปแบบใด รวมทั้งบัตรเดบิตทุกประเภทที่ไม่ใช่บัตรเครดิต ที่ออกโดยธนาคารหรือหน่วยงานธุรกิจที่ช่วยให้ลูกค้าสามารถใช้งานกับเครื่องจ่ายเงินอัตโนมัติเพื่อทำธุรกรรมได้ เช่น การฝากถอนเงิน การรับข้อมูลทางบัญชี และให้ถือว่าบัตรชำระเงินเป็นอุปกรณ์ในการเข้าถึงด้วยตามพระราชบัญญัตินี้”

ผลจากการนิยามคำว่าบัตรชำระเงินเพิ่มขึ้นจากพระราชบัญญัติเดิมที่มีแต่เพียงนิยามคำว่าอุปกรณ์ในการเข้าถึงนั้น ส่งผลให้กฎหมายของสาธารณรัฐฟิลิปปินส์มีความละเอียดมากขึ้น โดยสามารถนำกฎหมายไปปรับใช้ให้ครอบคลุมถึงวัตถุแห่งการกระทำความผิดที่เป็นบัตรต่างๆ ได้อย่างกว้างขวาง และเพื่อให้สอดคล้องกับฐานความผิดที่ได้แก้ไขเพิ่มเติมขึ้นใหม่นั้นด้วยเพราะฐานความผิดอันเกี่ยวกับการดึงข้อมูลของสาธารณรัฐฟิลิปปินส์ตามพระราชบัญญัติเดิมนั้นมีอยู่เพียงมาตราเดียว

---

[109] เพิ่มเติมโดย Section 2 of Republic Act No. 11449

[110] Republic Act No. 11449

จึงอาจมีวัตถุแห่งการกระทำบางประการที่ไม่เข้าคำนิยามของคำว่าอุปกรณ์ในการเข้าถึง อันอาจจะทำให้อาชญากรหลุดพ้นจากความผิดไปได้

พระราชบัญญัติฉบับนี้มีการกระทำที่เป็นความผิดอันเกี่ยวข้องต่อการศึกษาวิจัยในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ถูกกำหนดอยู่ในมาตรา 9 ซึ่งสามารถแบ่งออกได้เป็นดังนี้

4.3.2.1 การมีอุปกรณ์ในการเข้าถึงในครอบครองโดยมิได้รับอนุญาต

การมีอุปกรณ์ในการเข้าถึงในครอบครองโดยมิได้รับอนุญาต กำหนดอยู่ในมาตรา 9(k) และเป็นฐานความผิดตามพระราชบัญญัติเดิมก่อนที่มีการแก้ไขเพิ่มเติม ซึ่งบัญญัติไว้ดังนี้

มาตรา 9(k)[111] บัญญัติว่า “มีอุปกรณ์ในการเข้าถึงไว้ในครอบครอง (Possession) โดยมิได้รับอนุญาตจากเจ้าของหรือหน่วยงานที่เป็นเจ้าของ รวมถึงวัสดุใดๆ เช่น สลิป กระดาษคาร์บอน หรือสิ่งอื่นใดที่เขียน พิมพ์นูน หรือระบุไว้บนอุปกรณ์ในการเข้าถึงนั้น”

การกระทำความผิดตามมาตรา 9(k) นี้คือการครอบครองอุปกรณ์ในการเข้าถึงโดยมิได้รับอนุญาต โดยได้กล่าวมาแล้วว่าอุปกรณ์ในการเข้าถึงนั้นหมายถึง[112] บัตรในรูปแบบใดก็ตาม รหัส หมายเลขบัญชี หมายเลขบัตรประจำตัวประชาชน เป็นต้น ทั้งมาตรา 9(k) ดังกล่าวยังหมายรวมถึงการครอบครอง สลิป กระดาษคาร์บอน อันเป็นผลจากการใช้งานอุปกรณ์ในการเข้าถึงเหล่านั้นด้วย และยังรวมไปข้อมูลใดๆ ที่ถูกพิมพ์นูนหรือเขียนไว้บนอุปกรณ์นั้นด้วย ซึ่งบุคคลใดที่มีสิ่งเหล่านี้ไว้ในครอบครองโดยมิได้รับอนุญาตจากเจ้าของหรือหน่วยงานธนาคารที่ออกให้ก็จะเป็นความผิด แม้มาตราดังกล่าวจะไม่ใช่การดึงข้อมูลจากบัตรซึ่งเป็นอุปกรณ์ในการเข้าถึงโดยตรง แต่การครอบครองอุปกรณ์ในการเข้าถึงก็คือผลอันเกิดจากการดึงข้อมูลจากบัตรนั่นเอง ซึ่งมีความใกล้ชิดกันมากและสามารถใช้มาตราดังกล่าว ลงโทษแก่ผู้กระทำความผิดได้เช่นกัน อย่างไรก็ตาม การตีความในลักษณะนี้แม้จะใช้ได้แต่ก็อาจส่งผลต่อความชัดเจนแน่นอนของการปรับใช้กฎหมายต่อการกระทำความผิดดังกล่าวซึ่งอาจเปิดช่องให้อาชญากรยกขึ้นต่อสู้ในเชิงกฎหมายได้ ทั้งยังเป็นมาตราเดียวในพระราชบัญญัติฉบับเดิมที่สามารถใช้กับเรื่องการดึงข้อมูลจากบัตรได้ ดังนั้นต่อมาสาธารณรัฐฟิลิปปินส์จึงได้ทำการแก้ไขเพิ่มเติมพระราชบัญญัติดังกล่าวให้มีกฎหมายเฉพาะในการเอาผิดกับการดึงข้อมูลจากบัตรเพิ่มขึ้น อันจะกล่าวต่อไป

---

[111] Section 9(k) of Republic Act No. 8484

[112] มาตรา 3(a) (b) และ (o) จากการเพิ่มเติมมาตรา 2 of Republic Act No. 11449

4.3.2.2 การสกิมมิ่ง คัดลอก หรือปลอมแปลงบัตร

การสกิมมิ่ง คัดลอก หรือปลอมแปลงบัตร กำหนดอยู่ในมาตรา 9(q) และเป็นฐานความผิดตามพระราชบัญญัติที่ได้มีการแก้ไขเพิ่มเติมขึ้นใหม่ อันเป็นการเพิ่มเติมจากเดิมที่จะลงโทษผู้กระทำผิดในการดึงข้อมูลจากบัตรได้แต่เพียงฐานเดียว คือฐานมีอุปกรณ์ในการเข้าถึงในครอบครองโดยมิได้รับอนุญาต ในมาตรา 9(k) ของพระราชบัญญัติเดิม และเป็นบทบัญญัติที่กำหนดขึ้นมาเฉพาะเพื่อเอาผิดแก่การดึงข้อมูลจากบัตร ซึ่งบัญญัติไว้ดังนี้

มาตรา 9(q)[113] บัญญัติว่า “สกิมมิ่ง (Skimming) คัดลอก (Copying) หรือปลอมแปลงบัตรเครดิต บัตรชำระเงิน (Payment Card) หรือบัตรเดบิต และได้รับไป (Obtaining) ซึ่งข้อมูลใดๆ ในบัตรนั้นด้วยเจตนาในการเข้าถึงบัญชีหรือจัดการบัญชี ไม่ว่าจะได้ทำการถอนเงินหรือทำให้เกิดความเสียหายทางการเงินอย่างอื่นแก่เจ้าของบัญชีหรือธนาคารผู้รับฝากเงินหรือไม่ก็ตาม”

โดยในมาตรา 3(p) ของพระราชบัญญัติแก้ไขเพิ่มเติมดังกล่าว[114] ยังให้คำนิยามของการกระทำความผิดในลักษณะการสกิมมิ่ง (Skimming) ในมาตรา 9(q) นี้ด้วย โดยกำหนดว่า “การ์ดสกิมมิ่ง (Card Skimming) ให้หมายถึง การฉ้อโกงประเภทหนึ่ง ซึ่งเกี่ยวข้องกับการคัดลอกข้อมูลอย่างผิดกฎหมายจากแถบแม่เหล็กของบัตรชำระเงินเพื่อเป็นการเข้าถึง (Access) บัญชีของลูกค้า”

ดังนั้น การกระทำความผิดตามมาตรา 9(q) นี้จึงเป็นการคัดลอกข้อมูลใดๆ ก็ตามที่ได้บันทึกอยู่บัตรเครดิต บัตรเดบิต และบัตรชำระเงิน ซึ่งบัตรชำระเงินตามมาตรา 3(b) ก็ถูกอธิบายความเพิ่มเติมในมาตรา 3(o) และนับว่าเป็นอุปกรณ์ในการเข้าถึงตามมาตรา 3(a) ด้วย ซึ่งแปลได้ว่าบัตรประเภทต่างๆ ไม่ว่าจะทำขึ้นด้วยวัสดุใดหรือจะอยู่ในรูปแบบใด ที่ทางธนาคารได้ออกให้แก่ลูกค้าเพื่อใช้ในการทำธุรกรรมทางการเงิน กฎหมายของสาธารณรัฐฟิลิปปินส์ก็มุ่งที่จะคุ้มครองบัตรเหล่านั้นจากการกระทำความผิดจากการถูกดึงข้อมูลหรือถูกคัดลอกข้อมูลออกไปจากบัตร โดยไม่ต้องคำนึงว่าผู้กระทำความผิดจะได้มีการถอนเงินหรือทำให้เกิดความเสียหายทางการเงินอย่างอื่นแก่เจ้าของบัญชีหรือธนาคารผู้รับฝากเงินเพิ่มเติมอีกหรือไม่ เพียงแต่ผู้กระทำความผิดได้ทำการสกิมมิ่งหรือคัดลอกข้อมูลออกไปจากบัตรก็จะเป็นความผิดตามมาตรา 9(q) ทันที แม้จะได้มีบทบัญญัติมาตรา 9(q) เป็นการเฉพาะแล้ว แต่อย่างไรก็ตามกฎหมายของสาธารณรัฐฟิลิปปินส์ก็ได้บัญญัติลักษณะการกระทำ

---

[113] Section 9(q) of Republic Act No. 11449

[114] Republic Act No. 11449

ความผิดในมาตรา 9(s) และมาตรา 9(t) เพื่อให้กฎหมายมีความครอบคลุมกับการดึงข้อมูลจากบัตรในทุกรูปแบบ ดังจะกล่าวต่อไป

4.3.2.3 การเข้าถึงบัญชี หรือแฮกระบบคอมพิวเตอร์เพื่อขโมยข้อมูล

การเข้าถึงบัญชีและการแฮกระบบคอมพิวเตอร์เพื่อขโมยข้อมูลนั้น เป็นบทบัญญัติที่ถูกเพิ่มขึ้นจากการแก้ไขเพิ่มเติมพระราชบัญญัติ เป็นบทบัญญัติเสริมเพื่อให้ครอบคลุมกับการดึงข้อมูลจากบัตรในลักษณะอื่นๆ นอกจากการสกิมมิ่งตามมาตรา 9(q) ที่อาจจะเกิดขึ้นได้จากความซับซ้อนทางเทคโนโลยีที่ใช้ในการกระทำความผิดดังกล่าว อันเกิดจากการใช้งานบัตรในรูปแบบของข้อมูลในระบบออนไลน์หรือในระบบเซิร์ฟเวอร์ (Server) ของคอมพิวเตอร์ เป็นต้น โดยมีบทบัญญัติดังนี้

มาตรา 9(s) บัญญัติว่า “เข้าถึง (Accessing) คำร้องในการเปิดบัญชี บัญชีธนาคารออนไลน์ (Online Banking Account) บัญชีของบัตรเครดิต บัญชีเอทีเอ็ม บัญชีของบัตรเดบิต ไม่ว่าจะมีอำนาจหรือไม่ก็ตามในลักษณะเป็นการฉ้อโกง โดยการนั้นอาจทำให้เจ้าของบัญชีสูญเสียเงินหรือไม่ก็ได้”

บทบัญญัติมาตราดังกล่าวกำหนดขึ้นเพราะในการใช้งานบัตรนั้นในทางความเป็นจริงอาจจะเป็นการใช้งานบัตรในรูปแบบของบัญชีธนาคารออนไลน์ที่ทางธนาคารมิได้มีการออกตัวบัตรให้แก่ลูกค้าแต่ได้ออกเป็นหมายเลขบัตรพร้อมรหัสบัตรในการทำธุรกรรมผ่านระบบออนไลน์ได้ โดยมาตรา 3(r) ได้บัญญัติว่า “ธนาคารออนไลน์ (Online Banking) ให้ความหมายถึง การใช้งานผ่านระบบอินเตอร์เน็ตของลูกค้าธนาคารในการจัดการบัญชีธนาคารและการทำธุรกรรมต่างๆ” แต่มาตรา 9(s) นี้ได้บัญญัติครอบคลุมถึงบัญชีธนาคารในรูปแบบทั่วๆ ไปไม่ว่าจะเป็นบัญชีบัตรเครดิต บัญชีบัตรเอทีเอ็ม เป็นต้น เอาไว้ด้วย โดยเอาผิดเฉพาะการกระทำการเข้าถึง (Accessing) บัญชีของธนาคารเท่านั้น โดยไม่ได้ทำการคัดลอกหรือดึงข้อมูลบัญชีดังกล่าวไปด้วย จึงต้องมีบทบัญญัติเรื่องการแฮกระบบคอมพิวเตอร์เพื่อขโมยข้อมูลโดยเฉพาะขึ้นในมาตรา 9(t) ซึ่งบัญญัติดังนี้

มาตรา 9(t) บัญญัติว่า “ทำการแฮก (Hacking) หมายถึงเข้าถึงหรือแทรกแซงในระบบคอมพิวเตอร์ เซิฟเวอร์ ระบบข้อมูลหรือระบบสื่อสารโดยไม่ได้รับอนุญาต เพื่อทำการทุจริต แก้ไข ขโมย หรือทำลาย โดยใช้เครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารอื่นที่คล้ายกัน โดยไม่ได้รับความยินยอมจากเจ้าของคอมพิวเตอร์หรือเจ้าของข้อมูลหรือเจ้าของระบบสื่อสารนั้น รวมถึงการใช้ไวรัสคอมพิวเตอร์ (Computer Viruses) ซึ่งทำให้เกิดการทุจริต ทำลาย แก้ไข ขโมย หรือสูญเสียข้อมูลหรือเอกสารทางอิเล็กทรอนิกส์”

บทบัญญัตินี้กำหนดขึ้นมาเพื่อเอาผิดแก่การขโมยข้อมูลที่อยู่ในระบบคอมพิวเตอร์หรือในเซิฟเวอร์ ไม่ว่าจะเป็นการใช้คอมพิวเตอร์ อุปกรณ์ หรือไวรัสคอมพิวเตอร์ เพื่อให้ครอบคลุมถึงการใช้งานบัตรบางประเภทที่ธนาคารมิได้มีการออกบัตรให้ แต่มีการใช้งานบัตรในรูปของข้อมูลอิเล็กทรอนิกส์ลงในระบบคอมพิวเตอร์ ซึ่งหากมีการแฮกระบบคอมพิวเตอร์และขโมยข้อมูลบัตรเหล่านั้นออกไปจากระบบ แม้ผู้กระทำจะไม่มีความผิดตามมาตรา 9(q) ดังที่กล่าวมาแล้วเพราะมิใช่การคัดลอกข้อมูลในบัตร แต่ผู้กระทำก็จะมีความผิดตามมาตรา 9(t) นี้ อันเป็นการบัญญัติกฎหมายเพิ่มเติมขึ้นเพื่อให้ครอบคลุมในการกระทำความผิดเกี่ยวกับบัตรได้ทุกประเภทและเป็นการป้องกันปัญหาความไม่ครอบคลุมของกฎหมายในพระราชบัญญัติเดิมของสาธารณรัฐฟิลิปปินส์ด้วย

บทกำหนดโทษ บัญญัติไว้ในมาตรา 10 ซึ่งพระราชบัญญัติฉบับแก้ไขเพิ่มเติมนั้น ได้ทำการแก้ไขอัตราโทษจากเดิมที่มีอัตราโทษจำคุกตั้งแต่ 6 ปี ไปจนถึง 20 ปี ขึ้นอยู่กับจำนวนฐานความผิดที่ผู้กระทำได้กระทำลงไปตามพระราชบัญญัติฉบับเดิมและมีอัตราโทษปรับตั้งแต่ 10,000 เปโซฟิลิปปินส์ไปจนถึงสองเท่าของมูลค่าของประโยชน์ที่ผู้กระทำความผิดได้รับจากการกระทำความผิด ให้พระราชบัญญัติแก้ไขเพิ่มเติมนั้น มีอัตราโทษที่สูงขึ้นเป็นอย่างมาก เพื่อให้สามารถลงโทษผู้กระทำความผิดได้อย่างสาสม ซึ่งมีหลักเกณฑ์ดังนี้[115]

อัตราโทษของการกระทำความผิดในมาตรา 9(k) (s) และ (t) คือ จำคุกไม่น้อยกว่า 6 ปีไปจนถึง 10 ปี และปรับเป็นจำนวน 500,000 เปโซฟิลิปปินส์[116] หรือสองเท่าของมูลค่าของประโยชน์ที่ผู้กระทำความผิดได้รับขึ้นอยู่กับว่าจำนวนใดจะมากกว่ากัน โดยผู้กระทำมิได้มีความรับผิดทางแพ่งและมิได้กระทำความผิดฐานอื่นร่วมด้วย

อัตราโทษของการกระทำความผิดในมาตรา 9(k) (s) และ (t) คือ จำคุกไม่น้อยกว่า 6 ปีไปจนถึง 10 ปี และปรับเป็นจำนวน 500,000 เปโซฟิลิปปินส์หรือสองเท่าของมูลค่าของประโยชน์ที่ผู้กระทำความผิดได้รับขึ้นอยู่กับว่าจำนวนใดจะมากกว่ากัน โดยผู้กระทำมิได้มีความรับผิดทางแพ่งและมิได้กระทำความผิดฐานอื่นร่วมด้วย

อัตราโทษของการกระทำความผิดในมาตรา 9(q) คือ จำคุกไม่น้อยกว่า 10 ปีไปจนถึง 12 ปี และปรับเป็นจำนวน 500,000 เปโซฟิลิปปินส์หรือสองเท่าของมูลค่าของประโยชน์ที่ผู้กระทำความผิดได้รับขึ้นอยู่กับว่าจำนวนใดจะมากกว่ากัน โดยผู้กระทำมิได้มีความรับผิดทางแพ่งและมิได้กระทำความผิดฐานอื่นร่วมด้วย

---

[115] ตามมาตรา 10 ที่ถูกแก้ไขโดยมาตรา 4 ของ Republic Act No. 11449

[116] ประมาณ 320,324 บาท (อัตราแลกเปลี่ยนวันที่ 10 ธันวาคม 2563)

แต่ทั้งนี้หากผู้กระทำความผิดได้กระทำความผิดหลายฐานหรือพยายามกระทำความผิดในฐานอื่นๆ อีก อัตราโทษโทษจะเพิ่มขึ้นเป็นจำคุกไม่น้อยกว่า 12 ปีไปจนถึง 20 ปี และปรับเป็นจำนวน 800,000 เปโซฟิลิปปินส์[117] หรือสองเท่าของมูลค่าของประโยชน์ที่ผู้กระทำความผิดได้รับขึ้นอยู่กับว่าจำนวนใดจะมากกว่ากัน

หากเป็นการแฮกระบบของธนาคาร การสกิมมิ่งบัตรตั้งแต่ 50 ใบขึ้นไป หรือส่งผลกระทบต่อบัญชีธนาคารออนไลน์ตั้งแต่ 50 บัญชีขึ้นไป สาธารณรัฐฟิลิปปินส์จะถือว่าเป็นการก่อวินาศกรรมทางเศรษฐกิจต่อประเทศ ซึ่งมีอัตราโทษจำคุกตลอดชีวิตและปรับเป็นจำนวน 1,000,000 เปโซฟิลิปปินส์[118] แต่ไม่เกินกว่า 5,000,000 เปโซฟิลิปปินส์[119]

ดังนั้นจะเห็นได้ว่านอกจากสาธารณรัฐฟิลิปปินส์จะได้กำหนดบทลงโทษให้มีอัตราโทษจำคุกและปรับอย่างรุนแรงขึ้นอยู่กับประโยชน์ที่ผู้กระทำความผิดได้รับอันเป็นความพิเศษของกฎหมายของสาธารณรัฐฟิลิปปินส์แล้ว ยังกำหนดให้มีการลงโทษที่ถือว่าเป็นภัยต่อระบบเศรษฐกิจของประเทศโดยระบุหลักเกณฑ์ไว้อย่างชัดเจนและมีอัตราโทษที่สูงถึงจำคุกตลอดชีวิตและปรับเป็นจำนวนหลายล้านเปโซฟิลิปปินส์อีกด้วย

การที่สาธารณรัฐฟิลิปปินส์ได้มีการแก้ไขเพิ่มเติมบทบัญญัติของพระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 ให้มีความเฉพาะเจาะจงกับลักษณะของการกระทำความผิดและมีบทบัญญัติที่หลากหลายเพื่อใช้กับการกระทำความผิดอันเกี่ยวกับการดึงข้อมูลจากบัตรตามมาตราต่างๆ ตามที่ได้อธิบายมาแล้ว ทั้งยังเพิ่มอัตราโทษให้มีการลงโทษที่รุนแรงมากยิ่งขึ้น เป็นการแสดงให้เห็นว่าสาธารณรัฐฟิลิปปินส์มีความใส่ใจและมุ่งมั่นที่จะแก้ไขปัญหาอันเกี่ยวกับการกระทำความผิดที่เกิดขึ้นในปัจจุบันอย่างจริงจัง เพราะบทบัญญัติกฎหมายตามพระราชบัญญัติฉบับเดิมนั้นอาจไม่ครอบคลุมถึงลักษณะการกระทำความผิดได้อย่างครบถ้วนซึ่งจะเป็นช่องทางให้อาชญากรกระทำการโดยไม่มีความผิดตามกฎหมายได้

[117] ประมาณ 512,518 บาท (อัตราแลกเปลี่ยนวันที่ 10 ธันวาคม 2563)

[118] ประมาณ 640,648 บาท (อัตราแลกเปลี่ยนวันที่ 10 ธันวาคม 2563)

[119] ประมาณ 3,203,240 บาท (อัตราแลกเปลี่ยนวันที่ 10 ธันวาคม 2563)

ตารางที่ 10 เปรียบเทียบบทบัญญัติของกฎหมายสาธารณรัฐฟิลิปปินส์ที่เกี่ยวข้องกับการดึงข้อมูลจากบัตร

บทบัญญัติ	การกระทำ	วัตถุแห่งการกระทำ	เจตนา	โทษ
พระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012				
มาตรา 4(a)(1)	เข้าถึง (Access) (หมายถึง การดึงข้อมูลมา) โดยผิดกฎหมาย	อุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ (Computer data storage devices)	เจตนาธรรมดา	จำคุกตั้งแต่ 6 ปีกับหนึ่งวัน ถึง 20 ปี หรือปรับเป็นอย่างน้อย 200,000 ถึง 500,000 เปโซฟิลิปปินส์จนถึงจำนวนที่สมน้ำสมเนื้อกับความเสียหายที่เกิดขึ้น หรือทั้งจำทั้งปรับ
มาตรา 4(b)(3)	ขโมยข้อมูลประจำตัว (Identity Theft) โดยไม่มีสิทธิ	ข้อมูลประจำตัวของบุคคล (Identifying information)	เจตนาเข้ายึดถือ (Acquisition) ใช้ โอน ครอบครอง เปลี่ยนแปลงหรือลบ ข้อมูลประจำตัวของบุคคลอื่น	จำคุกตั้งแต่ 6 ปีกับหนึ่งวัน ถึง 12 ปี หรือปรับเป็นอย่างน้อย 200,000 เปโซฟิลิปปินส์จนถึงจำนวนที่สมน้ำสมเนื้อกับความเสียหายที่เกิดขึ้น หรือทั้งจำทั้งปรับ

บทบัญญัติ	การกระทำ	วัตถุแห่งการกระทำ	เจตนา	โทษ
พระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 ที่ได้แก้ไขเพิ่มเติมแล้ว				
มาตรา 9(q)	สกิมมิ่ง คัดลอก และได้รับไปซึ่งข้อมูลในบัตร	บัตรเครดิต บัตรชำระเงิน บัตรเดบิต	เจตนาในการเข้าถึงบัญชีหรือจัดการบัญชี	จำคุกไม่น้อยกว่า 10 ปี แต่ไม่เกิน 12 ปี หรือจำคุกตลอดชีวิต[120] และปรับเป็นจำนวน 5,000,000 เปโซ ฟิลิปปินส์ หรือสองเท่าของมูลค่าของประโยชน์ที่ผู้กระทำความผิดได้รับ
มาตรา 9(k)	มีในครอบครองโดยมิได้รับอนุญาติ	อุปกรณ์ในการเข้าถึง (Access Device)	เจตนาธรรมดา	จำคุกไม่น้อยกว่า 6 ปี แต่ไม่เกิน 10 ปี หรือจำคุกตลอดชีวิต และปรับเป็นจำนวน 5,000,000 เปโซ ฟิลิปปินส์ หรือสองเท่าของมูลค่าของประโยชน์ที่ผู้กระทำความผิดได้รับ
มาตรา 9(s)	เข้าถึง (Accessing) ในลักษณะเป็นการฉ้อโกง	บัญชีธนาคาร ออนไลน์ บัญชีบัตรเครดิต บัญชีเอทีเอ็ม บัญชีบัตรเดบิต	เจตนาธรรมดา	
มาตรา 9(t)	แฮก (Hacking) โดยไม่ได้รับอนุญาต	ข้อมูลในระบบคอมพิวเตอร์ เซิฟเวอร์ ระบบข้อมูลหรือระบบสื่อสาร	เพื่อทำการทุจริต แก้ไข ขโมย หรือทำลาย	

[120] ในกรณีที่เป็นการแฮกระบบของธนาคาร หรือ สกิมมิ่งบัตรชำระเงิน ตั้งแต่ 50 ใบขึ้นไป หรือ การกระทำความผิดนั้นกระทบบัญชีธนาคาร บัตรเครดิต บัตรชำระเงินหรือบัตรเดบิต ตั้งแต่ 50 บัญชีหรือใบขึ้นใบ

ดังนั้นในเรื่องการดึงข้อมูลจากบัตรนี้ สามารถใช้กฎหมายหลายของสาธารณรัฐฟิลิปปินส์ได้ ทั้งพระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012 (Cybercrime Prevention Act of 2012) และพระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 (Access Devices Regulation Act of 1998) ที่ได้ทำการแก้ไขเพิ่มเติมแล้ว ขึ้นอยู่กับว่าวัตถุแห่งการกระทำความผิดนั้นจะอยู่ในลักษณะใด หากเป็นการกระทำความผิดต่อบัตรชำระเงิน บัตรเครดิต บัตรเดบิต รวมถึงบัตรที่อยู่ในรูปของข้อมูลที่ทางธนาคารมิได้มีการออกเป็นตัวบัตรที่เป็นเอกสารให้ อันมีการใช้งานบัตรนั้นโดยมีวัตถุประสงค์เพื่อทำธุรกรรมทางการเงินโดยเฉพาะแล้วก็นำพระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 ที่ได้แก้ไขเพิ่มเติมมาบังคับใช้ โดยมีบทบัญญัติหลักคือมาตรา 9(q) และมีบทบัญญัติอื่นๆ คือมาตรา 9(k) (s) และ (t) ในการปรับใช้ แต่ถ้าหากเป็นการกระทำความผิดต่อบัตรอื่นๆ ที่ไม่ได้มีวัตถุประสงค์เพื่อทำธุรกรรมทางการเงิน เช่น บัตรประจำตัวพนักงาน บัตรประจำตัวประชาชน ซึ่งบัตรนั้นเองเนื่องจากได้บรรจุข้อมูลทางอิเล็กทรอนิกส์อันถือว่าเป็นอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ในรูปแบบหนึ่งเช่นกัน ก็จะนำพระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012 มาตรา 4(a) มาปรับใช้ สาธารณรัฐฟิลิปปินส์จึงนับว่าเป็นประเทศที่มีการบัญญัติกฎหมายให้ครอบคลุมในเรื่องการดึงข้อมูลจากบัตรได้อย่างดีและครบถ้วน

อย่างไรก็ตามก็มีนักกฎหมายของสาธารณรัฐฟิลิปปินส์บางท่านแสดงความเห็นว่าพระราชบัญญัติของสาธารณรัฐฟิลิปปินส์ทั้งสองฉบับนั้นมีความคล้ายคลึงกันและสามารถใช้ทดแทนกันได้ โดยสามารถใช้พระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012 แต่เพียงอย่างเดียวในการลงโทษผู้กระทำความผิดได้ การแก้ไขเพิ่มเติมพระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 โดยการเพิ่มฐานความผิดที่ซ้ำซ้อนและเพียงแต่เพิ่มโทษจะทำให้บทบัญญัติกฎหมายมีความฟุ่มเฟือยจนเกินไปได้[121]

[121] Abet Dela Cruz, "Was Access Devices Regulation Act Reboot Really Necessary?" [Online], Accessed: 10 October 2020. Available from: https://www.manilatimes.net/2019/10/02/opinion/columnists/topanalysis/was-access-devices-regulation-act-reboot-really-necessary/624758/.

4.4 เครือรัฐออสเตรเลีย

4.4.1 พระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001 (Cybercrime Act 2001)

พระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001 (Cybercrime Act 2001) หรือในชื่อเต็มคือ พระราชบัญญัติแก้ไขกฎหมายในความผิดอันเกี่ยวกับคอมพิวเตอร์และเพื่อวัตถุประสงค์อื่นๆ (An Act to amend the law relating to computer offences, and for other purposes) เป็นกฎหมายของเครือรัฐออสเตรเลีย ซึ่งได้ประกาศใช้เมื่อวันที่ 1 เมษายน 2545 จากการเสนอร่างกฎหมาย (Cybercrime Bill 2001) ของคณะกรรมการยกร่างประมวลกฎหมายอาญา (Model Criminal Code Officers Committee) ผ่านอัยการสูงสุดของออสเตรเลีย (Attorney-General of Australia) ในเดือนมิถุนายน ค.ศ. 2001 ซึ่งได้รับอิทธิพลจากพระราชบัญญัติการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Misuse Act 1990) ของประเทศอังกฤษ อันเป็นต้นแบบในการยกร่างกฎหมายเพื่อพัฒนากฎหมายของเครือรัฐออสเตรเลียโดยได้เพิ่มเติมบทบัญญัติที่มีลักษณะเฉพาะบางประการอันเป็นรูปแบบเฉพาะของพระราชบัญญัติฉบับนี้ขึ้น[122] เพราะความก้าวหน้าทางเทคโนโลยีที่มีความรวดเร็วอันส่งผลต่อรูปแบบของการกระทำความผิดที่พัฒนาขึ้นจนเกินกว่าที่กฎหมายอาญาฉบับเก่าของเครือรัฐออสเตรเลียจะใช้บังคับได้ (Criminal Code Act 1995) และจากเหตุการณ์โจมตี 11 กันยายน (11 September 2001) ในประเทศสหรัฐอเมริกาที่มีการโจมตีโดยปฏิเสธการให้บริการ (Denial of Service) ต่อระบบการสื่อสารและการเพิ่มขึ้นของการกระทำความผิดทางคอมพิวเตอร์ของเครือรัฐออสเตรเลียที่มากกว่าสหรัฐอเมริกาถึงสองเท่าซึ่งมีต้นทางการโจมตีมาจากภายนอกประเทศ กฎหมายของเครือรัฐออสเตรเลียจึงมาถึงจุดที่ต้องมีการแก้ไข[123] เพื่อปกป้องความปลอดภัย ความน่าเชื่อถือและความสมบูรณ์ของข้อมูลคอมพิวเตอร์และการสื่อสารทางอิเล็กทรอนิกส์ในประเทศ โดยให้อำนาจหน่วยงานบังคับใช้กฎหมายของรัฐบาลกลางในการตรวจสอบและดำเนินคดีกับกลุ่มที่ใช้อินเตอร์เน็ตในการวางแผนและโจมตีทางไซเบอร์ (Cyberattack) เช่น การแฮก การแพร่กระจายไวรัสที่อาจไปรบกวนการทำงานภาคการเงินและการอุตสาหกรรมของรัฐบาลกลางของประเทศอย่างจริงจัง[124]

---

[122] Parliament of Australia, "Cybercrime Bill 2001" [Online], Accessed: 12 October 2020. Available from: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd0102/02bd048.

[123] Andrew Michael Boulton, "Synopsis of the Cybercrime Act 2001" [Online], Accessed: 12 October 2020. Available from: https://www.giac.org/paper/gsec/4017/synopsis-cybercrime-act-2001/106427.

[124] Wikia.org, "Cybercrime Act 2001" [Online], Accessed: 12 October 2020. Available from: https://itlaw.wikia.org/wiki/Cybercrime_Act_2001.

พระราชบัญญัติฉบับนี้มีบทบัญญัติที่เกี่ยวข้องต่อการศึกษาวิจัยในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ดังต่อไปนี้

4.4.1.1 การเข้าถึง เปลี่ยนแปลง หรือทำให้เสียซึ่งข้อมูลโดยไม่มีอำนาจโดยเจตนาที่จะกระทำความผิดอย่างร้ายแรง

การเข้าถึง เปลี่ยนแปลง หรือทำให้เสียซึ่งข้อมูลโดยไม่มีอำนาจ โดยเจตนาที่จะกระทำความผิดอย่างร้ายแรง (Unauthorised access, modification or impairment with intent to commit a serious offence) อยู่ในมาตรา 477.1 ซึ่งบัญญัติว่า

มาตรา 477.1 บัญญัติว่า “บุคคล (A person) จะมีความผิด หากทำให้เกิด (a)(i) การเข้าถึงข้อมูลที่อยู่ในคอมพิวเตอร์ (Access to data held in computer) โดยไม่มีอำนาจ หรือ (a)(ii) การแก้ไขเปลี่ยนแปลงข้อมูลที่อยู่ในคอมพิวเตอร์โดยไม่มีอำนาจ หรือ (a)(iii) การทำให้เสียซึ่งการสื่อสารทางอิเล็กทรอนิกส์ในเครื่องคอมพิวเตอร์โดยไม่มีอำนาจ (b) ซึ่งเกิดจากบริการโทรคมนาคม (c) โดยบุคคลนั้นรู้ว่าตนไม่มีอำนาจ (d) โดยมีเจตนาที่จะกระทำหรืออำนวยความสะดวกให้ตนเองหรือผู้อื่น ในการกระทำความผิดร้ายแรงต่อกฎหมายของประเทศ รัฐ หรือเขตแดน อันเกิดจากการเข้าถึง เปลี่ยนแปลง หรือทำให้เสียนั้น”

ลักษณะของกระทำความผิดที่เกี่ยวข้องกับการดึงข้อมูลจากบัตร ก็คือการเข้าถึงข้อมูลที่อยู่ในคอมพิวเตอร์ (Access to data held in computer) โดยไม่มีอำนาจ ที่กำหนดไว้ในวรรค (a)(i) ของมาตราดังกล่าว ซึ่งตามมาตรา 476.1 ของพระราชบัญญัติฉบับนี้ได้ให้คำนิยามของการเข้าถึงข้อมูลที่อยู่ในคอมพิวเตอร์ว่าให้หมายถึง “(b) การคัดลอก (Copying) หรือเคลื่อนย้าย (Moving) ข้อมูลไปยังที่อื่นภายในคอมพิวเตอร์หรือไปยังอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ (Data storage device)” และมาตราดังกล่าวยังกำหนดเพิ่มเติมลงไปอีกโดยให้นิยามคำว่า ข้อมูลที่อยู่ในคอมพิวเตอร์ (Data held in computer) ให้รวมถึง “ข้อมูลที่อยู่ในอุปกรณ์จัดเก็บข้อมูล (Data storage device) ที่สามารถถอดออกไปได้ ในขณะที่ข้อมูลนั้นได้อยู่ในคอมพิวเตอร์” ดังนั้นลักษณะของการกระทำการเข้าถึง (Access) อันเป็นความผิดตามมาตรานี้จึงแบ่งได้เป็น 2 ลักษณะคือ

(ก) เป็นการคัดลอก หรือเคลื่อนย้าย ข้อมูลที่อยู่ในคอมพิวเตอร์ไปยังที่อื่นภายในคอมพิวเตอร์หรือไปยังอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์

กรณีแรก เป็นกรณีที่ใช้กับบัตรที่อยู่ในรูปแบบของข้อมูลในคอมพิวเตอร์ที่ผู้ออกมิได้ออกตัวบัตรให้แก่ผู้มีสิทธิใช้ เช่น เป็นรหัสตัวเลข หมายเลขบัญชี ดังนั้นข้อมูลของบัตรดังกล่าวจะถูก

ดึงได้เพียงวิธีการคัดลอกหรือเคลื่อนย้ายข้อมูลของบัตรนั้นไปยังที่อื่นหรือหน่วยความจำอื่นที่เป็นเครื่องคอมพิวเตอร์หรือได้บันทึกลงในอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ เช่น บันทึกข้อมูลบัตรนั้นลงในแผ่นดิสก์

(ข) เป็นการคัดลอก หรือเคลื่อนย้าย ข้อมูลที่อยู่ในอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูล (Data storage device) ภายในคอมพิวเตอร์หรือไปยังอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์

กรณีที่สอง เป็นกรณีที่ใช้กับบัตรที่มีการออกเป็นตัวบัตรที่เป็นเอกสารหรือวัตถุอื่นใดให้ เพราะในมาตรา 476.1 ได้ให้นิยามคำว่า อุปกรณ์ที่ใช้ในการจัดเก็บข้อมูล (Data storage device) หมายถึง “สิ่งใดก็ตาม (เช่น แผ่นดิสก์ หรือไฟล์เซิฟเวอร์) ที่ได้บรรจุ หรือออกแบบมาเพื่อบรรจุข้อมูลที่ใช้โดยเครื่องคอมพิวเตอร์” บัตรที่มีการออกเอกสารหรือวัตถุอื่นใดให้ตามสภาพซึ่งได้บรรจุข้อมูลในแหล่งบันทึกในบัตรและข้อมูลในบัตรนั้นก็เป็นข้อมูลที่ต้องใช้กับเครื่องคอมพิวเตอร์ด้วย บัตรนั้นจึงถือเป็นอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลด้วยตามคำนิยามในมาตรา 476.1 แต่จะเป็นการกระทำความผิดตามมาตรานี้ก็ต่อเมื่อได้กระทำต่อบัตรที่เป็นข้อมูลที่อยู่ในคอมพิวเตอร์ หมายถึงได้กระทำการคัดลอกหรือเคลื่อนย้ายข้อมูลของบัตรในขณะที่บัตรนั้นทำการเชื่อมต่อกับเครื่องคอมพิวเตอร์อยู่เท่านั้น เช่น การดึงข้อมูลออกจากบัตรในขณะที่บัตรถูกเสียบเข้าไปในเครื่องเอทีเอ็ม ซึ่งหากบัตรนั้นมิได้ทำการเชื่อมต่ออยู่กับเครื่องคอมพิวเตอร์ แม้บัตรจะเป็นอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลก็ตาม แต่ก็ไม่ใช่ข้อมูลที่อยู่ในคอมพิวเตอร์อันเป็นวัตถุแห่งการกระทำตามมาตรานี้

การกระทำความผิดตามมาตรานี้ผู้กระทำต้องมีเจตนาที่จะกระทำหรืออำนวยความสะดวกให้ตนเองหรือผู้อื่น ในการกระทำความผิดร้ายแรงต่อกฎหมายด้วย ซึ่งความผิดร้ายแรงในมาตรานี้ระบุว่าคือ ความผิดที่มีอัตราโทษจำคุกตลอดชีวิตหรือหรือจำคุกตั้งแต่ 5 ปีขึ้นไป โดยไม่จำต้องรู้ว่าความผิดที่จะกระทำนั้นเป็นความผิดร้ายแรง

ดังนั้นบทบัญญัติตามมาตรา มาตรา 477.1 นี้จึงบังคับได้แก่การกระทำความผิดในบางลักษณะเท่านั้นดังที่กล่าวมาแล้ว กฎหมายของเครือรัฐออสเตรเลียจึงได้กำหนดให้มีบทบัญญัติอื่นอีกเพื่อให้ครอบคลุมถึงการกระทำความผิดทั้งหมด ดังจะกล่าวต่อไป

4.4.1.2 การครอบครองหรือควบคุมข้อมูลโดยเจตนาที่จะกระทำความผิดทางคอมพิวเตอร์

การครอบครองหรือควบคุมข้อมูลโดยเจตนาที่จะกระทำความผิดทางคอมพิวเตอร์ (Possession or control of data with intent to commit a computer offence) อยู่ในมาตรา 478.3 ซึ่งบัญญัติว่า

มาตรา 478.3 บัญญัติว่า “บุคคล (A person) จะมีความผิดหาก (a) ครอบครองหรือควบคุม (Possession or control of) ข้อมูล และ (b) โดยมีเจตนาจะใช้เพื่อตนเองหรือผู้อื่นในการ (i) กระทำความผิดในหมวดมาตรา 477 หรือ (ii) อำนวยความสะดวกในการกระทำความผิดดังกล่าว”

โดยการครอบครองข้อมูลนั้น มาตรานี้ให้รวมถึง การครอบครองเครื่องคอมพิวเตอร์หรืออุปกรณ์ในการจัดเก็บข้อมูล (Data storage device) ที่ได้บรรจุข้อมูลเหล่านั้นไว้ด้วย

การกระทำความผิดตามมาตรานี้คือ การครอบครองหรือควบคุมข้อมูล (Data) รวมไปถึงการครอบครองเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลเหล่านั้นไว้ด้วย ซึ่งการครอบครองข้อมูลคือผลจากการดึงข้อมูลจากบัตรโดยวิธีการต่างๆ นั่นเอง ส่วนการครอบครองเครื่องคอมพิวเตอร์หรืออุปกรณ์ในการจัดเก็บข้อมูลนั้นมาตราดังกล่าวมิได้กำหนดว่าต้องเป็นการครอบครองโดยมีอำนาจหรือไม่ อาจเป็นการครอบครองโดยมีอำนาจ เช่น เป็นเจ้าของเครื่องคอมพิวเตอร์ หรือเป็นการครอบครองโดยไม่มีอำนาจก็ได้ เช่น ลักบัตรของผู้อื่นอันเป็นอุปกรณ์ในการจัดเก็บข้อมูลคอมพิวเตอร์มาใช้ แต่การครอบครองหรือควบคุมดังกล่าว ผู้กระทำต้องมีเจตนาที่จะนำไปใช้ในกระทำความผิดในหมวดมาตรา 477 ของพระราชบัญญัติฉบับนี้ด้วย อันหมายถึง ต้องการที่จะทำให้เกิดความผิดอันร้ายแรงที่เกี่ยวกับคอมพิวเตอร์ เช่น เจตนาจะนำข้อมูลที่ครอบครองนั้นไปเข้าถึง เปลี่ยนแปลง หรือทำให้เสียซึ่งข้อมูลที่อยู่ในคอมพิวเตอร์ ตัวอย่างเช่น นาย ก ได้ครอบครองข้อมูลในบัตรเอทีเอ็มของนาย ข อันเกิดจากการกระทำการดึงข้อมูลจากบัตร เพื่อที่จะนำข้อมูลที่ครอบครองนั้นไปใช้ทำบัตรปลอมแล้วนำบัตรปลอมไปใช้ในการเข้าถึงข้อมูลในเครื่องกดเงินอัตโนมัติซึ่งเป็นเครื่องคอมพิวเตอร์รูปแบบหนึ่ง ดังนี้การครอบครองข้อมูลดังกล่าวของนาย ก ย่อมจะเป็นความผิดตามมาตรานี้

แต่อย่างไรก็ตามการครอบครองข้อมูลตามมาตรานี้ ผู้ครอบครองอาจมีอำนาจในการครอบครองก็ได้ เช่น เป็นเจ้าของข้อมูล ดังนั้นจึงไม่อาจใช้มาตราดังกล่าวกับการกระทำความผิดในลักษณะการดึงข้อมูลจากบัตรได้ แม้ว่าจะบุคคลนั้นจะครอบครองข้อมูลดังกล่าวโดยมิได้มีอำนาจบุคคลนั้นก็อาจจะไม่ใช่ผู้กระทำการดึงข้อมูลจากบัตรนั้นก็ได้ ดังนั้นเพื่อให้กฎหมายมีความครอบคลุม

กับลักษณะของความผิดที่เกิดขึ้น พระราชบัญญัติฉบับนี้จึงได้มีบทบัญญัติแก่การกระทำความผิดเกี่ยวกับการดึงข้อมูลอันเป็นการเฉพาะ อันจะกล่าวต่อไป

4.4.1.3 การทำ จัดหา หรือได้รับข้อมูลโดยเจตนาที่จะกระทำความผิดทางคอมพิวเตอร์

การทำ จัดหา หรือได้รับข้อมูลโดยเจตนาที่จะกระทำความผิดทางคอมพิวเตอร์ (Producing, supplying or obtaining data with intent to commit a computer offence) อยู่ในมาตรา 478.4 ซึ่งบัญญัติว่า

มาตรา 478.4 บัญญัติว่า “บุคคล (A person) จะมีความผิด หาก (a) บุคคลนั้นได้ทำ จัดหาหรือได้รับ (Obtain) ข้อมูล (Data) และ (b) ด้วยเจตนาที่จะใช้ข้อมูลนั้นโดยตนเองหรือผู้อื่นในการ (i) กระทำความผิดต่อหมวดมาตรา 447 หรือ (ii) อำนวยความสะดวกในการกระทำความผิดดังกล่าว”

โดยมาตราดังกล่าวได้กำหนดเพิ่มเติมลงไปอีกว่า ข้อมูลที่ได้ถูกทำ จัดหาหรือได้รับไปนั้น หมายถึง ข้อมูลที่ได้ถูกเก็บไว้หรือบรรจุอยู่ในคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการจัดเก็บข้อมูล (Data storage device)

มาตรานี้เป็นบทบัญญัติที่บัญญัติขึ้นมาเฉพาะเพื่อใช้กับการกระทำความผิดในการได้รับ (Obtain) ข้อมูลที่ได้ถูกเก็บไว้หรือบรรจุในคอมพิวเตอร์หรือข้อมูลที่ถูกเก็บไว้ในอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูล ในกรณีที่ไม่สามารถใช้มาตรา 477.1 หรือมาตรา 478.3 ในการลงโทษผู้กระทำความผิดได้ ซึ่งเป็นการบัญญัติกฎหมายให้ครอบคลุมการกระทำความผิดในเรื่องการดึงข้อมูลจากบัตรทั้งหมด เพราะคำว่าข้อมูล (Data) ในมาตรา 476.1 นั้นได้ให้นิยามว่า หมายถึง “(a) ข้อมูลไม่ว่าจะอยู่ในรูปลักษณะใดก็ตามแต่” ดังนั้นข้อมูลของบัตรที่มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ที่อยู่ในคอมพิวเตอร์ หรือข้อมูลของบัตรที่ได้มีการออกเอกสารหรือวัตถุอื่นใดให้ที่ได้บันทึกไว้ในแหล่งบันทึกข้อมูลของบัตร เช่น ในแถบแม่เหล็กหรือในชิป หรือเป็นข้อมูลบนพื้นผิวของบัตรใบนั้น จึงเป็นข้อมูลที่อยู่ในบัตรซึ่งถือเป็นอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลด้วย ข้อมูล (Data) ของบัตรเหล่านี้ทุกรูปแบบก็ย่อมที่จะได้รับความคุ้มครองตามมาตรานี้ด้วยกันทั้งสิ้น ซึ่งหากมีการกระทำการดึงข้อมูลจากบัตรก็ย่อมเป็นการได้รับ (Obtain) ข้อมูลนั้นไปอันจะเป็นความผิดตามมาตรานี้ได้ แต่ผู้กระทำความผิดตามมาตรานี้จะต้องมีเจตนาที่จะใช้ข้อมูลนั้นในการกระทำความผิดหรืออำนวยความสะดวกในการกระทำความผิดต่อหมวดมาตรา 477 ของพระราชบัญญัติฉบับนี้ด้วย อันหมายถึง ต้องการที่จะทำให้เกิด

ความผิดอันร้ายแรงที่เกี่ยวกับคอมพิวเตอร์ เช่น เจตนาจะนำข้อมูลที่ได้รับมานั้นไปเข้าถึง เปลี่ยนแปลง หรือทำให้เสียซึ่งข้อมูลที่อยู่ในคอมพิวเตอร์ด้วย ตัวอย่างเช่น นาย ก ได้รับข้อมูลบัตรของนาย ข จากการกระทำการดึงข้อมูลบัตรด้วยวิธีสกิมมิ่งเพื่อจะนำข้อมูลบัตรนั้นไปทำบัตรปลอม แล้วนำบัตรปลอมไปใช้ในการเข้าถึงข้อมูลในเครื่องในเครื่องกดเงินอัตโนมัติซึ่งเป็นเครื่องคอมพิวเตอร์รูปแบบหนึ่ง การได้รับข้อมูลบัตรของนาย ก นั้นจึงเป็นความผิดตามมาตรานี้

อัตราโทษตามมาตราต่างๆ ที่ได้กล่าวมาแล้วนั้น มีดังนี้

การเข้าถึง เปลี่ยนแปลง หรือทำให้เสียซึ่งข้อมูลโดยไม่มีอำนาจ โดยเจตนาที่จะกระทำความผิดอย่างร้ายแรง ในมาตรา 477.1 มีอัตราโทษจำคุกตั้งแต่ 5 ปีขึ้นไปถึงจำคุกตลอดชีวิต

การครอบครองหรือควบคุมข้อมูลโดยเจตนาที่จะกระทำความผิดทางคอมพิวเตอร์ในมาตรา 478.3 และ การทำ จัดหา หรือได้รับข้อมูลโดยเจตนาที่จะกระทำความผิดทางคอมพิวเตอร์ในมาตรา 478.4 มีอัตราโทษจำคุก 3 ปี

จะเห็นได้ว่าโทษของเครือรัฐออสเตรเลียจะมีเพียงแต่โทษจำคุกเท่านั้น โดยไม่มีการลงโทษปรับเหมือนประเทศอื่นๆ ทั้งในหลายๆ มาตรา เช่น มาตรา 478.3 และมาตรา 478.4 นี้ซึ่งกฎหมายไม่ได้ถือว่าเป็นการกระทำความผิดอย่างร้ายแรง (Serious offence) ก็เป็นอัตราโทษจำคุกที่ตายตัว ไม่มีขั้นต่ำหรือขั้นสูงให้ศาลได้ใช้ดุลพินิจในการพิจารณากำหนดระยะเวลาของโทษจำคุกดังกล่าวได้เลย

ข้อสังเกต แม้พระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001 ฉบับนี้จะถูกมองว่าเป็นการพัฒนากฎหมายที่มีความสำคัญและมีแนวทางที่ถูกต้องในการดำเนินคดีและป้องกันการก่ออาชญากรรมทางไซเบอร์ แต่ก็มีความเห็นของผู้เชี่ยวชาญทางคอมพิวเตอร์และนักกฎหมายบางท่านเห็นว่าความผิดที่เสนอนั้นกว้างจนเกินไปและไม่อาจใช้ได้อย่างเฉพาะเจาะจงกับการกระทำความผิดที่เกิดขึ้นจริง อีกทั้งมีคำจำกัดความบางคำที่กว้างจนเกินไปซึ่งเป็นหน้าที่ของศาลที่จะต้องตีความต่อไป[125]

[125] Andrew Michael Boulton, “SYNOPSIS OF THE CYBERCRIME ACT 2001” [Online], Accessed: 12 October 2020. Available from: https://www.giac.org/paper/gsec/4017/synopsis-cybercrime-act-2001/106427.

4.4.2 พระราชบัญญัติแก้ไขกฎหมายอาชญากรรม (ความผิดด้านโทรคมนาคมและมาตรการอื่นๆ)(ฉบับที่ 2) ค.ศ. 2004 (Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004)

พระราชบัญญัติแก้ไขกฎหมายอาชญากรรม (ความผิดด้านโทรคมนาคมและมาตรการอื่นๆ) (ฉบับที่ 2) ค.ศ. 2004 (Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004) หรือในชื่อเต็มคือพระราชบัญญัติแก้ไขประมวลกฎหมายอาญา ค.ศ. 1995 และเพื่อวัตถุประสงค์อื่นที่เกี่ยวข้อง (An Act to amend the Criminal Code Act 1995, and for related purposes) เป็นกฎหมายของเครือรัฐออสเตรเลีย ซึ่งได้ประกาศใช้เมื่อวันที่ 31 สิงหาคม 2547 จากการยกเลิกความผิดเกี่ยวกับโทรคมนาคมในพระราชบัญญัติอาชญากรรม ค.ศ. 1995 (Criminal Code Act 1995) และบัญญัติความผิดใหม่ที่เกี่ยวข้องกับการใช้เครือข่ายโทรคมนาคมหรือการใช้บริการเครือข่ายต่างๆ เช่น อินเตอร์เน็ต อีเมล โทรศัพท์มือถือ ให้ได้รับความคุ้มครองมากขึ้นรวมถึงเรื่องอื่นๆ หนึ่งในนั้นคือการไม่สุจริตเกี่ยวกับการซื้อขายทางการเงิน (Dishonest financial dealing) โดยการเพิ่มหมวดความผิดอันเกี่ยวกับข้อมูลทางการเงินของบุคคล (Financial information offences) เป็นลักษณะที่ 10.8 จากการพิจารณารายงานของคณะกรรมการยกร่างประมวลกฎหมายอาญา (Model Criminal Code Officers Committee) ในเรื่องความผิดที่เกี่ยวกับการสกิมมิ่งบัตรเครดิต (Credit Card Skiming Offence) ซึ่งสนับสนุนให้มีการบัญญัติกฎหมายเกี่ยวกับการได้รับหรือซื้อขายข้อมูลทางการเงินของบุคคลโดยไม่ปราศจากความยินยอม โดยคณะกรรมการดังกล่าวให้เหตุผลว่ากฎหมายของเครือรัฐออสเตรเลียที่ใช้บังคับอยู่ในขณะนั้นครอบคลุมเพียงการกระทำผิดในลักษณะการฉ้อโกง (Fraud) และการปลอมแปลง (Forgery) จากการสกิมมิ่งบัตรเครดิตหรือบัตรเดบิตเท่านั้น ยังไม่ครอบคลุมการกระทำความผิดที่เกี่ยวกับการสกิมมิ่งข้อมูลหรือครอบครองข้อมูลหรือการนำเข้าอุปกรณ์ในการสกิมมิ่งมาในประเทศ จึงจำเป็นต้องมีการแก้ไขเพิ่มเติมกฎหมายของเครือรัฐออสเตรเลียที่มีอยู่ให้ครอบคลุมการกระทำความผิดให้มากขึ้น[126]

พระราชบัญญัติฉบับนี้มีบทบัญญัติที่เกี่ยวข้องต่อการศึกษาวิจัยในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ อยู่ในมาตรา 480.4 อันเป็นการได้รับ (Obtaining) หรือซื้อขายแลกเปลี่ยน (Dealing in) ข้อมูลทางการเงินของบุคคล (Personal financial information) โดยมิชอบ ซึ่งบัญญัติไว้ดังนี้

---

[126] Parliament of Australia, "Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill 2004" [Online], Accessed: 13 October 2020. Available from: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd0405/05bd013.

มาตรา 480.4 บัญญัติว่า “บุคคล (A person) จะมีความผิด ถ้าบุคคลนั้น (a) ได้รับ (Obtain) หรือซื้อขายแลกเปลี่ยน (Deal in) ข้อมูลทางการเงินของบุคคล (Personal financial information) และ (b) โดยปราศจากความยินยอมจากบุคคลที่เกี่ยวข้องกับข้อมูลนั้น”

โดยมาตรา 480.1 ได้ให้คำนิยามไว้ดังนี้

“ได้รับ (Obtaining) ข้อมูลทางการเงินของบุคคล รวมถึง ครอบครอง (Possessing) หรือทำ (Making) ข้อมูลทางการเงินของบุคคลด้วย

ซื้อขายแลกเปลี่ยน (Dealing in) ข้อมูลทางการเงินของบุคคล รวมถึง จัดหา (Supplying) หรือ ใช้ (Using) ข้อมูลทางการเงินของบุคคลด้วย

ข้อมูลทางการเงินของบุคคล (Personal financial information) หมายถึง ข้อมูลที่เกี่ยวข้องกับบุคคลที่อาจนำไปใช้โดยลำพังหรือประกอบกับข้อมูลอื่นในการเข้าถึงเงิน (Funds) เครดิต (Credit) หรือประโยชน์ทางการเงินอื่น”

ดังนั้นการกระทำความผิดตามมาตรานี้ก็คือการได้รับ ทำ ครอบครอง ซื้อขายแลกเปลี่ยน จัดหา หรือใช้ข้อมูลทางการเงินของบุคคลอื่น โดยปราศจากความยินยอมจากบุคคลที่เกี่ยวข้องกับข้อมูลนั้น อันนำมาใช้กับเรื่องการดึงข้อมูลจากบัตรได้โดยตรง เพราะการได้รับ (Obtaining) ข้อมูลนั้นก็คือลักษณะของการดึงข้อมูลในรูปแบบต่างๆ ที่ผู้กระทำความผิดได้ใช้โดยไม่ว่าจะใช้วิธีการดึงข้อมูลในรูปแบบใด เช่น การสกิมมิ่ง การฟิตชิ่ง หรือการแฮกคอมพิวเตอร์ ก็ย่อมเป็นการได้รับข้อมูลทั้งสิ้น และพระราชบัญญัติดังกล่าวยังใช้เฉพาะแก่การกระทำความผิดที่เป็นข้อมูลทางการเงินของบุคคล อันหมายถึงข้อมูลใดๆ ก็ตามที่ใช้โดยลำพังหรือประกอบข้อมูลอื่นๆ ในการเข้าถึงเงิน เครดิตหรือประโยชน์ทางการเงินอื่น ซึ่งบัตรทุกประเภทไม่ว่าจะได้มีการออกเอกสารหรือวัตถุอื่นใดให้ที่มีข้อมูลไว้ภายในแหล่งบันทึกหรือพื้นผิวบนบัตรนั้น หรือเป็นบัตรที่มีเพียงแต่ข้อมูลโดยผู้ออกมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ด้วย หากบัตรนั้นใช้ในการดำเนินธุรกรรมทางการเงิน ข้อมูลต่างๆ ที่เกี่ยวข้องกับบัตรใบนั้นย่อมเป็นข้อมูลทางการเงินของบุคคลที่มีการกระทำความผิดตามมาตรานี้ได้[127] อาทิเช่น บัตรเอทีเอ็มเป็นบัตรที่บุคคลใช้ในการเข้าถึงเงินในเครื่องจ่ายเงินอัตโนมัติ ซึ่งข้อมูลในบัตรเอทีเอ็มนั้นต้องใช้ประกอบกับรหัสผ่านหกตัวอันเป็นข้อมูลอื่นในการใช้งาน หรือบัตรเครดิตที่ผู้ออก

---

[127] THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA, "Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004 Explanatory Memoranda" [Online], Accessed: 12 October 2020. Available from: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr2131_ems_c79a0bd1-87a4-42e4-be65-485ba6850273%22.

มิได้มีการออกบัตรให้ ก็ต้องอาศัยรหัสซีวีวี (CVV) อันเป็นข้อมูลอื่นในการใช้งาน บัตรเหล่านี้จึงถือเป็นข้อมูลทางการเงินของบุคคลที่หากมีการได้รับข้อมูลในบัตรไปโดยการดึงข้อมูลจากบัตรด้วยวิธีการใดก็ตามแล้ว ผู้กระทำย่อมจะมีความผิดตามมาตรานี้

การกระทำความผิดตามมาตรานี้มีอัตราโทษจำคุก 5 ปี ไม่มีโทษปรับและเป็นอัตราโทษที่ตายตัวมิได้มีอัตราโทษขั้นต่ำหรือขั้นสูงอันเปิดช่องให้ผู้พิพากษาได้ใช้ดุลพินิจในการกำหนดโทษได้

ตารางที่ 11 เปรียบเทียบบทบัญญัติของกฎหมายเครือรัฐออสเตรเลียที่เกี่ยวข้องกับการดึงข้อมูลจากบัตร

บทบัญญัติ	การกระทำ	วัตถุแห่งการกระทำ	เจตนา	โทษ
พระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001				
มาตรา 477.1	เข้าถึง (Access) (หมายถึง คัดลอก (Copying)) โดยไม่มีอำนาจ	ข้อมูลที่อยู่ในคอมพิวเตอร์ (Data held in computer) (รวมถึงข้อมูลที่อยู่ในอุปกรณ์จัดเก็บข้อมูล (Data storage device) ในขณะที่ข้อมูลนั้นได้อยู่ในคอมพิวเตอร์ด้วย)	จะกระทำหรืออำนวยความสะดวก ในการกระทำความผิดร้ายแรงต่อกฎหมาย	จำคุกตั้งแต่ 5 ปีขึ้นไปถึงจำคุกตลอดชีวิต
มาตรา 478.3	ครอบครองหรือควบคุม (Possession or control)	ข้อมูล (Data)	จะใช้หรืออำนวยความสะดวกในการกระทำผิดอันร้ายแรงที่เกี่ยวกับคอมพิวเตอร์	จำคุก 3 ปี
มาตรา 478.4	ได้รับ (Obtain)	ข้อมูล (Data)		จำคุก 3 ปี

บทบัญญัติ	การกระทำ	วัตถุแห่งการกระทำ	เจตนา	โทษ
พระราชบัญญัติแก้ไขกฎหมายอาชญากรรม (ความผิดด้านโทรคมนาคม และมาตรการอื่นๆ)(ฉบับที่ 2) ค.ศ. 2004				
มาตรา 480.4	ได้รับ (Obtain) โดยปราศจากความยินยอม	ข้อมูลทางการเงินของบุคคล (Personal financial information)	เจตนาธรรมดา	จำคุก 5 ปี

ดังนั้นในเรื่องการดึงข้อมูลออกจากบัตรนี้ สามารถใช้พระราชบัญญัติของเครือรัฐออสเตรเลียดังที่กล่าวมาแล้วในการลงโทษผู้กระทำความผิดได้ทั้งสองฉบับขึ้นอยู่กับว่าข้อมูลในบัตรนั้นเกี่ยวข้องกับอะไร โดยพระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001 (Cybercrime Act 2001) นั้น มุ่งเอาผิดกับการกระทำต่อบัตรใดๆ ในฐานะเป็นข้อมูลประเภทหนึ่ง ซึ่งไม่จำกัดว่าข้อมูลนั้นจะต้องอยู่ในคอมพิวเตอร์ แต่รวมถึงข้อมูลที่อยู่ในตัวบัตรที่มีการออกเอกสารหรือวัตถุอื่นใดให้อันเป็นอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ด้วย และยังเอาผิดกับการได้รับข้อมูลบัตรในทุกรูปแบบ โดยไม่คำนึงว่าจะได้มีการออกเอกสารหรือวัตถุอื่นใดให้หรือไม่ เพื่อให้บทบัญญัติของกฎหมายครอบคลุมลักษณะในการกระทำความผิดทั้งหมด ส่วนพระราชบัญญัติแก้ไขกฎหมายอาชญากรรม (ความผิดด้านโทรคมนาคมและมาตรการอื่นๆ)(ฉบับที่ 2) ค.ศ. 2004 (Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004) จะมุ่งเอาผิดกับกระทำต่อบัตรที่เป็นข้อมูลทางการเงินของบุคคล ซึ่งผู้ใช้ต้องใช้ข้อมูลบัตรดังกล่าวนั้นโดยลำพังหรือประกอบข้อมูลอื่นในการเข้าถึงเงินหรือประโยชน์ทางการเงิน เช่น บัตรเอทีเอ็ม บัตรเดบิต หรือบัตรเครดิต โดยกำหนดให้การได้รับข้อมูลของบัตรนั้นเป็นความผิดด้วย แม้ว่าในกฎหมายเดิมของประเทศ (Criminal Code Act 1995) จะมีกฎหมายที่เอาผิดกับเรื่องการสกิมมิ่งได้อยู่แล้ว แต่ด้วยการเล็งเห็นปัญหาความไม่ครอบคลุมของกฎหมายของคณะกรรมการยกร่างประมวลกฎหมายอาญา (Model Criminal Code Officers Committee) จึงทำให้กฎหมายของเครือรัฐออสเตรเลียมีการพัฒนาที่ต่อเนื่องเพื่อใช้บังคับกับการกระทำความผิดในรูปแบบใหม่ๆ อันอาศัยความก้าวหน้าทางเทคโนโลยีเป็นเครื่องมือในการกระทำความผิด เครือรัฐออสเตรเลียจึงเป็นประเทศที่มีการบัญญัติกฎหมายอันเกี่ยวกับการดึงข้อมูลจากบัตรได้อย่างดีและครบถ้วนอีกประเทศหนึ่ง

ข้อสังเกต แม้ว่าเครือรัฐออสเตรเลียจะยังไม่มีการบัญญัติความผิดที่เกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคล (Identity theft) อันอาจส่งผลให้การดึงข้อมูลส่วนบุคคลจะเป็นความผิดแยกออกมาเป็นอีกบทบัญญัติเฉพาะก็ตาม[128] แต่การดึงข้อมูลบัตรโดยที่ข้อมูลนั้นเข้าลักษณะของการเป็นข้อมูลส่วนบุคคลด้วยก็สามารถปรับใช้มาตรา 478.4 ข้างต้นเพื่อเอาผิดกับผู้กระทำได้ เพราะมาตราดังกล่าวนั้นคุ้มครองข้อมูล (Data) “ไม่ว่าจะอยู่ในรูปลักษณะใดก็ตามแต่”[129] จึงรวมถึงการดึงข้อมูลในทุกประเภท แต่การดึงข้อมูลส่วนบุคคลดังกล่าวจะเป็นความผิดได้นั้นผู้กระทำจะต้องมีเจตนาจะใช้หรืออำนวยความสะดวกในการกระทำผิดอันร้ายแรงที่เกี่ยวกับคอมพิวเตอร์ต่อไปด้วย

[128] The Australian Law Reform Commission, "Criminalising Identity Theft" [Online], Accessed: 29 October 2020. Available from: https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/12-identity-theft/criminalising-identity-theft/.

[129] คำว่าข้อมูล (Data) ในมาตรา 476.1(a)

บทที่ 5
บทวิเคราะห์เปรียบเทียบแนวทางในการนำกฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศมาปรับใช้ในประเทศไทย

ในบทที่ 5 นี้ ผู้วิจัยจะทำการวิเคราะห์ถึงการนำแนวทางของกฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศมาปรับใช้กับประเทศไทย ตลอดจนพิจารณาถึงข้อดี ข้อเสียและอุปสรรคอันอาจจะเกิดขึ้น ทั้งความเหมาะสมในการนำมาปรับใช้กับบริบทกฎหมายของประเทศไทยที่มีอยู่ ซึ่งจะแยกการวิเคราะห์ออกเป็นประเด็นต่างๆ อันได้แก่ การวิเคราะห์ถึงความจำเป็นในการบัญญัติให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นความผิดทางอาญาในประเทศไทย เมื่อได้พิจารณาถึงความจำเป็นแล้วต่อมาจะทำการวิเคราะห์ว่าจะบัญญัติความผิดดังกล่าวไว้ในกฎหมายระดับใดและบรรจุในกฎหมายฉบับใด อันนำไปสู่การวิเคราะห์ถึงรูปแบบในการบัญญัติกฎหมายเพื่อให้ต้องตามความประสงค์ที่จะแก้ไขปัญหาการขาดบทบัญญัติในการลงโทษ[1] ซึ่งสามารถจำแนกออกได้เป็นสองประเด็น คือ ประเด็นปัญหาคำว่า“บัตรอิเล็กทรอนิกส์” ตามมาตรา 1(14) แห่งประมวลกฎหมายอาญาเมื่อเทียบกับความคุ้มครองที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ของกฎหมายต่างประเทศ และประเด็นปัญหาการขาดบทบัญญัติอันเป็นการเฉพาะในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เทียบกับบทบัญญัติกฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ และสุดท้ายจะทำการวิเคราะห์ถึงกำหนดโทษและอัตราโทษตามแนวทางของกฎหมายไทยและกฎหมายต่างประเทศเพื่อพิจารณาถึงความสอดคล้องและความเหมาะสมในการกำหนดโทษที่จะลงแก่ผู้กระทำความผิดตามกฎหมายไทย ซึ่งการวิเคราะห์และเปรียบเทียบดังกล่าวจะนำมาสู่การแสวงหาแนวทางในการแก้ไขหรือเพิ่มเติมบทบัญญัติกฎหมายให้สมประสงค์ตามสมมติฐานของงานวิจัยฉบับนี้ต่อไป

5.1 พิจารณาถึงความจำเป็นในการบัญญัติให้การดึงข้อมูลบัตรอิเล็กทรอนิกส์เป็นความผิดทางอาญา

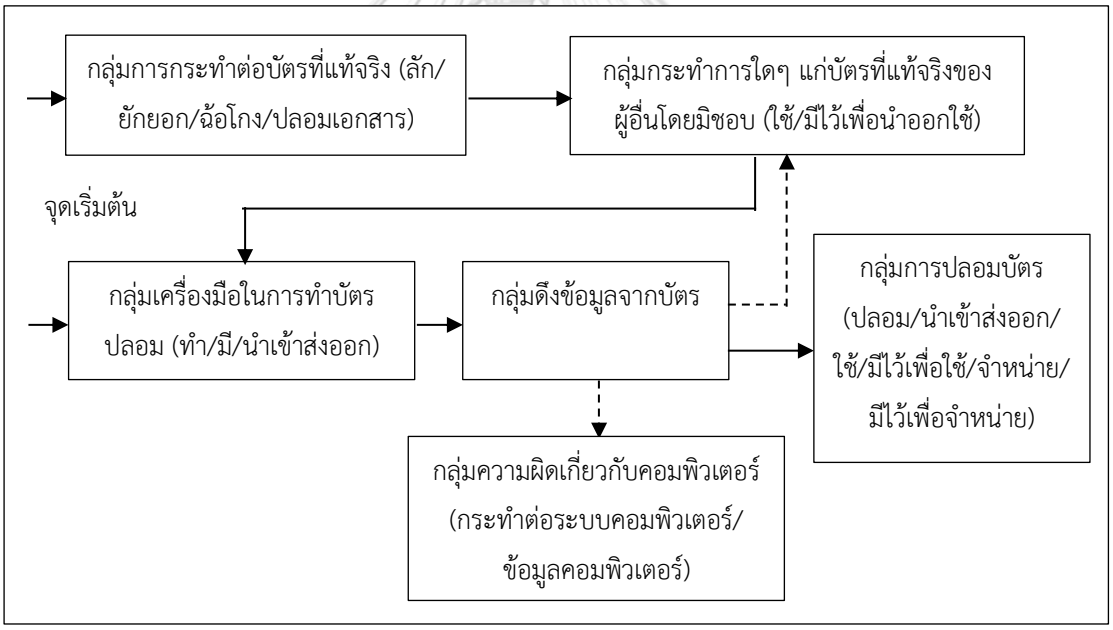
สิ่งสำคัญอันดับแรกในการวิเคราะห์ในหัวข้องานวิจัยเรื่องนี้คือ จำเป็นหรือไม่ที่จะต้องมีการบัญญัติให้การดึงข้อมูลบัตรอิเล็กทรอนิกส์นั้นเป็นความผิดทางอาญา ซึ่งในส่วนนี้เองจำต้องวิเคราะห์ถึงบทบัญญัติที่มีอยู่ของกฎหมายไทยเทียบกับกฎหมายของต่างประเทศที่ได้ทำการศึกษามาแล้ว

[1] โปรดดูหัวข้อที่ 3.3 ปัญหาการขาดบทบัญญัติในการลงโทษสำหรับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

ความสำคัญของข้อมูลบัตรอิเล็กทรอนิกส์กับบริบททางสังคมในประเทศไทยเทียบกับต่างประเทศ เหตุผลเบื้องหลังต่างๆ ที่กฎหมายไทยและกฎหมายต่างประเทศได้กำหนดขึ้นเพื่อคุ้มครองข้อมูลบัตรอิเล็กทรอนิกส์ ข้อดีและข้อเสียรวมทั้งอุปสรรคต่างๆ ที่อาจจะเกิดขึ้นจากการมีบทบัญญัติดังกล่าว เพื่อนำข้อพิจารณาทั้งหมดเหล่านี้มาเปรียบเทียบถึงผลประโยชน์ที่จะได้รับในการมีบทบัญญัติความผิดดังกล่าวในประเทศไทย

จากการศึกษาลักษณะของการกระทำความผิดที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ที่เกิดขึ้นในทางข้อเท็จจริงในบทที่ 2 และ 3 ที่ผ่านมานั้นพบว่าสามารถแบ่งการกระทำความผิดออกเป็นกลุ่มตามลำดับขั้นตอนก่อนหลังได้ดังนี้

ตารางที่ 12 รูปภาพแสดงลำดับขั้นตอนของกลุ่มการกระทำความผิดที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์



จุดเริ่มต้นของการการกระทำความผิดนั้นเริ่มขึ้นได้สองกรณีด้วยกัน กรณีแรกคือ เริ่มต้นด้วยกลุ่มการกระทำต่อบัตรที่แท้จริง อันเป็นการกระทำความผิดต่อตัวบัตรที่อยู่ในลักษณะของวัสดุใดๆ เช่น พลาสติกหรือกระดาษ โดยการลักบัตร ยักยอกบัตร ฉ้อโกงบัตร หรือปลอมเอกสารที่เป็น บัตร

อิเล็กทรอนิกส์[2] การกระทำในลักษณะนี้ผู้กระทำจะได้รับตัวบัตรที่แท้จริงของผู้อื่นมาในครอบครอง เมื่อมีบัตรอิเล็กทรอนิกส์นั้นอยู่กับผู้กระทำความผิดจึงเข้าลักษณะต่อไปคือกลุ่มการกระทำใดๆ แก่บัตรที่แท้จริงทันที โดยเป็นการนำบัตรอิเล็กทรอนิกส์ของผู้อื่นที่ได้ครอบครองมานั้นออกใช้หรือมีไว้เพื่อนำออกใช้ การกระทำเพียงเท่านี้ย่อมถือว่าน่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชนแล้วและต้องรับผิดด้วย[3] ซึ่งต่อมาผู้กระทำอาจนำบัตรที่ได้ครอบครองนั้นมาเข้าเครื่องมือในการทำบัตรปลอมก็ได้ ซึ่งเป็นกรณีที่สองคือการเริ่มต้นการกระทำความผิดด้วยการครอบครองบัตรของผู้อื่นจากกรณีแรกมาแล้วหรือเริ่มต้นด้วยการมิได้มีบัตรของผู้อื่นอยู่ในครอบครองก็ได้ และผู้กระทำความผิดได้กระทำการในกลุ่มเครื่องมือในการทำบัตรปลอม โดยการทำ มี หรือนำเข้าส่งออกเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์[4] ซึ่งหากผู้กระทำมิได้มีครอบครองบัตรอิเล็กทรอนิกส์ของผู้อื่นอยู่ก่อนเหมือนดังในกรณีแรก ผู้กระทำจะต้องนำเครื่องมือหรือวัตถุชนิดนี้ไปติดตั้งเข้ากับตู้เอทีเอ็ม (ใช้สกิมเมอร์) สมคบคิดกับพนักงานโรงแรมหรือร้านค้า (ใช้สกิมเมอร์หรือสกิมเมอร์แบบพกพา) ติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์ (ใช้ไวรัสคอมพิวเตอร์หรือมัลแวร์) หรือใช้การหลอกลวงอื่นๆ (สอบถามทางโทรศัพท์หรือคอลเซ็นเตอร์สแกมเมอร์ สร้างเว็บไซต์ปลอม ส่งจดหมายอิเล็กทรอนิกส์ปลอมหรือฟิชชิ่ง) เพื่อนำบัตรอิเล็กทรอนิกส์ของผู้อื่นที่ได้จากกรณีแรกหรือได้จากกรณีต่างๆ ที่ได้กล่าวมา มากระทำความผิดในกลุ่มต่อไปคือ กลุ่มดึงข้อมูลบัตรอิเล็กทรอนิกส์[5]

ซึ่ง ณ จุดนี้จะมีความสำคัญเป็นอย่างมากเพราะพฤติการณ์ในการกระทำความผิดในส่วนของวัตถุแห่งการกระทำความผิดได้เปลี่ยนจากการกระทำความผิดต่อตัวบัตรที่อยู่ในลักษณะของเอกสารหรือวัตถุใดๆ เป็นการกระทำความผิดต่อข้อมูลของบัตรนั้นๆ ซึ่งผู้วิจัยได้ค้นคว้าและศึกษาบทบัญญัติที่อาจนำมาปรับใช้เพื่อให้สามารถลงโทษผู้กระทำการดึงข้อมูลออกจากบัตรในขั้นตอนนี้ได้ และพบว่าในกฎหมายไทยนั้นเรื่องการดึงข้อมูลจากบัตรดังกล่าวเกี่ยวข้องกับประมวลกฎหมายอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งเมื่อนำบทบัญญัติที่เกี่ยวข้องมาปรับใช้กับการกระทำการดึงข้อมูลจากบัตรพบว่า มีเพียงข้อมูลบัตรอิเล็กทรอนิกส์บาง

---

[2] โปรดดูหัวข้อที่ 2.2.1 ถึง 2.2.4 การลักบัตรอิเล็กทรอนิกส์ การปลอมเอกสารที่เป็นบัตรอิเล็กทรอนิกส์ การยักยอกบัตรอิเล็กทรอนิกส์ และการฉ้อโกงบัตรอิเล็กทรอนิกส์

[3] โปรดดูหัวข้อที่ 2.2.7 การกระทำความผิดที่เกี่ยวข้องกับฐานใช้หรือมีไว้เพื่อนำออกใช้บัตรอิเล็กทรอนิกส์ที่แท้จริงของผู้อื่นโดยมิชอบ

[4] โปรดดูหัวข้อที่ 2.2.6 การกระทำความผิดที่เกี่ยวข้องกับฐานทำหรือมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์

[5] โปรดดูหัวข้อที่ 3.2 รูปแบบการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

ประเภทเท่านั้นที่ได้รับความคุ้มครองตามกฎหมายอาญา คือ “บัตรอิเล็กทรอนิกส์” ตามคำนิยามที่ได้กำหนดไว้ในมาตรา 1(14)(ข) ซึ่งเป็น “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ แต่มีวิธีการใช้ในทำนองเดียวกับ (ก)” และ “บัตรอิเล็กทรอนิกส์” ตามคำนิยามที่ได้กำหนดไว้ในมาตรา 1(14)(ค) ซึ่งเป็น “สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ” ซึ่งเมื่อเกิดการดึงข้อมูลประเภททั้งสองประเภทนี้ขึ้น ประมวลกฎหมายอาญานั้นได้คุ้มครองโดยการลงโทษผู้กระทำ[6] ในความผิดฐานมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/6 ทันที[7] หรือลงโทษเมื่อได้นำข้อมูลนั้นออกใช้ในฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/5[8] และด้วยลักษณะของข้อมูลประเภทที่มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ตามมาตรา 1(14)(ข) ข้อมูลประเภทนี้จึงต้องบันทึกอยู่ในรูปของข้อมูลคอมพิวเตอร์หรือในระบบคอมพิวเตอร์ซึ่งเมื่อเกิดการดึงข้อมูลจากคอมพิวเตอร์ขึ้น จึงเป็นการกระทำต่อระบบคอมพิวเตอร์อันเป็นความผิดฐานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ตามมาตรา 5 หรือ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์อันเป็นความผิดฐานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ตามมาตรา 7 และเป็นความผิดฐานกระทำโดยมิชอบเพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ ตามมาตรา 8 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550[9] ในขณะที่ข้อมูลบัตรอิเล็กทรอนิกส์ประเภทดังที่ได้กำหนดไว้ในมาตรา 1(14)(ก) อันเป็นข้อมูลที่อยู่ใน “เอกสารหรือวัตถุอื่นใดไม่ว่าจะมีรูปลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้” นั้นจะมิได้รับความคุ้มครองใดๆ จากกฎหมายจากการกระทำการดึงข้อมูลจากบัตรเลย[10]

---

[6] โปรดดูหัวข้อที่ 2.2.7 การกระทำความผิดที่เกี่ยวข้องกับฐานใช้หรือมีไว้เพื่อนำออกใช้บัตรอิเล็กทรอนิกส์ที่แท้จริงของผู้อื่นโดยมิชอบ

[7] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, พิมพ์ครั้งที่ 6 (กรุงเทพฯ: กรุงสยาม พับลิชชิ่ง, 2557), หน้า 337.

[8] เรื่องเดียวกัน, หน้า 333.

[9] โปรดดูหัวข้อที่ 3.4.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[10] ซึ่งผู้วิจัยได้วิเคราะห์ปัญหาดังกล่าวไว้อย่างถี่ถ้วนแล้ว โปรดดูหัวข้อที่ 3.3 ปัญหาการขาดบทบัญญัติในการลงโทษสำหรับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ประกอบหัวข้อที่ 3.4 อุปสรรคในการนำบทบัญญัติอื่นที่มีลักษณะใกล้เคียงมาบังคับใช้แทน

ต่อมาผู้กระทำก็อาจนำข้อมูลที่ได้จากการดึงจากบัตรไปกระทำความผิดในกลุ่มการปลอมบัตร โดยการทำบัตรปลอมขึ้น นำเข้าในหรือส่งออกไปนอกราชอาณาจักรซึ่งบัตรปลอม ใช้หรือมีไว้เพื่อใช้ซึ่งบัตรปลอม จำหน่ายหรือมีไว้เพื่อจำหน่ายบัตรอิเล็กทรอนิกส์ปลอม เป็นต้น[11] และในทุกการกระทำความผิดเกี่ยวกับอิเล็กทรอนิกส์นั้นหากเป็นการกระทำต่อบัตรประเภทเพื่อใช้ประโยชน์ในการชำระค่าสินค้า ค่าบริการหรือหนี้อื่นแทนการชำระด้วยเงินสดหรือใช้เบิกถอนเงินสด เป็นต้น ผู้กระทำนั้นจะต้องรับโทษหนักขึ้นด้วย[12]

ดังนั้นการกระทำความผิดที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ที่เกิดขึ้นในทางข้อเท็จจริงซึ่งได้กล่าวมานี้เมื่อนำมาสรุปความสัมพันธ์ระหว่างการกระทำและฐานความผิดที่ผู้กระทำต้องได้รับทั้งหมดตามกฎหมายอาญาของประเทศไทยแล้วย่อมสรุปออกมาอันแสดงในตารางได้ดังนี้

ตารางที่ 13 แสดงความสัมพันธ์ระหว่างการกระทำที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์และฐานความผิดต่างๆ ตามกฎหมายอาญาของประเทศไทย

กลุ่มการกระทำ	การกระทำที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์	กฎหมายอาญาของไทย
กลุ่มการกระทำต่อบัตรที่แท้จริง	ลักบัตรอิเล็กทรอนิกส์	ป.อ. มาตรา 334
	ยักยอกบัตรอิเล็กทรอนิกส์	ป.อ. มาตรา 352
	ฉ้อโกงบัตรอิเล็กทรอนิกส์	ป.อ. มาตรา 341, 342(2)
	ปลอมเอกสารที่เป็นบัตรอิเล็กทรอนิกส์	ป.อ. มาตรา 264, 265
กลุ่มการกระทำใดๆ แก่บัตรอิเล็กทรอนิกส์ที่แท้จริงของผู้อื่นโดยมิชอบ	ใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ	ป.อ. มาตรา 269/5
	มีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ	ป.อ. มาตรา 269/6

[11] โปรดดูหัวข้อที่ 2.2.5 การกระทำความผิดที่เกี่ยวข้องกับฐานปลอมบัตรอิเล็กทรอนิกส์

[12] โปรดดูหัวข้อที่ 2.2.8 การกระทำความผิดที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์บางประเภทที่ผู้กระทำต้องรับโทษหนักขึ้น

กลุ่มการกระทำ	การกระทำที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์	กฎหมายอาญาของไทย
กลุ่มเครื่องมือในการทำบัตรอิเล็กทรอนิกส์	ทำเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลงหรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์	ป.อ. มาตรา 269/2 ส่วนต้น
	มีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลงหรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์	ป.อ. มาตรา 269/2 ส่วนท้าย
	นำเข้าในหรือส่งออกไปนอกราชอาณาจักรซึ่งเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลงหรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์	ป.อ. มาตรา 269/3
กลุ่มดึงข้อมูลจากบัตร	ดึงข้อมูล “บัตรอิเล็กทรอนิกส์” ตามคำนิยามในมาตรา 1(14)(ก)	ไม่มีความผิดตามกฎหมายอาญา
	ดึงข้อมูล “บัตรอิเล็กทรอนิกส์” ตามคำนิยามในมาตรา 1(14)(ข)	ป.อ. มาตรา 269/6, พ.ร.บ.คอมฯ มาตรา 5, 7, 8
	ดึงข้อมูล “บัตรอิเล็กทรอนิกส์” ตามคำนิยามในมาตรา 1(14)(ค)	ป.อ. มาตรา 269/6
กลุ่มการปลอมบัตรอิเล็กทรอนิกส์	ปลอมบัตรอิเล็กทรอนิกส์	ป.อ. มาตรา 269/1
	นำเข้าในหรือส่งออกไปนอกราชอาณาจักรซึ่งบัตรอิเล็กทรอนิกส์ปลอม	ป.อ. มาตรา 269/3
	ใช้หรือมีไว้เพื่อใช้ซึ่งบัตรอิเล็กทรอนิกส์ปลอม	ป.อ. มาตรา 269/4 วรรคแรก
	จำหน่ายหรือมีไว้เพื่อจำหน่ายซึ่งบัตรอิเล็กทรอนิกส์ปลอม	ป.อ. มาตรา 269/4 วรรคสอง

จากตารางดังกล่าวข้างต้น จึงสรุปได้ว่าโดยส่วนใหญ่แล้วการกระทำที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ที่เกิดขึ้นในลักษณะต่างๆ นั้นจะมีบทบัญญัติกฎหมายของประเทศไทยที่ใช้ในการลงโทษทางอาญาได้เป็นการเฉพาะ เว้นแต่กลุ่มดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในบัตรอิเล็กทรอนิกส์บางประเภทซึ่งได้ใช้บทลงโทษตามประมวลกฎหมายอาญามาตรา 269/6 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ตามมาตรา 5 หรือมาตรา 7 หรือมาตรา 8 ซึ่งผู้วิจัยเห็นว่าการปรับใช้กฎหมายในบางกรณีนั้นไม่ถูกต้องด้วยเหตุดังต่อไปนี้

(ก) การใช้บทลงโทษตามประมวลกฎหมายอาญามาตรา 269/6

มาตรา 269/6 ดังที่กฎหมายได้บัญญัตินั้น[13] สามารถแยกองค์ประกอบความผิดออกได้เป็นดังนี้[14]

องค์ประกอบภายนอก (1) ผู้ใด (2) มีไว้ (3) ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่น (4) ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่น หรือประชาชน

องค์ประกอบภายใน (1) เจตนา (2) เจตนาพิเศษ “เพื่อนำออกใช้โดยมิชอบตามมาตรา 269/5”

องค์ประกอบความผิดในส่วนของการกระทำตามมาตรานี้คือการ “มีไว้” ซึ่งการ “มี” หมายถึงการยึดถือหรือครอบครองอย่างใดอย่างหนึ่งก็ได้[15] ในฉบับภาษาอังกฤษนั้น[16] ได้แปลการ “มีไว้” โดยใช้คำว่า “has to” ซึ่งเมื่อพิจารณาประกอบกับกฎหมายของต่างประเทศในเรื่องนี้[17] อันสามารถนำมาใช้ในการตีความกฎหมายอาญาของไทยได้เพราะกฎหมายเกี่ยวกับการมีและดึงข้อมูลบัตรนั้นได้มีใช้ในต่างประเทศมาก่อนกฎหมายไทยพบว่า ในสหรัฐอเมริกา สหราชอาณาจักร สาธารณรัฐฟิลิปปินส์และเครือรัฐออสเตรเลียนั้นจะใช้คำว่า ครอบครอง (Possesses หรือ

---

[13] มาตรา 269/6 บัญญัติไว้ว่า “ผู้ใดมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิสก์ของผู้อื่นโดยมิชอบตามมาตรา 269/5 ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

[14] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 2, หน้า 335.

[15] เรื่องเดียวกัน, หน้า 324.

[16] Section 269/6 “Whoever has to use the electronic card of other person wrongfully in accordance with Section 269/5 in a manner likely to cause detriment to other person or people, such person shall be punished imprisonment not more than three years or fined not more than six ten thousands Baht or both imprisonment and fine.”

[17] ที่ได้ทำการศึกษามาแล้วในบทที่ 4 กฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ

Possession)[18] เหมือนกันซึ่งประเทศเหล่านั้นมิได้นำการ “ครอบครอง” มาใช้กับการ “ดึง” ข้อมูลด้วย เว้นแต่ในสหราชอาณาจักรเพียงประเทศเดียวที่ได้กำหนดรวมกันไปให้การครอบครองกับการดึงนั้นสามารถใช้ร่วมกันได้ภายใต้ถ้อยคำว่าครอบครอง ในมาตรา 6 ของพระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006 (The Fraud Act 2006) แต่สหราชอาณาจักรก็ยังได้มีกฎหมายอื่นๆ ที่กำหนดให้มีการดึงข้อมูลบัตรโดยที่มิได้ใช้คำว่าครอบครองอยู่ด้วย เช่น ใช้คำว่าคัดลอก (Copies) หรือเคลื่อนย้าย (Moves)[19] หรือได้รับ (Obtain)[20] และนอกจากนั้นสาธารณรัฐฟิลิปปินส์และเครือรัฐออสเตรเลีย แม้จะได้มีบทบัญญัติเรื่องการครอบครองข้อมูลแล้ว ก็ยังมีบทบัญญัติเฉพาะเกี่ยวกับการดึงข้อมูล[21] ซึ่งป้องกันการตีความและเพื่อความชัดเจนแน่นอนของกฎหมายอาญาในการปรับใช้กฎหมายแก่ผู้กระทำความผิดอีกด้วย

การตีความว่าการดึงข้อมูลจะลงโทษฐาน “มีไว้” เพื่อนำออกใช้ซึ่งข้อมูลบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบนั้น นอกจากลักษณะของการกระทำจะไม่ตรงกันดังที่ได้กล่าวมาแล้ว ยังขัดกับหลักกฎหมายอาญาซึ่งต้องตีความโดยเคร่งครัดและจักนำกฎหมายที่ใกล้เคียงอย่างยิ่งมาปรับใช้เพื่อลงโทษบุคคลไม่ได้ ทั้งในด้านกรรมของการกระทำ ไม่ว่าผู้กระทำความผิดจะได้ทำการดึงข้อมูลกี่ครั้งก็ตามก็จะลงโทษฐานนี้เพียงกรรมเดียวซึ่งไม่สมเหตุผล ด้วยเหตุผลดังกล่าวทั้งหมดนี้จึงมิอาจปรับมาตรา 269/6 แห่งประมวลกฎหมายอาญาเพื่อใช้ในการลงโทษกับการกระทำในลักษณะของการ “ดึง” ข้อมูลบัตรได้

(ข) การใช้บทลงโทษตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 5 หรือ มาตรา 7 หรือมาตรา 8

ดังที่ได้ศึกษามาแล้วว่า คำว่า “บัตรอิเล็กทรอนิกส์” ประเภทที่เป็นข้อมูลซึ่งมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ ตามคำนิยามในประมวลกฎหมายอาญา มาตรา 1(14)(ข) นั้นต้องเป็นข้อมูล

---

[18] มาตรา 1028(a)(7) ในรัฐบัญญัติของสหรัฐอเมริกา ของสหรัฐอเมริกา มาตรา 6 ในพระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006 ของสหราชอาณาจักร มาตรา 4(b)(3) ในพระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012 และมาตรา 9(k) ในพระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 ของสาธารณรัฐฟิลิปปินส์ มาตรา 478.3 ในพระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001 ของเครือรัฐออสเตรเลีย

[19] มาตรา 1 ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990

[20] มาตรา 3A(3) ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 และมาตรา 170 ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018

[21] เช่นมาตรา 9(q) ในพระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 ของสาธารณรัฐฟิลิปปินส์ และมาตรา 478.4 ในพระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001 ของเครือรัฐออสเตรเลีย

ที่ได้บันทึกอยู่ในคอมพิวเตอร์หรือระบบคอมพิวเตอร์เท่านั้น[22] แต่มิได้หมายความว่าเมื่อข้อมูลดังกล่าวเป็นข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แล้ว การดึงข้อมูลประเภทนี้จะเป็นความผิดไปด้วย ซึ่งจากการศึกษาวิจัยสามารถอธิบายได้ดังนี้

บทบัญญัติในมาตรา 5[23] และมาตรา 7[24] ดังที่กฎหมายได้บัญญัตินั้น สามารถแยกองค์ประกอบความผิดออกได้เป็นดังนี้[25]

องค์ประกอบภายนอก (1) ผู้ใด (2) เข้าถึง (3) โดยมิชอบ (4) ซึ่งระบบคอมพิวเตอร์ (ตามมาตรา 5) หรือ ซึ่งข้อมูลคอมพิวเตอร์ (ตามมาตรา 7) (5) ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

องค์ประกอบภายใน (1) เจตนา

องค์ประกอบความผิดในส่วนของการกระทำตามมาตรานี้คือการ “เข้าถึง” หมายความว่าเป็นการล่วงล้ำเขตแดนความเป็นส่วนตัวต่อสิ่งที่ถูกเก็บไว้ในคอมพิวเตอร์แต่มิได้มีการทำร้ายข้อมูลที่ถูกเก็บไว้ดังกล่าว เปรียบเสมือนการเข้าไปในบ้านของผู้อื่นโดยใช้กุญแจผี แต่เพียงเข้าไปดูทรัพย์สินภายในบ้านโดยมิได้ลักหรือทำลายทรัพย์สินดังกล่าว[26] ในฉบับภาษาอังกฤษนั้น[27] ได้แปลคำว่า “เข้าถึง” ด้วยคำว่า “Accesses” ซึ่งเมื่อพิจารณาประกอบกับกฎหมายของต่างประเทศในเรื่องนี้[28] อันสามารถนำมาใช้ในการตีความกฎหมายอาญาของไทยได้ พบว่าในสหรัฐอเมริกาได้กำหนดให้มีการ

[22] โปรดดูหัวข้อที่ 3.4.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[23] มาตรา 5 บัญญัติไว้ว่า “ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ”

[24] มาตรา 7 บัญญัติไว้ว่า “ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ”

[25] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, พิมพ์ครั้งที่ 1 (กรุงเทพฯ: กรุงสยาม พับลิชชิ่ง, 2559), หน้า 134-137.

[26] เรื่องเดียวกัน, หน้า 134-135.

[27] Section 5 “Any person who illegally accesses a computer system for which a specific access prevention measure that is not intended for their own use is available shall be subject to imprisonment not exceeding six months or a fine not exceeding ten thousand baht, or both.”

[28] ที่ได้ทำการศึกษามาแล้วในบทที่ 4 กฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ

เข้าถึง (Accesses) เช่นกัน แต่จะเป็นการดึงข้อมูลได้นั้นกฎหมายดังกล่าว[29] ได้บัญญัติลงไปอีกว่าด้วยการเข้าถึงนั้นจึงได้รับ (Obtain) ข้อมูลมาด้วย ในสาธารณรัฐฟิลิปปินส์และเครือรัฐออสเตรเลียก็ได้กำหนดให้มีการเข้าถึง (Accesses) เช่นกัน แต่ก็ได้บัญญัติลงไปอีกด้วยว่าการเข้าถึงนี้รวมถึงการดึงข้อมูลมา (Retrieving Data from)[30] หรือให้หมายถึงการคัดลอก (Copying) หรือเคลื่อนย้าย (Moving) ข้อมูลในคอมพิวเตอร์ด้วย[31] ซึ่งเมื่อพิจารณาองค์ประกอบความผิดที่ได้บัญญัติไว้ในมาตรา 5 และมาตรา 7 ข้างต้นอันมีเพียงการกระทำการ “เข้าถึง” แต่เพียงอย่างเดียวเท่านั้น โดยมิได้บัญญัติเพิ่มเติมหรือให้คำนิยามการเข้าถึงนั้นรวมถึงการดึงข้อมูลดังเช่นที่ได้กำหนดไว้ในกฎหมายของประเทศที่กล่าวมาด้วย อีกทั้งกฎหมายอาญานั้นต้องตีความโดยเคร่งครัด ด้วยเหตุผลเหล่านี้การใช้บทลงโทษในมาตรา 5 หรือมาตรา 7 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับการดึงข้อมูลบัตรจึงไม่ถูกต้อง

บทบัญญัติในมาตรา 8 ดังที่กฎหมายได้บัญญัตินั้น[32] สามารถแยกองค์ประกอบความผิดออกได้เป็นดังนี้[33]

องค์ประกอบภายนอก (1) ผู้ใด (2) กระทำด้วยประการใดด้วยวิธีการทางอิเล็กทรอนิกส์ (3) โดยมิชอบ (4) ข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

องค์ประกอบภายใน (1) เจตนา (2) เจตนาพิเศษ “เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์”

องค์ประกอบความผิดในส่วนของการกระทำตามมาตรานี้คือการ “กระทำด้วยประการใดด้วยวิธีการทางอิเล็กทรอนิกส์” หมายความในทำนองเดียวกับการลักลอบดักฟัง หรือการทำให้ได้มา

---

[29] มาตรา 1030(a)(2) ในรัฐบัญญัติของสหรัฐอเมริกา ของสหรัฐอเมริกา

[30] มาตรา 4(a)(1) ในพระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012 ของสาธารณรัฐฟิลิปปินส์

[31] มาตรา 477.1 ในพระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001 ของเครือรัฐออสเตรเลีย

[32] มาตรา 8 บัญญัติไว้ว่า “ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

[33] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, หน้า 148-151.

ซึ่งเนื้อหาของข้อมูลด้วยการแอบบันทึกข้อมูลที่ส่งผ่านถึงกัน[34] ในฉบับภาษาอังกฤษ[35] ใช้คำว่า “Any act by electronic means” ซึ่งเมื่อพิจารณาประกอบกับกฎหมายของต่างประเทศในเรื่องนี้[36] อันสามารถนำมาใช้ในการตีความกฎหมายอาญาของไทยได้ พบว่าในสหราชอาณาจักร ก็ได้บัญญัติในลักษณะเดียวกันแต่ใช้คำว่า “ทำให้เครื่องคอมพิวเตอร์กระทำการใดๆ” (Perform any function) แต่กฎหมายดังกล่าว[37] ได้บัญญัติอย่างชัดแจ้งให้รวมถึงการคัดลอก (Copies) หรือเคลื่อนย้าย (Moves) ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ด้วย ในขณะที่บทบัญญัติในมาตรา 8 นั้นมิได้กำหนดอย่างชัดแจ้งว่าการ “กระทำด้วยประการใดด้วยวิธีการทางอิเล็กทรอนิกส์” จะรวมถึงการดึงข้อมูลด้วยหรือไม่ ดังนั้นจึงต้องพิจารณาเจตนารมณ์ของกฎหมายพบว่า แม้ไม่ได้มีการบัญญัติไว้โดยชัดแจ้งให้รวมถึงการดึงข้อมูลด้วยดังเช่นกฎหมายของสหราชอาณาจักร แต่โดยองค์ประกอบของเจตนาพิเศษ “เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์” นั้นย่อมแสดงว่าต้องเป็นการกระทำเพื่อ “ดักรับ” อันถือเสมือนเป็นการดึงข้อมูลเช่นกัน แต่บทบัญญัติมาตรา 8 นี้มีข้อจำกัดเพราะต้องเป็นการดักรับข้อมูล “ที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์” ด้วยจึงไม่รวมถึงข้อมูลคอมพิวเตอร์ที่จัดเก็บในรูปแบบของ ซีดี ดิสเกตต์ ฮาร์ดดิสหรือแฟลชไดร์ฟ เป็นต้น[38] ซึ่งต่างกับสหราชอาณาจักรที่กำหนดให้ ข้อมูลที่อยู่ในอุปกรณ์ในการจัดเก็บข้อมูล (Storage medium) ในขณะเวลาที่อุปกรณ์นั้นได้เชื่อมต่อและรับรู้โดยเครื่องคอมพิวเตอร์แล้วจะได้รับความคุ้มครองด้วย ผลดังกล่าวทำให้มาตรา 8 นี้สามารถปรับใช้กับการดึงข้อมูลบัตรเฉพาะประเภทที่มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ ตามประมวลกฎหมายอาญามาตรา 1(14)(ข) และต้องเป็นข้อมูลที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์เท่านั้น คือเป็นการดึงข้อมูลโดยการใช้ไวรัสคอมพิวเตอร์หรือมัลแวร์[39] แต่ไม่คุ้มครองถึงการดึงข้อมูลรูปแบบอื่นๆ เช่น การใช้สกิมเมอร์หรือการหลอกลวงอื่นๆ

---

[34] เรื่องเดียวกัน, หน้า 149.

[35] Section 8 “Any person who illegitimately perpetrates any act by electronic means to intercept computer data of other people during its transmission in a computer system, and that computer data is not intended for the public interest or the use of general people, shall be subject to imprisonment not exceeding three years or a fine not exceeding sixty thousand baht, or both.”

[36] ที่ได้ทำการศึกษามาแล้วในบทที่ 4 กฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ

[37] มาตรา 1 ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 ของสหราชอาณาจักร

[38] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, หน้า 150.

[39] โปรดดูหัวข้อที่ 3.2.2 การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์โดยการใช้มัลแวร์หรือไวรัสคอมพิวเตอร์ (Malware or Virus Computer)

โดยสรุปจึงกล่าวได้ว่ามีเพียงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ฐานกระทำโดยมิชอบเพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ตามมาตรา 8 เท่านั้นที่สามารถนำมาปรับใช้ในการลงโทษแก่การดึงข้อมูจากบัตรอิเล็กทรอนิกส์ได้ แต่ก็ปรับใช้ได้แต่เพียงรูปแบบของ “บัตรอิเล็กทรอนิกส์” เฉพาะที่เป็นข้อมูลที่มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ ตามประมวลกฎหมายอาญามาตรา 1(14)(ข) และต้องเป็นข้อมูลที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์เท่านั้นที่ได้รับความคุ้มครองตามกฎหมายอาญาของไทยซึ่งเป็นกรณีที่จำกัดมาก ส่วนการดึงข้อมูลบัตรในรูปแบบอื่นๆ[40] นั้น บทบัญญัติของกฎหมายอาญาในประเทศไทยยังมิได้กำหนดให้การกระทำในลักษณะดังกล่าวเป็นความผิดทางอาญา ซึ่งเมื่อหากพิจารณาเหตุผลของการบัญญัติกฎหมายอันเกี่ยวกับบัตรอิเล็กทรอนิกส์ที่กำหนดไว้ในหมายเหตุท้ายพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา ฉบับที่ 17 พ.ศ. 2547[41] ตอนหนึ่งว่า “สมควรกำหนดความผิดอาญาสำหรับการกระทำความผิดเกี่ยวกับบัตรและข้อมูลอิเล็กทร อนิกส์ดังกล่าวเพิ่มเติมให้ครอบคลุมการกระทำความผิดในรูปแบบต่างๆ” จะพบว่าเจตนารมณ์ในการยกร่างกฎหมายของประเทศไทยนั้นต้องการให้มีบทบัญญัติความผิดทางอาญาสำหรับใช้ในการลงโทษให้ครอบคลุมการกระทำความผิดที่เกี่ยวกับบัตรอิเล็กทรอนิกส์ในทุกลักษณะซึ่งรวมถึงการกระทำการดึงข้อมูลจากบัตรด้วยอันเป็นการคุ้มครองทั้งบัตรและข้อมูลอิเล็กทรอนิกส์ของบัตรนั้น จึงจะตรงตามเป้าปณิธานของกฎหมายไทยที่ได้ตั้งไว้

จากการศึกษากฎหมายต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลบัตรอิเล็กทรอนิกส์[42] พบว่าประเทศต่างๆ ไม่ว่าสหรัฐอเมริกา สหราชอาณาจักร สาธารณรัฐฟิลิปปินส์และเครือรัฐออสเตรเลียก็ต่างประสบปัญหาและได้รับผลกระทบจากการกระทำการอันมิชอบที่เกี่ยวกับบัตรอิเล็กทรอนิกส์ในรูปแบบต่างๆ ดังที่กล่าวมาแล้วข้างต้นเช่นเดียวกัน และต่างใช้การแก้ปัญหานี้ด้วยวิธีการทางกฎหมายโดยการกำหนดให้มีบทบัญญัติทางอาญาเพื่อเอาผิดแก่การกระทำเหล่านั้นให้ครอบคลุมถึงลักษณะการกระทำที่เกี่ยวกับบัตรอิเล็กทรอนิกส์ในทุกรูปแบบ รวมถึงการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ด้วย

---

[40] โปรดดูหัวข้อที่ 2.1.1 นิยามของบัตรอิเล็กทรอนิกส์ และหัวข้อที่ 3.1 รูปแบบการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

[41] เหตุผลในการประกาศใช้พระราชบัญญัตินี้ คือ เนื่องจากปัจจุบันการใช้เอกสาร วัตถุอื่นใดหรือข้อมูล ที่จัดทำขึ้นในลักษณะบัตรอิเล็กทรอนิกส์ เช่น บัตรเครดิต บัตรเดบิต บัตรสมาร์ทการ์ด หรือบัตรอื่นใดในลักษณะคล้ายกัน โดยมีวัตถุประสงค์เพื่อใช้ประโยชน์ในการชำระค่าสินค้า ค่าบริการ หรือหนี้อื่น หรือเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อย่างหนึ่งอย่างใด กำลังเพิ่มปริมาณและประเภทการใช้งานอย่างแพร่หลาย และปรากฏว่าได้มีการกระทำความผิดเกี่ยวกับบัตรและลักลอบนำข้อมูลอิเล็กทรอนิกส์ของผู้อื่นมาใช้อันส่งผลกระทบต่อเศรษฐกิจและผู้บริโภคในวงกว้าง สมควรกำหนดความผิดอาญาสำหรับการกระทำความผิดเกี่ยวกับบัตรและข้อมูลอิเล็กทรอนิกส์ดังกล่าวเพิ่มเติมให้ครอบคลุมการกระทำความผิดในรูปแบบต่าง ๆ และให้มีอัตราโทษเหมาะสมกับความร้ายแรงของการกระทำความผิด จึงจำเป็นต้องตราพระราชบัญญัตินี้

[42] ดังที่กล่าวไว้แล้วในบทที่ 4 กฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ

ซึ่งแม้ว่าการกำหนดคำนิยามและองค์ประกอบของการกระทำความผิดในการบัญญัติกฎหมาย ความละเอียดในเรื่องการลงโทษและจำนวนกฎหมายที่ใช้ลงโทษนั้นจะแตกต่างกันไปบ้างในแต่ละประเทศ แต่สิ่งที่เหมือนกันก็คือวัตถุประสงค์ของกฎหมายในทุกประเทศนั้นต่างมุ่งคุ้มครองข้อมูลในบัตรอิเล็กทรอนิกส์เป็นสำคัญไม่ยิ่งหย่อนกว่าการกระทำผิดต่อบัตรในรูปแบบอื่นๆ และได้กำหนดให้มีบทบัญญัติที่หลากหลายซึ่งอาจเป็นการกระทำความผิดอันเกี่ยวกับข้อมูลส่วนบุคคล การกระทำความผิดอันเกี่ยวกับบัตรชำระเงิน หรือการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ เพื่อให้มีการใช้งานที่ครอบคลุมกับการกระทำความผิดในการดึงข้อมูลในรูปแบบต่างๆ ที่อาจเกิดขึ้นได้ มิใช่การบทบัญญัติไว้แต่เพียงกฎหมายฉบับเดียวเช่นในประเทศไทย[43]

ในด้านบริบททางสังคมนั้น จากการศึกษาวิจัยพบว่า ในประเทศไทยและต่างประเทศนั้นมีปริมาณการใช้งานบัตรอิเล็กทรอนิกส์เพื่อความสะดวกในชีวิตประจำวันในอัตราที่สูงมากในรูปแบบต่างๆ[44] และในทางสถิตินั้นพบว่าโดยส่วนใหญ่แล้วจะเป็นการใช้งานในการทำธุรกรรมทางการเงินตามตารางดังต่อไปนี้

ตารางที่ 14 แสดงตัวอย่างสถิติปริมาณการใช้งานบัตรอิเล็กทรอนิกส์ในการทำธุรกรรมทางการเงินต่อสัดส่วนประชากรในประเทศต่างๆ พ.ศ. 2560

ประเทศ	อัตราการใช้งานต่อประชากรในประเทศ (คิดเป็นร้อยละ)	
	บัตรเดบิต[45]	บัตรเครดิต[46]
สหราชอาณาจักร	91.45	65.37
สหรัฐอเมริกา	80.23	65.60
เครือรัฐออสเตรเลีย	89.96	59.69

[43] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ฐานกระทำโดยมิชอบเพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ตามมาตรา 8

[44] โปรดดูหัวข้อที่ 2.1.2 ประเภทของบัตรอิเล็กทรอนิกส์

[45] The World Bank, "Percent People with Debit Cards - Country Rankings" [Online], Accessed: 1 November 2020. Available from: https://www.theglobaleconomy.com/rankings/people_with_debit_cards/.

[46] The World Bank, "Percent People with Credit Cards - Country Rankings" [Online], Accessed: 1 November 2020. Available from: https://www.theglobaleconomy.com/rankings/people_with_credit_cards/.

ประเทศ	อัตราการใช้งานต่อประชากรในประเทศ (คิดเป็นร้อยละ)	
	บัตรเดบิต[45]	บัตรเครดิต[46]
สาธารณรัฐฟิลิปปินส์	21.01	1.94
ไทย	59.85	9.80

ข้อสังเกต จากตารางดังกล่าวจะเห็นได้ว่าในสหรัฐอเมริกา สหราชอาณาจักรและเครือรัฐออสเตรเลียนั้นมีการใช้งานบัตรอิเล็กทรอนิกส์ต่อสัดส่วนประชากรที่สูง แม้ในสาธารณรัฐฟิลิปปินส์ที่มีการใช้งานบัตรอิเล็กทรอนิกส์ต่อสัดส่วนประชากรที่ต่ำกว่าในประเทศไทย ประเทศเหล่านั้นก็ยังได้กำหนดให้มีบทบัญญัติทางอาญาในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ด้วย เพราะต่างก็ได้รับผลกระทบจากการกระทำความผิดในรูปแบบดังกล่าวเช่นเดียวกัน[47]

ในปัจจุบันประชากรในประเทศต่างๆ นั้นมีแนวที่จะใช้บัตรอิเล็กทรอนิกส์ในการทำธุรกรรมทางการเงินแทนการใช้เงินสดมากขึ้น[48] เช่นเดียวกับในประเทศไทยที่อยู่ในระยะเริ่มต้นของกระบวนการก้าวไปสู่สังคมไร้เงินสด (Cashless Society) ซึ่งหมายความว่า ประชากรส่วนใหญ่ยังมีปริมาณการใช้บัตรอิเล็กทรอนิกส์ในการทำธุรกรรมทางการเงินอยู่สูง เช่น การใช้ฝากถอนเงินหรือการโอนเงิน มากกว่าการชำระด้วยช่องทางออนไลน์ (e-Payments)[49] อันแสดงได้จากปริมาณการใช้บัตรอิเล็กทรอนิกส์ที่เพิ่มมากขึ้นในทุกๆ ปี ตามตารางดังต่อไป

[47] ดูบทที่ 4 กฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ

[48] Jason Steele, "Payment Method Statistics" [Online], Accessed: 1 November 2020. Available from: https://www.creditcards.com/credit-card-news/payment-method-statistics-1276/.

[49] ธนาคารแห่งประเทศไทย, "สังคมไทย (กำลัง) ไร้เงินสด ?" [ออนไลน์], เข้าถึงเมื่อ 1 พฤศจิกายน 2563. แหล่งที่มา: https://www.bot.or.th/Thai/MonetaryPolicy/ArticleAndResearch/Pages/FAQ169.aspx.

ตารางที่ 15 แสดงจำนวนบัตรอิเล็กทรอนิกส์ที่ใช้ในประเทศไทย พ.ศ. 2558 ถึง พ.ศ. 2562[50]

(หน่วย : ใบ)

ประเภทของบัตร	พ.ศ.				
	2558	2559	2560	2561	2562
บัตรเครดิต	18,974,195	20,136,341	20,334,780	22,105,472	23,998,653
บัตรเอทีเอ็ม	13,397,755	10,791,481	8,758,043	7,080,324	15,318,234
บัตรเดบิต	46,989,719	50,199,427	54,329,727	57,407,185	64,773,018
รวมทั้งสิ้น	79,361,669	81,127,249	83,422,550	86,592,981	104,089,905

จากการศึกษาวิจัยพบว่าใน พ.ศ. 2561 ธนาคารกสิกรไทยของประเทศไทยมีปริมาณจำนวนบัตรที่ออกให้ มีมูลค่าเงินในบัตรและปริมาณการใช้จ่ายผ่านบัตรอิเล็กทรอนิกส์ติดอันดับ 1 ใน 50 ของสถิติทั้งหมดในภูมิภาคเอเชียแปซิฟิก (Asia-Pacific) ตามมาด้วยธนาคารกรุงศรีอยุธยาที่ติด 1 ใน 50 ธนาคารที่มีปริมาณการใช้จ่ายผ่านบัตรเดบิตซึ่งรองลงมาจากธนาคารกสิกรไทย[51] อันบ่งชี้ได้ว่าประเทศไทยนั้นมีปริมาณการใช้บัตรอิเล็กทรอนิกส์ในการดำเนินธุรกรรมทางการเงินเป็นจำนวนมาก

ด้วยปริมาณการใช้งานบัตรอิเล็กทรอนิกส์ที่มากขึ้นนี้เองจึงเป็นสิ่งที่ล่อให้อาชญากรหันมากระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์มากขึ้น อันทำให้จำนวนคดีที่เกี่ยวกับอิเล็กทรอนิกส์ในประเทศไทยนั้นยังคงมีอยู่อย่างต่อเนื่องและมีแนวโน้มที่จะสูงขึ้นในทุกปีอันแสดงในตารางดังต่อไปนี้

[50] ธนาคารแห่งประเทศไทย, “จำนวนบัตรพลาสติก” [ออนไลน์], เข้าถึงเมื่อ 22 กรกฎาคม 2563. แหล่งที่มา https://www.bot.or.th/App/BTWS_STAT/statistics/ReportPage.aspx?reportID=685&language=th.

[51] The Nilson Report, "Top 50 Card Issuers in Asia-Pacific" [Online], Accessed: 1 November 2020. Available from: https://nilsonreport.com/upload/content_promo/The_Nilson_Report_Issue_1164.pdf.

ตารางที่ 16 แสดงสถิติการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ (ตามประมวลกฎหมายอาญา มาตรา 269/1 – 269/7) ทั่วทั้งประเทศไทย ของศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ[52]

(หน่วย : ราย)

รายการ	พ.ศ.				
	2558	2559	2560	2561	2562
รับแจ้ง	175	116	152	290	220
จับกุม	113	68	101	193	154
คิดเป็นร้อยละ	64.57	58.62	66.44	66.55	70

นอกจากปริมาณการกระทำความผิดที่เกี่ยวกับบัตรอิเล็กทรอนิกส์ที่สูงขึ้นอย่างต่อเนื่องตามตารางดังกล่าวแล้ว ใน พ.ศ. 2560 นายพงษ์สิทธิ ชัยฉัตรพรสุข รองผู้จัดการใหญ่และผู้บริหารสูงสุดในการป้องกันอาชญากรรมทางการเงินของธนาคารไทยพาณิชย์ ยังพบว่าประเทศไทยเป็นประเทศที่มีอาชญากรรมการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นอันดับ 6 ของโลกอีกด้วย[53]

บัตรอิเล็กทรอนิกส์นั้นไม่ว่าจะมีวัตถุประสงค์เพื่อใช้งานในการทำธุรกรรมทางการเงินหรือไม่ก็ตาม ข้อมูลที่บรรจุไว้ในบัตรหรือบนพื้นผิวของบัตรอิเล็กทรอนิกส์ทุกรูปแบบนั้นยังมีลักษณะเป็นข้อมูลส่วนบุคคล (Data Privacy) ซึ่งสังคมยุคใหม่[54] และประชาชนในประเทศไทยนั้นให้ความสำคัญข้อมูลเป็นอย่างมากไม่น้อยกว่าความสำคัญในด้านทรัพย์สิน โดยข้อมูลส่วนบุคคลนี้เป็นสิทธิมนุษยชนขั้นพื้นฐานที่สำคัญในความเป็นส่วนตัวของประชาชน (Privacy Right) ที่ต้องได้รับการคุ้มครองอันจะ

---

[52] ศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ, "สถิติฐานความผิดคดีอาญา" [ออนไลน์], เข้าถึงเมื่อ 2 สิงหาคม 2563. แหล่งที่มา http://pitc.police.go.th/dirlist/dirlist.php?dir=/crimes.

[53] มติชนออนไลน์, "รวบ 5 จีนแผ่นดินใหญ่ แก๊งสกิมเมอร์คัดลอกข้อมูลตู้เอทีเอ็มไทย แฉแฮกวันเดียว 200 ใบรวบ 5 จีนแผ่นดินใหญ่ แก๊งสกิมเมอร์คัดลอกข้อมูลตู้เอทีเอ็มไทย แฉแฮกวันเดียว 200 ใบ" [ออนไลน์], เข้าถึงเมื่อ 1 พฤศจิกายน 2563. แหล่งที่มา: https://www.matichon.co.th/local/crime/news_580604.

[54] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, 4, 5 (1890): 193-220.

ทำให้ประชาชนมีความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์[55] ซึ่งในประเทศไทยนั้นก็ได้เล็งเห็นความสำคัญ ซึ่งรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 4 นั้นได้รับรองให้สิทธิของบุคคลย่อมได้รับความคุ้มครอง[56] และมาตรา 32 ยังบัญญัติเพิ่มเติมอีกว่า บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัวซึ่งการกระทำใดที่เป็นการละเมิดหรือกระทบต่อสิทธินี้ หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าทางใดๆ จะกระทำมิได้ เว้นแต่อาศัยอำนาจตามกฎหมาย[57] และแม้ว่ารัฐจะได้ออกกฎหมายต่างๆ เพื่อคุ้มครองข้อมูลส่วนบุคคล เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 อันเป็นการกำหนดหน้าที่เกี่ยวกับข้อมูลส่วนบุคคลที่อยู่ในความควบคุมดูแลขององค์กรของรัฐและเอกชน เช่น การเก็บรวบรวม การกำกับ การใช้งาน การป้องกัน การรับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ แต่เมื่อได้ศึกษาวิจัยแล้วพบว่า แม้พระราชบัญญัติเหล่านี้ของประเทศไทยจะได้รับแนวทางในการบัญญัติกฎหมายมาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation : GDPR)[58] ก็ตาม แต่ก็ไม่มีบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลจากการกระทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ตามเจตจำนงของรัฐธรรมนูญแห่งราชอาณาจักรไทยในการที่จะให้มีการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวหรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไว้ในพระราชบัญญัติเหล่านั้นเลย อันแตกต่างจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018 (Data Protection Act 2018) ของสหราชอาณาจักร ที่มีต้นแบบมาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปเช่นกัน แต่สหราชอาณาจักรนั้นได้ให้ความสำคัญแก่การกระทำความผิดในลักษณะการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ จึงได้กำหนดให้มีบทบัญญัติอันเป็นการเฉพาะในการ

---

[55] คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, "การคุ้มครองข้อมูลส่วนบุคคล (Data Privacy)" [ออนไลน์], เข้าถึงเมื่อ 1 พฤศจิกายน 2563. แหล่งที่มา: https://www.etcommission.go.th/files/article/article-dp.pdf.

[56] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 4 บัญญัติว่า "ศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพ และความเสมอภาคของบุคคลย่อมได้รับความคุ้มครอง

ปวงชนชาวไทยย่อมได้รับความคุ้มครองตามรัฐธรรมนูญเสมอกัน"

[57] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 32 บัญญัติว่า "บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัวการกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใดๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ"

[58] ACinfotec, "สรุปใจความสำคัญของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ผู้ประกอบการควรรู้" [ออนไลน์], เข้าถึงเมื่อ 1 พฤศจิกายน 2563. แหล่งที่มา: https://www.acinfotec.com/2019/07/23/data-protection-law-2562/.

คุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ไว้ในมาตรา 170 แห่งพระราชบัญญัติดังกล่าวให้เป็นการกระทำความผิดทางอาญาด้วย[59]

ข้อสังเกต เพื่อให้เกิดผลในการคุ้มครองข้อมูลส่วนบุคคลได้อย่างแท้จริง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดโทษทางอาญาไว้แบ่งออกเป็น 3 กรณีด้วยกัน[60] คือ กรณีผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนเกี่ยวกับการเก็บรวบรวมข้อมูล เปิดเผย ส่งหรือโอนข้อมูลโดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหายหรือเพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย ตามมาตรา 79 กรณีผู้ที่ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่แล้วนำไปเปิดเผย ตามมาตรา 80 และกรณีผู้กระทำความผิดเป็นนิติบุคคล ตามมาตรา 81 แต่อย่างไรก็ตามพระราชบัญญัติดังกล่าวก็มิได้กำหนดให้การดึงข้อมูลส่วนบุคคลเป็นความรับผิดทางอาญาไว้แต่ประการใด

จากการศึกษาพบว่า ตั้งแต่ในอดีตจนถึงปัจจุบันนั้นอาชญากรรมที่เกี่ยวข้องกับการฉ้อโกงบัตรอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการโจรกรรมข้อมูลส่วนบุคคลในต่างประเทศนั้นมีแนวโน้มสูงขึ้นอย่างต่อเนื่อง[61] และอาชญากรรมทางคอมพิวเตอร์ที่เกี่ยวข้องกับการดึงข้อมูลต่างๆ ก็สูงขึ้นอย่างมากเช่นกัน[62] ซึ่งมีผู้ได้รับความเสียหายและได้รับการสูญเสียทางการเงินเป็นจำนวนมากจากการกระทำความผิดดังกล่าว การกระทำความผิดที่เกิดขึ้นนี้ทำให้ความเชื่อใจในการใช้บัตรอิเล็กทรอนิกส์ของสาธารณะชนลดลงเป็นอย่างมากอันส่งผลกระทบต่อการใช้งานข้อมูลเหล่านั้นกับระบบอื่นๆ ในประเทศ[63] ด้วยเหตุผลนี้เองหลากหลายประเทศจึงต่างผลักดันให้เกิดกฎหมายในการคุ้มครองข้อมูลดังกล่าวขึ้นเพราะเห็นว่าสามารถนำมาใช้ป้องกันควบคุมอาชญากรรมดังกล่าวได้ในฐานะของกฎหมาย

---

[59] โปรดดูหัวข้อที่ 4.2.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018 (Data Protection Act 2018)

[60] สุพิศ ปราณีตพลกรัง, การคุ้มครองข้อมูลส่วนบุคคล, พิมพ์ครั้งที่ 1 (กรุงเทพ: นิติธรรม, 2563), หน้า 79-81.

[61] Lyle Daly, "Identity Theft and Credit Card Fraud Statistics for 2020" [Online], Accessed: 8 November 2020. Available from: https://www.fool.com/the-ascent/research/identity-theft-credit-card-fraud-statistics/.

[62] Insurance information instatute, "Facts + Statistics: Identity Theft and Cybercrime" [Online], Accessed: 8 November 2020. Available from: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1)/.

[63] David S. Wall, “Future Identities: Changing identities in the UK – the next 10 years” [Online], Accessed: 25 October 2020. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/275784/13-521-identity-related-crime-uk.pdf.

ที่มีความจำเป็นเพื่อจัดการกับอาชญากรรมเหล่านี้[64] เพื่อตัดแรงจูงใจในการกระทำความผิดของอาชญากรจากการลงโทษทางกฎหมาย และทำให้อาชญากรกระทำความผิดยากขึ้นเมื่อใช้ควบคู่กันกับการพัฒนาทางเทคโนโลยีในการป้องกันข้อมูลของภาคเอกชน[65]

ปัญหาที่เกิดขึ้นจากการที่ไม่มีบทบัญญัติในการลงโทษแก่การกระทำความผิดดังกล่าวนี้เองทำให้ประเทศไทยนั้นเป็นแหล่งอาชญากรรมในการกระทำความผิดดังกล่าวอย่างต่อเนื่องและเป็นอันดับต้นๆ ของภูมิภาคเอเชีย[66] ทั้งพบว่าเมื่อไม่มีบทบัญญัติดังกล่าวแล้ว ผู้ใช้กฎหมายจึงต้องหลีกเลี่ยงไปใช้กฎหมายอื่นๆ ในเรื่องเดียวกัน เช่น ความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ตามประมวลกฎหมายอาญา มาตรา 269/1 ความผิดฐานมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลงหรือสำหรับให้ได้ข้อมูลสำหรับปลอมหรือแปลง ตามมาตรา 269/2 หรือความผิดฐานใช้หรือมีไว้เพื่อใช้ซึ่งบัตรอิเล็กทรอนิกส์ตามมาตรา 269/4 วรรคแรก ตามแต่หลักฐานที่พบเจอในที่เกิดเหตุโดยมิได้คำนึงถึงข้อมูลในบัตรอิเล็กทรอนิกส์ว่าจะมีจำนวนมากเท่าไหร่ หรือคิดเป็นมูลค่าความเสียหายเท่าไหร่ ซึ่งถ้าหากมีบทบัญญัติเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ใช้บังคับ เมื่อรวมจำนวนกรรมของการกระทำความผิดต่อข้อมูลเหล่านั้นเข้าด้วยกัน อาจจะทำให้ผู้กระทำความผิดต้องรับโทษในสถานหนักกว่าบทบัญญัติที่ได้กล่าวมาแล้ว เพื่อให้การลงโทษนั้นมีความรุนแรงเหมาะสมกับพฤติการณ์ที่เกิดขึ้นจริงและทำให้เกิดการป้องกันและปราบปรามการกระทำความผิดดังกล่าวได้อย่างมีประสิทธิภาพ

ข้อเสียที่อาจจะเกิดขึ้นจากการมีบทบัญญัติให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นความผิดทางอาญามีดังต่อไปนี้

(1) เนื่องจากบัตรอิเล็กทรอนิกส์นั้นมีใช้อยู่หลากหลายและเป็นจำนวนมากจึงทำให้เกิดการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ที่ใดก็ได้ในราชอาณาจักรซึ่งทำให้เกิดความยุ่งยากในการสืบสวนว่าผู้กระทำผิดได้กระทำผิด ณ ที่ใด อันส่งผลต่อการกำหนดพนักงานสอบสวนผู้รับผิดชอบ ซึ่งหากไม่

---

[64] HOUSE OF REPRESENTATIVES, "Do the Payment Card Industry Data Standards Reduce Cybercrime?" [Online], Accessed: 8 November 2020. Available from: https://www.govinfo.gov/content/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm.

[65] Roza Lozusic, "Fraud and Identity Theft" [Online], Accessed: 8 November 2020. Available from: https://www.parliament.nsw.gov.au/researchpapers/Documents/fraud-and-identity-theft/08-03.pdf.

[66] Nophakhun Limsamarnphun, "Sharp Rise in Credit-Card Fraud Tipped" [Online], Accessed: 8 November 2020. Available from: https://www.nationthailand.com/business/30264690.

เป็นไปตามหลักเกณฑ์ที่กำหนดไว้ในประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 19[67] แล้วจะทำให้การสอบสวนนั้นเสียไปอันทำให้พนักงานอัยการไม่มีอำนาจฟ้องในคดีดังกล่าว

(2) เนื่องจากข้อมูลในบัตรอิเล็กทรอนิกส์นั้นเป็นพยานหลักฐานทางอิเล็กทรอนิกส์จึงทำให้การแสวงหาพยานหลักฐานทำได้ยากเพราะด้วยลักษณะของการเป็นข้อมูลที่เปลี่ยนแปลงได้ง่าย หมายความว่าสามารถลบ ย้ายหรือทำลายได้ก่อนที่จะพบการกระทำความผิดและก่อนที่ผู้กระทำความผิดจะถูกจับกุม ด้วยเหตุนี้เองในบางครั้งการเข้าตรวจค้นหรือเข้าจับกุมของเจ้าหน้าในการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์นั้นมักจะไม่พบเครื่องมืออื่นๆ นอกเสียจากบัตรอิเล็กทรอนิกส์ที่ได้ทำปลอมขึ้น อันส่งผลต่อข้อหาที่จำกัดในการดำเนินคดีแก่ผู้กระทำความผิดที่ต้องยึดโยงกับกลุ่มการปลอมบัตรอิเล็กทรอนิกส์หรือกลุ่มเครื่องมือในการทำบัตรอิเล็กทรอนิกส์ปลอมเท่านั้น[68] ดังที่พบบ่อยคือการฟ้องแต่เพียงความผิดฐานปลอมบัตรอิเล็กทรอนิกส์[69] ตามมาตรา 269/1 ฐานใช้หรือมีไว้เพื่อใช้ซึ่งบัตรอิเล็กทรอนิกส์ปลอม[70] ตามมาตรา 269/4 หรือฐานมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลงหรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์[71] ตามมาตรา 269/2 เท่านั้น นอกจากนั้นองค์ความรู้เรื่องการจัดการกับพยานหลักฐานอิเล็กทรอนิกส์ยังเป็น

---

[67] ป.วิ.อ. มาตรา 19 บัญญัติว่า “ในกรณีดังต่อไปนี้

(1) เป็นการไม่แน่ว่าการกระทำผิดอาญาได้กระทำในท้องที่ใดในระหว่างหลายท้องที่

(2) เมื่อความผิดส่วนหนึ่งกระทำในท้องที่หนึ่ง แต่อีกส่วนหนึ่งในอีกท้องที่หนึ่ง

(3) เมื่อความผิดนั้นเป็นความผิดต่อเนื่องและกระทำต่อเนื่องกันในท้องที่ต่าง ๆ เกินกว่าท้องที่หนึ่งขึ้นไป

(4) เมื่อเป็นความผิดซึ่งมีหลายกรรม กระทำลงในท้องที่ต่าง ๆ กัน

(5) เมื่อความผิดเกิดขึ้นขณะผู้ต้องหากำลังเดินทาง

(6) เมื่อความผิดเกิดขึ้นขณะผู้เสียหายกำลังเดินทาง

พนักงานสอบสวนในท้องที่หนึ่งท้องที่ใดที่เกี่ยวข้องมีอำนาจสอบสวนได้

ในกรณีข้างต้นพนักงานสอบสวนต่อไปนี้ เป็นผู้รับผิดชอบในการสอบสวน

(ก) ถ้าจับผู้ต้องหาได้แล้ว คือพนักงานสอบสวนซึ่งท้องที่ที่จับได้อยู่ในเขตอำนาจ

(ข) ถ้าจับผู้ต้องหายังไม่ได้ คือพนักงานสอบสวนซึ่งท้องที่ที่พบการกระทำผิดก่อนอยู่ในเขตอำนาจ”

[68] โปรดดูหัวข้อที่ 2.2.5 การกระทำความผิดที่เกี่ยวข้องกับฐานปลอมบัตรอิเล็กทรอนิกส์ และหัวข้อที่ 2.2.6 การกระทำความผิดที่เกี่ยวข้องกับฐานทำหรือมีเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์

[69] โพสต์ทูเดย์, "ไม่รอด!ผู้ต้องหาแก๊งสกริมเมอร์จนมุมตำรวจหลังหนีคดีนาน 10 ปี" [ออนไลน์], เข้าถึงเมื่อ 1 พฤศจิกายน 2563. แหล่งที่มา: https://www.posttoday.com/social/general/589470.

[70] เชียงใหม่นิวส์, "ตำรวจสืบภาค 5 โชว์รวบแก๊งสกิมเมอร์" [ออนไลน์], เข้าถึงเมื่อ 1 พฤศจิกายน 2563. แหล่งที่มา: https://www.chiangmainews.co.th/page/archives/668270/.

[71] กรุงเทพธุรกิจ, “จับคาหนังคาเขาแก๊งสกิมเมอร์จีนขณะติดอุปกรณ์คาตู้เอทีเอ็ม” [ออนไลน์], เข้าถึงเมื่อ 1 พฤศจิกายน 2563. แหล่งที่มา https://www.bangkokbiznews.com/news/detail/759274.

เรื่องใหม่สำหรับประเทศไทย ทำให้การเข้ารหัสข้อมูล (Encryption) ยังเป็นอุปสรรคที่ทำให้การเข้าถึงข้อมูลเพื่อแสวงหาว่ามีการดึงข้อมูลบัตรอิเล็กทรอนิกส์มาหรือไม่ อันเป็นพยานหลักฐานของเจ้าหน้าที่มีความยุ่งยาก และแม้ว่าจะสามารถเข้าถึงข้อมูลได้แต่ก็ต้องประสบกับปัญหาการขาดผู้เชี่ยวชาญในการวิเคราะห์เพื่อหาความเชื่อมโยงระหว่างผู้กระทำความผิดกับพยานหลักฐานที่เกิดขึ้นจากการกระทำความผิดนั้น[72] จึงทำให้การพิสูจน์ความผิดของผู้กระทำจนสิ้นความสงสัยตามสมควร (Beyond a Reasonable Doubt) ต่อศาลนั้นเป็นเรื่องยากหากจะบัญญัติให้มีการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นความผิดทางอาญา

(3) จากการศึกษาวิจัยกฎหมายเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศนั้น พบว่า การที่มีบทบัญญัติซึ่งกำหนดโทษทางอาญาแก่การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์มากกว่าหนึ่งมาตราและกระจัดกระจายออกไปในกฎหมายคนละฉบับกันจะทำให้ผู้ใช้กฎหมายไม่ว่าทั้งตำรวจอัยการและศาลที่ไม่เข้าใจปัญหาในเรื่องทางอิเล็กทรอนิกส์นั้นสับสนในการเลือกใช้บทบัญญัติในการลงโทษแก่ผู้กระทำความผิด[73] และอัยการจะมีแนวโน้มในการฟ้องผู้ต้องหาในบทบัญญัติที่มีอัตราโทษที่สูงกว่าบทบัญญัติในเรื่องดึงข้อมูลอื่นๆ[74] และหากเป็นเพียงการเพิ่มฐานความผิดที่มีความซ้ำซ้อนกับบทบัญญัติที่มีอยู่แล้วหรือเพียงแต่เป็นการเพิ่มโทษอันมากจนเกินไปก็จะทำให้บทบัญญัติกฎหมายนั้นมีความฟุ่มเฟือยได้[75] และการบัญญัติกฎหมายเกี่ยวกับการดึงข้อมูลโดยใช้คำที่กว้างจนเกินไปอาจจะทำให้ไม่อาจใช้ได้อย่างเฉพาะเจาะจงกับความผิดที่เกิดขึ้นจริงและต้องให้มีการตีความโดยศาลอีกครั้ง

---

[72] Thai netizen network, "พยานหลักฐานอิเล็กทรอนิกส์ แยกไม่ออกจาก “เศรษฐกิจดิจิทัล”" [ออนไลน์], เข้าถึงเมื่อ 1 พฤศจิกายน 2563. แหล่งที่มา: https://thainetizen.org/2016/01/digital-forensics-seminar-etda/.

[73] Peter Yapp, “The 30-year-old Computer Misuse Act is not fit for purpose” [Online], Accessed: 1 November 2020. Available from: https://www.scl.org/articles/10854-the-30-year-old-computer-misuse-act-is-not-fit-for-purpose.

[74] The Crown Prosecution Service, “Computer Misuse Act” [Online], Accessed: 17 October 2020. Available from: https://www.cps.gov.uk/legal-guidance/computer-misuse-act.

[75] Abet Dela Cruz, “Was Access Devices Regulation Act reboot really necessary?” [Online], Accessed: 10 October 2020. Available from: https://www.manilatimes.net/2019/10/02/opinion/columnists/topanalysis/was-access-devices-regulation-act-reboot-really-necessary/624758/.

หนึ่ง[76] และหากบทบัญญัตินั้นกำหนดอัตราโทษที่ตายตัวก็จะมิเปิดช่องให้ผู้พิพากษาได้ใช้ดุลพินิจในการกำหนดโทษตามสภาพความร้ายแรงในการกระทำความผิดเป็นกรณีๆ ไปได้[77]

อย่างไรก็ตามเมื่อชั่งน้ำหนักระหว่างผลเสียที่อาจจะเกิดขึ้น ความจำเป็นและผลดีของการกำหนดให้มีบทบัญญัติให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นความผิดทางอาญาแล้ว พบว่าการกำหนดให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นความผิดทางอาญาในประเทศไทยนั้นย่อมมีน้ำหนักมากกว่าผลเสียจากการไม่มีบทบัญญัติดังกล่าว ทั้งการกำหนดบทบัญญัติดังกล่าวนั้นมีความจำเป็นสอดคล้องกับสภาพการณ์ในปัจจุบันดังที่ได้กล่าวมาแล้ว ไม่ซ้ำซ้อนกับกฎหมายที่มีอยู่ ทั้งการบังคับใช้นี้จะไม่ก่อให้เกิดภาระกับประชาชนเกินสมควร ตามหลักการที่รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 77[78] ได้กำหนดไว้[79]

5.2 พิจารณาถึงลักษณะของกฎหมายอาญาที่จะให้มีการบัญญัติความผิดในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

เมื่อมีความจำเป็นต้องมีการบัญญัติให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้นเป็นความผิดทางอาญาแล้ว สิ่งที่จะต้องทำการวิเคราะห์ต่อไปก็คือสมควรที่จะให้บัญญัติไว้ในกฎหมายระดับใดและอยู่ในกฎหมายฉบับใด ซึ่งจำต้องนำกฎหมายที่ผู้วิจัยได้ทำการศึกษาคือ ประมวลกฎหมายอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาพิจารณาประกอบกับวัตถุประสงค์ที่กฎหมายต่างประเทศได้กำหนดไว้ เพื่อค้นหาข้อดี ข้อเสียและผลกระทบที่อาจจะเกิดขึ้นต่อบทบัญญัติข้างเคียงหากมีกฎหมายดังกล่าว เพื่อให้มีความเหมาะสมในการปรับใช้ต้องตามเจตนารมณ์ของกฎหมายได้มากที่สุด

---

[76] Andrew Michael Boulton, “SYNOPSIS OF THE CYBERCRIME ACT 2001” [Online], Accessed: 12 October 2020. Available from: https://www.giac.org/paper/gsec/4017/synopsis-cybercrime-act-2001/106427.

[77] ดูอัตราโทษของกฎหมายเครือรัฐออสเตรเลียที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ในหัวข้อที่ 4.4

[78] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 77 วรรคแรก บัญญัติว่า “รัฐพึงจัดให้มีกฎหมายเพียงเท่าที่จำเป็น และยกเลิกหรือปรับปรุงกฎหมายที่หมดความจำเป็นหรือไม่สอดคล้องกับสภาพการณ์ หรือที่เป็นอุปสรรคต่อการดำรงชีวิตหรือการประกอบอาชีพโดยไม่ชักช้าเพื่อไม่ให้เป็นภาระแก่ประชาชน และดำเนินการให้ประชาชนเข้าถึงตัวบทกฎหมายต่างๆ ได้โดยสะดวกและสามารถเข้าใจกฎหมายได้ง่ายเพื่อปฏิบัติตามกฎหมายได้อย่างถูกต้อง”

[79] สำนักงานเลขาธิการสภาผู้แทนราษฎร, "มาตรา 77 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย" [ออนไลน์], เข้าถึงเมื่อ 8 พฤศจิกายน 2563. แหล่งที่มา: https://www.parliament.go.th/section77/survey_about.php.

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 หมวด 3 สิทธิและเสรีภาพของปวงชนชาวไทย มาตรา 29 วางหลักไว้ว่า “บุคคลไม่ต้องรับโทษอาญา เว้นแต่ได้กระทำการอันกฎหมายที่ใช้อยู่ในเวลาที่กระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้” ดังนั้นความผิดทางอาญาใดๆ ดังเช่น การกำหนดให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นความผิดทางอาญานี้ จึงสมควรให้บัญญัติไว้เป็นกฎหมายในระดับพระราชบัญญัติ อันเป็นกฎหมายชั้นรองจากรัฐธรรมนูญเพราะเป็นกฎหมายที่ออกมาโดยอาศัยอำนาจของรัฐธรรมนูญโดยตรง[80] ซึ่งสอดคล้องกับกฎหมายของต่างประเทศที่ได้บัญญัติให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นความผิดทางอาญาอยู่ในกฎหมายในระดับพระราชบัญญัติทั้งสิ้น[81]

จากการศึกษาวิจัยพบว่า กฎหมายที่บัญญัติให้มีการกระทำความผิดอันเกี่ยวกับบัตรอิเล็กทรอนิกส์ในประเทศไทยนั้นมีอยู่เพียงสองฉบับ คือ ประมวลกฎหมายอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ดังนั้นการจะกำหนดให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ไปอยู่ในกฎหมายฉบับใด อันดับแรกจำต้องพิจารณาเจตนารมณ์และความมุ่งหมายของกฎหมายแต่ละฉบับเทียบกันเสียก่อน

เจตนารมณ์ของกฎหมายนั้น พิจารณาได้จากเหตุผลในหมายเหตุท้ายพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547 ที่ระบุว่า “เนื่องจากปัจจุบันการใช้เอกสาร วัตถุอื่นใดหรือข้อมูล ที่จัดทำขึ้นในลักษณะบัตรอิเล็กทรอนิกส์... กำลังเพิ่มปริมาณและประเภทการใช้งานอย่างแพร่หลาย และปรากฏว่าได้มีการกระทำความผิดเกี่ยวกับบัตรและลักลอบนำข้อมูลอิเล็กทรอนิกส์ของผู้อื่นมาใช้... สมควรกำหนดความผิดอาญาสำหรับการกระทำความผิดเกี่ยวกับบัตรและข้อมูลอิเล็กทรอนิกส์ดังกล่าวเพิ่มเติมให้ครอบคลุมการกระทำความผิดในรูปแบบต่างๆ” ด้วยเหตุผลดังกล่าวประกอบกับการที่มีบทบัญญัติในมาตรา 269/1 ถึงมาตรา 269/7 อันเป็นความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ซึ่งได้บัญญัติไว้แล้ว พบว่าประมวลกฎหมายอาญานั้น มุ่งจะกำหนดความผิดเพื่อใช้กับการกระทำต่างๆ ที่เกี่ยวกับบัตรอิเล็กทรอนิกส์โดยตรง ต้องตามความประสงค์ของการเป็นประมวลกฎหมายที่มีลักษณะให้การกระทำความผิดในเรื่องเดียวกันได้มีการเรียบเรียงไว้อย่างเป็นหมวดหมู่เดียวกันและมีความสัมพันธ์เกี่ยวเนื่องกัน

---

[80] รติกร เจือกโว้น, "กฎหมาย" [ออนไลน์], เข้าถึงเมื่อ 2 พฤศจิกายน 2563. แหล่งที่มา: http://wiki.kpi.ac.th/index.php?title=กฎหมาย.

[81] ดูบทที่ 4 กฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ

ส่วนเหตุผลในหมายเหตุท้ายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้นระบุว่า “เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญ... หากมีผู้... ใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ... สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว” ด้วยเหตุผลดังกล่าวประกอบกับการศึกษาบทบัญญัติที่เกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ที่กำหนดไว้ในมาตรา 8 และบทบัญญัติอื่นๆ ในพระราชบัญญัตินี้ พบว่าพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้นมุ่งคุ้มครองระบบคอมพิวเตอร์และข้อมูลในระบบคอมพิวเตอร์เป็นสำคัญ แม้จะได้มีการกำหนดให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ที่อยู่ในระบบคอมพิวเตอร์นั้นเป็นความผิดด้วยตามมาตรา 8 แต่ก็เพราะข้อมูลบัตรนั้นมีลักษณะเป็นข้อมูลคอมพิวเตอร์ซึ่งพระราชบัญญัตินี้มุ่งคุ้มครอง และใช้ในกรณีที่เกิดขึ้นกับระบบคอมพิวเตอร์อันเป็นการเฉพาะและอย่างจำกัดเท่านั้น[82] ซึ่งไม่รวมถึงการกระทำความผิดอันเกี่ยวกับบัตรอิเล็กทรอนิกส์อื่นหรือการดึงข้อมูลจากบัตรในรูปแบบอื่นๆ ด้วย

จากการศึกษากฎหมายของต่างประเทศ[83] พบว่าประเทศเหล่านั้นก็ได้บัญญัติเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ให้เป็นความผิดทางอาญาสอดแทรกอยู่ในกฎหมายหลายฉบับ อันจำแนกตามวัตถุประสงค์ของกฎหมายแต่ละฉบับ ได้ดังตารางต่อไปนี้

[82] จากการวิเคราะห์ในหัวข้อที่ 5.1 พิจารณาถึงความจำเป็นในการบัญญัติให้การดึงข้อมูลบัตรอิเล็กทรอนิกส์เป็นความผิดทางอาญา

[83] ดูบทที่ 4 กฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ

ตารางที่ 17 แสดงการบัญญัติกฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรในประเทศต่างๆ จำแนกตามวัตถุประสงค์ของกฎหมายแต่ละฉบับ

ประเทศ	วัตถุประสงค์ของกฎหมาย		
	เพื่อคุ้มครองข้อมูลส่วนบุคคล	เพื่อคุ้มครองข้อมูลคอมพิวเตอร์	เพื่อคุ้มครองข้อมูลบัตรที่ใช้เพื่อทำธุรกรรมทางการเงิน
สหรัฐอเมริกา	รัฐบัญญัติของสหรัฐอเมริกา (พัฒนามาจากพระราชบัญญัติข้อสันนิษฐานในการขัดขวางและการโจรกรรมข้อมูลส่วนบุคคล ค.ศ. 1998)	รัฐบัญญัติของสหรัฐอเมริกา (พัฒนามาจากพระราชบัญญัติการละเมิดและการฉ้อโกงทางคอมพิวเตอร์ ค.ศ. 1986)	รัฐบัญญัติของสหรัฐอเมริกา (พัฒนามาจากพระราชบัญญัติการฉ้อโกงบัตรเครดิต ค.ศ. 1984)
	มาตรา 1028(a)(7)	มาตรา 1030(a)(2)	มาตรา 1029(a)(1)
สหราชอาณาจักร	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990	พระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006
	มาตรา 170	มาตรา 1, 3A(3)	มาตรา 6
สาธารณรัฐฟิลิปปินส์	พระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012	พระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012	พระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988
	มาตรา 4(b)(3)	มาตรา 4(a)(1)	มาตรา 9(q), 9(k), 9(s), 9(t)

ประเทศ	วัตถุประสงค์ของกฎหมาย		
	เพื่อคุ้มครองข้อมูลส่วนบุคคล	เพื่อคุ้มครองข้อมูลคอมพิวเตอร์	เพื่อคุ้มครองข้อมูลบัตรที่ใช้เพื่อทำธุรกรรมทางการเงิน
เครือรัฐออสเตรเลีย	-	พระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001	พระราชบัญญัติแก้ไขกฎหมายอาชญากรรม (ความผิดด้านโทรคมนาคมและมาตรการอื่นๆ)(ฉบับที่ 2) ค.ศ. 2004
	-	มาตรา 477.1, 478.3, 478.4	มาตรา 480.4

ข้อสังเกต แม้สหรัฐอเมริกาจะมีรัฐบัญญัติของสหรัฐอเมริกาเพียงฉบับเดียว ที่มีบทบัญญัติเรื่องการดึงข้อมูลจากบัตรก็ตาม แต่ก็ได้รับการบัญญัติโดยมีที่มาจากการรวบรวมพระราชบัญญัติต่างๆ ในอดีตมารวมเข้าไว้ด้วยกันเป็นฉบับเดียวในลักษณะของประมวลกฎหมาย ดังนั้นแม้ว่าการดึงข้อมูลจากบัตรในสหรัฐอเมริกาจะอยู่ในกฎหมายฉบับเดียวกัน แต่ก็ได้แยกย่อยออกไปเป็นบทบัญญัติต่างๆ อันมีวัตถุประสงค์ในการคุ้มครองแตกต่างกันไปตามพระราชบัญญัติต่างๆ ที่ได้รวบรวมเอาไว้

จากตารางข้างต้นจึงสรุปได้ว่า การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ซึ่งเป็นความผิดอาญาที่บัญญัติในกฎหมายหลายฉบับของประเทศเหล่านั้น สามารถแบ่งจำแนกตามวัตถุประสงค์ของกฎหมายที่มุ่งจะคุ้มครองข้อมูลในรูปแบบต่างๆ กัน ได้ออกเป็น 3 รูปแบบดังนี้

(1) กฎหมายที่มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคล

กฎหมายที่มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคล (Personal Data) ได้รับการบัญญัติขึ้นเพื่อแก้ไขปัญหาการโจรกรรมข้อมูลส่วนบุคคล (Identity Theft) และเพื่อคุ้มครองข้อมูลของประชาชนจากการกระทำละเมิดจากองค์กรของภาครัฐและภาคเอกชนต่างๆ ที่ได้ควบคุมข้อมูลดังกล่าวไว้ ซึ่งประเทศต่างๆ เหล่านั้นก็ได้ให้คำนิยามของการเป็นข้อมูลส่วนบุคคลต่างกัน โดยอาจ

แจกแจงไว้เป็นกลุ่มๆ อย่างสหรัฐอเมริกา บัญญัติไว้กว้างๆ อย่างสหราชอาณาจักร หรือใช้การวางหลักโดยคำพิพากษาของศาลอย่างสาธารณรัฐฟิลิปปินส์ ก็ได้

(2) กฎหมายที่มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลคอมพิวเตอร์

กฎหมายที่มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลคอมพิวเตอร์ ได้รับการบัญญัติขึ้นเพื่อแก้ไขปัญหาอาชญากรรมทางคอมพิวเตอร์และการโจมตีทางไซเบอร์ เช่น การเข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือเกินกว่าที่ได้รับอนุญาต การกระทำที่กระทบต่อการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่อกับระบบอินเตอร์เน็ต เช่น การแฮกเข้าไปในระบบคอมพิวเตอร์ การใช้มัลแวร์ การแพร่กระจายไวรัส และเพื่อคุ้มครองข้อมูลในคอมพิวเตอร์ และที่สำคัญคือจะไม่คุ้มครองไปถึงข้อมูลที่บรรจุไว้ในแหล่งบันทึกข้อมูลคอมพิวเตอร์ (Computer data storage device) ต่างๆ ด้วย หากมิได้มีการบัญญัติไว้เป็นการเฉพาะ เช่น รัฐบัญญัติของสหรัฐอเมริกา

(3) กฎหมายที่มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลบัตรที่ใช้เพื่อทำธุรกรรมทางการเงิน

กฎหมายที่มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลบัตรที่ใช้เพื่อทำธุรกรรมทางการเงิน ได้รับการบัญญัติขึ้นเพื่อแก้ไขปัญหาอาชญากรรมบัตรชำระเงิน (Payment Card Fraud) เช่น การปลอมหรือแปลงบัตรและการกระทำความผิดในลักษณะอื่นๆ ที่มีบัตรที่ใช้ในการทำธุรกรรมทางการเงินเป็นวัตถุแห่งการกระทำความผิด เช่น รหัส หมายเลขใดๆ ของบัตรเอทีเอ็ม บัตรเครดิต บัตรเดบิต บัตรเงินสด บัตรเติมเงิน โดยสหรัฐอเมริกาและสาธารณรัฐฟิลิปปินส์ได้เรียกบัตรเหล่านั้นรวมกันไปว่าเป็น “อุปกรณ์ในการเข้าถึง” (Access device) ส่วนในสหราชอาณาจักรจะใช้คำว่า “สิ่งของ” (Article) และเครือรัฐออสเตรเลียจะใช้คำว่า “ข้อมูลทางการเงินของบุคคล” (Personal financial information)

เมื่อพิจารณาวัตถุประสงค์ของกฎหมายต่างประเทศแต่ละฉบับที่ได้กำหนดไว้ข้างต้น เมื่อนำมาเปรียบเทียบกับเจตนารมณ์และความมุ่งหมายของประมวลกฎหมายอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทยนั้น พบว่าจะมีข้อดีข้อเสียและผลกระทบที่อาจจะเกิดขึ้นต่อบทบัญญัติข้างเคียงหากมีบทบัญญัติให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้บรรจุไว้ในกฎหมายไทยดังกล่าว ดังนี้

(ก) การบัญญัติให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์บรรจุไว้ในประมวลกฎหมายอาญา

ข้อดี แม้ประมวลกฎหมายอาญาจะไม่ได้มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลในลักษณะใดลักษณะหนึ่งอันเป็นการเฉพาะเหมือนในกฎหมายต่างประเทศที่ได้กล่าวมาแล้ว แต่ก็เป็นการรวบรวมกฎหมายในเรื่องต่างๆ ที่มีโทษทางอาญาคล้ายกับรัฐบัญญัติของสหรัฐอเมริกา และถือเป็นกฎหมาย

หลักที่ได้มุ่งหมายให้มีการกำหนดความผิดอันเกี่ยวกับบัตรอิเล็กทรอนิกส์ในลักษณะต่างๆ ดังปรากฏในพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547 ที่มีเจตนารมณ์ให้มีการกำหนดความผิดอาญาสำหรับการกระทำความผิดเกี่ยวกับบัตรและข้อมูลอิเล็กทรอนิกส์เพิ่มเติมให้ครอบคลุมการกระทำความผิดในรูปแบบต่างๆ จึงมีวัตถุประสงค์เพื่อคุ้มครองข้อมูลบัตรในรูปแบบที่หลากหลาย ไม่ว่าบัตรนั้นจะมีลักษณะเป็นข้อมูลส่วนบุคคล ข้อมูลคอมพิวเตอร์ หรือข้อมูลเพื่อใช้ในการดำเนินธุรกรรมทางการเงินก็ตาม ดังนั้นหากได้มีการกำหนดความผิดในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ไว้ในประมวลกฎหมายอาญา ก็จะเป็นการทำตามเป้าปณิธานที่กฎหมายได้กำหนดไว้ให้มีบทบัญญัติที่ครอบคลุมกับการกระทำความผิดที่เกิดขึ้นจริงอย่างครบถ้วน โดยมีการเรียบเรียงการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ไว้อย่างเป็นหมวดหมู่และสัมพันธ์เกี่ยวเนื่องกัน และป้องกันความสับสนในการค้นหากฎหมายเพื่อนำมาลงโทษผู้กระทำความผิด ทำให้โทษในการดึงข้อมูลจากบัตรที่จะนำมาลงแก่ผู้กระทำความผิดนั้นสอดรับกับบทบัญญัติอื่นๆ ข้างเคียงในทิศทางเดียวกัน ทั้งการบัญญัติกฎหมายเกี่ยวกับการดึงข้อมูลบัตรไว้ในกฎหมายหลายฉบับ[84] นั้นก็เป็นการเพิ่มความหลากหลายในการเลือกใช้กฎหมายที่มีความเหมาะสมกับพฤติการณ์ในการกระทำความผิดที่เกิดขึ้นได้มากขึ้น ดังตัวอย่างในกฎหมายต่างประเทศที่มีบทบัญญัติอันสามารถใช้กับเรื่องดึงข้อมูลจากบัตรได้อยู่ในกฎหมายหลายฉบับ

ข้อเสีย การบัญญัติให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์บรรจุไว้ในประมวลกฎหมายอาญานั้น หากบัญญัติไว้ไม่รอบคอบแล้วก็อาจเกิดผลกระทบต่อบทบัญญัติใกล้เคียงในเรื่องการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์อื่นๆ ได้ ซึ่งอาจส่งผลให้บรรดาผู้ใช้กฎหมายที่ไม่เข้าใจในด้านเทคโนโลยีหรืออุปกรณ์อิเล็กทรอนิกส์นั้นสับสนในการปรับบทกฎหมายได้ ซึ่งความไม่เข้าใจและสับสนดังกล่าวอาจนำไปสู่การมองว่าเป็นการบัญญัติซ้ำซ้อนกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 8 อันเป็นกฎหมายที่มีอยู่แล้วได้

(ข) การบัญญัติให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์บรรจุไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ข้อดี การบัญญัติให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์บรรจุไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้นจะเป็นการสอดคล้องกับที่กฎหมายต่างประเทศได้กำหนดไว้ ซึ่งมีวัตถุประสงค์เพื่อคุ้มครองข้อมูลคอมพิวเตอร์ และเป็นการแก้ไขกฎหมายที่ง่ายเพราะเพียงแต่เพิ่มบทบัญญัติที่เกี่ยวกับการดึงข้อมูลจากบัตรในรูปแบบอื่นๆ นอกจากที่ได้กำหนดไว้แล้วในมาตรา 8

[84] คือ การบัญญัติไว้ทั้งในประมวลกฎหมายอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

และเมื่ออยู่ในกฎหมายฉบับเดียวกันจึงป้องกันการสับสนในการปรับใช้กฎหมายเพื่อลงโทษแก่ผู้กระทำความผิด

ข้อเสีย แม้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จะได้กำหนดความผิดเกี่ยวกับการดึงข้อมูลบัตรไว้แล้วในมาตรา 8 แต่ก็เพราะด้วยลักษณะของข้อมูลบัตรดังกล่าวนั้นเป็นข้อมูลคอมพิวเตอร์ด้วยตามความมุ่งหมายที่พระราชบัญญัตินี้ได้คุ้มครอง ซึ่งไม่รวมถึงข้อมูลบัตรอิเล็กทรอนิกส์ประเภทอื่นๆ ที่มิได้อยู่ในคอมพิวเตอร์ด้วย[85] ดังเช่นกฎหมายของสหรัฐอเมริกาหากจะให้รวมถึงข้อมูลบัตรในรูปแบบอื่นๆ ด้วยนั้น จะต้องมีการกำหนดหรือเปลี่ยนคำนิยามของคำว่า “ข้อมูลคอมพิวเตอร์” หรือ “ระบบคอมพิวเตอร์” ในพระราชบัญญัติให้รวมถึง “ข้อมูลที่บรรจุไว้ในแหล่งบันทึกข้อมูลคอมพิวเตอร์” (Computer data storage device) ด้วย ดังเช่นกฎหมายเกี่ยวกับคอมพิวเตอร์ของสหราชอาณาจักร สาธารณรัฐฟิลิปปินส์และเครือรัฐออสเตรเลีย อันเป็นการเปลี่ยนแปลงโครงสร้างกฎหมายของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้คุ้มครองข้อมูลอื่นๆ นอกเหนือไปจากข้อมูลในคอมพิวเตอร์ตามเจตนารมณ์ที่พระราชบัญญัติดังกล่าวได้กำหนดไว้ และการเปลี่ยนแปลงนี้จะก่อให้เกิดผลกระทบต่อหลักเกณฑ์ของบทบัญญัติข้างเคียงอื่นๆ ในพระราชบัญญัติฉบับนี้เป็นอย่างมาก ทั้งพระราชบัญญัติดังกล่าวนั้นเป็นกฎหมายเฉพาะที่ใช้ในการกระทำความผิดที่มีการกระทำการดึงข้อมูลบัตรอิเล็กทรอนิกส์ในระหว่างเครื่องคอมพิวเตอร์เท่านั้น ไม่รวมถึงการดึงข้อมูลบัตรอิเล็กทรอนิกส์ในรูปแบบอื่นๆ ที่ไม่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ด้วย หากกำหนดให้การดึงข้อมูลบัตรอิเล็กทรอนิกส์ทุกรูปแบบไปบัญญัติไว้ในพระราชบัญญัติดังกล่าว ก็อาจทำให้มีการตีความให้แคบลงเฉพาะที่เป็นการดึงข้อมูลในเครื่องคอมพิวเตอร์ตามวัตถุประสงค์ของพระราชบัญญัติดังกล่าว หรือทำให้บทบัญญัตินั้นบังคับใช้กับเรื่องที่ไม่ใช่คอมพิวเตอร์ซึ่งเกินเลยไปจากขอบเขตของกฎหมายดังกล่าวได้

เมื่อได้ชั่งน้ำหนักระหว่างผลดีและผลเสียดังกล่าว ทั้งพิเคราะห์ถึงเจตนารมณ์และความมุ่งหมายของกฎหมาย ประกอบการศึกษาวัตถุประสงค์ในการคุ้มครองข้อมูลของกฎหมายต่างประเทศแล้ว ผู้วิจัยจึงเห็นควรกำหนดให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นความผิดทางอาญาโดยการบัญญัติเป็นกฎหมายในระดับพระราชบัญญัติและบรรจุไว้ในประมวลกฎหมายอาญาในภาค 2 ลักษณะ 7 หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ต่อไป

---

[85] จากการศึกษาอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime : ETS No.185) อันเป็นที่มาของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทยนั้น พบว่ามิได้บัญญัติให้ ข้อมูลที่บรรจุไว้ในแหล่งบันทึกข้อมูลคอมพิวเตอร์ (Computer data storage device) เป็นข้อมูลคอมพิวเตอร์ (computer data) หรือระบบคอมพิวเตอร์ (computer system) ด้วย

5.3 พิจารณาถึงรูปแบบในการบัญญัติกฎหมายเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

เมื่อเห็นสมควรกำหนดให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นความผิดทางอาญาในประมวลกฎหมายอาญาแล้วนั้น ประเด็นต่อไปที่จะต้องทำการวิเคราะห์ก็คือจะบัญญัติกฎหมายในลักษณะใด เพื่อให้ต้องตามความประสงค์ที่จะแก้ไขปัญหาการขาดบทบัญญัติในการลงโทษ[86] ซึ่งสามารถจำแนกปัญหาดังกล่าวออกได้เป็นสองลักษณะคือ ปัญหาจากคำนิยามในประมวลกฎหมายอาญามาตรา 1(14) และปัญหาการขาดบทบัญญัติเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์อันเป็นการเฉพาะ ดังนั้นจึงสมควรพิจารณารูปแบบในการบัญญัติกฎหมายโดยแบ่งเป็นสองลักษณะประกอบกันคือ การบัญญัติกฎหมายโดยการแก้ไขคำนิยามที่มีอยู่เดิมในกฎหมายและการเพิ่มเป็นบทบัญญัติเฉพาะ ทั้งนำกฎหมายของต่างประเทศที่ศึกษามาแล้ว[87] มาพิจารณาประกอบด้วย เพื่อหาแนวทางที่เหมาะสมที่สุดในการบัญญัติกฎหมายเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ดังกล่าว

5.3.1 พิจารณาถึงรูปแบบในการบัญญัติกฎหมายโดยการแก้ไขคำนิยามที่มีอยู่เดิมในประมวลกฎหมายอาญา

เนื่องจากปัญหาในประการแรกนั้นคือ ปัญหาของคำนิยามคำว่า “บัตรอิเล็กทรอนิกส์” ที่ได้บัญญัติไว้ในประมวลกฎหมายอาญามาตรา 1(14) ซึ่งไม่ครอบคลุม ข้อมูลที่ได้บันทึกไว้บนพื้นผิวของบัตรหรือในแหล่งบันทึกความจำของบัตร เช่น ข้อมูลในแถบแม่เหล็ก (Magnetic Strip) หรือในชิป (Chip) ของบัตรที่ “มีการออกเอกสารหรือวัตถุอื่นใดให้” ด้วย[88] ซึ่งทำให้เกิดปัญหาว่า ข้อมูลบัตรอิเล็กทรอนิกส์นั้นจะไม่ได้รับความคุ้มครองอย่างเสมอภาคกันในทุกประเภท ดังนั้นในหัวข้อนี้ ผู้วิจัยจะทำการวิเคราะห์การเป็นบัตรอิเล็กทรอนิกส์ของประมวลกฎหมายอาญาเทียบกับความคุ้มครองที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ในกฎหมายต่างประเทศ[89] เพื่อหาแนวทางที่เหมาะสมในการบัญญัตินิยามคำว่า “บัตรอิเล็กทรอนิกส์” ในประมวลกฎหมายอาญาของประเทศไทยต่อไป

---

[86] โปรดดูหัวข้อที่ 3.3 ปัญหาการขาดบทบัญญัติในการลงโทษสำหรับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

[87] ดูบทที่ 4 กฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ

[88] โปรดดูหัวข้อที่ 3.3.1 ปัญหาจากคำนิยาม ตามมาตรา 1(14)

[89] ดูบทที่ 4 กฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ

จากการนำความหมายของ “บัตรอิเล็กทรอนิกส์” ในประมวลกฎหมายอาญามาตรา 1(14)[90] มาพิเคราะห์ร่วมกับปัญหาจากคำนิยามนั้น[91] จึงสามารถจำแนกการเป็นบัตรอิเล็กทรอนิกส์ได้ตามตารางดังต่อไปนี้

ตารางที่ 18 แสดงการเป็นบัตรอิเล็กทรอนิกส์ตามคำนิยาม ในประมวลกฎหมายอาญามาตรา 1(14)

รูปแบบของบัตร	มาตรา	การเป็น “บัตรอิเล็กทรอนิกส์” ในประมวลกฎหมายอาญา	
		เป็นบัตรอิเล็กทรอนิกส์	ไม่เป็นบัตรอิเล็กทรอนิกส์
เอกสาร ไม่ว่าจะมีรูปลักษณะใด ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์	1(14)(ก)	/	
วัตถุอื่นใด ไม่ว่าจะมีรูปลักษณะใด ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์	1(14)(ก)	/	
ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ <u>โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้</u>	1(14)(ข)	/	

[90] โปรดดูหัวข้อที่ 2.1.1 นิยามของบัตรอิเล็กทรอนิกส์

[91] โปรดดูหัวข้อที่ 3.3.1 ปัญหาจากคำนิยาม ตามมาตรา 1(14)

รูปแบบของบัตร	มาตรา	การเป็น “บัตรอิเล็กทรอนิกส์” ในประมวลกฎหมายอาญา	
		เป็นบัตรอิเล็กทรอนิกส์	ไม่เป็นบัตรอิเล็กทรอนิกส์
ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยมีการออกเอกสารหรือวัตถุอื่นใดตามมาตรา 1(14)(ก) ให้ด้วย	-		/
สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ	1(14)(ค)	/	

จากตารางดังกล่าวจึงสรุปได้ว่า เฉพาะข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยมีการออกเอกสารหรือวัตถุอื่นใดตามมาตรา 1(14)(ก) ให้ด้วย จะไม่เป็น “บัตรอิเล็กทรอนิกส์” ตามคำนิยามในประมวลกฎหมายอาญา ไม่ว่าข้อมูล รหัส หมายเลขนั้น จะบันทึกไว้บนพื้นผิวของบัตรหรือในแหล่งบันทึกความจำของบัตรก็ตาม

ในกฎหมายต่างประเทศที่ผู้วิจัยได้ทำการศึกษาแล้วนั้น พบว่ามีการกำหนดลักษณะการคุ้มครองอันเกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ดังนี้

(1) ความคุ้มครองที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ในกฎหมายของสหรัฐอเมริกา

สหรัฐอเมริกานั้นได้ให้ความคุ้มครองกับข้อมูลส่วนบุคคล ที่ได้กำหนดให้เป็น “สิ่งที่อ้างอิงในการระบุตัวตน” (A means of identification) ซึ่งหมายถึงชื่อหรือหมายเลขใดๆ ที่ใช้ในการระบุตัวตนของบุคคลโดยเฉพาะเจาะจง รวมถึงเอกลักษณ์ทางชีวภาพ (Biometric data) ของบุคคลด้วย ทั้งให้ความคุ้มครองบัตรที่ใช้เพื่อทำธุรกรรมทางการเงิน ซึ่งได้กำหนดให้เป็น “อุปกรณ์ในการเข้าถึง” (Access device) โดยไม่ว่าจะอยู่ในรูปของวัตถุเช่น บัตร ป้าย อุปกรณ์หรือเครื่องมือต่างๆ หรือในรูปของข้อมูล เช่น รหัส หมายเลขบัญชี หรือในรูปของวิธีการอื่นใดก็ตามที่สามารถใช้เพื่อดำเนินธุรกรรมทางการเงินได้ รวมทั้งส่วนประกอบของสิ่งเหล่านั้น และยังให้ความคุ้มครองข้อมูลในรูปแบบ

อิเล็กทรอนิกส์ที่อยู่ในคอมพิวเตอร์ซึ่งได้กำหนดไว้สามประเภท คือ ข้อมูลของสถาบันการเงิน หน่วยงานหรือองค์กรของรัฐและข้อมูลในเครื่องคอมพิวเตอร์ที่มีการป้องกันอีกด้วย

ข้อดีของกฎหมายของสหรัฐอเมริกาคือ การกำหนดลักษณะของข้อมูลที่คุ้มครองพร้อมกับบัญญัติตัวอย่างให้ผู้ใช้กฎหมายได้เข้าใจไว้อย่างละเอียดพอสมควร แต่ข้อเสียคือ การกำหนดลักษณะบางอย่างมีความซับซ้อนและอาจทำให้เข้าใจได้ยาก เช่น การกำหนดลักษณะบัตรที่ต้องการคุ้มครองให้เรียกรวมกันว่าเป็น “อุปกรณ์ในการเข้าถึง” ทั้งมิได้ให้ความคุ้มครองแก่อุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ให้เป็นข้อมูลคอมพิวเตอร์อย่างประเทศอื่นๆ ด้วย แต่อย่างไรก็ตามอุปกรณ์ชนิดนี้ก็อาจได้รับการคุ้มครองในฐานะที่เป็น “สิ่งที่อ้างอิงในการระบุตัวตน” หรือ “อุปกรณ์ในการเข้าถึง” ก็ได้

(2) ความคุ้มครองที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ในกฎหมายของสหราชอาณาจักร

สหราชอาณาจักรนั้นได้ให้ความคุ้มครองกับข้อมูลส่วนบุคคล ซึ่งหมายถึงข้อมูลใดๆ ก็ตามที่เกี่ยวข้องกับบุคคลที่ใช้ระบุตัวตนได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ หมายเลขประจำตัว ที่อยู่ รวมถึงข้อมูลทางสรีระ ลักษณะทางพันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรมและสังคมของบุคคล และให้ความคุ้มครองกับข้อมูลหรือโปรแกรมใดๆ ก็ตามที่อยู่ในรูปแบบอิเล็กทรอนิกส์ ที่ได้กำหนดให้เป็น “สิ่งของ” (Article) ซึ่งจะเป็นข้อมูลใดๆ ก็ได้ อาทิ ข้อมูลส่วนบุคคล ข้อมูลทางการเงินหรือข้อมูลคอมพิวเตอร์ ทั้งให้ความคุ้มครองข้อมูลใดๆ ที่อยู่ในเครื่องคอมพิวเตอร์และข้อมูลที่อยู่ในอุปกรณ์ในการจัดเก็บข้อมูล (Storage medium) ในขณะเวลาที่อุปกรณ์นั้นได้เชื่อมต่อและรับรู้โดยเครื่องคอมพิวเตอร์แล้วด้วย

ข้อดีของกฎหมายของสหราชอาณาจักรคือ การคุ้มครองข้อมูลส่วนบุคคลที่มีความครอบคลุมมากกว่าประเทศอื่นๆ และการกำหนดลักษณะบัตรไว้อย่างกว้างๆ กระชับ เช่น การกำหนดให้เป็น “สิ่งของ” (Article) ซึ่งจะเป็นข้อมูลใดๆ ก็ได้ รวมถึงการคุ้มครองข้อมูลในอุปกรณ์ในการจัดเก็บข้อมูลในขณะเวลาที่ได้เชื่อมต่อกับคอมพิวเตอร์ด้วย แต่ข้อเสียคือ ไม่ได้กำหนดความคุ้มครองแก่ตัวบัตรที่อยู่ในรูปแบบของเอกสารหรือวัตถุใดๆ ซึ่งไม่ได้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ด้วย

(3) ความคุ้มครองที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ในกฎหมายของสาธารณรัฐฟิลิปปินส์

สาธารณรัฐฟิลิปปินส์นั้นได้ให้ความคุ้มครองกับข้อมูลประจำตัวของบุคคลที่เกี่ยวข้องกับคอมพิวเตอร์ ซึ่งศาลฎีกาของสาธารณรัฐฟิลิปปินส์ได้อธิบายว่าคือ ข้อมูลประจำตัวปกติเกี่ยวกับบุคคล เช่น ชื่อ ที่อยู่ หมายเลขติดต่อ ข้อมูลบัตรเครดิต และยังให้ความคุ้มครองบัตรที่ใช้เพื่อทำธุรกรรมทางการเงิน ซึ่งได้กำหนดให้เป็น “อุปกรณ์ในการเข้าถึง” (Access device) หมายถึง บัตรใดๆ ก็ตาม

ไม่ว่าจะอยู่ในรูปของวัตถุเช่น บัตร ป้าย อุปกรณ์ที่ใช้ในการโทรคมนาคมหรือในการระบุตัวตน หรืออยู่ในรูปของข้อมูลเช่น รหัส หมายเลขบัญชี หมายเลขทางอิเล็กทรอนิกส์ หมายเลขประจำตัวบุคคล รวมถึง สลิป กระดาษ หรือสิ่งใดที่พิมพ์นูนหรือระบุไว้บนอุปกรณ์ในการเข้าถึง และยังรวมถึง “บัตรชำระเงิน” (Payment Card) ซึ่งไม่ว่าจะทำด้วยวัสดุใดหรืออยู่ในรูปแบบใดด้วย รวมถึงข้อมูลในบัตรเครดิต บัตรเดบิต บัญชีธนาคารออนไลน์ บัญชีบัตรเครดิต บัญชีเอทีเอ็ม บัญชีบัตรเดบิต ทั้งยังให้ความคุ้มครองข้อมูลในระบบคอมพิวเตอร์ เซิฟเวอร์ ระบบข้อมูลหรือระบบสื่อสาร และอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ (Computer data storage devices) ด้วย

ข้อดีของกฎหมายของสาธารณรัฐฟิลิปปินส์คือ มีการกำหนดลักษณะบัตรที่เกี่ยวข้องกับการดำเนินธุรกรรมทางการเงินไว้อย่างละเอียดกว่าประเทศอื่นๆ รวมถึงการคุ้มครองข้อมูลที่อยู่ในอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ด้วย แต่ข้อเสียคือ มิได้ให้คำนิยามของข้อมูลประจำตัวของบุคคลไว้จนทำให้ต้องตีความโดยศาล ทั้งข้อมูลประจำตัวดังกล่าวนั้นต้องเกี่ยวข้องกับคอมพิวเตอร์เท่านั้น ไม่ได้รวมถึงข้อมูลส่วนบุคคลทั่วๆ ไป ทั้งไม่รวมถึงข้อมูลทางชีวภาพของบุคคลด้วย

(4) ความคุ้มครองที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ในกฎหมายของเครือรัฐออสเตรเลีย

เครือรัฐออสเตรเลียนั้นได้ให้ความคุ้มครองบัตรที่ใช้เพื่อทำธุรกรรมทางการเงิน ซึ่งได้กำหนดให้เป็น “ข้อมูลทางการเงินของบุคคล” (Personal financial information) อันหมายถึงข้อมูลที่เกี่ยวข้องกับบุคคลที่นำไปใช้ในการเข้าถึงเงิน เครดิต หรือประโยชน์ทางการเงินได้ และคุ้มครองข้อมูล (Data) ไม่ว่าอยู่ในรูปลักษณะใดก็ตาม และยังให้ความคุ้มครองข้อมูลที่อยู่ในคอมพิวเตอร์ รวมถึงข้อมูลที่อยู่ในอุปกรณ์จัดเก็บข้อมูล (Data storage device) ในขณะที่ข้อมูลนั้นได้อยู่ในคอมพิวเตอร์ด้วย

ข้อดีของกฎหมายของเครือรัฐออสเตรเลียคือ การบัญญัติกฎหมายไว้อย่างกว้างๆ ซึ่งครอบคลุมลักษณะของบัตรได้มาก เช่น ข้อมูล (Data) ที่ได้กำหนดว่า ไม่ว่าอยู่ในรูปลักษณะใด รวมถึงการคุ้มครองข้อมูลที่อยู่ในอุปกรณ์จัดเก็บข้อมูลในขณะที่อุปกรณ์นั้นได้เชื่อมต่ออยู่กับคอมพิวเตอร์ด้วย แต่ข้อเสียคือ การกำหนดไว้กว้างจนเกินไปจนเปิดช่องให้อาจต้องตีความอีกครั้ง และแม้ว่าจะคุ้มครองข้อมูลไม่ว่าอยู่ในรูปลักษณะใด แต่ก็ต้องมีเจตนาพิเศษที่จะใช้หรืออำนวยความสะดวกในการกระทำผิดอันร้ายแรงที่เกี่ยวกับคอมพิวเตอร์ต่อไปด้วย ซึ่งเป็นการจำกัดความหมายของข้อมูลดังกล่าว ทั้งเครือรัฐออสเตรเลียก็ยังไม่มีกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลอันเป็นการเฉพาะอีกด้วย

ตารางที่ 19 สรุปลักษณะความคุ้มครองที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ในกฎหมายฉบับต่างๆ ของต่างประเทศ

ประเทศ	กฎหมาย		ลักษณะของความคุ้มครองที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์
	พระราชบัญญัติ	มาตรา	
สหรัฐอเมริกา	รัฐบัญญัติของสหรัฐอเมริกา	1028 (a)(7)	สิ่งที่อ้างอิงในการระบุตัวตน (A means of identification) ของผู้อื่น
		1029 (e)(1)	อุปกรณ์ในการเข้าถึง (Access devices)
		1029 (a)(1)	อุปกรณ์ในการเข้าถึงปลอม (Counterfeit access devices) หมายถึง ข้อมูลของบัตรใดๆ ที่มีวัตถุประสงค์ในการใช้ทำธุรกรรมทางการเงิน
		1030 (a)(2)	ข้อมูลในรูปแบบอิเล็กทรอนิกส์ที่อยู่ในคอมพิวเตอร์ที่ได้กำหนดไว้สามประเภท
สหราชอาณาจักร	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990	1, 17(6)	ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ (รวมถึงข้อมูลที่อยู่ในอุปกรณ์ในการจัดเก็บข้อมูล (Storage medium) ในขณะเวลาที่อุปกรณ์นั้นได้เชื่อมต่อและรับรู้โดยเครื่องคอมพิวเตอร์แล้ว)
		3A(3), 3A(4)	สิ่งของ (Article) หมายถึง ข้อมูล หรือโปรแกรมใดๆ ก็ตามที่อยู่ในรูปแบบอิเล็กทรอนิกส์
	พระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006	6, 8	สิ่งของ (Article) หมายถึง ข้อมูล หรือโปรแกรมใดๆ ก็ตามที่อยู่ในรูปแบบอิเล็กทรอนิกส์
	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018	170, 3(2)	ข้อมูลส่วนบุคคล (Personal data) หมายถึง ข้อมูลใดๆ ที่เกี่ยวข้องกับบุคคลที่มีชีวิตที่ระบุตัวตนได้

ประเทศ	กฎหมาย		ลักษณะของความคุ้มครองที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์
	พระราชบัญญัติ	มาตรา	
	กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR)	4(1)	ข้อมูลส่วนบุคคล (Personal data) หมายถึง ข้อมูลใดๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัวตนได้ ทั้งทางตรงหรือทางอ้อม
สาธารณรัฐฟิลิปปินส์	พระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012	4(a)(1)	อุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ (Computer data storage devices)
		4(b)(3)	ข้อมูลประจำตัวของบุคคล (Identifying information) หมายถึง ข้อมูลประจำตัวปกติเกี่ยวกับบุคคล
	พระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 ที่ได้แก้ไขเพิ่มเติมแล้ว	9(q), 3(b), 3(o)	บัตรเครดิต บัตรชำระเงิน บัตรเดบิต
		9(k), 3(a)	อุปกรณ์ในการเข้าถึง (Access Device)
		9(s)	บัญชีธนาคารออนไลน์ บัญชีบัตรเครดิต บัญชีเอทีเอ็ม บัญชีบัตรเดบิต
		9(t)	ข้อมูลในระบบคอมพิวเตอร์ เซิฟเวอร์ ระบบข้อมูล หรือระบบสื่อสาร

ประเทศ	กฎหมาย		ลักษณะของความคุ้มครอง ที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์
	พระราชบัญญัติ	มาตรา	
เครือรัฐออสเตรเลีย	พระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001	477.1, 476.1	ข้อมูลที่อยู่ในคอมพิวเตอร์ (Data held in computer) (รวมถึงข้อมูลที่อยู่ในอุปกรณ์จัดเก็บข้อมูล (Data storage device) ในขณะที่ข้อมูลนั้นได้อยู่ในคอมพิวเตอร์ด้วย)
		478.3, 478.4, 476.1	ข้อมูล (Data) ไม่ว่าอยู่ในรูปลักษณะใดก็ตาม
	พระราชบัญญัติแก้ไขกฎหมายอาชญากรรม (ความผิดด้านโทรคมนาคม และมาตรการอื่นๆ) (ฉบับที่ 2) ค.ศ. 2004	480.4	ข้อมูลทางการเงินของบุคคล (Personal financial information) หมายถึง ข้อมูลที่เกี่ยวข้องกับบุคคลที่อาจนำไปใช้โดยลำพังหรือประกอบกับข้อมูลอื่นในการเข้าถึงเงิน เครดิต หรือประโยชน์ทางการเงินอื่น

เมื่อพิจารณาการเป็นบัตรอิเล็กทรอนิกส์ของประมวลกฎหมายอาญาเปรียบเทียบกับความคุ้มครองที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ในกฎหมายต่างประเทศที่กล่าวไว้ข้างต้นแล้วพบว่า ไม่ว่ากฎหมายไทยหรือกฎหมายต่างประเทศนั้นก็ได้บัญญัติให้มีการคุ้มครองบัตรอิเล็กทรอนิกส์ไม่ว่าจะอยู่ในรูปแบบของเอกสารหรือวัตถุอื่นใด หรือจะอยู่ในรูปแบบของข้อมูลก็ตาม ข้อแตกต่างกันก็คือกฎหมายของต่างประเทศนั้นส่วนใหญ่แล้วจะบัญญัติโดยกล่าวถึงลักษณะของข้อมูลที่กฎหมายมุ่งจะคุ้มครองเป็นสำคัญมากกว่าจะบัญญัติโดยการกล่าวถึงอุปกรณ์ที่ข้อมูลนั้นได้บรรจุไว้อยู่ กล่าวคือในเรื่องเกี่ยวกับบัตรอิเล็กทรอนิกส์นี้ กฎหมายต่างประเทศนั้นมุ่งจะคุ้มครองข้อมูลในบัตร มากกว่าการคุ้มครองตัวบัตรในฐานะที่เป็นเพียงเอกสารหรือวัตถุอื่นใดชิ้นหนึ่ง และที่สำคัญคือกฎหมายต่างประเทศนั้น มิได้นำการออกเอกสารหรือวัตถุอื่นใด มาเป็นข้อจำกัดในการคุ้มครองข้อมูลอย่างที่ประมวลกฎหมายอาญามาตรา 1(14)(ข) ได้บัญญัติไว้ กฎหมายของต่างประเทศจึงให้ความคุ้มครอง

ข้อมูลที่ได้บันทึกไว้ไม่ว่าที่ใดๆ ก็ตาม เช่น บันทึกไว้ในแหล่งบันทึกของบัตรอิเล็กทรอนิกส์อันถือได้ว่าเป็นอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์รูปแบบหนึ่ง หรือบันทึกไว้ในเครื่องคอมพิวเตอร์

ข้อมูลที่กฎหมายต่างประเทศให้ความสำคัญในการคุ้มครองนั้นแบ่งได้ออกเป็น 3 ประเภท คือ ข้อมูลส่วนบุคคล ข้อมูลคอมพิวเตอร์และข้อมูลที่ใช้ในการทำธุรกรรมทางการเงิน โดยบัญญัติกระจัดกระจายกันไปขึ้นอยู่กับวัตถุประสงค์ของกฎหมายในแต่ละฉบับและมีรายละเอียดในการบัญญัติไม่เท่ากัน เช่น กฎหมายของสหรัฐอเมริกาจะรวมประเภทของข้อมูลเป็นกลุ่มๆ พร้อมกับการบัญญัติชื่อของกลุ่มนั้นใหม่และบัญญัติตัวอย่างไว้อย่างละเอียดพอสมควร กฎหมายของสหราชอาณาจักรจะบัญญัติเรื่องข้อมูลส่วนบุคคลไว้อย่างละเอียดมากกว่าประเทศอื่นๆ กฎหมายของสาธารณรัฐฟิลิปปินส์จะบัญญัติเรื่องข้อมูลที่เกี่ยวข้องกับการดำเนินธุรกรรมทางการเงินไว้อย่างละเอียดมากกว่าประเทศอื่นๆ กฎหมายของเครือรัฐออสเตรเลียจะบัญญัติเรื่องข้อมูลไว้อย่างกว้างๆ แต่ไม่ว่าอย่างไรก็ตาม การบัญญัติกฎหมายของต่างประเทศเหล่านั้นก็ย่อมมีข้อบกพร่องและไม่ครอบคลุมถึงลักษณะบางอย่างดังที่กล่าวไปแล้ว เช่น มิได้บัญญัติให้ข้อมูลบางอย่างเป็นข้อมูลคอมพิวเตอร์ด้วย มิได้กำหนดไปถึงบัตรอิเล็กทรอนิกส์ที่เป็นเอกสารหรือวัตถุอื่นใด มิได้บัญญัติรวมไปถึงข้อมูลทางชีวภาพของบุคคล หรือแม้กระทั่งไม่มีกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลเลย

บทบัญญัติในประมวลกฎหมายอาญามาตรา 1(14) แม้ว่าจะมิได้แยกออกเป็น ข้อมูลส่วนบุคคล ข้อมูลคอมพิวเตอร์และข้อมูลที่ใช้ในการทำธุรกรรมทางการเงินอย่างชัดเจนเหมือนในกฎหมายต่างประเทศ แต่มาตรา 1(14)(ข) ก็ได้บัญญัติถึงข้อมูล รหัส หมายเลขชุดทางอิเล็กทรอนิกส์ ในความหมายทั่วไปและมิได้เจาะจงว่าจะเป็นข้อมูลในลักษณะใด อาจจะเป็นข้อมูลส่วนบุคคล ข้อมูลคอมพิวเตอร์ หรือข้อมูลที่ใช้ในการทำธุรกรรมทางการเงินก็ได้ ซึ่งผู้วิจัยเห็นว่าการบัญญัติแบบนี้จะเป็นผลดีมากกว่าการลงรายละเอียดต่างๆ เพื่อให้กฎหมายอาญามีความยืดหยุ่น รองรับพฤติการณ์ในการกระทำความผิดที่เกี่ยวกับข้อมูลต่างๆ ตามเทคโนโลยีที่อาจเกิดขึ้นได้ในอนาคต และแม้จะมิได้บัญญัติข้อมูลที่ใช้ในการทำธุรกรรมทางการเงินเอาไว้เป็นการเฉพาะ แต่หากบัตรอิเล็กทรอนิกส์นั้นเป็นบัตรที่เกี่ยวข้องกับการดำเนินธุรกรรมทางการเงินแล้ว ผู้กระทำความผิดก็ต้องรับโทษหนักขึ้นตามมาตรา 269/7 ทั้งมาตรา 1(14)(ค) ก็ได้บัญญัติถึงข้อมูลที่เป็นเอกลักษณ์ทางชีวภาพของบุคคล อันถือว่าเป็นข้อมูลส่วนบุคคลประเภทหนึ่งที่กำหนดไว้ในกฎหมายของต่างประเทศเช่นกัน ดังนั้นจะเห็นได้ว่า แม้คำนิยามของคำว่า “บัตรอิเล็กทรอนิกส์” ในประมวลกฎหมายอาญาของประเทศไทยจะแตกต่างไปจากความคุ้มครองที่กฎหมายต่างประเทศได้บัญญัติไว้บ้าง แต่ก็มีความใกล้เคียงกันและได้รับความคุ้มครองคล้ายกัน โดยกฎหมายต่างประเทศนั้นจะให้ความสำคัญกับการคุ้มครองข้อมูลเป็นหลัก ดังนั้นบัตรอิเล็กทรอนิกส์ไม่ว่ารูปแบบใด หากเป็นวัตถุหรือข้อมูลที่ต่างประเทศได้กำหนดไว้ก็จะได้รับความคุ้มครองหมดทั้งสิ้น ในขณะที่ประมวลกฎหมายอาญาของไทยนั้นจะแบ่งบัตร

อิเล็กทรอนิกส์ออกเป็น 3 ประเภทใหญ่ๆ คือ (1) บัตรหรือวัตถุอื่นใดในลักษณะที่จับต้องได้ (Physical Cards) ในมาตรา 1(14)(ก) (2) ข้อมูล รหัส หมายเลขชุดทางอิเล็กทรอนิกส์ใดๆ ในลักษณะที่จับต้องไม่ได้ (Virtual Cards) ในมาตรา 1(14)(ข) และ (3) เอกลักษณ์ทางชีวภาพของบุคคลในลักษณะที่เป็นส่วนหนึ่งของมนุษย์ (Biometric data) ในมาตรา 1(14)(ค)

เมื่อพิจารณาเจตนารมณ์กฎหมายในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ที่ได้กำหนดไว้ในหมายเหตุท้ายพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา ฉบับที่ 17 พ.ศ. 2547 ตอนหนึ่งว่า “สมควรกำหนดความผิดอาญา... เกี่ยวกับบัตรและข้อมูลอิเล็กทรอนิกส์...ให้ครอบคลุม” และจากการศึกษากฎหมายของต่างประเทศแล้ว การบัญญัติคำนิยามของบัตรอิเล็กทรอนิกส์ โดยการนำข้อความว่า “โดยมิได้มีการนำการออกเอกสารหรือวัตถุอื่นใดให้” มาเป็นข้อจำกัดในการคุ้มครองข้อมูลอย่างที่ประมวลกฎหมายอาญามาตรา 1(14)(ข) ได้บัญญัติไว้ จึงไม่ต้องตามเจตนารมณ์ของประมวลกฎหมายอาญาและขัดกับความคุ้มครองที่กฎหมายของต่างประเทศได้กำหนดไว้ด้วย ประกอบกับผู้วิจัยเห็นว่าเนื้อหาของกฎหมายที่แท้จริงแล้ว บัตรอิเล็กทรอนิกส์น่าจะหมายถึงเอกสารหรือวัตถุอื่นใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งรวมถึงข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ ที่อยู่ในบัตรนั้นด้วย[92] เพียงแต่ผู้เสนอร่าง...[93] เกรงว่าจะไม่ครอบคลุมถึงรูปแบบของบัตรอิเล็กทรอนิกส์ทั้งหมด จึงเพิ่มข้อความในตอนท้ายว่า “และให้หมายความรวมถึง ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้” ด้วย อันเป็นการขยายความเพิ่มเติมเพียงเท่านั้น[94]

---

[92] โดยในร่าง...ที่คณะรัฐมนตรีเสนอ ได้บัญญัติให้เพิ่มมาตรา 1(14) โดยให้ความหมายของคำว่า “บัตรอิเล็กทรอนิกส์” ว่าหมายถึง

“เอกสารหรือวัตถุอื่นใด ไม่ว่าจะมีรูปลักษณะใด ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็ก ให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า และให้หมายความรวมถึง ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ แต่มีวิธีการใช้ในทำนองเดียวกัน”

[93] ร่างพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่...) พ.ศ. ... ที่ นร 0503/2883 วันที่ 4 มีนาคม 2546 ลงชื่อ พันตำรวจโท ทักษิณ ชินวัตร เสนอโดยนายพงศ์เทพ เทพกาญจนา รัฐมนตรีว่าการกระทรวงยุติธรรมในสมัยนั้น

[94] โปรดดูหัวข้อที่ 3.3.3 ปัญหาในชั้นยกร่างกฎหมายกับเรื่องข้อมูลในบัตรอิเล็กทรอนิกส์

ดังนั้น ผู้วิจัยจึงเสนอให้แก้ไขคำนิยามของคำว่า “บัตรอิเล็กทรอนิกส์” ในมาตรา 1(14)(ข) โดยตัดคำว่า “โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้” ทิ้ง และเปลี่ยนคำว่า “แต่” เป็น “และ” นอกจากนั้นให้คงเดิม ซึ่งจะได้เป็น

มาตรา 1(14) “บัตรอิเล็กทรอนิกส์” หมายความว่า

(ก) เอกสารหรือวัตถุอื่นใดไม่ว่าจะมีรูปลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า

(ข) ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ และมีวิธีการใช้ในทำนองเดียวกับ (ก) หรือ

(ค) สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ

ข้อดีของการแก้ไขคำนิยามในลักษณะดังกล่าวคือ เป็นการแก้ไขเพียงเล็กน้อยแต่ได้ประโยชน์เป็นอย่างมาก โดยที่กฎหมายยังคงความคุ้มครองแก่บัตรอิเล็กทรอนิกส์ในรูปแบบของข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ อยู่ดังเดิม และเป็นการลบข้อจำกัดในการคุ้มครองข้อมูลออกไปทำให้กฎหมายสามารถคุ้มครองข้อมูลทุกประเภทได้อย่างเสมอภาคและอย่างมากขึ้น ไม่ว่าข้อมูลนั้นจะอยู่ในรูปลักษณะใดหรือบันทึกไว้ในแหล่งใดก็ตาม และทำให้บทบัญญัติในเรื่องบัตรอิเล็กทรอนิกส์อื่นๆ ที่กำหนดไว้ในมาตรา 269/1 ถึง 269/7 ที่คุ้มครองข้อมูลบัตรอิเล็กทรอนิกส์อยู่เดิมนั้นมิได้รับผลกระทบจากการแก้ไขในลักษณะดังกล่าวไปด้วย แต่ข้อเสียก็คือ มิได้เป็นการเพิ่มรายละเอียดใดๆ ขึ้นใหม่จากที่กฎหมายได้บัญญัติไว้อยู่เดิมเพราะผู้วิจัยเห็นว่าเนื้อหาของคำนิยามดังกล่าวนั้นมีความสมบูรณ์ ใกล้เคียงกันกับที่กฎหมายของต่างประเทศที่ได้ให้ความคุ้มครองไว้ดังที่ได้ทำการศึกษาวิจัยมาแล้ว

อย่างไรก็ตามการแก้ไขบทบัญญัตินิยามคำว่า “บัตรอิเล็กทรอนิกส์” ในประมวลกฎหมายอาญา มาตรา 1(14) นี้ เป็นเพียงการแก้ปัญหาคำนิยามในประมวลกฎหมายอาญาซึ่งเป็นปัญหาประการแรกของการศึกษาวิจัยในปัญหาการขาดบทบัญญัติในการลงโทษ[95] อันกล่าวได้ว่าเป็นเพียงการแก้ไขรายละเอียดในส่วนของวัตถุแห่งการกระทำซึ่งเป็นเพียงองค์ประกอบภายนอกของการ

[95] โปรดดูหัวข้อที่ 3.3 ปัญหาการขาดบทบัญญัติในการลงโทษสำหรับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

กระทำความผิดเท่านั้น แต่ยังมีปัญหาการขาดบทบัญญัติอันเป็นการเฉพาะที่เกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เพื่อนำมาใช้ประกอบกัน ดังนั้นจึงต้องทำการแก้ไขปัญหาประการที่สอง คือการขาดบทบัญญัติเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ซึ่งจะกล่าวในหัวข้อต่อไป

5.3.2 พิจารณาถึงรูปแบบในการบัญญัติกฎหมายโดยการเพิ่มเป็นบทบัญญัติเฉพาะ

เนื่องจากปัญหาประการถัดมาคือ ปัญหาการขาดบทบัญญัติอันเป็นการเฉพาะในการปรับใช้กับการกระทำในลักษณะที่เกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในรูปแบบต่างๆ[96] ซึ่งทำให้เกิดปัญหาว่า กฎหมายอาญาของประเทศไทยที่มีอยู่นั้นไม่ครอบคลุมกับการกระทำความผิดอันเกี่ยวกับบัตรอิเล็กทรอนิกส์ในทุกลักษณะ[97] ดังนั้นในหัวข้อนี้ ผู้วิจัยจะทำการวิเคราะห์บทบัญญัติกฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ[98] เพื่อหาแนวทางที่เหมาะสมในการกำหนดให้มีบทบัญญัติอันเป็นการเฉพาะแก่การกระทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ในประมวลกฎหมายอาญาของประเทศไทยต่อไป

ก่อนที่จะทำการวิเคราะห์เปรียบเทียบเพื่อหาแนวทางในการกำหนดบทบัญญัติความผิดนั้นจะต้องทำการวิเคราะห์เสียก่อนว่าจะกำหนดให้มีเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ไว้เป็นบทบัญญัติในลักษณะใดของประมวลกฎหมายอาญาในภาค 2 ลักษณะ 7 หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ซึ่งจำต้องคำนึงถึงลักษณะของการกระทำ ความเหมาะสมในการบัญญัติและลักษณะการบัญญัติการกระทำความผิดเกี่ยวกับการดึงข้อมูลในกฎหมายต่างประเทศมาพิจารณาประกอบกันด้วย

จากการศึกษากฎหมายต่างประเทศ[99] สามารถแจกแจงการกระทำความผิดต่างๆ ในบทบัญญัติของกฎหมายต่างประเทศ ซึ่งได้กำหนดให้มีการดึงข้อมูลที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์อันเป็นความผิด ได้ดังตารางต่อไปนี้

---

[96] โปรดดูหัวข้อที่ 3.3.2 ปัญหาการนำบทบัญญัติในหมวดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์มาใช้กับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ และหัวข้อที่ 3.4 อุปสรรคในการนำบทบัญญัติอื่นที่มีลักษณะใกล้เคียงมาบังคับใช้แทน

[97] จากการวิเคราะห์ในหัวข้อที่ 5.1 พิจารณาถึงความจำเป็นในการบัญญัติให้การดึงข้อมูลบัตรอิเล็กทรอนิกส์เป็นความผิดทางอาญา

[98] ดูบทที่ 4 กฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ

[99] ดูบทที่ 4 กฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ

ตารางที่ 20 แสดงการกระทำความผิดต่างๆ ในบทบัญญัติของกฎหมายต่างประเทศ ซึ่งได้กำหนดให้มีการดึงข้อมูลที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์

ประเทศ	กฎหมาย		การดึงข้อมูล	การกระทำอื่นๆ ในบทบัญญัติ
	กฎหมาย	มาตรา		
สหรัฐอเมริกา	รัฐบัญญัติของสหรัฐอเมริกา	1028(a)(7)	โอน	ครอบครอง, ใช้
		1029(a)(1)	ผลิต, เคลื่อนย้าย	ใช้
		1030(a)(2)	ได้รับ	เข้าถึง
สหราชอาณาจักร	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990	1	ทำให้กระทำการใดๆ	-
		3A(3)	ได้รับ	-
	พระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006	6	มีไว้ในครอบครอง, ควบคุม	-
	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018	170	ได้รับ	เปิดเผย
สาธารณรัฐฟิลิปปินส์	พระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012	4(a)(1)	เข้าถึง	-
		4(b)(3)	ขโมย	-
	พระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 ที่ได้แก้ไขเพิ่มเติมแล้ว	9(k)	มีไว้ในครอบครอง	-
		9(q)	สกิมมิ่ง, คัดลอก, ได้รับไป	ปลอมแปลง
		9(s)	เข้าถึง	-
		9(t)	แฮก, ใช้ไวรัส	-

ประเทศ	กฎหมาย		การดึงข้อมูล	การกระทำอื่นๆ ในบทบัญญัติ
	กฎหมาย	มาตรา		
เครือรัฐออสเตรเลีย	พระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001	477.1	เข้าถึง	แก้ไข เปลี่ยนแปลง, ทำให้เสีย
		478.3	ครอบครอง, ควบคุม	-
		478.4	ได้รับ	จัดหา
	พระราชบัญญัติแก้ไขกฎหมายอาชญากรรม (ความผิดด้านโทรคมนาคม และมาตรการอื่นๆ)(ฉบับที่ 2) ค.ศ. 2004	480.4	ได้รับ	ซื้อขาย, แลกเปลี่ยน

จากตารางดังกล่าวพบว่า บทบัญญัติของกฎหมายต่างประเทศซึ่งได้กำหนดให้มีการดึงข้อมูลที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์นั้นมีรูปแบบของการบัญญัติไว้โดยแบ่งออกได้เป็นสองลักษณะคือ แยกการดึงข้อมูลจากบัตรเป็นการกระทำเพียงลักษณะเดียวในบทบัญญัติ กับ รวมการกระทำความผิดอื่นๆ ซึ่งไม่เกี่ยวข้องกับการดึงข้อมูลจากบัตรเข้ามาอยู่ในบทบัญญัติเดียวกันด้วย เช่น การใช้ เปิดเผย ปลอมแปลง แก้ไขเปลี่ยนแปลง ทำให้เสีย จัดหา ซื้อขายแลกเปลี่ยน อันอาจเทียบได้กับบทบัญญัติของประมวลกฎหมายอาญาของประเทศไทยที่มีอยู่แล้ว เช่น การปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/1 การจำหน่ายหรือมีไว้เพื่อจำหน่ายซึ่งบัตรอิเล็กทรอนิกส์ปลอม ตามมาตรา 269/4 วรรคสอง การใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/5 ซึ่งดูเหมือนว่าจะบัญญัติให้มีการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เข้าไปรวมไว้กับบทบัญญัติเหล่านั้นที่ได้มีอยู่แล้วได้ แต่เมื่อพิเคราะห์ดูแล้วพบว่า การกระทำความผิดอื่นเหล่านั้นมิได้บัญญัติให้เหมือนกันในแต่ละประเทศ ทั้งในประเทศเดียวกันก็บัญญัติบ้างไม่บัญญัติบ้างตามแต่กฎหมายในแต่ละฉบับ เท่ากับว่าการกระทำความผิดอื่นเหล่านั้นมิได้มีความสัมพันธ์ร่วมกับการดึงข้อมูลจากบัตรและขึ้นอยู่กับดุลพินิจในการบัญญัติกฎหมายของแต่ละประเทศเป็นสำคัญ ซึ่งโดยส่วนใหญ่แล้วจะแยกการดึงข้อมูลจากบัตรให้เป็น

การกระทำเพียงลักษณะเดียวในบทบัญญัติ ซึ่งมีข้อดีในแง่ของความชัดเจนในการกำหนดความผิดแต่ละลักษณะการกระทำให้แยกกันออกไปเป็นเรื่องๆ แต่ข้อเสียคือ ถ้าหากลักษณะการกระทำความผิดที่เป็นเรื่องเดียวกันหรือใกล้เคียงกัน การแยกบทบัญญัติออกจากกันก็จะทำให้การบัญญัติกฎหมายมีความฟุ่มเฟือยจนเกินไปได้ เช่น ความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/5 และฐานมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/6 นั้นแทบจะเป็นเรื่องเดียวกันหรือใกล้เคียงกันและการบัญญัติกฎหมายก็คล้ายกันมากจนไม่สมควรแยกออกจากกัน

ในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นี้แม้ว่าจะคล้ายกับการมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/6 แต่ในด้านกรรมของการกระทำความผิดนั้นก็มีความต่างกันและการตีความโดยการนำกฎหมายของต่างประเทศมาพิจารณาประกอบก็บ่งชี้ว่ามิใช่เรื่องเดียวกัน[100] ซึ่งผู้วิจัยเห็นว่า การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นี้มีลักษณะเป็นการเฉพาะตัวและสามารถแยกออกจากการกระทำความผิดในลักษณะอื่นๆ ที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ได้[101] ทั้งเป็นการกระทำที่มีอยู่หลากหลายรูปแบบ[102] จึงมิใช่การกระทำความผิดที่เป็นเพียงรายละเอียดเล็กน้อยจนเกินไปอันอาจต้องนำไปบัญญัติรวมกับบทบัญญัติอื่นที่มีอยู่แล้วในเรื่องความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ผู้วิจัยจึงเห็นควร ให้มีบทบัญญัติเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นบทบัญญัติเฉพาะในหมวดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ แยกออกจากการกระทำความผิดในลักษณะอื่นๆ ซึ่งได้กำหนดไว้ในหมวดเดียวกันนั้นต่อไป

ลำดับต่อไปนั้น ผู้วิจัยจะทำการวิเคราะห์เปรียบเทียบบทบัญญัติกฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ[103] เพื่อหาแนวทางที่เหมาะสมในการกำหนดให้มีบทบัญญัติความผิดอันเป็นการเฉพาะแก่การกระทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ในประมวลกฎหมายอาญาของประเทศไทย โดยแบ่งการวิเคราะห์เปรียบเทียบตามองค์ประกอบความผิดที่จะบัญญัติขึ้นในส่วนขององค์ประกอบภายนอก ได้แก่ ผู้กระทำ การกระทำ วัตถุแห่งการกระทำ และส่วนขององค์ประกอบภายใน อันได้แก่ เจตนาและเจตนาพิเศษ ดังนี้

---

[100] จากการวิเคราะห์ในหัวข้อที่ 5.1 พิจารณาถึงความจำเป็นในการบัญญัติให้การดึงข้อมูลบัตรอิเล็กทรอนิกส์เป็นความผิดทางอาญา

[101] ดูตารางที่ 12 “รูปภาพแสดงลำดับขั้นตอนของกลุ่มการกระทำความผิดที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์” และจากการวิเคราะห์ในหัวข้อที่ 5.1 พิจารณาถึงความจำเป็นในการบัญญัติให้การดึงข้อมูลบัตรอิเล็กทรอนิกส์เป็นความผิดทางอาญา

[102] โปรดดูหัวข้อที่ 3.2 รูปแบบการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

[103] ดูบทที่ 4 กฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ

5.3.2.1 องค์ประกอบภายนอกส่วนของผู้กระทำ

จากการศึกษาองค์ประกอบภายนอกส่วนของผู้กระทำความผิดในบทบัญญัติของกฎหมายต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ สามารถสรุปเป็นตารางได้ดังนี้

ตารางที่ 21 แสดงองค์ประกอบภายนอกส่วนของผู้กระทำความผิดในกฎหมายต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

ประเทศ	กฎหมาย		ผู้กระทำความผิด
	พระราชบัญญัติ	มาตรา	
สหรัฐอเมริกา	รัฐบัญญัติของสหรัฐอเมริกา	1028(a)(7)	ผู้ใด (Whoever)
		1029(a)(1)	ผู้ใด (Whoever)
		1030(a)(2)	ผู้ใด (Whoever)
สหราชอาณาจักร	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990	1	บุคคล (A person)
		3A(3)	บุคคล (A person)
	พระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006	6	บุคคล (A person)
	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018	170	บุคคล (A person)
สาธารณรัฐฟิลิปปินส์	พระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012	4(a)(1), 8	บุคคลใด (Any person)
		4(b)(3), 8	บุคคลใด (Any person)
	พระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 ที่ได้แก้ไขเพิ่มเติมแล้ว	9(k), 10	บุคคลใด (Any person)
		9(q), 10	บุคคลใด (Any person)
		9(s), 10	บุคคลใด (Any person)
		9(t), 10	บุคคลใด (Any person)

ประเทศ	กฎหมาย		ผู้กระทำความผิด
	พระราชบัญญัติ	มาตรา	
เครือรัฐออสเตรเลีย	พระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001	477.1	บุคคล (A person)
		478.3	บุคคล (A person)
		478.4	บุคคล (A person)
	พระราชบัญญัติแก้ไขกฎหมายอาชญากรรม (ความผิดด้านโทรคมนาคม และมาตรการอื่นๆ)(ฉบับที่ 2) ค.ศ. 2004	480.4	บุคคล (A person)

จากตารางดังกล่าวพบว่า กฎหมายต่างประเทศนั้นได้กำหนดองค์ประกอบภายนอกส่วนของผู้กระทำโดยให้หมายถึงบุคคลทั่วๆ ไป ซึ่งมิได้เฉพาะเจาะจงบุคคลใดบุคคลหนึ่งโดยเฉพาะ และในประเทศเดียวกันก็จะใช้คำเหมือนกันในการกำหนดผู้กระทำความผิดในกฎหมายอาญาคือคำว่า “ผู้ใด” (Whoever) ในสหรัฐอเมริกา คำว่า “บุคคล” (A person) ในสหราชอาณาจักรและเครือรัฐออสเตรเลีย และคำว่า “บุคคลใด” (Any person) ในสาธารณรัฐฟิลิปปินส์ ซึ่งเหมือนกับที่ประเทศไทยได้ใช้คำว่า “ผู้ใด” ในการขึ้นต้นความผิดอาญาในแต่ละมาตรา[104] และจากการพิจารณาบทบัญญัติอื่นๆ ในหมวดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์พบว่า ต่างใช้คำว่า “ผู้ใด” เป็นองค์ประกอบภายนอกส่วนของผู้กระทำความผิดด้วยกันทั้งสิ้น ดังนั้นผู้วิจัยจึงเห็นควรให้ใช้คำว่า “ผู้ใด” ในการกำหนดองค์ประกอบภายนอกส่วนของผู้กระทำความผิดเช่นเดียวกัน กับบทบัญญัติเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ อันจะส่งผลดีต่อการบัญญัติคำในกฎหมายเพื่อให้สอดคล้องไปในทิศทางเดียวกันและสามารถปรับใช้กฎหมายอาญากับบุคคลใดก็ตามที่ได้กระทำความผิดโดยไม่มีข้อจำกัดในด้านฐานะทางสังคม[105] เศรษฐกิจ ความสัมพันธ์ของบุคคล[106] เชื้อชาติ สัญชาติ การนับถือศาสนาและอื่นๆ มาเกี่ยวข้องในการลงโทษบุคคลในทางอาญาเพื่อให้สามารถบังคับใช้กฎหมายได้อย่างเท่าเทียมกัน ข้อเสียของการกำหนดคำว่า “ผู้ใด” กับการกระทำความผิดในด้านเทคโนโลยีนี้ คือความรับผิด

---

[104] เกียรติขจร วัจนะสวัสดิ์, คำอธิบายฎหมายอาญา ภาค 1, พิมพ์ครั้งที่ 10 (กรุงเทพฯ: พลสยาม พริ้นติ้ง, 2551), หน้า 128.

[105] เช่น การเป็นเจ้าพนักงาน ในประมวลกฎหมายอาญา มาตรา 289 หรือ เรื่องความผิดต่อตำแหน่งหน้าที่ราชการ

[106] เช่น ผู้บุพการีและผู้สืบสันดาน ในประมวลกฎหมายอาญา มาตรา 289 ความสัมพันธ์ระหว่างสามีและภริยาในความผิดอันเกี่ยวกับทรัพย์ ตามมาตรา 71 ผู้ดำรงชีพจากรายได้ของผู้ซึ่งค้าประเวณี ตามมาตรา 286

ทางอาญาจะเกิดขึ้นแก่บุคคลเท่านั้น สัตว์และสิ่งของย่อมไม่มีความรับผิดทางอาญา[107] หากเป็นการทำงานของโปรแกรมคอมพิวเตอร์หรืออุปกรณ์ในการดึงข้อมูลบัตรที่ได้ติดตั้งไว้แล้วและมีการทำงานโดยอัตโนมัตินั้น อาจถูกมองว่าเป็นการกระทำของสิ่งของซึ่งไม่มีผู้กระทำความผิดได้ ซึ่งในทางกฎหมายอาญาของประเทศไทยแท้จริงแล้วการใช้สัตว์หรือสิ่งของเป็นเครื่องมือในการกระทำความผิดเท่ากับว่าผู้นั้นได้กระทำความผิดโดยตรงนั่นเอง[108]

5.3.2.2 องค์ประกอบภายนอกส่วนของการกระทำ

จากการศึกษาองค์ประกอบภายนอกส่วนของการกระทำความผิดในบทบัญญัติของกฎหมายต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์สามารถสรุปเป็นตารางได้ดังนี้

ตารางที่ 22 แสดงองค์ประกอบภายนอกส่วนของการกระทำความผิดในกฎหมายต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

ประเทศ	กฎหมาย		การกระทำความผิด
	พระราชบัญญัติ	มาตรา	
สหรัฐอเมริกา	รัฐบัญญัติของสหรัฐอเมริกา	1028(a)(7)	โอน (Transfers)
		1029(a)(1)	ผลิต (Produce), เคลื่อนย้าย (Traffics in)
		1030(a)(2)	เข้าถึง (Accesses) จึงได้รับ (Obtain)
สหราชอาณาจักร	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990	1	ทำให้กระทำการใดๆ (Perform any function) เพื่อจะได้รับการเข้าถึง (Access) หรือข้อมูล (Data)
		3A(3)	ได้รับ (Obtains)

[107] เกียรติขจร วัจนะสวัสดิ์, คำอธิบายกฎหมายอาญา ภาค 1, หน้า 128.

[108] เรื่องเดียวกัน.

ประเทศ	กฎหมาย		การกระทำความผิด
	พระราชบัญญัติ	มาตรา	
	พระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006	6	มีไว้ในครอบครอง (Possession), ควบคุม (Control)
	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018	170	ได้รับ (Obtain)
สาธารณรัฐฟิลิปปินส์	พระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012	4(a)(1)	เข้าถึง (Access)
		4(b)(3)	ขโมย (Theft)
	พระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 ที่ได้แก้ไขเพิ่มเติมแล้ว	9(k)	มีไว้ในครอบครอง (Possession)
		9(q)	สกิมมิ่ง (Skimming), คัดลอก (Copying), ได้รับไป (Obtaining)
		9(s)	เข้าถึง (Accessing)
		9(t)	แฮก (Hacking), ใช้ไวรัส (Computer Viruses)
เครือรัฐออสเตรเลีย	พระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001	477.1	เข้าถึง (Access)
		478.3	ครอบครอง (Possession), ควบคุม (Control of)
		478.4	ได้รับ (Obtain)
	พระราชบัญญัติแก้ไขกฎหมายอาชญากรรม (ความผิดด้านโทรคมนาคม และมาตรการอื่นๆ)(ฉบับที่ 2) ค.ศ. 2004	480.4	ได้รับ (Obtain)

จากตารางดังกล่าว สามารถจำแนกลักษณะของการกระทำความผิดในกฎหมายต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรได้เป็นกลุ่มๆ ดังนี้

(1) กลุ่มการครอบครอง (Possession) หรือควบคุม (Control) ข้อมูลที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์

การกระทำในลักษณะนี้พบได้ในกฎหมายของสหราชอาณาจักร มาตรา 6 สาธารณรัฐฟิลิปปินส์ มาตรา 9(k) และเครือรัฐออสเตรเลีย มาตรา 478.3 การกระทำการครอบครองหรือควบคุมข้อมูลนั้นในความหมายที่กฎหมายของสาธารณรัฐฟิลิปปินส์และเครือรัฐออสเตรเลียได้บัญญัติไว้ไม่ใช่การกระทำการดึงข้อมูลโดยตรง แต่คือผลที่ได้จากการกระทำการดึงข้อมูลที่เกิดขึ้นมาก่อนแล้ว ซึ่งในบางครั้งมีความใกล้ชิดกับการดึงข้อมูลมากเพราะเมื่อเกิดการกระทำในลักษณะดึงข้อมูลแล้วข้อมูลนั้นก็จะไปอยู่ในความครอบครองหรือควบคุมของผู้กระทำความผิดทันที ซึ่งด้วยเหตุผลนี้เองกฎหมายของสหราชอาณาจักรจึงกำหนดให้สามารถใช้เรื่องการครอบครองหรือควบคุมกับการกระทำความผิดที่เป็นการดึงข้อมูลได้เพราะถือว่าผู้กระทำความผิดได้รับ (Obtain) ข้อมูลนั้นมาแล้ว แต่กฎหมายดังกล่าวของสหราชอาณาจักรนั้นก็มีเพียงบทบัญญัติเดียวที่ตีความในลักษณะนี้ ซึ่งกฎหมายอื่นๆ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018 ที่ออกมาภายหลังก็ได้เปลี่ยนคำโดยไปใช้คำอื่นที่มิใช่การครอบครองหรือควบคุมกับเรื่องการดึงข้อมูลดังกล่าว แนวความคิดนี้ตรงกันกับกฎหมายของสาธารณรัฐฟิลิปปินส์และเครือรัฐออสเตรเลียที่ได้เพิ่มบทบัญญัติอันเป็นการเฉพาะที่เป็นเรื่องการดึงข้อมูล จากเดิมที่มีเฉพาะการครอบครองหรือการควบคุมข้อมูล เพื่อให้กฎหมายมีความชัดเจนแน่นอน ป้องกันการตีความและอาจเป็นการเปิดช่องให้อาชญากรยกขึ้นเป็นข้อต่อสู้ในเชิงกฎหมายได้

ข้อดีของการใช้คำว่าครอบครองหรือควบคุมกับเรื่องการดึงข้อมูลบัตรคือ ทำให้การบัญญัติกฎหมายมีความกระชับ โดยอาจอาศัยการตีความให้การครอบครองหรือควบคุมในกฎหมายที่มีอยู่เดิมนั้น รวมไปถึงการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์โดยอาศัยคำพิพากษาของศาลอย่างในสหราชอาณาจักรก็ได้ โดยไม่จำต้องแก้ไขบทบัญญัติที่มีอยู่เดิมในกฎหมาย อันทำให้กฎหมายสามารถใช้กับการกระทำความผิดได้กว้างขึ้น แต่ข้อเสียคือการขาดความชัดเจนแน่นอนของกฎหมายในทางอาญา ซึ่งต้องตีความโดยเคร่งครัดและอาจเป็นข้อต่อสู้ของอาชญากรเพื่อหลุดพ้นความผิดได้ และทำให้กฎหมายมีความล้าหลังเมื่อเทียบกับกฎหมายในประเทศอื่นๆ ในเรื่องการกระทำความผิดที่เกี่ยวกับบัตรอิเล็กทรอนิกส์ที่ต่างก็ได้บัญญัติความผิดอันเป็นการเฉพาะแยกออกมาจากการครอบครองหรือควบคุมข้อมูลนั้น

(2) กลุ่มการเข้าถึง (Access) ข้อมูลที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์

การกระทำลักษณะนี้พบได้ในกฎหมายของทุกประเทศ ซึ่งเกี่ยวข้องเฉพาะกับข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ (Computer data storage device) เท่านั้น ซึ่งก่อนที่ผู้กระทำจะทำการดึงข้อมูลนั้น ผู้กระทำต้องทำการเข้าถึงเครื่องคอมพิวเตอร์หรืออุปกรณ์ดังกล่าวก่อน อันเปรียบได้กับการเข้าไปโดยไม่มีเหตุอันสมควรในความผิดฐานบุกรุกเคหสถาน ตามประมวลกฎหมายอาญามาตรา 364[109] และด้วยการเข้าไปนั้นทำให้ผู้กระทำความผิดได้รับ (Obtain) ข้อมูลในรูปแบบอิเล็กทรอนิกส์ที่ได้บันทึกในเครื่องหรืออุปกรณ์ดังกล่าวมา ซึ่งในกฎหมายของสหรัฐอเมริกานั้นแม้จะยังไม่มีคำอธิบายที่แน่นอนว่าการเข้าถึงหมายความว่าอย่างไร[110] แต่ก็ย่อมหมายถึงการบุกรุกคอมพิวเตอร์ (Computer trespassing) โดยใช้วิธีการต่างๆ เช่น การแฮก (Hacking)[111] หรือการใช้ไวรัส (Computer Viruses) ซึ่งได้กำหนดไว้ในกฎหมายของสาธารณรัฐฟิลิปปินส์ มาตรา 9(t) ด้วย การเข้าถึงนี้กฎหมายบางประเทศอย่างสหราชอาณาจักรอาจไม่ใช้คำว่า “เข้าถึง” ในบทบัญญัติ แต่ใช้คำว่า “ทำให้กระทำการใดๆ” (Perform any function) ในมาตรา 1 ซึ่งก็หมายถึงการเข้าถึงเช่นเดียวกัน[112]

การเข้าถึงนี้นอกจากจะหมายความว่าเป็นการบุกรุกแล้ว ในกฎหมายของสหราชอาณาจักรและเครือรัฐออสเตรเลีย ก็ยังบัญญัติเพิ่มเติมลงไปอีกว่าให้หมายถึง การคัดลอก (Copies) หรือการเคลื่อนย้าย (Moves) ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้บันทึกข้อมูลคอมพิวเตอร์ด้วย[113] หรือในกฎหมายของสาธารณรัฐฟิลิปปินส์ที่ได้บัญญัติให้การเข้าถึง คือ การดึงข้อมูลมา (Retrieving data from) ซึ่งโดยปกติแล้วการเข้าถึงนั้น จะมิได้หมายรวมถึงการคัดลอก เคลื่อนย้ายหรือดึงข้อมูลด้วย กล่าวคือ การเข้าถึงเปรียบเสมือนกับการที่ผู้กระทำความผิดได้บุกรุกเข้าไปในบ้านอันเป็นการไม่มีเหตุอันสมควรเท่านั้น โดยมิได้ทำอันตรายหรือลักทรัพย์ที่อยู่ภายใน

---

[109] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, หน้า 133-134.

[110] พิญดา เลิศกิตติกุล, “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์,” (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2550), หน้า 88.

[111] Charles Doyle, Cybercrime: “A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws” [Online], Accessed: 20 October 2020. Available from: https://fas.org/sgp/crs/misc/RS20830.pdf.

[112] โดยพิจารณาจากชื่อฐานของการกระทำความผิดที่ได้กำหนดไว้ว่า “การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต” (Unauthorised access to computer material) ในมาตรา 1 ของกฎหมายของสหราชอาณาจักร

[113] มาตรา 17(2)(b) ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 ของสหราชอาณาจักร และมาตรา 476.1 ของพระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001 ของเครือรัฐออสเตรเลีย

บ้านเพิ่มเติมด้วย[114] แต่ที่กฎหมายของทั้งสามประเทศดังกล่าวได้กำหนดเพิ่มเติมลงไปด้วยเพราะเห็นได้ว่า การเข้าถึงที่จะเป็นการดึงข้อมูลได้นั้น ต้องมีการคัดลอก เคลื่อนย้าย หรือดึงข้อมูลประกอบกับการเข้าถึงด้วย ซึ่งเป็นดุลพินิจในการบัญญัติกฎหมายของแต่ละประเทศ เช่น กฎหมายของสหรัฐอเมริกามิได้บัญญัติให้รวมถึงการคัดลอก (Copies) หรือการเคลื่อนย้าย (Moves) ไว้ในความหมายของคำว่าเข้าถึงด้วย ซึ่งแม้ไม่ได้บัญญัติไว้ก็มีความหมายในแนวเดียวกันคือเป็นการเข้าถึงและได้รับข้อมูลมาเช่นเดียวกัน

ข้อดีของการใช้คำว่าเข้าถึงกับเรื่องการดึงข้อมูลบัตรคือ สามารถใช้กฎหมายที่มีอยู่เดิมเพื่อลงโทษผู้กระทำความผิดได้โดยมิต้องบัญญัติเรื่องการดึงข้อมูลจากบัตรเป็นมาตราใหม่หรืออาศัยการแก้ไขกฎหมายเดิมเพียงเล็กน้อย เพราะในประเทศต่างๆ ก็ได้มีกฎหมายอาญาเรื่องการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์บังคับใช้อยู่แล้ว[115] แต่มีข้อเสียคือ การเข้าถึงนั้นใช้ได้กับข้อมูลที่อยู่ในคอมพิวเตอร์หรืออุปกรณ์ที่จัดเก็บข้อมูลคอมพิวเตอร์ที่กฎหมายได้กำหนดให้หมายถึงคอมพิวเตอร์ด้วยเท่านั้น จึงไม่ครอบคลุมข้อมูลที่อยู่ในรูปแบบอื่นๆ ที่มิใช่ข้อมูลคอมพิวเตอร์ด้วย และถ้าหากกฎหมายมิได้บัญญัติให้อุปกรณ์ที่จัดเก็บข้อมูลคอมพิวเตอร์เป็นคอมพิวเตอร์ด้วยแล้ว คำว่าเข้าถึงอันเป็นการดึงข้อมูลนั้นจะไม่สามารถใช้เพื่อคุ้มครองข้อมูลที่บรรจุไว้ในอุปกรณ์ดังกล่าวได้เลย เช่น ในกฎหมายของสหรัฐอเมริกา และด้วยความหมายของคำว่า “เข้าถึง” นั้นมิได้หมายถึงการดึงข้อมูล จึงจำต้องมีการบัญญัติเพิ่มเติมด้วยคำอื่นต่อท้ายในบทบัญญัติ เช่น “เพื่อจะได้รับข้อมูล” หรือ “และด้วยการกระทำดังกล่าวจึงได้รับข้อมูล” หรือบัญญัติว่าให้หมายถึง การคัดลอก เคลื่อนย้าย หรือการดึงข้อมูล ในบทบัญญัติอื่นไว้ด้วย อันทำให้กฎหมายไม่กระชับและเกิดความสับสนแก่ผู้ใช้กฎหมายได้ และหากด้วยการพัฒนาทางเทคโนโลยีในอนาคต ซึ่งทำให้มีการดึงข้อมูลได้โดยมิต้องมีการเข้าถึงเครื่องคอมพิวเตอร์เสียก่อน อาจทำให้บทบัญญัติที่ใช้คำว่า “เข้าถึง” มีปัญหาในการบังคับใช้ได้

---

[114] สุเนติ คงเทพ, คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์, หน้า 133-134.

[115] พิจารณาจากจำนวนประเทศที่มีการให้สัตยาบัน หรือภาคยานุวัติในอนุสัญญาว่าด้วยอาชญากรรมไซเบอร์ (Convention on Cybercrime) ซึ่งเป็นแม่แบบของกฎหมายอาญาเรื่องการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ ซึ่งมีจำนวนถึง 65 ประเทศด้วยกัน และประเทศอื่นๆ อีกมากที่มีกฎหมายดังกล่าว ทั้งที่มิได้มีการให้สัตยาบัน หรือภาคยานุวัติ ในอนุสัญญาดังกล่าวด้วย เช่น ประเทศไทย

(3) กลุ่มได้รับ (Obtain) ข้อมูลที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์

การกระทำลักษณะนี้พบได้ในกฎหมายของทุกประเทศ และมักจะเป็นบทบัญญัติพื้นฐานที่ทุกประเทศต้องมีในการคุ้มครองข้อมูลจากการกระทำความผิดที่เกี่ยวกับการดึงข้อมูลจากบัตร ซึ่งคำว่า “Obtain” ที่ผู้วิจัยแปลว่าได้รับนั้น ในภาษาอังกฤษสามารถแปลได้หลากหลายมาก เช่น แปลว่าได้รับโดยต้องอาศัยการพยายามเพื่อให้ได้รับมาด้วย[116] แปลว่าเอา (Take, Get, Have) แปลว่าได้มา (Gain, Acquire) โดยรัฐสภาสหรัฐ (United States Congress) ได้กล่าวว่านอกจากจะหมายถึงการคัดลอก (Copied) หรือการขนส่ง (Transported) แล้ว เพียงแต่การอ่าน (Reading) ก็ถือว่าเป็นการได้รับไปแล้วด้วย[117] และนอกจากคำว่าได้รับแล้ว บางประเทศก็ได้บัญญัติโดยใช้คำอื่น ที่สื่อความหมายได้ชัดเจนกว่าคำว่าได้รับ อันสื่อถึงลักษณะหรือวิธีที่ทำให้ได้รับข้อมูลนั้นมา เช่น กฎหมายของสหรัฐอเมริกาได้ใช้คำว่าโอน (Transfers) ในมาตรา 1028(a)(7) เช่นคดี U. S. v. Amry (2003) ใช้คำว่า เคลื่อนย้าย (Traffics in) หรือผลิต (Produce) ซึ่งหมายถึง การโอน (Transfer) หรือได้รับ (Obtain) หรือทำซ้ำ (Duplicate) ในมาตรา 1029(a)(1) เช่นคดี U. S. v. Amry (2003) แม้แต่ในกฎหมายของสาธารณรัฐฟิลิปปินส์ที่ได้บัญญัติให้สื่อถึงรูปแบบการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์รูปแบบใดรูปแบบหนึ่งโดยเฉพาะ เช่น ใช้คำว่า ขโมย (Theft) ในมาตรา 4(b)(3) หรือใช้คำว่า สกิมมิ่ง (Skimming) และคัดลอก (Copying) ข้อมูล ในมาตรา 9(q) แต่ไม่ว่าจะใช้คำว่าอย่างไรก็มีความหมายไปในแนวทางเดียวกันก็คือ เป็นการได้รับไปซึ่งข้อมูลโดยที่มิได้ทำอันตรายใดๆ กับข้อมูลต้นฉบับโดยที่ต้นฉบับข้อมูลยังคงอยู่ครบถ้วน กล่าวคือ เป็นการทำให้ผู้กระทำการได้รับสิ่งใดไป (Obtain something)[118] เพิ่มขึ้น โดยผู้ถูกกระทำมิได้เกิดการสูญเสียสิ่งใดไปจากตน นอกจากการถูกละเมิดสิทธิในความเป็นส่วนตัวของบุคคล (Privacy Right) เท่านั้น อันเป็นลักษณะเฉพาะตัวของการเป็นข้อมูลอิเล็กทรอนิกส์ ซึ่งต่างกับการเป็นทรัพย์ที่หากมีการกระทำความผิดกับทรัพย์เกิดขึ้นมักจะทำให้ผู้ถูกกระทำต้องเกิดการสูญเสียสิ่งนั้นไปจากตนด้วย เช่น การลักทรัพย์ การทำให้เสียทรัพย์

---

[116] Oxford Learner's Dictionaries, "Obtain" [Online], Accessed: 7 October 2020. Available from: https://www.oxfordlearnersdictionaries.com/definition/english/obtain?q=obtain.

[117] Charles Doyle, “Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws” [Online], Accessed: 20 October 2020. Available from: https://www.everycrsreport.com/files/20141015_97-1025_31056cd16cc55cc39047e24e327a15875045157f.pdf.

[118] Oxford Learner's Dictionaries, “Obtain” [Online], Accessed: 7 October 2020. Available from: https://www.oxfordlearnersdictionaries.com/definition/english/obtain?q=obtain.

ข้อดีของการใช้คำว่าได้รับกับเรื่องการดึงข้อมูลบัตรคือ เป็นคำที่สามารถใช้ได้กับการดึงข้อมูลในทุกรูปแบบโดยไม่จำกัดว่าข้อมูลนั้นจะอยู่ในแหล่งบันทึกใดหรือลักษณะใด แต่ข้อเสียคือด้วยการใช้ภาษาไทย ผู้ใช้กฎหมายที่ไม่เข้าใจ อาจตีความและทำให้ความหมายคำว่าได้รับนั้นผิดเพี้ยนไปจากที่กฎหมายมุ่งประสงค์ได้ เช่น ผู้วิจัยต้องการให้คำว่าได้รับข้อมูลหมายถึงการดึงข้อมูลในขั้นตอนแรกเท่านั้นอันเปรียบได้กับความผิดฐานลักทรัพย์ มิใช่หมายถึงการซื้อข้อมูล หรือการส่งต่อข้อมูลให้กับบุคคลใดคนหนึ่งอันเปรียบได้กับความผิดฐานรับของโจร ซึ่งอาจเกิดการตีความที่ผิดเพี้ยนนี้ในทางภาษาได้ และในกรณีที่ร้ายแรงที่สุดคือ การส่งข้อมูลให้บุคคลใดคนหนึ่ง เพื่อให้บุคคลนั้น “ได้รับ” ข้อมูล แล้วตีความว่าคนนั้นได้ทำความผิดอาญาในเรื่องการดึงข้อมูลอันเป็นการใช้กฎหมายอาญาเพื่อกลั่นแกล้งหรือทำให้เสียหายแก่บุคคลอื่น

ตารางที่ 23 สรุปและแจกแจงกลุ่มของการกระทำความผิดอันเป็นองค์ประกอบภายนอกในกฎหมายต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

ประเทศ	กลุ่มการครอบครอง (Possession) หรือควบคุม (Control) ข้อมูล	กลุ่มการเข้าถึง (Access) ข้อมูล	กลุ่มได้รับ (Obtain) ข้อมูล
สหรัฐอเมริกา	-	- เข้าถึง (Accesses) จึงได้รับ (Obtain)	- โอน (Transfers) - ผลิต (Produce) - เคลื่อนย้าย (Traffics in)
สหราชอาณาจักร	- มีไว้ในครอบครอง (Possession) - ควบคุม (Control)	- ทำให้กระทำการใดๆ (Perform any function) เพื่อเข้าถึง (Access)	- ได้รับ (Obtains)

ประเทศ	กลุ่มการครอบครอง (Possession) หรือควบคุม (Control) ข้อมูล	กลุ่มการเข้าถึง (Access) ข้อมูล	กลุ่มได้รับ (Obtain) ข้อมูล
สาธารณรัฐฟิลิปปินส์	- มีไว้ในครอบครอง (Possession)	- เข้าถึง (Access) - แฮก (Hacking) - ใช้ไวรัส (Computer Viruses)	- ขโมย (Theft) - สกิมมิ่ง (Skimming) - คัดลอก (Copying) และได้รับไป (Obtaining)
เครือรัฐออสเตรเลีย	- ครอบครอง (Possession) - ควบคุม (Control of)	- เข้าถึง (Access)	- ได้รับ (Obtain)

จากการเปรียบเทียบองค์ประกอบภายนอกส่วนของการกระทำในกฎหมายของต่างประเทศที่กล่าวมาแล้วข้างต้นแล้วนั้น ผู้วิจัยเห็นว่า คำว่าครอบครองหรือควบคุมข้อมูลนั้นหากนำมาใช้บัญญัติกฎหมาย อาจทำให้ผู้ใช้กฎหมายมีความสับสนกับ ความผิดฐานใช้หรือมีไว้เพื่อนำออกใช้บัตรซึ่งอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามประมวลกฎหมายอาญามาตรา 269/5 และมาตรา 269/6 ได้ เพราะมีความหมายในภาษาไทยไปในทางเดียวกัน ทั้งคำว่าเข้าถึงนั้น ก็มีใช้อยู่แล้วในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในความผิดฐานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ ตามมาตรา 5 หรือความผิดฐานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ตามมาตรา 7 อันทำให้ผู้ใช้กฎหมายคิดว่ากฎหมายมีความซ้ำซ้อนกันได้ จึงเหลือกลุ่มของคำว่าได้รับข้อมูลจากบัตรอิเล็กทรอนิกส์เพียงกลุ่มเดียวซึ่งอาจนำมาใช้บัญญัติเป็นกฎหมายได้ แต่การบัญญัติเพียงคำว่า “ได้รับ” เพียงคำเดียวนั้นอาจจะไม่ครอบคลุมรูปแบบการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้ทั้งหมด[119] และการบัญญัติคำว่า “ได้รับ” อาจจะเกิดปัญหาในการตีความได้ เพราะคำว่า “ได้รับ” ในทางภาษาไทยนั้นแสดงถึงการที่ผู้กระทำความผิดได้กระทำการดึงข้อมูลบัตรอิเล็กทรอนิกส์ด้วยตนเอง หรือแสดงถึงการส่งต่อข้อมูลให้ผู้อื่นให้ได้รับข้อมูลบัตรอิเล็กทรอนิกส์นั้น ซึ่งผู้วิจัยประสงค์จะให้หมายถึงการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์อันเป็นการกระทำเพื่อให้ได้มาซึ่งข้อมูลบัตรอิเล็กทรอนิกส์ในครั้งแรกเท่านั้น ไม่รวมถึงการส่งต่อข้อมูลนั้นให้บุคคลอื่นๆ ด้วย ครั้นจะให้นำรูปแบบ

[119] โปรดดูหัวข้อที่ 3.2 รูปแบบการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

ของการดึงข้อมูลต่างๆ ทุกรูปแบบ มาบัญญัติให้เป็นการกระทำความผิดก็จะทำให้บทบัญญัติของกฎหมายมีความฟุ่มเฟือยมากจนเกินไปและอาจไม่รองรับกับรูปแบบการดึงข้อมูลจากบัตรใหม่ๆ จากความก้าวหน้าทางเทคโนโลยีในอนาคตได้ ดังนั้น องค์ประกอบภายนอกในส่วนของการกระทำนี้ผู้วิจัยจึงเห็นควรให้มีการบัญญัติว่า “กระทำโดยประการใดๆ อันเป็นการได้มา” ซึ่งการบัญญัติในลักษณะดังกล่าวจะมีข้อดีคือ เป็นการสื่อให้เห็นว่าต้องมีการกระทำบางอย่างในรูปแบบใดรูปแบบหนึ่งอันเป็นการขวนขวายให้ตนเองได้รับข้อมูลจากบัตรอิเล็กทรอนิกส์มาเพื่อป้องกันการกลั่นแกล้งในทางอาญา จากการส่งข้อมูลให้บุคคลคนใดคนหนึ่งได้รับข้อมูลโดยที่บุคคลนั้นไม่เต็มใจ เมื่อบุคคลนั้นไม่มีการกระทำโดยประการใดๆ อันเป็นการได้มาซึ่งข้อมูลบัตรอิเล็กทรอนิกส์ บุคคลนั้นจึงไม่มีความผิดในเรื่องนี้ และการกำหนดการกระทำในลักษณะดังกล่าวก็มิได้ซ้ำซ้อนกับคำในบทบัญญัติกฎหมายที่มีอยู่แล้ว ทั้งยังสามารถใช้กับการกระทำอันเป็นการดึงข้อมูลจากบัตรได้ทุกรูปแบบ[120] ลดความฟุ่มเฟือยของคำในบทบัญญัติให้กฎหมายอาญามีความกระชับ และรองรับกับรูปแบบการดึงข้อมูลจากบัตรที่อาจเกิดขึ้นในอนาคตได้ ข้อเสียก็คือ เป็นการซ้ำซ้อนกับความผิดฐานกระทำโดยมิชอบเพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ ตามมาตรา 8 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งผู้วิจัยเห็นว่าไม่ทำให้เกิดปัญหา ดังที่กฎหมายของต่างประเทศซึ่งมีเรื่องที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์อยู่ในกฎหมายหลายฉบับ ซึ่งในการใช้กฎหมายนั้นเจ้าหน้าที่ผู้ใช้กฎหมายจะปรับใช้กฎหมายโดยเลือกเฉพาะมาตราใดมาตราหนึ่งหรือใช้ทุกมาตราที่เกี่ยวข้องตามลักษณะและพฤติการณ์ในการกระทำความผิดที่เหมาะสมที่สุดตามแต่ละคดีที่เกิดขึ้น

การ “กระทำโดยประการใดๆ อันเป็นการได้มา” ซึ่งข้อมูลบัตรอิเล็กทรอนิกส์ ที่ผู้วิจัยได้เสนอนี้ คือ การกระทำเฉพาะขั้นตอนการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ซึ่งเป็นการกระทำในขั้นตอนแรกต่อข้อมูลของบัตรอิเล็กทรอนิกส์เท่านั้นอันเปรียบได้กับการลักทรัพย์ จึงไม่รวมการซื้อข้อมูล การส่งต่อข้อมูล การแจกจ่ายข้อมูล หรือการกระทำใดๆ ในรูปแบบเดียวกัน ซึ่งเป็นการกระทำที่เกิดขึ้นภายหลังจากที่ผู้กระทำได้รับข้อมูลมาแล้วอันเปรียบได้กับการรับของโจร

ข้อสังเกต ตามหลักกฎหมายอาญานั้น การกระทำซึ่งเป็นองค์ประกอบภายนอกนี้ผู้กระทำจะต้องถึงขั้น “ลงมือ” กระทำความผิด ตามประมวลกฎหมายอาญา มาตรา 80 เสียก่อนจึงจะครบองค์ประกอบความผิดในส่วนของการกระทำ[121] ซึ่งหากเป็นการกระทำความผิดซึ่งหน้า คือเห็นว่าผู้กระทำกำลังใช้เครื่องมือใดๆ ในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์หรือกำลังจดข้อมูลบัตรนั้นอยู่

---

[120] โปรดดูหัวข้อที่ 3.2 รูปแบบการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

[121] เกียรติขจร วัจนะสวัสดิ์, คำอธิบายกฎหมายอาญา ภาค 1, หน้า 143.

ก็คงไม่มีปัญหา แต่เนื่องจากการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นี้โดยส่วนใหญ่แล้วจะเป็นวิธีการที่ปกปิดที่มาในการส่งมัลแวร์หรือไวรัส จดหมายอิเล็กทรอนิกส์ปลอม ใช้เบอร์โทรปลอม หรือแอบติดตั้งหรือแอบใช้เครื่องมือโดยไม่ให้ผู้เสียหายรู้ตัว จึงแทบจะไม่พบการกระทำความผิดซึ่งหน้ากับการกระทำดังกล่าวเลย ดังนั้นจึงมีปัญหาว่า จะทราบได้อย่างไรว่ามีการ “ลงมือ” กระทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เกิดขึ้นแล้ว ซึ่งต้องพิจารณาจากพฤติการณ์ในการกระทำความผิดที่เกิดขึ้นโดยแบ่งได้เป็น 2 ช่วงเวลา ดังนี้

(ก) ช่วงเวลาก่อนเกิดการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

การกระทำในช่วงเวลานี้คือ การที่ผู้กระทำความผิดได้ทำการลงมือใช้เครื่องมือหรือวัตถุเพื่อให้ได้ข้อมูลสำหรับปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ โดยการติดตั้งเครื่องมือหรือวัตถุนั้นไว้กับอุปกรณ์ต่างๆ เช่น ติดตั้งเครื่องสกิมเมอร์เข้ากับเครื่องจ่ายเงินอัตโนมัติหรือหัวจ่ายปั๊มน้ำมัน หรือทำการสลับเครื่องชำระเงินที่อยู่ในห้างร้านกับเครื่องสกิมเมอร์ของตนเอง ติดตั้งหรือส่งมัลแวร์ ไวรัสคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ปลอม หรือทำการปลอมเว็บไซต์และส่งเข้าไปในอีเมลของผู้อื่น การกระทำเหล่านี้จะถือว่าผู้กระทำนั้นได้กระทำ “ขั้นสุดท้าย” (Last Act) ตามหลักความใกล้ชิดต่อผล (The Proximity Rule) แล้ว โดยไม่ต้องคำนึงว่าจะมีการกระทำของผู้เสียหายมาเกี่ยวข้องหรือไม่และไม่ว่าการดึงข้อมูลนั้นจะยังไม่แน่นอนว่าจะนานเท่าใด ก็ถือว่าเป็นการ “ลงมือ” กระทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์แล้ว[122] ซึ่งหากเครื่องมือหรืออุปกรณ์นั้นยังไม่ได้ทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ใดๆ เลย การกระทำนั้นก็เป็นเพียงการพยายามกระทำความผิด ตามประมวลกฎหมายอาญา มาตรา 80

(ข) ช่วงเวลาหลังจากเกิดการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

การกระทำในช่วงเวลานี้คือ การที่ผู้กระทำความผิดได้ลงมือดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ไปแล้ว ซึ่งจะทราบได้จากการตรวจล็อกไฟล์ (Log File) หรือข้อมูลที่บันทึกไว้ใน EEPROM[123] ที่ได้บันทึกไว้ในหน่วยความจำของเครื่องมือหรือวัตถุที่ใช้ในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ เช่น ในเมมโมรี (Memory) หรือในชิป (Chip)[124] ของเครื่องสกิมเมอร์ ในฮาร์ดดิส

---

[122] เรื่องเดียวกัน, หน้า 542-544.

[123] Nathan Seidle, "Gas Pump Skimmers" [Online], Accessed: 8 November 2020. Available from: https://learn.sparkfun.com/tutorials/gas-pump-skimmers/all.

[124] Krebsonsecurity, "Romanian Skimmer Gang in Mexico Outed by Krebsonsecurity Stole $1.2 Billion" [Online], Accessed: 8 November 2020. Available from: https://krebsonsecurity.com/category/all-about-skimmers/.

(Hard Disk) ของเครื่องคอมพิวเตอร์ ที่จะบันทึกวันที่ เวลา ที่เครื่องมือหรือวัตถุนั้นได้ทำการลงมือดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ไป ซึ่งนับว่าเป็นข้อได้เปรียบของการกระทำความผิดในลักษณะนี้ที่สามารถสืบย้อนหลังไปทราบถึงวัน เวลาและจำนวนครั้งของการกระทำความผิดได้ แต่ข้อเสียคือ การตรวจและการกู้คืนดังกล่าวต้องอาศัยผู้เชี่ยวชาญเฉพาะด้านและอุปกรณ์ทางเทคโนโลยีที่ทันสมัย ซึ่งอาจเป็นอุปสรรคในการสืบสวนและสอบสวนในประเทศไทยได้

5.3.2.3 องค์ประกอบภายนอกส่วนของวัตถุแห่งการกระทำ

การกระทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้นจะต้องเป็นการกระทำต่อ “ข้อมูล” (Information) อันหมายถึง ข้อมูลส่วนบุคคล (Personal data) คือข้อมูลใดๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัวตนได้ ทั้งทางตรงหรือทางอ้อม เช่น ชื่อ หมายเลขประจำตัว ตำแหน่งที่อยู่ ข้อมูลที่ระบุทางออนไลน์ ปัจจัยที่เกี่ยวกับสรีระวิทยา ลักษณะทางพันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรมหรือสังคม ของบุคคลผู้นั้น[125] หรือ ข้อมูลทางการเงินของบุคคล (Personal financial information) คือ ข้อมูลที่เกี่ยวข้องกับบุคคลที่อาจนำไปใช้โดยลำพังหรือประกอบกับข้อมูลอื่นในการเข้าถึงเงิน (Funds) เครดิต (Credit) หรือประโยชน์ทางการเงินอื่น[126] หรือข้อมูลอื่นๆ โดยไม่จำต้องคำนึงว่าข้อมูลนั้นจะเป็น “ข้อมูลคอมพิวเตอร์” ตามคำนิยามใน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือจะเป็น “ข้อมูลอิเล็กทรอนิกส์” ตามคำนิยามในพระราชบัญญัติว่าว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544[127] หรือไม่ก็ตาม

ถ้าหากข้อมูลนั้น เป็นข้อมูลของ “บัตรอิเล็กทรอนิกส์” ทั้งสามรูปแบบที่ประมวลกฎหมายอาญามาตรา 1(14) ได้กำหนดไว้ตามที่ผู้วิจัยได้ทำการเสนอแก้ไขคำนิยามไปแล้ว[128] ข้อมูล

---

[125] มาตรา 4(1) ของ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation)

[126] มาตรา 480.1 ใน พระราชบัญญัติแก้ไขกฎหมายอาชญากรรม (ความผิดด้านโทรคมนาคมและมาตรการอื่นๆ) (ฉบับที่ 2) ค.ศ. 2004 ของเครือรัฐออสเตรเลีย

[127] ดูตารางที่ 1 “เปรียบเทียบการเป็นบัตรอิเล็กทรอนิกส์ ตามคำนิยามในมาตรา 1(14) แห่งประมวลกฎหมายอาญา” ในหัวข้อที่ 2.1.1.3

[128] โปรดดูหัวข้อที่ 5.3.1 ซึ่งผู้วิจัยได้เสนอแก้ไขโดยให้บัญญัติว่า “มาตรา 1(14) “บัตรอิเล็กทรอนิกส์” หมายความว่า

(ก) เอกสารหรือวัตถุอื่นใดไม่ว่าจะมีรูปลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า

เหล่านั้นย่อมจะได้รับความคุ้มครองจากการกระทำการดึงข้อมูลจากบัตรในงานวิจัยนี้ด้วยกันทั้งสิ้น ไม่ว่าข้อมูลนั้นจะได้บันทึกไว้ในแหล่งใดของบัตรอิเล็กทรอนิกส์ เช่น บนพื้นผิวหรือแหล่งบันทึกความจำของบัตรที่เป็นเอกสารหรือวัตถุอื่นใด บันทึกไว้ในคอมพิวเตอร์หรืออุปกรณ์ในการจัดเก็บข้อมูลคอมพิวเตอร์ใดๆ หรือที่บันทึกไว้ในตัวของบุคคลผู้เป็นเจ้าของสิ่งอื่นใดนั้น

ประเด็นที่จะต้องพิจารณาต่อไปคือการดึง “ข้อมูลบัตรอิเล็กทรอนิกส์” นี้ต้องเป็นข้อมูลบัตรอิเล็กทรอนิกส์ของ “ผู้อื่น” หรือไม่ จากการศึกษาบทบัญญัติของกฎหมายต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้นพบว่า บทบัญญัติกฎหมายบางประเทศ เช่น รัฐบัญญัติของสหรัฐอเมริกา มาตรา 1028(a)(7) ได้บัญญัติคำว่าของ “ผู้อื่น” หรือในพระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012 มาตรา 4(b)(3) ของสาธารณรัฐฟิลิปปินส์ ได้บัญญัติคำว่าของ “บุคคลอื่น” ลงไปอย่างชัดแจ้ง ในขณะที่บทบัญญัติอื่นๆ ของกฎหมายในหลายประเทศนั้น แม้มิได้บัญญัติคำว่า ผู้อื่น ไว้ในบทบัญญัติโดยตรง แต่ก็ได้บัญญัติคำอื่นที่มีความหมายไปในเชิงเดียวกันว่าต้องเป็นข้อมูลที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ของผู้อื่น เช่น กฎหมายของสหรัฐอเมริกาได้กล่าวถึง บันทึกของสถาบันการเงินหรือของผู้ออกบัตร ของกระทรวงหรือองค์กรใดๆ ของสหรัฐอเมริกา ของคอมพิวเตอร์ที่มีการป้องกัน (โดยบุคคลอื่นหรือสถาบันการเงินหรือรัฐบาลสหรัฐ) ในกฎหมายของสหราชอาณาจักรใช้คำว่า โดยมิได้รับอนุญาต โดยมิได้รับความยินยอม หรือในการฉ้อโกง (ผู้อื่น) ในกฎหมายของสาธารณรัฐฟิลิปปินส์ใช้คำว่า โดยไม่มีสิทธิ โดยมิได้รับอนุญาตจากเจ้าของหรือหน่วยงานที่เป็นเจ้าของ ทำให้เกิดความเสียหายแก่เจ้าของบัญชีหรือธนาคารผู้รับฝากเงินหรืออาจทำให้เจ้าของบัญชีสูญเสียเงิน และในกฎหมายของเครือรัฐฟิลิปปินส์ใช้คำว่า โดยไม่มีอำนาจหรือปราศจากความยินยอมจากบุคคลที่เกี่ยวข้องกับข้อมูลนั้น เป็นต้น ซึ่งเมื่อพิจารณาบทบัญญัติในความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ในประมวลกฎหมายอาญาของประเทศไทยแล้ว พบว่ามีเพียงมาตรา 269/5 และมาตรา 269/6 อันเป็นการใช้หรือมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นเท่านั้นที่ได้บัญญัติคำว่า “ผู้อื่น” ไว้ ต่างกับความผิดในกลุ่มการปลอมบัตรอิเล็กทรอนิกส์ และกลุ่มเครื่องมือในการทำบัตรอิเล็กทรอนิกส์ปลอม ในมาตราอื่นๆ ที่เหลือ ซึ่งแม้เป็นการปลอมบัตรอิเล็กทรอนิกส์ของตนเอง หรือ ทำหรือมีเครื่องมือนั้นเพื่อสำหรับใช้ปลอมบัตรอิเล็กทรอนิกส์ของตนเอง หรือให้ได้ข้อมูลบัตรอิเล็กทรอนิกส์ของตนเองก็อาจมีความผิดได้ หากเป็นการ “น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน” อันกฎหมายไทยนั้นมุ่งคุ้มครองความสงบสุขของประชาชนด้วย

(ข) ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ และมีวิธีการใช้ในทำนองเดียวกับ (ก) หรือ

(ค) สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ”

ต่างจากเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นี้ที่ผู้เสียหายจากการดึงข้อมูลจากบัตรจะมีได้อย่างมากเพียง 2 คนเท่านั้น คือ (1) เจ้าของข้อมูล เช่น ผู้ออกบัตรอิเล็กทรอนิกส์ ตามมาตรา 1(14)(ก) และมาตรา 1(14)(ข) หรือบุคคลผู้เป็นเจ้าของสิ่งอื่นใด ตามมาตรา 1(14)(ค) และ (2) ผู้มีสิทธิใช้บัตรนั้น ตามมาตรา 1(14)(ก) และมาตรา 1(14)(ข) เท่านั้น และเมื่อนำแนวคิดของกฎหมายในต่างประเทศข้างต้นมาพิจารณาประกอบกันแล้วจึงสรุปได้ว่า การดึงข้อมูลบัตรอิเล็กทรอนิกส์ของตนเองนั้นไม่มีความผิดทางอาญา ดังนั้นเพื่อให้บทกฎหมายมีความชัดเจน ผู้วิจัยจึงเห็นควรให้มีการบัญญัติคำว่า “ของผู้อื่น” ลงไปด้วยในกฎหมาย

ปัญหาต่อมาคือจะต้องมีคำว่า “หรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วย” หรือไม่ ดังปรากฏในความผิดฐานลักทรัพย์ ตามมาตรา 334 ฐานยักยอกทรัพย์ ตามมาตรา 352 หรือฐานทำให้เสียทรัพย์ตามมาตรา 358 ประเด็นนี้เกิดขึ้นจากการที่ทรัพย์ชิ้นหนึ่งนั้นสามารถมีบุคคลผู้เป็นเจ้าของกรรมสิทธิ์ในทรัพย์ได้หลายคน ซึ่งกฎหมายได้คุ้มครองผู้อื่นซึ่งเป็นเจ้าของกรรมสิทธิ์ในทรัพย์ร่วมกันนั้นจากการกระทำความผิดอาญาในบางลักษณะอันเป็นการลดทอนหรือสิ้นไปซึ่งการใช้ทรัพย์ของผู้อื่นนั้นด้วย แต่จากศึกษาลักษณะของการเป็นข้อมูลแล้วพบว่า ข้อมูลนั้นจะเกิดขึ้นพร้อมกับบุคคล เช่น วันเดือนปีเกิด หรือร่างกายของบุคคลอันเป็นสิ่งอื่นใด ตามมาตรา 1(14)(ค) และจะคงอยู่ไปจนกว่าบุคคลนั้นจะตาย หรือเกิดขึ้นจากการออกให้บุคคลนั้นมีสิทธิใช้ เช่น ชื่อ นามสกุล หมายเลขรหัส ต่างๆ ที่ได้บันทึกไว้ในบัตร ตามมาตรา 1(14)(ก) และมาตรา 1(14)(ข) และคงอยู่กับบุคคลไปจนกว่าจะสิ้นสิทธิในการใช้ เท่านั้น มิได้เกิดจากการยึดถือครอบครองด้วยเจตนาจะเป็นเจ้าของอย่างทรัพย์และสิ้นไปด้วยการสละเจตนานั้น ทั้งการใช้งานข้อมูลบัตรอิเล็กทรอนิกส์นั้นก็เป็นการใช้โดยส่วนตัวของบุคคลโดยแท้และไม่ได้ร่วมกันใช้กับบุคคลอื่นด้วย และในทางข้อเท็จจริงนั้นแทบไม่ปรากฏว่าได้มีการออกบัตรอิเล็กทรอนิกส์ใดที่สามารถใช้ข้อมูลบัตรนั้นโดยบุคคลหลายคนได้ และแม้ว่าในอนาคตจะมีบัตรประเภทใดที่สามารถใช้งานโดยผู้มีสิทธิใช้หลายคนได้ หากเกิดการดึงข้อมูลจากบัตรขึ้นโดยเจ้าของข้อมูลคนใดคนหนึ่ง การใช้งานข้อมูลของผู้อื่นอันเป็นผู้ใช้รวมก็มิได้ลดทอนหรือสิ้นไปด้วยการกระทำการดึงข้อมูลนั้น ซึ่งเป็นคุณสมบัติพิเศษของการเป็นข้อมูลอันต่างจากทรัพย์ และจากการศึกษากฎหมายของต่างประเทศก็ไม่ปรากฏประเด็นดังกล่าวในกฎหมายของประเทศเหล่านั้น ดังนั้นจึงไม่จำต้องบัญญัติคำว่า “หรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วย” ไว้ในบทบัญญัติ

โดยสรุปแล้ว องค์ประกอบภายนอกส่วนของวัตถุแห่งการกระทำนี้ ผู้วิจัยจึงเห็นควรให้บัญญัติว่า “ข้อมูลบัตรอิเล็กทรอนิกส์ของผู้อื่น” ซึ่งเป็นการเหมาะสมและตรงตามวัตถุประสงค์ของการวิจัยในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นี้มากที่สุด

ข้อสังเกต การที่ผู้วิจัยได้เสนอให้บัญญัติกำกับคำว่า “ข้อมูล” ลงไปในคำว่า “บัตรอิเล็กทรอนิกส์” ด้วย เพราะผู้วิจัยต้องการเน้นถึงการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์อันเป็นการกระทำที่เกี่ยวข้องกับข้อมูลของบัตรอิเล็กทรอนิกส์เป็นสำคัญ อันสอดคล้องกับการบัญญัติคำว่า “ข้อมูล” ลงไปในคำว่า “บัตรอิเล็กทรอนิกส์” ในความผิดฐานใช้หรือมีไว้เพื่อนำออกใช้ซึ่งข้อมูลบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ในการเสนอให้มีการยกร่างพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา ฉบับที่ 17 พ.ศ. 2547 ที่ร่าง... ของคณะรัฐมนตรีและของสมาชิกสภาผู้แทนราษฎรได้เสนอให้มีการคุ้มครองข้อมูลบัตรอิเล็กทรอนิกส์ด้วย[129] แต่กลับถูกแก้ไขเสียในชั้นแปรญัตติในวาระที่สอง แต่เนื่องจากความหมายของคำว่า “บัตรอิเล็กทรอนิกส์” นั้นก็ได้รวมถึง “ข้อมูล” อยู่แล้วในมาตรา 1(14)(ข) จึงอาจถูกมองว่าเป็นการบัญญัติคำที่ซ้ำซ้อนกับคำว่า “ข้อมูล” และไม่จำเป็นต้องบัญญัติคำว่า “ข้อมูล” กำกับลงไปอีก แต่ผู้วิจัยเห็นว่าการบัญญัติเพียงแต่คำว่า “บัตรอิเล็กทรอนิกส์” เพียงคำเดียวแก่องค์ประกอบภายนอกส่วนของวัตถุแห่งการกระทำนั้น เมื่อรวมกับส่วนของการกระทำซึ่งได้เป็นคำว่า “กระทำโดยประการใดๆ อันเป็นการได้มาซึ่งบัตรอิเล็กทรอนิกส์” แล้ว จะทำให้ความหมายของบทบัญญัตินี้รวมถึงการได้มาซึ่งบัตรอิเล็กทรอนิกส์ที่เป็นเอกสารหรือวัตถุอื่นใดอันเป็นทรัพย์ ตามมาตรา 1(14)(ก) ด้วย ซึ่งอาจมีความซ้ำซ้อนกับความผิดฐานลักทรัพย์ ฐานยักยอกทรัพย์หรือฐานฉ้อโกงได้ และทำให้ความมุ่งหมายของบทบัญญัตินี้ที่ผู้วิจัยมุ่งให้ใช้บังคับเฉพาะกับการดึงข้อมูลบัตรอิเล็กทรอนิกส์นั้นผิดเพี้ยนไป หรือถูกตีความไปในทางอื่นได้ การกำกับคำว่า “ข้อมูล” ลงไปด้วยนั้นจึงทำให้บทบัญญัติดังกล่าวมีความชัดเจนและต้องตามความประสงค์ของวิทยานิพนธ์ฉบับนี้มากยิ่งขึ้น

5.3.2.4 องค์ประกอบภายในส่วนของเจตนา

จากการศึกษาองค์ประกอบภายในส่วนของเจตนาในบทบัญญัติกฎหมายของต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์พบว่า การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศนั้นได้กำหนดให้ผู้กระทำต้องมีเจตนาในการกระทำด้วย มีเพียง

---

[129] ร่าง... ของสมาชิกสภาผู้แทนราษฎร บัญญัติไว้ว่า

มาตรา 269/6 “ผู้ใดใช้ข้อมูลบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

และร่าง... ของคณะรัฐมนตรี บัญญัติไว้ว่า

มาตรา 269/6/1 “ผู้ใดมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/5 หรือซึ่งข้อมูลหรือรหัสบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/6 ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018 มาตรา 170 ของสหราชอาณาจักร กรณีเดียวเท่านั้นที่กำหนดให้มีการกระทำโดยประมาทแก่การได้รับข้อมูลโดยมิได้รับความยินยอมจากผู้ควบคุม เพราะอาจเกิดกรณีที่บุคคลได้รับข้อมูลมาโดยชอบจากผู้ควบคุมแต่บุคคลนั้นได้เก็บรักษาข้อมูลนั้นไว้ไม่ส่งคืนแก่ผู้ควบคุมโดยเจตนาหรือโดยประมาท จึงได้บัญญัติให้ลงโทษแก่ผู้กระทำที่มิได้เจตนาแต่ไม่ระมัดระวังไม่ส่งข้อมูลคืนดังกล่าวด้วย[130] อันเป็นการคุ้มครองข้อมูลนั้นที่อยู่ในความดูแลของหน่วยงานหรือองค์กรภาครัฐหรือเอกชนมากกว่าการคุ้มครองผู้กระทำซึ่งเป็นกรณีเฉพาะเท่านั้น แต่โดยทั่วไปแล้วการกระทำการดึงข้อมูลนั้นต้องเกิดจากการกระทำโดยเจตนาเท่านั้นเพราะผู้กระทำต้องรู้สำนึกคือมีการกระทำการดึงข้อมูลเกิดขึ้น[131] และผู้กระทำประสงค์ต่อผลหรือย่อมเล็งเห็นผลจากการดึงข้อมูลนั้นเพื่อให้ตนเองได้รับข้อมูลจากบัตรอิเล็กทรอนิกส์มาสู่ตน ดังนั้น ผู้วิจัยจึงเห็นควรกำหนดให้การกระทำตามบทบัญญัตินี้ต้องเป็นการกระทำโดยเจตนาเท่านั้นไม่รวมถึงการกระทำโดยประมาทด้วย แต่ไม่จำต้องเขียนคำว่า “เจตนา” ลงในบทบัญญัติเพราะสามารถอาศัยหลักกฎหมายอาญา ตามประมวลกฎหมายอาญา มาตรา 59 ปรับใช้ได้อยู่แล้ว ข้อดีของการบัญญัติในลักษณะนี้คือทำให้สามารถปรับใช้กฎหมายเพื่อลงโทษแก่ผู้ที่กระทำการดึงข้อมูลบัตรจริงๆ เท่านั้น ไม่รวมถึงบุคคลอื่นที่ไม่มีเจตนาจะได้รับข้อมูลบัตรมาด้วย ในทางความเป็นจริงที่ข้อมูลนั้นสามารถส่งถึงกันได้โดยไม่ต้องได้รับความยินยอมของผู้รับก่อน เช่น ส่งเข้าในโทรศัพท์มือถือ อีเมลของผู้รับ อันเป็นการคุ้มครองบุคคลอื่นที่มิได้กระทำความผิดมิให้ต้องถูกดำเนินคดีตามกฎหมายอาญาด้วย ข้อเสียคือ การคุ้มครองข้อมูลจะถูกลดระดับลงไปจากการยินยอมให้การไม่ระมัดระวังนั้นไม่เป็นความผิดใดๆ ตามกฎหมาย

5.3.2.5 องค์ประกอบภายในส่วนของเจตนาพิเศษ

จากการศึกษาองค์ประกอบภายในส่วนของเจตนาพิเศษในบทบัญญัติกฎหมายของต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์พบว่า บทบัญญัติส่วนใหญ่ของต่างประเทศได้กำหนดให้การกระทำการดึงข้อมูลนั้นต้องมีเจตนาพิเศษนอกเหนือจากเจตนาธรรมดาด้วย อันแสดงในตารางได้ดังนี้

---

[130] Legislation.gov.uk, "Data Protection Act 2018" [Online], Accessed: 8 November 2020. Available from: https://www.legislation.gov.uk/ukpga/1982/48/section/37.

[131] เกียรติขจร วัจนะสวัสดิ์, คำอธิบายกฎหมายอาญา ภาค 1, หน้า 149.

ตารางที่ 24 แสดงองค์ประกอบภายในส่วนของเจตนาพิเศษในกฎหมายต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

ประเทศ	กฎหมาย		เจตนาพิเศษ
	กฎหมาย	มาตรา	
สหรัฐอเมริกา	รัฐบัญญัติของสหรัฐอเมริกา	1028(a)(7)	เจตนาที่จะกระทำหรือช่วยเหลือหรือสนับสนุนหรือเกี่ยวข้องกับการกระทำที่ผิดกฎหมายใดๆ ที่ถือเป็นการละเมิดต่อกฎหมายของรัฐบาลกลาง หรือก่อให้เกิดความผิดอาญาร้ายแรงภายใต้กฎหมายของมลรัฐหรือท้องถิ่น
		1029(a)(1)	เจตนาที่จะฉ้อโกง
สหราชอาณาจักร	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990	1	เพื่อจะได้รับการเข้าถึง (Access) โปรแกรม (Program) หรือข้อมูล (Data) ใดๆ ที่อยู่ในเครื่องคอมพิวเตอร์
		3A(3)	เพื่อจะใช้หรือช่วยเหลือในการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ ต่อไป
	พระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006	6	เพื่อจะใช้ในการดำเนินการหรือเกี่ยวข้องในการฉ้อโกงต่อไป
สาธารณรัฐฟิลิปปินส์	พระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012	4(b)(3)	เจตนาเข้ายึดถือ (Acquisition) ใช้ โอน ครอบครอง เปลี่ยนแปลงหรือลบ ข้อมูลประจำตัวของบุคคลอื่น
	พระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 ที่ได้แก้ไขเพิ่มเติมแล้ว	9(k)	เจตนาในการเข้าถึงบัญชีหรือจัดการบัญชี
		9(t)	เพื่อทำการทุจริต แก้ไข ขโมย หรือทำลาย

ประเทศ	กฎหมาย		เจตนาพิเศษ
	กฎหมาย	มาตรา	
เครือรัฐออสเตรเลีย	พระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001	477.1	จะกระทำหรืออำนวยความสะดวก ในการกระทำความผิดร้ายแรงต่อกฎหมาย
		478.3	จะใช้หรืออำนวยความสะดวกในการกระทำผิดอันร้ายแรงที่เกี่ยวกับคอมพิวเตอร์
		478.4	

จากตารางดังกล่าวพบว่า นอกจากเจตนาธรรมดาแล้ว[132] บทบัญญัติกฎหมายของต่างประเทศโดยส่วนใหญ่จะกำหนดให้มีเจตนาพิเศษบัญญัติไว้เป็นองค์ประกอบภายในด้วย ซึ่งแบ่งได้เป็น 2 ประเภท คือ เจตนาพิเศษเพื่อกระทำการใดๆ ต่อข้อมูลนั้น และเจตนาพิเศษเพื่อนำข้อมูลที่ได้นั้นไปใช้ต่อไป ซึ่งอาจบัญญัติไว้ต่างกันในแต่กฎหมายแต่ละฉบับ กันดังนี้

(1) เจตนาพิเศษเพื่อกระทำการใดๆ ต่อข้อมูลนั้น

เจตนาพิเศษนี้คือ ผู้กระทำมุ่งที่จะกระทำการใดๆ ต่อข้อมูลนั้น เช่น เจตนาที่จะฉ้อโกง หมายถึง ผู้กระทำนั้นรู้ว่ามีคนที่กำลังจะถูกฉ้อโกงจากการดึงข้อมูลนั้นอยู่และตนตั้งใจว่าจะให้คนนั้นถูกฉ้อโกงจากการดึงข้อมูลของตน หรือ เจตนาที่จะเข้าถึงโปแกรมหรือข้อมูลใดๆ ที่อยู่ในเครื่องคอมพิวเตอร์ หรือ เจตนาจะยึดถือ (Acquisition) ขโมย ใช้ โอน ครอบครอง แก้ไขเปลี่ยนแปลง ลบ หรือทำลาย ข้อมูลนั้น หรือ เจตนาเข้าไปจัดการข้อมูลนั้น อาทิ การเข้าไปจัดการบัญชี

(2) เจตนาพิเศษเพื่อนำข้อมูลที่ได้นั้นไปใช้ต่อไป

เจตนาพิเศษนี้คือ ผู้กระทำจะนำข้อมูลที่ได้จากการดึงนั้นไปใช้กระทำการใดๆ ต่อไป เช่น จะนำไปข้อมูลที่ได้นั้นใช้ในการดำเนินการหรือในการฉ้อโกงต่อไป เช่น นำข้อมูลนั้นไปทำบัตรปลอม หรือ จะนำข้อมูลนั้นไปกระทำ ช่วยเหลือ หรือสนับสนุนในการกระทำความผิดต่อกฎหมายอื่นๆ หรือต่อเครื่องคอมพิวเตอร์ ต่อไป

[132] โปรดดูหัวข้อที่ 5.3.2.4 องค์ประกอบภายในส่วนของเจตนา

เมื่อพิจารณาบทบัญญัติในหมวด ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ แห่งประมวลกฎหมายอาญาแล้วพบว่า ส่วนใหญ่แล้วก็ได้บัญญัติให้มีเจตนาพิเศษในบทบัญญัติต่างๆ เหล่านั้นเช่นเดียวกัน อันแสดงในตารางดังต่อไปนี้

ตารางที่ 25 แสดงองค์ประกอบภายในส่วนของเจตนาพิเศษในบทบัญญัติหมวด ความผิดเกี่ยวกับบัตรเล็กทรอนิกส์ ในประมวลกฎหมายอาญา

มาตรา	เจตนาพิเศษ
269/1	- เพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นบัตรอิเล็กทรอนิกส์ที่แท้จริง - เพื่อใช้ประโยชน์อย่างหนึ่งอย่างใด
269/2	- เพื่อใช้ในการปลอมหรือแปลงสิ่งใดๆ ซึ่งระบุไว้ในมาตรา 269/1 - เพื่อให้ได้ข้อมูลในการปลอมหรือแปลงสิ่งใดๆ ซึ่งระบุไว้ในมาตรา 269/1
269/4	- เพื่อใช้ - เพื่อจำหน่าย
269/6	- เพื่อนำออกใช้โดยมิชอบตามมาตรา 269/5

ซึ่งเจตนาพิเศษที่บัญญัติในหมวด ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ นี้มักจะมีลักษณะเหมือนที่กฎหมายต่างประเทศได้กำหนดไว้เป็นประเภทใดประเภทหนึ่งใน 2 ประเภท คือ (1) เจตนาพิเศษเพื่อกระทำการใดๆ ต่อบัตรอิเล็กทรอนิกส์นั้น เช่น เพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นบัตรอิเล็กทรอนิกส์ที่แท้จริง ตามมาตรา 269/1 หรือเพื่อให้ได้ข้อมูลในการปลอมหรือแปลง ตามมาตรา 269/2 และ (2) เจตนาพิเศษเพื่อนำบัตรอิเล็กทรอนิกส์นั้นไปใช้ต่อไป เช่น เพื่อใช้ ตามมาตรา 269/1 มาตรา 269/4 และมาตรา 269/6 หรือเพื่อใช้ในการปลอมหรือแปลง ตามมาตรา 269/2

ในการดึงข้อมูลบัตรอิเล็กทรอนิกส์นี้ ข้อมูลบัตรอิเล็กทรอนิกส์บางประเภทเมื่อดึงข้อมูลมาแล้ว ผู้กระทำจะสามารถนำข้อมูลนั้นออกใช้ได้ ยึดถือ โอน แก้ไขเปลี่ยนแปลง หรือกระทำการอื่นๆ ได้ทันที เช่น หมายเลข รหัสของบัตรเครดิต ชื่อ นามสกุล หมายเลขบัญชี แต่ข้อมูลบางประเภทที่ดึงมานั้น จำเป็นต้องนำไปทำอย่างใดอย่างหนึ่งก่อนจึงจะกระทำความผิดอื่นๆ ได้ เช่น ข้อมูลจากบัตรเอทีเอ็ม ผู้กระทำต้องนำข้อมูลนั้นไปทำบัตรปลอมก่อนจึงจะเข้าถึงเครื่องจ่ายเงิน

อัตโนมัติและถอนเงินออกมาได้ หรือ ข้อมูลของบัตรเครดิตที่เป็นเอกสารที่มีการออกให้นั้น ต้องนำไปทำบัตรปลอมก่อนเช่นกัน จึงจะนำไปใช้รูดซื้อสินค้าหรือบริการได้ ดังนั้นเจตนาพิเศษในการดึงข้อมูลจากบัตรนี้ จึงประกอบไปด้วยเจตนาพิเศษทั้ง 2 ประเภทดังที่ได้กล่าวมาแล้ว คือ เจตนาพิเศษเพื่อกระทำการใดๆ ต่อข้อมูลนั้น และเจตนาพิเศษเพื่อนำข้อมูลที่ได้นั้นไปใช้ต่อไป ดังนั้นเพื่อมิให้เกิดปัญหา ผู้วิจัยจึงเห็นควรให้มีการบัญญัติเจตนาพิเศษในบทบัญญัติการดึงข้อมูลบัตรอิเล็กทรอนิกส์ว่า “โดยทุจริต” อันหมายถึง เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ตามประมวลกฎหมายอาญา มาตรา 1(1) ซึ่งมีข้อดีคือ เป็นเจตนาที่ครอบคลุมเจตนาพิเศษทั้ง 2 ประเภทดังที่ได้กล่าวมาแล้วโดยไม่เป็นการเฉพาะเจาะจงลักษณะใดลักษณะหนึ่งอันทำให้กฎหมายสามารถปรับใช้กับการดึงบัตรอิเล็กทรอนิกส์เพื่อนำข้อมูลนั้นไปกระทำการใดๆ ที่เป็นการใหม่ๆ ในอนาคตได้ และการบัญญัติเจตนาพิเศษกำกับไว้ก็เพื่อการคุ้มครองมิให้มีการกลั่นแกล้งกันให้เป็นความทางอาญา ในยุคที่การรับส่งข้อมูลสามารถทำได้ง่าย หากการส่งข้อมูลให้แก่บุคคลใดเพื่อให้บุคคลนั้นได้รับข้อมูลบัตรอิเล็กทรอนิกส์ของผู้อื่น โจทก์จะต้องพิสูจน์ถึงเจตนาโดยทุจริตของผู้รับข้อมูลนั้นด้วย จึงจะทำให้บุคคลนั้นต้องรับผิด อันเป็นการคุ้มครองบุคคลมิให้ต้องรับโทษทางอาญาจากการกระทำอันไม่เป็นธรรมทางกฎหมาย และทำให้การรับส่งข้อมูลที่อยู่ในภาคธุรกิจนั้นอิสระมากขึ้นโดยไม่ต้องกังวลถึงความรับผิดตามกฎหมายอาญา แต่มีข้อเสียคือ ในเมื่อมีเจตนาพิเศษบัญญัติไว้ในกฎหมาย โจทก์จะต้องนำสืบเพื่อพิสูจน์ถึงเจตนาพิเศษของจำเลยนั้นด้วย ซึ่งในบางครั้งเป็นเรื่องยากที่จะทำให้ศาลนั้นสิ้นข้อสงสัยเพื่อจะตัดสินลงโทษผู้กระทำความผิดได้

ถึงอย่างไรก็ตาม เมื่อผู้วิจัยได้ขอคำปรึกษาจากคณะกรรมการการสอบวิทยานิพนธ์ฉบับนี้ในประเด็นการกำหนดองค์ประกอบภายในส่วนของเจตนาพิเศษดังกล่าว พบว่าการกำหนดเจตนาพิเศษเพิ่มเติมเข้าไปในการบัญญัติกฎหมายอันเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นี้อาจก่อให้เกิดความยุ่งยากแก่ผู้ปฏิบัติงานทางกฎหมายในการพิสูจน์ความผิดของจำเลยจนกว่าศาลจะสิ้นข้อสงสัยในทางปฏิบัติได้ ดังนั้น ผู้วิจัยจึงได้ทำการตัดข้อเสนอในส่วนของเจตนาพิเศษออกไป แล้วกำหนดคำว่า “โดยมิชอบ” อันเป็นการเพิ่มเติมองค์ประกอบภายนอกส่วนของการกระทำแทนที่ลงไปตามข้อเสนอของคณะกรรมการการสอบวิทยานิพนธ์ เพื่อให้เนื้อหาในบทบัญญัติการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์มีความสมบูรณ์ขึ้น

5.4 พิจารณาถึงโทษและอัตราโทษที่ผู้กระทำความผิดสมควรจะได้รับตามบทบัญญัติกฎหมายการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

ในหัวข้อนี้ ผู้วิจัยจะทำการวิเคราะห์เปรียบเทียบในเรื่องโทษและอัตราโทษของบทบัญญัติกฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ[133] กับโทษที่ได้กำหนดไว้ในความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์อื่นๆ ในประมวลกฎหมายอาญา เพื่อหาแนวทางที่เหมาะสมในการกำหนดโทษที่จะลงแก่ผู้กระทำความผิดตามบทบัญญัติการดึงข้อมูลบัตรอิเล็กทรอนิกส์ ดังที่ได้เสนอไปแล้วในหัวข้อก่อน

ในการวิเคราะห์เพื่อหาแนวทางในการกำหนดโทษและอัตราโทษที่บัญญัติไว้ในบทบัญญัติการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ดังที่ได้เสนอไปแล้ว ผู้วิจัยจึงได้ทำการศึกษาโทษและอัตราโทษในกฎหมายต่างประเทศและในประมวลกฎหมายอาญาของไทยที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์โดยการเทียบกับความผิดในลักษณะอื่นๆ ที่เป็นการกระทำความผิดอันเกี่ยวกับกับบัตรอิเล็กทรอนิกส์แล้ว พบว่าการลงโทษและอัตราโทษที่กฎหมายของต่างประเทศและประเทศไทยได้กำหนดไว้นั้น สามารถนำมาแสดงในตารางได้ดังนี้

[133] ดูบทที่ 4 กฎหมายที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศ

ตารางที่ 26 แสดงโทษและอัตราโทษในกฎหมายของต่างประเทศและประเทศไทย ที่เกี่ยวข้องกับการกระทำความผิดอันเกี่ยวกับบัตรอิเล็กทรอนิกส์[134]

<table>
<tr><th rowspan="2">การกระทำผิด</th><th rowspan="2">สหรัฐอเมริกา</th><th colspan="2">สหราชอาณาจักร</th><th rowspan="2">สาธารณรัฐฟิลิปปินส์</th><th rowspan="2">เครือรัฐออสเตรเลีย</th><th rowspan="2">ประเทศไทย</th></tr>
<tr><th>Summary Offences</th><th>Indictable Offences</th></tr>
<tr><td>ปลอมบัตร</td><td>จำคุกไม่เกิน 10 ปีหรือปรับหรือทั้งจำทั้งปรับ</td><td rowspan="3">จำคุกไม่เกิน 12 เดือนหรือปรับไม่เกิน 5,000 ปอนด์สเตอร์ลิงหรือทั้งจำทั้งปรับ</td><td rowspan="2">จำคุกไม่เกิน 10 ปีหรือปรับหรือทั้งจำทั้งปรับ</td><td rowspan="3">จำคุกไม่น้อยกว่า 10 ปี แต่ไม่เกิน 12 ปี และปรับเป็นจำนวน 500,000 เปโซฟิลิปปินส์หรือสองเท่าของมูลค่าของประโยชน์ที่ผู้กระทำความผิดได้รับ</td><td>จำคุก 10 ปี</td><td rowspan="2">จำคุกตั้งแต่ 1 ปี ถึง 5 ปี และปรับตั้งแต่ 20,000 ถึง 100,000 บาท</td></tr>
<tr><td>มีเครื่องมือในการปลอม</td><td>จำคุกไม่เกิน 15 ปีหรือปรับหรือทั้งจำทั้งปรับ</td><td>จำคุก 3 ปี</td></tr>
<tr><td>ดึงข้อมูลบัตร</td><td>จำคุกไม่เกิน 10 ปีหรือปรับหรือทั้งจำทั้งปรับ</td><td>จำคุกไม่เกิน 5 ปีหรือปรับหรือทั้งจำทั้งปรับ</td><td>จำคุก 5 ปี</td><td>จำคุกไม่เกิน 3 ปีหรือปรับไม่เกิน 60,000 บาท หรือทั้งจำทั้งปรับ</td></tr>
</table>

[134] มาตรา 1029(a)(1), (a)(2), (a)(4) และ (a)(6) ในรัฐบัญญัติของสหรัฐอเมริกา ของสหรัฐอเมริกา มาตรา 6 และ 7(1) ในพระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006 ของสหราชอาณาจักร มาตรา 9(a), (b), (c), (f), (q) และมาตรา 10 ในพระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 ของสาธารณรัฐฟิลิปปินส์ มาตรา 144.1 และ 145.1 ในประมวลกฎหมายอาญา ค.ศ. 1995 มาตรา 480.4 และ 480.5 ในพระราชบัญญัติแก้ไขกฎหมายอาชญากรรม (ความผิดด้านโทรคมนาคมและมาตรการอื่นๆ)(ฉบับที่ 2) ค.ศ. 2004 ของเครือรัฐออสเตรเลีย

การกระทำผิด	สหรัฐอเมริกา	สหราชอาณาจักร		สาธารณรัฐฟิลิปปินส์	เครือรัฐออสเตรเลีย	ประเทศไทย
		Summary Offences	Indictable Offences			
นำเข้าส่งออกบัตรปลอม	จำคุกไม่เกิน 10 ปีหรือปรับหรือทั้งจำทั้งปรับ	-	-	จำคุกไม่น้อยกว่า 6 ปี แต่ไม่เกิน 10 ปี และปรับเป็นจำนวน 500,000 เปโซฟิลิปปินส์หรือสองเท่าของมูลค่าของประโยชน์ที่ผู้กระทำความผิดได้รับ	จำคุก 10 ปี	จำคุกตั้งแต่ 3 ปี ถึง 10 ปี และปรับตั้งแต่ 60,000 ถึง 200,000 บาท
ใช้บัตรปลอม	จำคุกไม่เกิน 10 ปีหรือปรับหรือทั้งจำทั้งปรับ	จำคุกไม่เกิน 12 เดือน หรือปรับไม่เกิน 5,000 ปอนด์สเตอร์ลิงหรือทั้งจำทั้งปรับ	จำคุกไม่เกิน 10 ปีหรือปรับหรือทั้งจำทั้งปรับ		จำคุก 10 ปี	จำคุกตั้งแต่ 1 ปี ถึง 7 ปี และปรับตั้งแต่ 20,000 ถึง 140,000 บาทหรือทั้งจำทั้งปรับ

จากตารางดังกล่าวพบว่า การกำหนดโทษและอัตราโทษที่ได้กำหนดไว้ในกฎหมายที่เกี่ยวข้องกับการกระทำความผิดอันเกี่ยวกับบัตรอิเล็กทรอนิกส์จะมีความแตกต่างกันไปตามแต่ละประเทศ ซึ่งส่วนใหญ่แล้วทุกประเทศนั้นจะกำหนดให้มีทั้งโทษจำคุกและโทษปรับด้วย โดยมีเครือรัฐออสเตรเลียเพียงประเทศเดียวที่กำหนดให้มีแต่โทษจำคุกโดยมิได้กำหนดให้มีโทษปรับ และอัตราโทษที่ได้กำหนดไว้นั้นโดยเฉลี่ยแล้วในต่างประเทศนั้นจะมีอัตราโทษที่ใกล้เคียงกันและสูงกว่าในประเทศไทยทั้งอัตราโทษจำคุกขั้นสูงสุดหรืออัตราโทษปรับที่ห่างกันมากอย่างมีนัยสำคัญ สิ่งที่เหมือนกันในกฎหมายต่างประเทศคือ ต่างได้บัญญัติให้การปลอมบัตรอิเล็กทรอนิกส์นั้นมีอัตราโทษที่สูงที่สุด ซึ่งผู้กระทำ

ความผิดอาจได้รับโทษจำคุกเป็นระยะเวลาเป็น 10 ปี ซึ่งสวนทางกับกฎหมายอาญาของประเทศไทยที่ให้การปลอมบัตรอิเล็กทรอนิกส์นั้นมีอัตราโทษที่น้อยที่สุดเมื่อเทียบกัน โดยกฎหมายของประเทศไทยนั้นจะลงโทษหนักขึ้นเมื่อนำบัตรปลอมนั้นไปนำเข้าในหรือส่งออกไปนอกราชอาณาจักรหรือนำไปใช้ต่อ ในขณะที่กฎหมายของสหรัฐอเมริกาและเครือรัฐออสเตรเลียนั้น การนำบัตรปลอมไปนำเข้าในหรือส่งออกไปนอกราชอาณาจักรหรือนำไปใช้ต่อ จะมีอัตราโทษที่เหมือนกับการปลอมบัตรอิเล็กทรอนิกส์ เว้นแต่สาธารณรัฐฟิลิปปินส์ที่กำหนดให้มีอัตราโทษที่น้อยลง และมีข้อสังเกตคือสหรัฐอเมริกาเป็นเพียงประเทศเดียวเท่านั้นซึ่งกำหนดให้การมีเครื่องมือในการปลอมบัตรอิเล็กทรอนิกส์นั้นมีอัตราโทษจำคุกสูงที่สุดในการกระทำความผิดอันเกี่ยวกับบัตรอิเล็กทรอนิกส์

ในด้านอัตราโทษของการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้น มีการบัญญัติที่แตกต่างกันไปตามแต่ละประเทศอีกเช่นเดียวกัน โดยในสหรัฐอเมริกา สหราชอาณาจักรเฉพาะความผิดในกรณีคดีอาญาสามัญ (Summary Offences) และสาธารณรัฐฟิลิปปินส์ นั้นจะให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้นมีอัตราโทษเท่ากันกับการปลอมบัตรอิเล็กทรอนิกส์ ส่วนในสหราชอาณาจักรเฉพาะความผิดในกรณีคดีอาญาอุกฉกรรจ์ (Indictable Offences) เครือรัฐออสเตรเลีย และประเทศไทยในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 8 นั้นจะกำหนดให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์มีอัตราโทษที่น้อยกว่าการปลอมบัตรอิเล็กทรอนิกส์อย่างชัดเจน ดังนั้นจึงสรุปได้ว่า การกำหนดอัตราโทษในเรื่องการกระทำความผิดอันเกี่ยวกับบัตรอิเล็กทรอนิกส์และการดึงข้อมูลบัตรอิเล็กทรอนิกส์นี้ ขึ้นกับดุลพินิจตามแต่ละประเทศจะได้กำหนดไว้ในกฎหมายของตน

ดังนั้นการกำหนดโทษและอัตราโทษของบทบัญญัติเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในงานวิจัยนี้จึงต้องพิจารณาแนวทางในกฎหมายอาญาของประเทศไทยเป็นหลัก โดยในกฎหมายไทยนั้นจะให้ความสำคัญแก่การกระทำความผิดในกลุ่มการปลอมบัตรอิเล็กทรอนิกส์ เช่น การปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/1 การนำเข้าในหรือส่งออกไปซึ่งบัตรอิเล็กทรอนิกส์ปลอม ตามมาตรา 269/3 การใช้หรือมีไว้เพื่อใช้ซึ่งบัตรอิเล็กทรอนิกส์ปลอม ตามมาตรา 269/4 วรรคแรก หรือการจำหน่ายหรือมีไว้เพื่อจำหน่ายซึ่งบัตรอิเล็กทรอนิกส์ปลอม ตามมาตรา 269/4 วรรคสอง มากกว่าให้ความสำคัญกับกลุ่มการกระทำใดๆ ต่อบัตรที่แท้จริง เช่น การใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/5[135] หรือ การมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/6[136] โดยสังเกตได้จาก กลุ่มการปลอมบัตรอิเล็กทรอนิกส์นั้นจะมีการกำหนด

[135] มาตรา 269/5 มีอัตราโทษ “จำคุกไม่เกิน 5 ปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

[136] มาตรา 269/6 มีอัตราโทษ “จำคุกไม่เกิน 3 ปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

ความผิดอัตราโทษขั้นต่ำ (จำคุกตั้งแต่) และต้องปรับด้วย ในบทบัญญัติ ในขณะที่กลุ่มการกระทำใดๆ ต่อบัตรที่แท้จริงนั้น ไม่มีการกำหนดอัตราโทษขั้นต่ำไว้ (จำคุกไม่เกิน) หรือปรับก็ได้ ดังนั้นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ซึ่งเป็นการกระทำที่ยังไม่ถึงขั้นตอนในการปลอมบัตรอิเล็กทรอนิกส์นั้น จึงควรต้องมีอัตราโทษที่น้อยกว่ากลุ่มการปลอมบัตรอิเล็กทรอนิกส์ตามแนวทางการกำหนดโทษดังกล่าวในกฎหมายด้วย

การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้นก็นับได้ว่าเป็นการกระทำใดๆ ต่อบัตรอิเล็กทรอนิกส์ที่แท้จริงของผู้อื่นโดยมิชอบเช่นเดียวกัน แต่เกิดขึ้นก่อนการมีไว้เพื่อนำออกใช้และการใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ และเมื่อนำพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 8 ซึ่งเป็นบทบัญญัติที่มีอยู่แล้วในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์บางรูปแบบ[137] มาพิจารณาประกอบกันด้วย จึงสามารถเรียงอัตราโทษได้ดังตารางต่อไปนี้

ตารางที่ 27 แสดงอัตราโทษการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์บางลักษณะเทียบกับกลุ่มการกระทำใดๆ ต่อบัตรอิเล็กทรอนิกส์ที่แท้จริงของผู้อื่นโดยมิชอบ

ลำดับการกระทำความผิด (ก่อนไปหลัง)	อัตราโทษจำคุก	อัตราโทษปรับ	หรือ
การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ตาม พ.ร.บ. คอมพิวเตอร์	ไม่เกิน 3 ปี	60,000 บาท	ทั้งจำทั้งปรับ
การมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ	ไม่เกิน 3 ปี	60,000 บาท	ทั้งจำทั้งปรับ
การใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ	ไม่เกิน 5 ปี	100,000 บาท	ทั้งจำทั้งปรับ

[137] หมายถึง “บัตรอิเล็กทรอนิกส์” ที่ได้บัญญัติไว้ในมาตรา 1(14)(ข)

จากที่ได้กล่าวไว้ในการวิเคราะห์ในหัวข้อก่อนหน้าว่า การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้นมีความใกล้เคียงกับการมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามมาตรา 269/6 มาก เพียงแต่แตกต่างกันในเรื่ององค์ประกอบของกฎหมายและจำนวนกรรมที่จะลงแก่ผู้กระทำความผิด ดังนั้น เพื่อให้โทษและอัตราโทษในบทบัญญัติเรื่องการดึงข้อมูลจากบัตรนี้เป็นไปในแนวเดียวกันกับแนวทางที่มาตราอื่นๆ ในกฎหมายอาญาทั้งประมวลกฎหมายอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 8 ได้กำหนดไว้ ผู้วิจัยจึงเห็นควรให้บัญญัติอัตราโทษในบทบัญญัติในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นี้ว่า “ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ” ข้อดีคือ เพื่อให้กฎหมายในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ทั้งในประมวลกฎหมายอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 8 ซึ่งมีลักษณะเป็นการกระทำความผิดรูปแบบเดียวกันนั้นมีความเท่าเทียมกัน และสอดคล้องกับอัตราโทษตามที่บทบัญญัติอื่นๆ ในประมวลกฎหมายอาญาได้กำหนดไว้ตามแนวทางของกฎหมายอาญาของไทย ข้อเสียก็คือ อัตราโทษที่ได้นี้เป็นอัตราโทษที่ถือว่าค่อนข้างต่ำเมื่อเทียบกับความเสียหายในทางความเป็นจริงที่เกิดขึ้นจากการกระทำความผิด แต่ในส่วนนี้ผู้วิจัยเห็นว่า เป็นข้อดีที่ศาลอาจให้ดุลพินิจในการรอการกำหนดโทษหรือรอการลงโทษ ตามมาตรา 56 เพื่อให้ผู้กระทำความผิดนั้นกลับตัวกลับใจไม่กระทำความผิดอีกโดยศาลอาจกำหนดเงื่อนไขเพื่อคุมประพฤติบุคคลนั้นไว้ได้ และเป็นการหลีกเลี่ยงการจำคุกในระยะสั้นอันจะเกิดประวัติติดตัวผู้กระทำความผิดซึ่งจะเปลี่ยนผู้กระทำความผิดเป็นอาชญากรเต็มตัวจากการกดดันทางสังคม และในอีกด้านหนึ่งอัตราโทษที่เหมือนจะน้อยนี้ ถ้าหากเป็นการกระทำความผิดที่รุนแรงอันเป็นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์หลายใบหรือหลายครั้ง ศาลจะต้องลงโทษทุกกรรมเป็นกระทงความผิดไป[138] ตามมาตรา 90 ซึ่งอาจทำให้ผู้กระทำความผิดต้องรับโทษอย่างหนักได้เช่นเดียวกัน อันเป็นการลงโทษอย่างสาสมกับความเสียหายที่เกิดขึ้นแก่ผู้เสียหาย สังคม เศรษฐกิจ ในทางข้อเท็จจริงได้ อันนำมาสู่การป้องกันและปราบปรามการกระทำความผิดในลักษณะนี้ได้เช่นกัน

[138] เทียบคำพิพากษาศาลฎีกาที่ 6820/2552 “นำบัตรวีซ่าการ์ดใช้ชำระค่าสินค้าแทนเงินสดรวม 3 ครั้งย่อมเป็นความผิดหลายกรรม หาใช่กรรมเดียวไม่” และฎีกาที่ 2512/2550 “จำเลยกระทำความผิดโดยมีเจตนาต่างกัน การกระทำของจำเลยย่อมเป็นความผิดหลายกรรมหาใช่กรรมเดียว”

บทที่ 6
บทสรุปและข้อเสนอแนะ

ในบทที่ 6 อันเป็นบทสุดท้ายนี้ ผู้วิจัยจะนำเสนอสาระสำคัญของเนื้อหาทั้งหมดในการวิจัยที่ได้กล่าวมาแล้วโดยย่อ โดยในหัวข้อที่ 6.1 จะประกอบด้วยความเป็นมาและความสำคัญของปัญหา ความทั่วไปเกี่ยวกับบัตรอิเล็กทรอนิกส์ ลักษณะการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ปัญหาและอุปสรรคอันเกี่ยวกับการบังคับใช้กฎหมายอาญาในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในประเทศไทย บทบัญญัติกฎหมายอาญาของต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ การวิเคราะห์เปรียบเทียบบทบัญญัติของกฎหมายไทยและกฎหมายต่างประเทศประกอบกับความจำเป็นในการบัญญัติกฎหมาย เพื่อนำมากล่าวในหัวข้อที่ 6.2 ถึงข้อเสนอแนะในการแก้ไขและเพิ่มเติมบทบัญญัติในกฎหมายอาญาของประเทศไทย เพื่อให้ต้องตามสมมติฐานของงานวิจัยฉบับนี้ต่อไป

6.1 บทสรุป

บัตรอิเล็กทรอนิกส์ เป็นผลิตผลที่เกิดจากการพัฒนาทางเทคโนโลยีที่ใช้ในการเก็บข้อมูลของมนุษย์ที่ใช้ยืนยันตัวของบุคคล ซึ่งมีรูปแบบการใช้งานที่หลากหลายและช่วยอำนวยความสะดวกในชีวิตประจำวันของบุคคลเป็นอย่างมาก ไม่ว่าจะใช้ในการระบุตัวตนของบุคคล (Identity Card) เช่น บัตรประจำตัวประชาชน บัตรประจำตัวบุคลากรในองค์กรหรือหน่วยงานใดๆ ทั้งภาครัฐและภาคเอกชน หรือไม่ว่าจะใช้ในการแสดงสิทธิต่างๆ เช่น บัตรกำนัล บัตรเติมเงิน ตั๋วรับชมภาพยนตร์ ตั๋วรถไฟฟ้าหรือเครื่องบิน หรือจะใช้ในการดำเนินธุรกรรมทางการเงินในรูปแบบต่างๆ เช่น โอนเงิน ฝากถอนเงิน หรือใช้ซื้อสินค้าและบริการในห้างร้าน ผ่านการใช้งานบัตรเอทีเอ็ม บัตรเครดิต บัตรเดบิต ทั้งจากการใช้งานบัตรอิเล็กทรอนิกส์ที่มีลักษณะเป็นเอกสารหรือวัตถุใดๆ หรือเป็นการใช้งานในรูปแบบของข้อมูล รหัส หมายเลข ของบัตรอิเล็กทรอนิกส์นั้น ด้วยประโยชน์ที่หลากหลายนี้เองจึงทำให้ในประเทศไทยและต่างประเทศนั้นมีปริมาณการใช้งานบัตรอิเล็กทรอนิกส์ในอัตราที่สูงมากและเนื่องด้วยลักษณะเฉพาะตัวของบัตรอิเล็กทรอนิกส์ที่ประกอบไปด้วยข้อมูลส่วนบุคคลและข้อมูลอื่นๆ ที่มีมูลค่าอันมหาศาล จึงเป็นสิ่งล่อใจให้อาชญากรพัฒนาเทคนิคและวิธีการในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ด้วยรูปแบบต่างๆ เช่น การใช้เครื่องดูดข้อมูลแถบรหัสแม่เหล็ก (Skimmer) การใช้โปรแกรมมัลแวร์ (Malware) หรือไวรัสคอมพิวเตอร์ (Virus Computer) หรือแม้กระทั่งการใช้เทคนิคการหลอกลวงอันหลากหลายเพื่อให้ได้มาซึ่งข้อมูลในบัตรอิเล็กทรอนิกส์ อันก่อให้เกิดความเสียหายแก่

ประชาชนและส่งผลกระทบต่อความเชื่อมั่นในการใช้งานบัตรอิเล็กทรอนิกส์ต่อระบบอื่นๆ ในประเทศเป็นอย่างมากทั้งในประเทศไทยและต่างประเทศ โดยเฉพาะในประเทศไทยที่นับว่าเป็นแหล่งอาชญากรรมในการกระทำความผิดดังกล่าวอย่างต่อเนื่องและมีสถิติการกระทำความผิดเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นอันดับต้นๆ ของภูมิภาคเอเชียและของโลก

จากการศึกษาพบว่า การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์มีลักษณะและองค์ประกอบพิเศษเฉพาะตัวแตกต่างจากการกระทำความผิดอันเกี่ยวกับบัตรอิเล็กทรอนิกส์ในรูปแบบอื่นๆ ที่กฎหมายได้กำหนดไว้ และจากการพิเคราะห์บทบัญญัติของกฎหมายอาญาในประเทศไทยที่มีใช้อยู่แล้วดังกล่าว พบว่า ไม่มีบทบัญญัติของกฎหมายที่ใช้บังคับกับลักษณะการกระทำความผิดรูปแบบนี้ได้โดยตรง ส่วนบทบัญญัติของกฎหมายที่มีใช้บังคับอยู่แล้วก็ไม่ครบถ้วนครอบคลุมถึงลักษณะของการกระทำความผิดได้ทั้งหมดและอย่างเจาะจงตามวัตถุประสงค์ของกฎหมาย และอาจเกิดการตีความบทบัญญัติที่มีอยู่เพื่อลงโทษผู้กระทำความผิดในลักษณะพิเศษนั้นซึ่งขัดกับหลักกฎหมายอาญาได้ อันทำให้เกิดปัญหาการบังคับใช้กฎหมายจากการขาดบทบัญญัติของกฎหมายในการลงโทษผู้กระทำความผิด ซึ่งเป็นปัญหาอันเกิดจากบทบัญญัติของกฎหมาย 2 ประการคือ ปัญหาจากคำนิยามของคำว่า “บัตรอิเล็กทรอนิกส์” ตามประมวลกฎหมายอาญา มาตรา 1(14) และปัญหาจากการขาดบทบัญญัติที่มีลักษณะเป็นการเฉพาะเพื่อใช้ลงโทษกับการกระทำความผิดดังกล่าว

(1) ปัญหาจากคำนิยามของคำว่า “บัตรอิเล็กทรอนิกส์” ตามประมวลกฎหมายอาญา มาตรา 1(14)

จากการพิจารณาคำนิยามของคำว่า “บัตรอิเล็กทรอนิกส์” ตามมาตรา 1(14) ทั้ง (ก) และ (ข) ประกอบกัน พบว่า มาตรา 1(14)(ก) นั้นระบุให้ “เอกสารหรือวัตถุอื่นใด” เป็นบัตรอิเล็กทรอนิกส์โดยมุ่งถึงตัวบัตรในลักษณะที่จับต้องได้ (Physical Cards) เป็นสำคัญ ในขณะที่มาตรา 1(14)(ข) นั้นระบุให้ “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” เป็นบัตรอิเล็กทรอนิกส์ด้วย โดยมุ่งถึงข้อมูลเกี่ยวกับบัตรอิเล็กทรอนิกส์นั้นในลักษณะที่จับต้องไม่ได้ (Virtual Cards) เป็นสำคัญ แต่เนื่องจาก มาตรา 1(14)(ข) ได้ระบุเพิ่มเติมต่อไปด้วยว่าข้อมูลนั้นจะต้อง “มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้” ด้วย จึงจะเข้าลักษณะของการเป็น “บัตรอิเล็กทรอนิกส์” ตามคำนิยามดังกล่าว ซึ่งการกำหนดคำนิยามในลักษณะนี้เองนอกจากจะทำให้ “ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์ หรือเครื่องมือทางตัวเลขใดๆ” ที่อยู่ในบัตรอิเล็กทรอนิกส์ที่มีการออกเอกสารหรือวัตถุอื่นใดให้ ตามคำนามในมาตรา 1(14)(ก) นั้นไม่เป็น “บัตรอิเล็กทรอนิกส์” ตามคำนิยามในกฎหมายอาญาแล้ว ยังทำให้การกระทำความผิดใดๆ ต่อข้อมูลบัตรอิเล็กทรอนิกส์ในลักษณะนั้นจะไม่เป็นความผิดอาญาอีกด้วย อัน

เป็นการจำกัดความคุ้มครองโดยกฎหมายและทำให้ข้อมูลบัตรอิเล็กทรอนิกส์นั้นจะไม่ได้รับความคุ้มครองอย่างเสมอภาคกันในทุกประเภท

(2) ปัญหาจากการขาดบทบัญญัติที่มีลักษณะเป็นการเฉพาะเพื่อใช้ในการลงโทษแก่การกระทำที่เป็นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

จากการศึกษาบทบัญญัติของกฎหมายอาญาในประเทศไทยที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์พบว่ามีเพียงประมวลกฎหมายอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เท่านั้นที่อาจนำมาปรับใช้เพื่อลงโทษแก่การกระทำในลักษณะดังกล่าวได้ ผู้วิจัยจึงได้ทำการวิเคราะห์บทบัญญัติในกฎหมายทั้งสองฉบับนี้ โดยพิจารณา คำนิยาม องค์ประกอบของบทบัญญัติ หลักกฎหมายอาญาและเจตนารมณ์ของบทบัญญัติ ในความผิดฐานลักทรัพย์ ตามมาตรา 334 ความผิดฐานปลอมเอกสาร ตามมาตรา 264 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/1 ถึงมาตรา 269/7 แห่งประมวลกฎหมายอาญา และความผิดฐานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ ตามมาตรา 5 ความผิดฐานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ ตามมาตรา 7 ความผิดฐานกระทำโดยมิชอบเพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ ตามมาตรา 8 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แล้วพบว่า มีเพียงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ฐานกระทำโดยมิชอบเพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ ตามมาตรา 8 เท่านั้นที่สามารถนำมาปรับใช้ในการลงโทษแก่การดึงข้อมูจากบัตรอิเล็กทรอนิกส์ได้ แต่ก็ปรับใช้ได้แต่เพียงรูปแบบของ “บัตรอิเล็กทรอนิกส์” เฉพาะที่เป็นข้อมูลที่มิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ ตามประมวลกฎหมายอาญามาตรา 1(14)(ข) และต้องเป็นข้อมูลที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์เท่านั้นที่ได้รับความคุ้มครองตามกฎหมายอาญาของไทยซึ่งเป็นกรณีที่จำกัด ไม่ครอบคลุมการดึงข้อมูลบัตรอิเล็กทรอนิกส์ในรูปแบบอื่นๆ ด้วยเพราะกฎหมายอาญาของประเทศไทยนั้นยังมิได้มีบทบัญญัติอันเป็นการเฉพาะเพื่อใช้ในการลงโทษแก่การกระทำความผิดในลักษณะดังกล่าว ซึ่งหากพิจารณาเหตุผลของการบัญญัติกฎหมายอันเกี่ยวกับบัตรอิเล็กทรอนิกส์ที่กำหนดไว้ในหมายเหตุท้ายพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา ฉบับที่ 17 พ.ศ. 2547 ตอนหนึ่งว่า “สมควรกำหนดความผิดอาญาสำหรับการกระทำความผิดเกี่ยวกับบัตรและข้อมูลอิเล็กทรอนิกส์ดังกล่าวเพิ่มเติมให้ครอบคลุมการกระทำความผิดในรูปแบบต่างๆ” จะพบว่าเจตนารมณ์ในการยกร่างกฎหมายของประเทศไทยนั้นต้องการให้มีบทบัญญัติความผิดทางอาญาสำหรับใช้ในการลงโทษให้ครอบคลุมการกระทำความผิดที่เกี่ยวกับบัตรอิเล็กทรอนิกส์ในทุกลักษณะซึ่งรวมถึงการกระทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นี้

ด้วย อันเป็นการคุ้มครองทั้งบัตรและข้อมูลอิเล็กทรอนิกส์ของบัตรนั้นจึงจะตรงตามเป้าปณิธานของกฎหมายไทยที่ได้ตั้งไว้

ด้วยปัญหาในด้านบริบททางสังคมและปัญหาในด้านกฎหมายที่กล่าวมาเหล่านี้เอง จึงมีความจำเป็นต้องทำการศึกษาวิจัย เพื่อหาแนวทางในการแก้ไขและเพิ่มเติมบทบัญญัติของกฎหมายอาญาอันมีลักษณะเป็นการเฉพาะกับการกระทำความผิดในลักษณะการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เพื่อนำผู้กระทำความผิดมาลงโทษอันเป็นการตัดแรงจูงใจในการกระทำความผิดของอาชญากรจากการลงโทษทางกฎหมายและเพื่อป้องกันและปราบปรามการกระทำความผิดดังกล่าวต่อไป

ผู้วิจัยจึงได้ทำการศึกษาบทบัญญัติกฎหมายอาญาในต่างประเทศอันได้แก่ สหรัฐอเมริกา สหราชอาณาจักร สาธารณรัฐฟิลิปปินส์และเครือรัฐออสเตรเลีย ซึ่งเป็นประเทศที่ได้รับผลกระทบจากการกระทำความผิดในลักษณะดังกล่าวเป็นอย่างมาก และพบว่า ต่างก็ใช้การแก้ปัญหาโดยการบัญญัติกฎหมายอันมีลักษณะเฉพาะขึ้นเพื่อกำหนดความผิดในการดึงข้อมูลบัตรอิเล็กทรอนิกส์ในรูปแบบต่างๆ ซึ่งแม้ว่าการกำหนดคำนิยามและองค์ประกอบของการกระทำความผิดในการบัญญัติกฎหมายความละเอียดในเรื่องการลงโทษและจำนวนกฎหมายที่ใช้ลงโทษนั้นจะแตกต่างกันไปบ้างในแต่ละประเทศ แต่สิ่งที่เหมือนกันก็คือวัตถุประสงค์ของกฎหมายในทุกประเทศนั้นต่างมุ่งคุ้มครองข้อมูลในบัตรอิเล็กทรอนิกส์เป็นสำคัญไม่ยิ่งหย่อนกว่าการกระทำผิดต่อบัตรอิเล็กทรอนิกส์ในรูปแบบอื่นๆ เพื่อป้องกันและปราบปรามการกระทำความผิดและเพื่อให้กฎหมายมีความทันสมัยครอบคลุมกับลักษณะความผิดที่เกิดขึ้น

โดยกฎหมายของต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้นผู้วิจัยได้ทำเป็นตารางสรุปเปรียบเทียบไว้ท้ายบทที่ 6 นี้แล้ว

ผู้วิจัยจึงได้ทำการวิเคราะห์เปรียบเทียบบทบัญญัติที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในกฎหมายต่างประเทศเหล่านั้น เพื่อแสวงหาแนวทางในการนำมาแก้ไขและปรับใช้ในการกำหนดบทบัญญัติกฎหมายอันเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในประเทศไทย รวมถึงการพิจารณาถึงข้อดีและข้อเสียในด้านต่างๆ ที่อาจเกิดขึ้น ตลอดจนพิจารณาความเหมาะสมในการนำมาปรับใช้กับบริบทกฎหมายของประเทศไทยที่มีอยู่แล้ว ซึ่งจากการวิเคราะห์เปรียบเทียบดังกล่าวนั้น ได้ข้อสรุปดังนี้

6.1.1 การพิจารณาถึงลักษณะของกฎหมายอาญาที่จะให้มีการบัญญัติความผิดในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

จากการศึกษาพบว่า การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศนั้นล้วนแต่เป็นบทบัญญัติที่กำหนดไว้ในกฎหมายในระดับพระราชบัญญัติทั้งสิ้น และสามารถแบ่งจำแนกกฎหมายหลายฉบับของต่างประเทศเหล่านั้น ตามวัตถุประสงค์ของกฎหมายที่มุ่งจะคุ้มครองข้อมูลในรูปแบบต่างๆ กันได้ออกเป็น 3 รูปแบบ คือ กฎหมายที่มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคล (Personal Data) กฎหมายที่มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลคอมพิวเตอร์ และกฎหมายที่มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลบัตรที่ใช้เพื่อทำธุรกรรมทางการเงิน ซึ่งเมื่อพิจารณากฎหมายอาญาในประเทศไทยที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์อันได้แก่ ประมวลกฎหมายอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พบว่ากฎหมายทั้งสองฉบับนั้นต่างก็ต่างก็มีวัตถุประสงค์ในการคุ้มครองข้อมูลในลักษณะต่างๆ เหล่านั้นเช่นเดียวกัน โดยกฎหมายอาญาจะคุ้มครองข้อมูลดังกล่าวในลักษณะอันเป็นการทั่วไปและหลากหลายมากกว่าพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่มุ่งคุ้มครองข้อมูลคอมพิวเตอร์แต่เพียงอย่างเดียว ซึ่งการบัญญัติความผิดในเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ไว้ในประมวลกฎหมายอาญาจะเหมาะสมมากกว่าการบัญญัติไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

6.1.2 การพิจารณาถึงรูปแบบในการบัญญัติกฎหมาย

จากปัญหาการขาดบทบัญญัติในการลงโทษแก่การกระทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้น สามารถจำแนกปัญหาดังกล่าวออกได้เป็นสองลักษณะคือ ปัญหาจากคำนิยามในประมวลกฎหมายอาญามาตรา 1(14) และปัญหาการขาดบทบัญญัติเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์อันเป็นการเฉพาะ ซึ่งได้ข้อสรุปจากการวิเคราะห์เปรียบเทียบกับกฎหมายของต่างประเทศได้ดังนี้

6.1.2.1 การพิจารณาถึงรูปแบบในการบัญญัติกฎหมายโดยการแก้ไขคำนิยามที่มีอยู่เดิมในประมวลกฎหมายอาญา

จากการศึกษาพบว่า ไม่ว่ากฎหมายไทยหรือกฎหมายต่างประเทศนั้นก็ได้บัญญัติให้มีการคุ้มครองบัตรอิเล็กทรอนิกส์ไม่ว่าจะอยู่ในรูปแบบของเอกสารหรือวัตถุอื่นใด หรือจะอยู่ในรูปแบบของข้อมูลก็ตาม ข้อแตกต่างกันก็คือ กฎหมายของต่างประเทศนั้นส่วนใหญ่แล้วจะบัญญัติโดยกล่าวถึงลักษณะของข้อมูลที่กฎหมายมุ่งจะคุ้มครองเป็นสำคัญมากกว่าจะบัญญัติโดยการกล่าวถึงอุปกรณ์ที่ข้อมูลนั้นได้บรรจุไว้อยู่ กล่าวคือ ในเรื่องเกี่ยวกับบัตรอิเล็กทรอนิกส์นี้ กฎหมายต่างประเทศนั้นมุ่งจะคุ้มครองข้อมูลในบัตรอิเล็กทรอนิกส์ มากกว่าการคุ้มครองตัวบัตรอิเล็กทรอนิกส์ในฐานะที่เป็นเพียงเอกสารหรือวัตถุอื่นใดชิ้นหนึ่ง โดยการคุ้มครองนั้นแบ่งได้ออกเป็น 3 ประเภท คือ ข้อมูลส่วนบุคคล ข้อมูลคอมพิวเตอร์และข้อมูลที่ใช้ในการทำธุรกรรมทางการเงิน โดยบัญญัติกระจัดกระจายกันไปขึ้นอยู่กับวัตถุประสงค์ของกฎหมายในแต่ละฉบับและมีรายละเอียดในการบัญญัติไม่เท่ากัน แม้คำนิยามของคำว่า “บัตรอิเล็กทรอนิกส์” ในประมวลกฎหมายอาญาของประเทศไทยจะแตกต่างไปจากความคุ้มครองที่กฎหมายต่างประเทศได้บัญญัติไว้บ้าง แต่ก็มีความใกล้เคียงกันและได้รับความคุ้มครองคล้ายกัน แต่ที่สำคัญคือกฎหมายต่างประเทศนั้น มิได้นำการออกเอกสารหรือวัตถุอื่นใด มาเป็นข้อจำกัดในการคุ้มครองข้อมูลบัตรอิเล็กทรอนิกส์อย่างที่ประมวลกฎหมายอาญามาตรา 1(14)(ข) ได้บัญญัติไว้ กฎหมายของต่างประเทศจึงให้ความคุ้มครองข้อมูลที่ได้บันทึกไว้ไม่ว่าที่ใดๆ ก็ตามด้วย เช่น บันทึกไว้ในแหล่งบันทึกของบัตรอิเล็กทรอนิกส์อันถือได้ว่าเป็นอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์รูปแบบหนึ่งหรือบันทึกไว้ในเครื่องคอมพิวเตอร์ ดังนั้นการนำข้อจำกัดในลักษณะดังกล่าวออกไปจากคำนิยามในมาตรา 1(14)(ข) จะส่งผลดีมากกว่าในการคุ้มครองข้อมูลทุกประเภทได้อย่างเสมอภาค ดังที่กฎหมายต่างประเทศได้กำหนดไว้

6.1.2.2 การพิจารณาถึงรูปแบบในการบัญญัติกฎหมายโดยการเพิ่มเป็นบทบัญญัติเฉพาะ

จากการศึกษาพบว่า บทบัญญัติของกฎหมายต่างประเทศซึ่งได้กำหนดให้มีการดึงข้อมูลที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์นั้นมีรูปแบบของการบัญญัติไว้โดยแบ่งออกได้เป็นสองลักษณะ คือ แยกการดึงข้อมูลจากบัตรเป็นการกระทำเพียงลักษณะเดียวในบทบัญญัติ กับ รวมการกระทำความผิดอื่นๆ ซึ่งไม่เกี่ยวข้องกับการดึงข้อมูลจากบัตรเข้ามาอยู่ในบทบัญญัติเดียวกันด้วยแต่ก็มิได้มีความสัมพันธ์ร่วมกันกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์และขึ้นอยู่กับดุลพินิจในการบัญญัติ

กฎหมายของแต่ละประเทศเป็นสำคัญ ดังนั้นจึงสามารถบัญญัติเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์เป็นบทบัญญัติเฉพาะแยกออกจากการกระทำความผิดในลักษณะอื่นๆ ได้

ซึ่งในการแสวงหาแนวทางในการบัญญัติกฎหมายอันเป็นบทบัญญัติเฉพาะนี้ ผู้วิจัยได้แบ่งการวิเคราะห์เปรียบเทียบตามองค์ประกอบความผิดที่จะบัญญัติขึ้นในส่วนขององค์ประกอบภายนอก ได้แก่ ผู้กระทำ การกระทำ วัตถุแห่งการกระทำ และส่วนขององค์ประกอบภายใน อันได้แก่ เจตนาและเจตนาพิเศษ ซึ่งได้ข้อสรุปดังนี้

6.1.2.2.1 องค์ประกอบภายนอกส่วนของผู้กระทำ

จากการศึกษาพบว่า กฎหมายต่างประเทศนั้นได้กำหนดองค์ประกอบภายนอกส่วนของผู้กระทำโดยให้หมายถึงบุคคลทั่วๆ ไป ซึ่งมิได้เฉพาะเจาะจงบุคคลใดบุคคลหนึ่งโดยเฉพาะ โดยการใช้คำว่า “ผู้ใด” (Whoever) “บุคคล” (A person) และคำว่า “บุคคลใด” (Any person) ในกฎหมายอาญาเหมือนกับที่ประเทศไทยใช้คำว่า “ผู้ใด” ในการขึ้นต้นความผิดอาญาในแต่ละมาตรา

6.1.2.2.2 องค์ประกอบภายนอกส่วนของการกระทำ

จากการศึกษาพบว่า สามารถจำแนกลักษณะของการกระทำความผิดในกฎหมายต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ได้ออกเป็น 3 กลุ่ม คือ กลุ่มการครอบครอง (Possession) หรือควบคุม (Control) ข้อมูลที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ กลุ่มการเข้าถึง (Access) ข้อมูลที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ และกลุ่มได้รับ (Obtain) ข้อมูลที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ ซึ่งการใช้คำในแต่ละกลุ่มก็จะมีข้อดีและข้อเสียในการสื่อความหมายอันแตกต่างกันออกไป ผู้วิจัยจึงเห็นว่าควรกำหนดคำขึ้นมาใหม่เพื่อให้สามารถสื่อถึงการดึงข้อมูลในแต่ละรูปแบบได้อย่างครอบคลุมและครบถ้วนนอกจากที่กฎหมายของต่างประเทศนั้นได้บัญญัติไว้

6.1.2.2.3 องค์ประกอบภายนอกส่วนของวัตถุแห่งการกระทำ

จากการศึกษาพบว่า การกระทำการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้นจะต้องเป็นการกระทำต่อ “ข้อมูล” (Information) อันหมายถึง ข้อมูลส่วนบุคคล (Personal data) หรือ ข้อมูลทางการเงินของบุคคล (Personal financial information) หรือข้อมูลอื่นๆ เป็นต้น โดย

ไม่จำต้องคำนึงว่าข้อมูลนั้นจะเป็น “ข้อมูลคอมพิวเตอร์” ตามคำนิยามใน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือจะเป็น “ข้อมูลอิเล็กทรอนิกส์” ตามคำนิยามในพระราชบัญญัติว่าว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 หรือไม่ก็ตาม หากข้อมูลนั้น เป็นข้อมูลของ “บัตรอิเล็กทรอนิกส์” ทั้งสามรูปแบบที่ประมวลกฎหมายอาญามาตรา 1(14) ได้กำหนดไว้ตามที่ผู้วิจัยได้ทำการเสนอแก้ไขคำนิยามไปแล้ว ข้อมูลเหล่านั้นย่อมจะได้รับความคุ้มครองจากการกระทำการดึงข้อมูลจากบัตรในงานวิจัยนี้ด้วยกันทั้งสิ้น และต้องเป็นข้อมูลบัตรอิเล็กทรอนิกส์ของ “ผู้อื่น” ด้วย ตามแนวคิดของกฎหมายในต่างประเทศ

6.1.2.2.4 องค์ประกอบภายในส่วนของเจตนา

จากการศึกษาพบว่า การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในต่างประเทศนั้นโดยทั่วไปแล้วจะต้องเกิดจากการกระทำโดยเจตนาเท่านั้น โดยเพียงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018 มาตรา 170 ของสหราชอาณาจักร กรณีเดียวเท่านั้นที่กำหนดให้มีการกระทำโดยประมาทแก่การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ด้วย และสามารถใช้มาตรา 59 แห่งประมวลกฎหมายอาญาเรื่องเจตนาอันเป็นบทบัญญัติทั่วไปในการปรับใช้ได้อยู่แล้วโดยมิต้องบัญญัติคำว่า “เจตนา” ลงในบทบัญญัติเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ดังกล่าวไปอีกครั้งหนึ่ง

6.1.2.2.5 องค์ประกอบภายในส่วนของเจตนาพิเศษ

จากการศึกษาพบว่า นอกจากเจตนาธรรมดาแล้ว บทบัญญัติกฎหมายของต่างประเทศโดยส่วนใหญ่จะกำหนดให้มีเจตนาพิเศษบัญญัติไว้เป็นองค์ประกอบภายในด้วย ซึ่งแบ่งได้เป็น 2 ประเภท คือ เจตนาพิเศษเพื่อกระทำการใดๆ ต่อข้อมูลนั้น และเจตนาพิเศษเพื่อนำข้อมูลที่ได้นั้นไปใช้ต่อไป เช่นเดียวกันกับมาตราอื่นๆ ในหมวดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ แห่งประมวลกฎหมายอาญา แต่การกำหนดเพิ่มเจตนาพิเศษลงไปในบทบัญญัติการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์อาจจะก่อให้เกิดปัญหาแก่การพิสูจน์ความผิดของจำเลยในทางปฏิบัติได้

6.1.3 การพิจารณาเกี่ยวกับโทษและอัตราโทษที่ผู้กระทำความผิดสมควรจะได้รับตามบทบัญญัติกฎหมายการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

จากการศึกษาพบว่า การกำหนดโทษและอัตราโทษที่ได้กำหนดไว้ในกฎหมายที่เกี่ยวข้องกับการกระทำความผิดอันเกี่ยวกับบัตรอิเล็กทรอนิกส์จะมีความแตกต่างกันไปตามแต่ละประเทศ ซึ่งส่วนใหญ่แล้วทุกประเทศนั้นจะกำหนดให้มีทั้งโทษจำคุกและโทษปรับด้วย ในด้านอัตราโทษของการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้น มีการบัญญัติที่แตกต่างกันไปตามแต่ละประเทศอีกเช่นเดียวกัน โดยในสหรัฐอเมริกา สหราชอาณาจักรเฉพาะความผิดในกรณีคดีอาญาสามัญ (Summary Offences) และสาธารณรัฐฟิลิปปินส์ นั้นจะให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์นั้นมีอัตราโทษเท่ากันกับการปลอมบัตรอิเล็กทรอนิกส์ซึ่งมีอัตราโทษที่สูง ส่วนในสหราชอาณาจักรเฉพาะความผิดในกรณีคดีอาญาอุกฉกรรจ์ (Indictable Offences) เครือรัฐออสเตรเลีย และประเทศไทยในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 8 นั้นจะกำหนดให้การดึงข้อมูลจากบัตรอิเล็กทรอนิกส์มีอัตราโทษที่น้อยกว่าการปลอมบัตรอิเล็กทรอนิกส์อย่างชัดเจน จึงสรุปได้ว่า การกำหนดอัตราโทษในเรื่องการกระทำความผิดอันเกี่ยวกับบัตรอิเล็กทรอนิกส์และการดึงข้อมูลบัตรอิเล็กทรอนิกส์นี้ ขึ้นกับดุลพินิจตามแต่ละประเทศจะได้กำหนดไว้ในกฎหมายของตน ดังนั้นการกำหนดโทษและอัตราโทษของบทบัญญัติเรื่องการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในงานวิจัยนี้จึงต้องพิจารณาแนวทางในกฎหมายอาญาของประเทศไทยเป็นหลัก ซึ่งเมื่อผู้วิจัยได้ทำการเปรียบเทียบอัตราโทษของมาตราอื่นๆ ในหมวดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ในประมวลกฎหมายอาญากับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 8 ซึ่งเป็นบทบัญญัติที่มีอยู่แล้วในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์บางรูปแบบ พบว่า การกำหนดอัตราโทษในบทบัญญัติเรื่องการดึงข้อมูลจากบัตรซึ่งมีลักษณะเป็นการกระทำความผิดรูปแบบเดียวกันนั้นให้มีความเท่าเทียมกัน จะเหมาะสมและสอดคล้องกับอัตราโทษตามที่บทบัญญัติอื่นๆ ในประมวลกฎหมายได้กำหนดไว้ตามแนวทางของกฎหมายอาญาของไทยมากกว่า

6.2 ข้อเสนอแนะ

จากการศึกษาบทบัญญัติของกฎหมายในต่างประเทศที่เกี่ยวข้องกับกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ และจากการวิเคราะห์เปรียบเทียบบทบัญญัติกฎหมายของต่างประเทศดังกล่าวประกอบกับบทบัญญัติในกฎหมายอาญาของประเทศไทย รวมถึงการพิจารณาถึงข้อดีและข้อเสียในด้านต่างๆ ที่อาจเกิดขึ้น ตลอดจนพิจารณาความเหมาะสมในการนำมาปรับใช้กับบริบทกฎหมายของประเทศไทยที่มีอยู่แล้ว เพื่อแสวงหาแนวทางในการแก้ไขและปรับใช้ในการกำหนดบทบัญญัติกฎหมายอันเกี่ยวกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ในประเทศไทย ผู้วิจัยจึงได้เสนอแนะการแก้ไขปัญหา การขาดบทบัญญัติในการลงโทษในการกระทำความผิดที่มีลักษณะเป็นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ซึ่งต้องอาศัยการแก้ไขคำนิยามที่มีอยู่เดิมในกฎหมายและการเพิ่มบทบัญญัติเฉพาะในกฎหมายประกอบกัน จึงจะเป็นการแก้ไขปัญหาของงานวิจัยฉบับนี้ได้อย่างครบถ้วน ตามข้อเสนอแนะดังต่อไปนี้

6.2.1 การแก้ไขคำนิยามที่มีอยู่เดิมในประมวลกฎหมายอาญา

ผู้วิจัยเห็นควรให้มีการแก้ไขนิยามของคำว่า “บัตรอิเล็กทรอนิกส์” ในมาตรา 1(14)(ข) แห่งประมวลกฎหมายอาญา โดยการตัดคำว่า “โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้” ทิ้ง และเปลี่ยนคำว่า “แต่” เป็น “และ” นอกจากนั้นให้คงเดิม ซึ่งจะได้เป็น

“มาตรา 1(14) “บัตรอิเล็กทรอนิกส์” หมายความว่า

(ก) เอกสารหรือวัตถุอื่นใดไม่ว่าจะมีรูปลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า

(ข) ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ และมีวิธีการใช้ในทำนองเดียวกับ (ก) หรือ

(ค) สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ”

การแก้ไขในลักษณะดังกล่าวจะสามารถลดข้อจำกัดในการคุ้มครองข้อมูลดังที่ได้กำหนดไว้ในกฎหมายเดิมออกไป ทำให้กฎหมายสามารถคุ้มครองข้อมูลทุกประเภทจากการดึงข้อมูลได้อย่างเสมอภาคและอย่างครอบคลุม ไม่ว่าข้อมูลนั้นจะอยู่ในรูปลักษณะใดหรือบันทึกไว้ในแหล่งใดก็ตาม อันสอดคล้องกับความคุ้มครองที่เกี่ยวข้องกับข้อมูลในประเภทต่างๆ ที่กฎหมายต่างประเทศนั้นให้ความสำคัญและได้บัญญัติความคุ้มครองนั้นไว้ในกฎหมายหลายฉบับแตกต่างกันไป

6.2.2 การเพิ่มเป็นบทบัญญัติเฉพาะ

ผู้วิจัยเห็นควรให้มีการเพิ่มเป็นบทบัญญัติอันเป็นการเฉพา**ะ** ในการกำหนดความผิดที่มีลักษณะการกระทำเป็นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ ซึ่งจะบัญญัติไว้ในประมวลกฎหมายอาญา ในภาค 2 ลักษณะ 7 หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ อันบัญญัติไว้ว่า

“มาตรา... ผู้ใด กระทำโดยประการใดๆ อันเป็นการได้มาซึ่งข้อมูลบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

การเพิ่มบัญญัติกฎหมายอันเป็นการเฉพาะดังกล่าวนี้ เมื่อใช้ประกอบกันกับการแก้ไขคำนิยามตามข้อ 6.2.1 แล้ว จะเป็นการแก้ไขปัญหาการขาดบทบัญญัติในการลงโทษในการกระทำความผิดที่มีลักษณะเป็นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์อย่างครบถ้วน ซึ่งไม่ว่าข้อมูลบัตรอิเล็กทรอนิกส์นั้นจะอยู่ในรูปแบบใดรูปแบบหนึ่งของบัตรอิเล็กทรอนิกส์ดังที่ได้บัญญัติไว้ในมาตรา 1(14) คือ

(1) บัตรหรือวัตถุอื่นใดในลักษณะที่จับต้องได้ (Physical Cards) ในมาตรา 1(14)(ก)

(2) ข้อมูล รหัส หมายเลขชุดทางอิเล็กทรอนิกส์ใดๆ ในลักษณะที่จับต้องไม่ได้ (Virtual Cards) ในมาตรา 1(14)(ข)

(3) เอกลักษณ์ทางชีวภาพของบุคคลในลักษณะที่เป็นส่วนหนึ่งของมนุษย์ (Biometric data) ในมาตรา 1(14)(ค)

ข้อมูลในบัตรอิเล็กทรอนิกส์ทั้งสามรูปแบบดังกล่าวนี้ก็ย่อมจะได้รับความคุ้มครองตามกฎหมาย จากการกระทำความผิดที่เป็นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์ทั้งสิ้น การบัญญัติกฎหมายในลักษณะดังกล่าวนอกจากจะทำให้มีบทบัญญัติที่ชัดเจน ครอบคลุมกับลักษณะความผิดอันเกี่ยวกับบัตรอิเล็กทรอนิกส์ในลักษณะต่างๆ ที่เกิดขึ้นจริงในปัจจุบันแล้ว ยังเป็นการแก้ไขปรับปรุงกฎหมายอาญาของประเทศไทยให้ทัดเทียมกับบทบัญญัติของกฎหมายในต่างประเทศและตรงตาม

เป้าปณิธานของกฎหมายไทยที่ได้ตั้งไว้ตามเจตนารมณ์ของการแก้ไขเพิ่มเติมประมวลกฎหมายอาญา ฉบับที่ 17 พ.ศ. 2547

นอกจากนั้นโทษที่ได้กำหนดไว้ยังมีความเหมาะสมกับการบังคับใช้กฎหมายดังกล่าว โดยการบัญญัติอัตราโทษให้สอดคล้องกับความผิดฐานดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ ตามมาตรา 8 ซึ่งเป็นบทบัญญัติที่มีอยู่แล้วในการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์บางรูปแบบ[1] เพื่อให้การกระทำความผิดในรูปแบบเดียวกันนั้นมีอัตราโทษที่เท่าเทียมกัน และสอดคล้องกับอัตราโทษตามที่บทบัญญัติอื่นๆ ในประมวลกฎหมายอาญาได้กำหนดไว้ตามแนวทางของกฎหมายอาญาไทย และด้วยอัตราโทษที่ได้กำหนดเพียงเท่านี้ จะเป็นข้อดีที่ศาลอาจใช้ดุลพินิจในการรอการกำหนดโทษหรือรอการลงโทษ ตามมาตรา 56 เพื่อให้ผู้กระทำความผิดนั้นกลับตัวกลับใจไม่กระทำความผิดอีกโดยศาลอาจกำหนดเงื่อนไขเพื่อคุมประพฤติบุคคลนั้นไว้ได้ และเป็นการหลีกเลี่ยงการจำคุกในระยะสั้นอันจะเกิดประวัติติดตัวผู้กระทำความผิดซึ่งจะเปลี่ยนผู้กระทำความผิดเป็นอาชญากรเต็มตัวจากการกดดันทางสังคม และในอีกด้านหนึ่ง ถ้าหากเป็นการกระทำความผิดที่รุนแรงอันเป็นการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์หลายใบหรือหลายครั้ง ศาลจะต้องลงโทษทุกกรรมเป็นกระทงความผิดไป ตามมาตรา 90 ซึ่งอาจทำให้ผู้กระทำความผิดต้องรับโทษอย่างหนักได้เช่นเดียวกัน อันเป็นการลงโทษอย่างสาสมกับความเสียหายที่เกิดขึ้นแก่ผู้เสียหาย สังคม เศรษฐกิจ ในทางข้อเท็จจริงได้ อันนำมาสู่การบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพ เพื่อนำผู้กระทำความผิดมาลงโทษตามกฎหมายและเป็นการป้องกันและปราบปรามการกระทำความผิดในลักษณะนี้ได้ อันเป็นการสมประสงค์ตามสมมติฐานของงานวิจัยฉบับนี้ได้อย่างแท้จริง

[1] หมายถึง “บัตรอิเล็กทรอนิกส์” ที่ได้บัญญัติไว้ในมาตรา 1(14)(ข)

ตารางที่ 28 เปรียบเทียบองค์ประกอบความผิดของบทบัญญัติกฎหมายในต่างประเทศที่เกี่ยวข้องกับการดึงข้อมูลจากบัตรอิเล็กทรอนิกส์

สหรัฐอเมริกา

บทบัญญัติ (มาตรา)	ผู้กระทำ	การกระทำ การดึงข้อมูล	วัตถุแห่งการกระทำ	เจตนา	เจตนาพิเศษ	โทษ	การกระทำอื่นๆ ในบทบัญญัติ
รัฐบัญญัติของสหรัฐอเมริกา (The United States Code)							
1028(a)(7)	ผู้ใด (Whoever)	โอน (Transfers)	สิ่งที่อ้างอิงในการระบุตัวตน (A means of identification) ของผู้อื่น	เจตนา	เจตนาที่จะกระทำหรือช่วยเหลือหรือสนับสนุนหรือเกี่ยวข้องกับการกระทำที่ผิดกฎหมายใดๆ ที่ถือเป็นการละเมิดต่อกฎหมายของรัฐบาลกลางหรือก่อให้เกิดความผิดอาญาร้ายแรงภายใต้กฎหมายของมลรัฐหรือท้องถิ่น	จำคุกไม่เกิน 5 ปี ถึง 30 ปี ขึ้นอยู่กับลักษณะของการกระทำความผิดหรือปรับหรือทั้งจำทั้งปรับ และริบทรัพย์สินใดๆ ที่เป็นของผู้กระทำความผิดที่ได้ใช้หรือมีไว้เพื่อจะใช้ในการกระทำความผิด ให้ตกเป็นของสหรัฐด้วย	ครอบครอง, ใช้

บทบัญญัติ (มาตรา)	ผู้กระทำ	การกระทำ การดึงข้อมูล	วัตถุแห่งการกระทำ	เจตนา	เจตนาพิเศษ	โทษ	การกระทำอื่นๆ ในบทบัญญัติ
1029(a)(1)	ผู้ใด (Whoever)	ผลิต (Produce), เคลื่อนย้าย (Traffics in)	อุปกรณ์ในการเข้าถึงปลอม (Counterfeit access devices) หมายถึง ข้อมูลของบัตรใดๆ ที่มีวัตถุประสงค์ในการใช้ทำธุรกรรมทางการเงิน	เจตนา	เจตนาที่จะฉ้อโกง	จำคุกไม่เกิน 10 ปี หรือไม่เกิน 20 ปีในกรณีการกระทำความผิดซ้ำ หรือปรับหรือทั้งจำทั้งปรับ	ใช้
1030(a)(2)	ผู้ใด (Whoever)	เข้าถึง (Accesses) จึงได้รับ (Obtain)	ข้อมูลในรูปแบบอิเล็กทรอนิกส์ที่อยู่ในคอมพิวเตอร์ที่ได้กำหนดไว้สามประเภท	เจตนา	-	จำคุกไม่เกิน 1 ปี ถึง 5 ปี ขึ้นอยู่กับลักษณะของการกระทำความผิด หรือไม่เกิน 10 ปีในกรณีการกระทำความผิดซ้ำ หรือปรับหรือทั้งจำทั้งปรับ	เข้าถึง

สหราชอาณาจักร

บทบัญญัติ (มาตรา)	ผู้กระทำ	การกระทำการดึงข้อมูล	วัตถุแห่งการกระทำ	เจตนา	เจตนาพิเศษ	โทษ		การกระทำอื่นๆ ในบทบัญญัติ
						Summary Offences	Indictable Offences	
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990)								
1	บุคคล (A person)	ทำให้กระทำการใดๆ (Perform any function) เพื่อจะได้รับการเข้าถึง (Access) หรือข้อมูล (Data)	ข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ (รวมถึงข้อมูลที่อยู่ในอุปกรณ์ในการจัดเก็บข้อมูล (Storage medium) ในขณะเวลาที่อุปกรณ์นั้นได้เชื่อมต่อและรับรู้โดยเครื่องคอมพิวเตอร์แล้ว)	เจตนา	เพื่อจะได้รับการเข้าถึง (Access) โปรแกรม (Program) หรือข้อมูล (Data) ใดๆ ที่อยู่ในเครื่องคอมพิวเตอร์	จำคุกไม่เกิน 12 เดือนหรือปรับไม่เกิน 5,000 ปอนด์สเตอร์ลิงหรือทั้งจำทั้งปรับ	จำคุกไม่เกิน 2 ปีหรือปรับหรือทั้งจำทั้งปรับ	-

บทบัญญัติ (มาตรา)	ผู้กระทำ	การกระทำการดึงข้อมูล	วัตถุแห่งการกระทำ	เจตนา	เจตนาพิเศษ	โทษ		การกระทำอื่นๆ ในบทบัญญัติ
						Summary Offences	Indictable Offences	
3A(3)	บุคคล (A person)	ได้รับ (Obtains)	สิ่งของ (Article) หมายถึง ข้อมูล หรือโปรแกรมใดๆ ก็ตามที่อยู่ในรูปแบบอิเล็กทรอนิกส์	เจตนา	เพื่อจะใช้หรือช่วยเหลือในการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ต่อไป	จำคุกไม่เกิน 12 เดือนหรือปรับไม่เกิน 5,000 ปอนด์สเตอร์ลิงหรือทั้งจำทั้งปรับ	จำคุกไม่เกิน 2 ปีหรือปรับหรือทั้งจำทั้งปรับ	-
พระราชบัญญัติว่าด้วยการฉ้อโกง ค.ศ. 2006 (The Fraud Act 2006)								
6	บุคคล (A person)	มีไว้ในครอบครอง (Possession), ควบคุม (Control)	สิ่งของ (Article) หมายถึง ข้อมูล หรือโปรแกรมใดๆ ก็ตามที่อยู่ในรูปแบบอิเล็กทรอนิกส์	เจตนา	เพื่อจะใช้ในการดำเนินการหรือเกี่ยวข้องในการฉ้อโกงต่อไป	จำคุกไม่เกิน 12 เดือนหรือปรับไม่เกิน 5,000 ปอนด์สเตอร์ลิงหรือทั้งจำทั้งปรับ	จำคุกไม่เกิน 5 ปีหรือปรับหรือทั้งจำทั้งปรับ	-

บทบัญญัติ (มาตรา)	ผู้กระทำ	การกระทำการดึงข้อมูล	วัตถุแห่งการกระทำ	เจตนา	เจตนาพิเศษ	โทษ		การกระทำอื่นๆ ในบทบัญญัติ
						Summary Offences	Indictable Offences	
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018 (Data Protection Act 2018)								
170	บุคคล (A person)	ได้รับ (Obtain)	ข้อมูลส่วนบุคคล (Personal data) หมายถึง ข้อมูลใดๆ ที่เกี่ยวข้องกับบุคคลที่มีชีวิตที่ระบุตัวตนได้	เจตนา, ประมาท	-	จำคุกไม่เกิน 12 เดือนหรือปรับไม่เกิน 5,000 ปอนด์สเตอร์ลิง (อังกฤษและเวลส์ ปรับไม่มีจำนวนจำกัด)	จำคุกไม่เกิน 5 ปีหรือปรับ (ไม่มีจำนวนจำกัด)	เปิดเผย

สาธารณรัฐฟิลิปปินส์

บทบัญญัติ (มาตรา)	ผู้กระทำ	การกระทำการดึงข้อมูล	วัตถุแห่งการกระทำ	เจตนา	เจตนาพิเศษ	โทษ	การกระทำอื่นๆ ในบทบัญญัติ
พระราชบัญญัติป้องกันอาชญากรรมไซเบอร์ ค.ศ. 2012 (Cybercrime Prevention Act of 2012)							
4(a)(1)	บุคคลใด (Any person)	เข้าถึง (Access)	อุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลคอมพิวเตอร์ (Computer data storage devices)	เจตนา	-	จำคุกตั้งแต่ 6 ปีกับหนึ่งวัน ถึง 20 ปี หรือปรับเป็นอย่างน้อย 200,000 ถึง 500,000 เปโซฟิลิปปินส์จนถึงจำนวนที่สมน้ำสมเนื้อกับความเสียหายที่เกิดขึ้น หรือทั้งจำทั้งปรับ	-
4(b)(3)	บุคคลใด (Any person)	ขโมย (Theft)	ข้อมูลประจำตัวของบุคคล (Identifying information) หมายถึง ข้อมูลประจำตัวปกติเกี่ยวกับบุคคล	เจตนา	เจตนาเข้ายึดถือ (Acquisition) ใช้ โอน ครอบครอง เปลี่ยนแปลงหรือลบ ข้อมูลประจำตัวของบุคคลอื่น	จำคุกตั้งแต่ 6 ปีกับหนึ่งวัน ถึง 12 ปี หรือปรับเป็นอย่างน้อย 200,000 เปโซฟิลิปปินส์จนถึงจำนวนที่สมน้ำสมเนื้อกับความเสียหายที่เกิดขึ้น หรือทั้งจำทั้งปรับ	-

บทบัญญัติ (มาตรา)	ผู้กระทำ	การกระทำการดึงข้อมูล	วัตถุแห่งการกระทำ	เจตนา	เจตนาพิเศษ	โทษ	การกระทำอื่นๆ ในบทบัญญัติ
พระราชบัญญัติควบคุมอุปกรณ์ในการเข้าถึง ค.ศ. 1988 ที่ได้แก้ไขเพิ่มเติมแล้ว (Access Devices Regulation Act of 1998 and An Act Providing for Additional Prohibitions to and Increasing Penalties for Violations of Republic Act No. 8484)							
9(k)	บุคคลใด (Any person)	มีไว้ในครอบครอง (Possession)	อุปกรณ์ในการเข้าถึง (Access Device)	เจตนา	เจตนาในการเข้าถึงบัญชีหรือจัดการบัญชี	จำคุกไม่น้อยกว่า 6 ปี แต่ไม่เกิน 10 ปี หรือจำคุกตลอดชีวิต และปรับเป็นจำนวน 5,000,000 เปโซฟิลิปปินส์ หรือสองเท่าของมูลค่าของประโยชน์ที่ผู้กระทำความผิดได้รับ	-
9(s)	บุคคลใด (Any person)	เข้าถึง (Accessing)	บัญชีธนาคารออนไลน์ บัญชีบัตรเครดิต บัญชีเอทีเอ็ม บัญชีบัตรเดบิต	เจตนา	-		-
9(t)	บุคคลใด (Any person)	แฮก (Hacking), ใช้ไวรัส (Computer Viruses)	ข้อมูลในระบบคอมพิวเตอร์ เซิฟเวอร์ ระบบข้อมูลหรือระบบสื่อสาร	เจตนา	เพื่อทำการทุจริต แก้ไข ขโมย หรือทำลาย		-

บทบัญญัติ (มาตรา)	ผู้กระทำ	การกระทำการดึงข้อมูล	วัตถุแห่งการกระทำ	เจตนา	เจตนาพิเศษ	โทษ	การกระทำอื่นๆ ในบทบัญญัติ
9(q)	บุคคลใด (Any person)	สกิมมิ่ง (Skimming), คัดลอก (Copying), ได้รับไป (Obtaining)	บัตรเครดิต บัตรชำระเงิน บัตรเดบิต	เจตนา	-	จำคุกไม่น้อยกว่า 10 ปี แต่ไม่เกิน 12 ปีหรือจำคุกตลอดชีวิต[1] และปรับเป็นจำนวน 5,000,000 เปโซฟิลิปปินส์ หรือสองเท่าของมูลค่าของประโยชน์ที่ผู้กระทำความผิดได้รับ	ปลอมแปลง

[1] ในกรณีที่เป็นการแฮกระบบของธนาคาร หรือ สกิมมิ่งบัตรชำระเงิน ตั้งแต่ 50 ใบขึ้นไป หรือ การกระทำความผิดนั้นกระทบบัญชีธนาคาร บัตรเครดิต บัตรชำระเงินหรือบัตรเดบิต ตั้งแต่ 50 บัญชีหรือใบขึ้นใบ

เครือรัฐออสเตรเลีย

บทบัญญัติ (มาตรา)	ผู้กระทำ	การกระทำการดึงข้อมูล	วัตถุแห่งการกระทำ	เจตนา	เจตนาพิเศษ	โทษ	การกระทำอื่นๆ ในบทบัญญัติ
พระราชบัญญัติอาชญากรรมไซเบอร์ ค.ศ. 2001 (Cybercrime Act 2001)							
477.1	บุคคล (A person)	เข้าถึง (Access)	ข้อมูลที่อยู่ในคอมพิวเตอร์ (Data held in computer) (รวมถึงข้อมูลที่อยู่ในอุปกรณ์จัดเก็บข้อมูล (Data storage device) ในขณะที่ข้อมูลนั้นได้อยู่ในคอมพิวเตอร์ด้วย)	เจตนา	จะกระทำหรืออำนวยความสะดวก ในการกระทำความผิดร้ายแรงต่อกฎหมาย	จำคุกตั้งแต่ 5 ปีขึ้นไปถึงจำคุกตลอดชีวิต	แก้ไข เปลี่ยนแปลง, ทำให้เสีย
478.3	บุคคล (A person)	ครอบครอง (Possession), ควบคุม (Control of)	ข้อมูล (Data) ไม่ว่าอยู่ในรูปลักษณะใดก็ตาม	เจตนา	จะใช้หรืออำนวยความสะดวกในการกระทำผิดอันร้ายแรงที่เกี่ยวกับคอมพิวเตอร์	จำคุก 3 ปี	-

บทบัญญัติ (มาตรา)	ผู้กระทำ	การกระทำการดึงข้อมูล	วัตถุแห่งการกระทำ	เจตนา	เจตนาพิเศษ	โทษ	การกระทำอื่นๆ ในบทบัญญัติ
478.4	บุคคล (A person)	ได้รับ (Obtain)	ข้อมูล (Data) ไม่ว่าอยู่ในรูปลักษณะใดก็ตาม	เจตนา	จะใช้หรืออำนวยความสะดวกในการกระทำผิดอันร้ายแรงที่เกี่ยวกับคอมพิวเตอร์	จำคุก 3 ปี	จัดหา
พระราชบัญญัติแก้ไขกฎหมายอาชญากรรม (ความผิดด้านโทรคมนาคม และมาตรการอื่นๆ)(ฉบับที่ 2) ค.ศ. 2004 (Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004)							
480.4	บุคคล (A person)	ได้รับ (Obtain)	ข้อมูลทางการเงินของบุคคล (Personal financial information)	เจตนา	-	จำคุก 5 ปี	ซื้อขาย, แลกเปลี่ยน

บรรณานุกรม

หนังสือและวารสารภาษาไทย

เกียรติขจร วัจนะสวัสดิ์. กฎหมายอาญาภาคความผิด เล่ม 2. พิมพ์ครั้งที่ 6. กรุงเทพฯ: กรุงสยาม พับลิชชิ่ง, 2557.

————. กฎหมายอาญาภาคความผิด เล่ม 3. พิมพ์ครั้งที่ 1. กรุงเทพฯ: หจก.จิรรัชการพิมพ์, 2550.

————. คำอธิบายฎหมายอาญา ภาค 1. พิมพ์ครั้งที่ 10. กรุงเทพฯ: พลสยาม พริ้นติ้ง, 2551.

คณิต ณ นคร. กฎหมายอาญาภาคความทั่วไป. พิมพ์ครั้งที่ 4. กรุงเทพฯ: สำนักพิมพ์วิญญูชน, 2554.

————. กฎหมายอาญาภาคความผิด. พิมพ์ครั้งที่ 11. กรุงเทพฯ: วิญญูชน, 2559.

————. ประมวลกฎหมายอาญา หลักกฎหมายและพื้นฐานการเข้าใจ. พิมพ์ครั้งที่ 5. กรุงเทพฯ: นิติธรรม, 2538.

จิตติ ติงศภัทิย์. กฎหมายอาญา ภาค 2 ตอน 1. พิมพ์ครั้งที่ 5. กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2523.

————. คำอธิบายประมวลกฎหมายอาญา ภาค 2 ตอน 2 และภาค 3. พิมพ์ครั้งที่ 3. กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2532.

ทวีเกียรติ มีนะกนิษฐ์. ความผิดฐานลักทรัพย์. วารสารนิติศาสตร์, 16 (2529).

————. คำอธิบายกฎหมายอาญา ภาคความผิดและลหุโทษ. พิมพ์ครั้งที่ 17. กรุงเทพฯ: สำนักพิมพ์วิญญูชน, 2562.

ทวียศ ศรีเกตุ. ภัยร้ายจากบัตรเครดิต. บทความใช้เพื่อการนำออกอากาศทางสถานีวิทยุกระจายเสียงรัฐสภา รายการเจตนารมณ์กฎหมาย, สำนักงานเลขาธิการสภาผู้แทนราษฎร (2557).

บัญญัติ สุชีวะ. คำอธิบายกฎหมายลักษณะทรัพย์. พิมพ์ครั้งที่ 15. กรุงเทพฯ: กรุงสยามพับลิชชิ่ง, 2556.

พระยานิพนธ์พจนาตถ์. กฎหมายลักษณะอาญา รศ. 127. พระนคร: กรุงเทพ-บรรณาคาร, 2478.

มนต์ชัย ชนินทรลีลา. คู่มือประมวลกฎหมายอาญา ภาค 2 ความผิด ภาค 3 ลหุโทษ พร้อมตัวอย่างย่อหลักกฎหมายจากคำพิพากษาศาลฎีกา,. พิมพ์ครั้งที่ 1. กรุงเทพฯ: พลสยาม, 2547.

มานิตย์ จุมปา. คำอธิบายกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์. พิมพ์ครั้งที่ 2. กรุงเทพฯ: วิญญูชน, 2554.

ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน (ศคง.). รายงานผลการดำเนินงานของศูนย์คุ้มครองผู้ใช้บริการทางการเงิน (ศคง.) ในการให้ข้อมูล/คำปรึกษา และรับเรื่องร้องเรียน ปี 2561. (3 มกราคม 2562).

สมยศ เชื้อไทย. คำอธิบายวิชากฎหมายแพ่ง : หลักทั่วไป. พิมพ์ครั้งที่ 25. กรุงเทพฯ: วิญญูชน, 2562.

สมศักดิ์ เอี่ยมพลับใหญ่. กฎหมายอาญา ภาคความผิดเกี่ยวกับความเท็จ การปลอมและการแปลง. พิมพ์ครั้งที่ 1. กรุงเทพฯ: นิติธรรม, 2554.

สราวุธ ปิติยาศักดิ์. คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ (ฉบับที่ 2) พ.ศ. 2560. พิมพ์ครั้งที่ 2. กรุงเทพฯ: นิติธรรม, 2561.

สำนักงานอัยการพิเศษฝ่ายสารสนเทศ. อัยการนิเทศ, 6 (2544).

สุเนติ คงเทพ. กฎหมายเกี่ยวกับคอมพิวเตอร์. พิมพ์ครั้งที่ 2. กรุงเทพฯ: มังกุ๊ดดิจิตอลเพรส, 2561.

————. คำอธิบายกฎหมายเกี่ยวกับคอมพิวเตอร์. พิมพ์ครั้งที่ 1. กรุงเทพฯ: กรุงสยาม พับลิชชิ่ง, 2559.

สุพิศ ปราณีตพลกรัง. กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์. พิมพ์ครั้งที่ 1. กรุงเทพฯ: นิติธรรม, 2560.

————. การคุ้มครองข้อมูลส่วนบุคคล. พิมพ์ครั้งที่ 1. กรุงเทพ: นิติธรรม, 2563.

สุรศักดิ์ ลิขสิทธิ์วัฒนสกุล. คำอธิบายความผิดเกี่ยวกับการปลอมและการแปลงตามประมวลกฎหมายอาญา. พิมพ์ครั้งที่ 1. กรุงเทพฯ: สำนักพิมพ์วิญญูชน, 2555.

แสวง บุญเฉลิมวิภาส. หลักกฎหมายอาญา. พิมพ์ครั้งที่ 1. กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2539.

หยุด แสงอุทัย. กฎหมายอาญา ภาค 2-3. พิมพ์ครั้งที่ 7. กรุงเทพฯ: สำนักพิมพ์วิทยาลัยธรรมศาสตร์, 2538.

รายงานการวิจัยและวิทยานิพนธ์

จนิษฐ คันธสมบูรณ์. การทุจริตโดยใช้บัตรเครดิต,. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 2538.

จรัสศรี จริยากูล. มาตรการทางกฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมบัตรเครดิต. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 2533.

ชาตรี ส่งสัมพันธ์. อาชญากรรมคอมพิวเตอร์ : ศึกษาวิเคราะห์การเข้าโดยมิชอบ. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สำนักวิชานิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. 2552.

ฐาปณีย์ รติจารุภัทร. การกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 2555.

ธวัชชัย สมบุญเจริญ. ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สำนักวิชานิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. 2549.

พรทิพย์ ตัณฑวนันท์. อาชญากรรมเกี่ยวกับข้อมูลอิเล็กทรอนิกส์. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สำนักวิชานิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. 2548.

พรรณสุวัชร รติพงค์สิทธิ์. อาชญากรรมทางคอมพิวเตอร์ : ศึกษาวิเคราะห์หลักเกณฑ์ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ... . วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สำนักวิชานิติศาสตร์ มหาวิทยาลัยรามคำแหง. 2550.

พิญดา เลิศกิตติกุล. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต , สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 2550.

พีรพันธุ์ เปรมภูติ. มาตรการทางกฎหมายในการป้องกันปราบปรามการปลอมบัตรเครดิต. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 2539.

เลิศชาย สุธรรมพร. อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีความปลอดภัยของข้อมูล. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 2541.

ศิริภัทร ธรรมเขต. ความผิดฐานลักทรัพย์ : ศึกษากรณีการลักทรัพย์ไม่มีรูปร่าง. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สำนักวิชานิติศาสตร์ มหาวิทยาลัยรามคำแหง. 2550.

สมศักดิ์ เธียรจรูญกุล. รายงานการวิจัย เรื่อง ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา. รายงานการวิจัย, สาขานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช. 2558.

อัญธิกา ณ พิบูลย์. ปัญหาและอุปสรรคในการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สำนักวิชานิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 2551.

เว็บไซต์ภาษาไทย

77ข่าวเด็ด. รวบแก๊งสกิมเมอร์ชาวจีนปลอมบัตรATM ตระเวนกดเงินสดทั่วชลบุรี [ออนไลน์]. แหล่งที่มา: https://www.77kaoded.com/news/sangk/1036335 [6 สิงหาคม 2563]

ACinfotec. สรุปใจความสำคัญของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ผู้ประกอบการควรรู้ [ออนไลน์]. แหล่งที่มา: https://www.acinfotec.com/2019/07/23/data-protection-law-2562/ [1 พฤศจิกายน 2563]

Deenamtang. การป้องกัน การ Skimming ขโมยข้อมูล บัตร ATM หรือ บัตร Credit [ออนไลน์]. แหล่งที่มา: https://www.deenamtang.com/14928366/การป้องกัน-การ-skimming-ขโมยข้อมูล-บัตร-atm-หรือ-บัตร-credit [25 กรกฎาคม 2563]

It24hrs.com. อุปกรณ์ที่ทำให้ Smartphone แปลงร่างเป็นเครื่องอ่านบัตรเครดิต เริ่มให้บริการในไทยแล้ว [ออนไลน์]. แหล่งที่มา: https://www.it24hrs.com/2013/iphone-credit-card-reader-come-to-thailand/ [20 พฤศจิกายน 2560]

MGRonline. ระวัง! แก๊งสกิมเมอร์ชาวจีนระบาดอีกแล้ว ตร.ภูเก็ตรวบได้ 2 คน ตระเวนกดเงินตู้เอทีเอ็ม [ออนไลน์]. แหล่งที่มา: https://mgronline.com/south/detail/9600000065820 [6 สิงหาคม 2563]

———. รวบคู่หูแดนมังกรตั้งแก๊งสกิมเมอร์ดูดข้อมูลบัตรเอทีเอ็ม ตระเวนกดเงินสดใน จ.ชลบุรี [ออนไลน์]. แหล่งที่มา: https://mgronline.com/local/detail/9620000111983 [6 สิงหาคม 2563]

Moneyhub. มาอีกแล้ว! แก๊งสกิมเมอร์ปลอมบัตรเครดิตข้ามชาติ [ออนไลน์]. แหล่งที่มา: https://moneyhub.in.th/article/skimmer-atm/ [6 สิงหาคม 2563]

R&D smart shop. เครื่องอ่านบัตรแม่เหล็ก [ออนไลน์]. แหล่งที่มา: http://rd-comp.com/index.aspx?pid=dba21964-3b89-486b-969f-9cc86808d1ee&igid=13c1a775-8bde-494c-a208-0b826a843337 [20 พฤศจิกายน 2560]

Thai netizen network. พยานหลักฐานอิเล็กทรอนิกส์ แยกไม่ออกจาก “เศรษฐกิจดิจิทัล” [ออนไลน์]. แหล่งที่มา: https://thainetizen.org/2016/01/digital-forensics-seminar-etda/ [1 พฤศจิกายน 2563]

กรุงเทพธุรกิจ. จับคาหนังคาเขาแก๊งสกิมเมอร์จีน ขณะติดอุปกรณ์คาตู้เอทีเอ็ม [ออนไลน์]. แหล่งที่มา: https://www.bangkokbiznews.com/news/detail/759274 [6 สิงหาคม 2563]

กรุงเทพธุรกิจออนไลน์. 'ข้อมูลส่วนบุคคล' สำคัญแค่ไหน ตามกฎหมาย GDPR ยุโรป [ออนไลน์]. แหล่งที่มา: https://www.bangkokbiznews.com/news/detail/882376

ข่าวเด็ดเจ็ดสี. ตร.รวบสามีภรรยา คดีบัตรเครดิต ยักยอกทรัพย์ [ออนไลน์]. แหล่งที่มา: https://news.ch7.com/detail/366214 [2 สิงหาคม 2563]

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. การคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) [ออนไลน์]. แหล่งที่มา: https://www.etcommission.go.th/files/article/article-dp.pdf [1 พฤศจิกายน 2563]

คณะนิติศาสตร์ มหาลัยสงขลานครินทร์. การโจรกรรมเอกลักษณ์บุคคล (Identity Theft) [ออนไลน์]. แหล่งที่มา: https://www.bangkokbiznews.com/blog/detail/646271 [15 ตุลาคม 2563]

เชียงใหม่นิวส์. ตำรวจสืบภาค 5 โชว์รวบแก๊งสกิมเมอร์ [ออนไลน์]. แหล่งที่มา: https://www.chiangmainews.co.th/page/archives/668270/ [1 พฤศจิกายน 2563]

ไทยรัฐ. จับมาเลย์แสบ! ทำบัตรเครดิตปลอม รูดข้ามโลก [ออนไลน์]. แหล่งที่มา: https://www.thairath.co.th/news/local/516310 [6 สิงหาคม 2563]

ธนาคารกรุงไทย. เตือนเว็บไซต์ปลอม หลอกโจรกรรมข้อมูลส่วนตัว [ออนไลน์]. แหล่งที่มา: https://krungthai.com/th/content/financial-partner/security-tips-for-digital-life/web-phishing [25 กรกฎาคม 2563]

ธนาคารไทยพาณิชย์. กดเงินไม่ใช้บัตร [ออนไลน์]. แหล่งที่มา: https://www.scb.co.th/th/personal-banking/digital-banking/scb-easy/how-to/cardless.html [2 กุมภาพันธ์ 2563]

———. กลโกงแก๊งคอลเซ็นเตอร์ รู้ทันไม่เสียที [ออนไลน์]. แหล่งที่มา: https://www.scb.co.th/th/personal-banking/stories/gang-callcenter.html [25 กรกฎาคม 2563]

ธนาคารแห่งประเทศไทย. ข่าวธนาคารแห่งประเทศไทย ฉบับที่49/2562 [ออนไลน์]. แหล่งที่มา: https://www.bot.or.th/Thai/PressandSpeeches/Press/News2562/n4962t.pdf [22 กรกฎาคม 2563]

———. สังคมไทย (กำลัง) ไร้เงินสด ? [ออนไลน์]. แหล่งที่มา: https://www.bot.or.th/Thai/MonetaryPolicy/ArticleAndResearch/Pages/FAQ169.aspx [1 พฤศจิกายน 2563]

———. จำนวนบัตรพลาสติก [ออนไลน์]. แหล่งที่มา: https://www.bot.or.th/App/BTWS_STAT/statistics/ReportPage.aspx?reportID=685&language=th [22 กรกฎาคม 2563]

บรรณศักดิ์ ยุวมิตร. Phishing คืออะไร ป้องกันอย่างไร [ออนไลน์]. แหล่งที่มา: https://www.catcyfence.com/it-security/article/what-is-phishing/ [25 กรกฎาคม 2563]

โพสต์ทูเดย์. จับหนุ่มอินเดียใช้บัตรเครดิตปลอมรูดซื้อสินค้า [ออนไลน์]. แหล่งที่มา: https://www.posttoday.com/social/local/341878 [6 สิงหาคม 2563]

———. จับโจรฝรั่งเศสฉกข้อมูลบัตรเครดิตจับโจรฝรั่งเศสฉกข้อมูลบัตรเครดิต [ออนไลน์]. แหล่งที่มา: https://www.posttoday.com/social/general/279509 [25 กรกฎาคม 2563]

———. จับพนักงานห้างรูดบัตรเครดิตสาวมะกันเกลี้ยง [ออนไลน์]. แหล่งที่มา: https://www.posttoday.com/social/general/47753 [2 สิงหาคม 2563]

———. ไม่รอด!ผู้ต้องหาแก๊งสกิมเมอร์จนมุมตำรวจหลังหนีคดีนาน 10 ปี [ออนไลน์]. แหล่งที่มา: https://www.posttoday.com/social/general/589470 [1 พฤศจิกายน 2563]

มติชนออนไลน์. รวบ 5 จีนแผ่นดินใหญ่ แก๊งสกิมเมอร์คัดลอกข้อมูลตู้เอทีเอ็มไทย แฉแฮกวันเดียว 200 ใบรวบ 5 จีนแผ่นดินใหญ่ แก๊งสกิมเมอร์คัดลอกข้อมูลตู้เอทีเอ็มไทย แฉแฮกวันเดียว 200 ใบ [ออนไลน์]. แหล่งที่มา: https://www.matichon.co.th/local/crime/news_580604 [1 พฤศจิกายน 2563]

รติกร เจือกโว้น. กฎหมาย [ออนไลน์]. แหล่งที่มา: http://wiki.kpi.ac.th/index.php?title=กฎหมาย [2 พฤศจิกายน 2563]

ลาภลอย วานิชอังกูร. สกิมเมอร์ : เทคโนโลยีโฉดเพื่อทรชน [ออนไลน์]. แหล่งที่มา: https://www.kroobannok.com/33613 [7 สิงหาคม 2563]

ศูนย์คุ้มครองผู้ใช้บริการทางการเงิน ธนาคารแห่งประเทศไทย. กลโกงบัตรต่างๆ [ออนไลน์]. แหล่งที่มา: https://www.1213.or.th/th/finfrauds/CardFraud/Pages/CardFraud.aspx [20 กุมภาพันธ์ 2561]

ศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ. สถิติฐานความผิดคดีอาญา [ออนไลน์]. แหล่งที่มา: http://pitc.police.go.th/dirlist/dirlist.php?dir=/crimes [2 สิงหาคม 2563]

สำนักงานราชบัณฑิตยสภา. พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554 [ออนไลน์]. แหล่งที่มา: http://www.royin.go.th/dictionary/index.php [19 กรกฎาคม 2563]

สำนักงานเลขาธิการสภาผู้แทนราษฎร. รายงานของคณะกรรมาธิการขับเคลื่อนการปฏิรูปประเทศด้านกฎหมายและกระบวนการยุติธรรม สภาขับเคลื่อนประเทศ เรื่อง การใช้อุปกรณ์อิเล็กทรอนิกส์ติดตามตัวในกระบวนการยุติธรรมทางอาญา [ออนไลน์]. แหล่งที่มา:

https://library2.parliament.go.th/giventake/content_nrsa2558/d111559-01.pdf [29 กรกฎาคม 2563]

————. มาตรา 77 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย [ออนไลน์]. แหล่งที่มา: https://www.parliament.go.th/section77/survey_about.php [8 พฤศจิกายน 2563]

สำนักประธานศาลฎีกา สำนักวิชาการ สำนักงานศาลยุติธรรม. ข้อสังเกตพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547 [ออนไลน์]. แหล่งที่มา: www.library.coj.go.th/Info/44300?c=20348014 [21 พฤศจิกายน 2560]

หนังสือและวารสารภาษาอังกฤษ

Vasiu, J., and Vasiu, L. Riders on the Storm: An Analysis of Credit Card Fraud Cases. Suffolk Journal of Trial & Appellate Advocacy 20 (2015).

Warren, S. D., and Brandeis, L. D. The Right to Privacy. Harvard Law Review 4, 5 (1890).

เว็บไซต์ภาษาอังกฤษ

Aliexpress. Card Skimmer [Online]. Available from: https://www.aliexpress.com/w/wholesale-card-skimmer.html [25 July 2020]

Australian competition and consumer commission. Online Shopping Scams [Online]. Available from: https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/online-shopping-scams [25 July 2020]

Australian Payments Network Limited. Australian Payment Card Fraud 2018 [Online]. Available from: https://www.auspaynet.com.au/sites/default/files/2018-08/AustralianPaymentCardFraud-2018-eport.pdf [25 July 2020]

Bangkokpost. Cops Nab 10 for Call Centre Fraud Scam [Online]. Available from: https://www.bangkokpost.com/thailand/general/1832039/cops-nab-10-for-call-centre-fraud-scam [25 July 2020]

Boulton, A. M. Synopsis of the Cybercrime Act 2001 [Online]. Available from: https://www.giac.org/paper/gsec/4017/synopsis-cybercrime-act-2001/106427 [12 October 2020]

Bradbury, D. Has Chip-and-Pin Failed to Foil Fraudsters? [Online]. Available from: https://www.theguardian.com/technology/2008/jan/03/hitechcrime.news [3 February 2020]

Bukh, A. Credit Card Fraud [Online]. Available from: https://nyccriminallawyer.com/fraud-charge/credit-card-fraud-charge/ [24 October 2020]

———. Skimming [Online]. Available from: https://nyccriminallawyer.com/fraud-charge/credit-card-fraud-charge/skimming/ [22 October 2020]

Cruz, A. D. Was Access Devices Regulation Act Reboot Really Necessary? [Online]. Available from: https://www.manilatimes.net/2019/10/02/opinion/columnists/topanalysis/was-access-devices-regulation-act-reboot-really-necessary/624758/ [10 October 2020]

Daly, L. Identity Theft and Credit Card Fraud Statistics for 2020 [Online]. Available from: https://www.fool.com/the-ascent/research/identity-theft-credit-card-fraud-statistics/ [8 November 2020]

Doyle, C. Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws [Online]. Available from: https://fas.org/sgp/crs/misc/RS20830.pdf [20 October 2020]

———. Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws [Online]. Available from: https://www.everycrsreport.com/files/20141015_97-1025_31056cd16cc55cc39047e24e327a15875045157f.pdf [20 October 2020]

Eisner Gorin LLP. Credit Card Fraud [Online]. Available from: https://www.thefederalcriminalattorneys.com/fraud-crimes/federal-credit-card-fraud/ [22 October 2020]

European Central Bank. Fourth Report on Card Fraud [Online]. Available from: https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf [20 February 2018]

Experian.com. Credit Card Fraud: What to Do If You're a Victim [Online]. Available from: https://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/credit-card-fraud-what-to-do-if-you-are-a-victim/ [17 October 2020]

FindLaw. Identity Theft [Online]. Available from: https://criminal.findlaw.com/criminal-charges/identity-theft.html [22 October 2020]

———. United States V. Barsumyan [Online]. Available from: https://caselaw.findlaw.com/us-9th-circuit/1410201.html#footnote_ref_3 [20 October 2020]

Geuss, M. An Atm Hack and a Pin-Pad Hack Show Chip Cards Aren't Impervious to Fraud [Online]. Available from: https://arstechnica.com/information-technology/2016/08/an-atm-hack-and-a-pin-pad-hack-show-chip-cards-arent-impervious-to-fraud/ [3 February 2020]

———. Why Aren't Chip Credit Cards Stopping "Card Present" Fraud in the Us? [Online]. Available from: https://arstechnica.com/information-technology/2018/11/why-arent-chip-credit-cards-stopping-card-present-fraud-in-the-us/ [25 July 2020]

Hansard. Computer Misuse Bill [Online]. Available from: https://api.parliament.uk/historic-hansard/commons/1990/feb/09/computer-misuse-bill [16 October 2020]

Hopkins, R. The Data Protection Bill: A Brief Overview What Does the Data Protection Bill Do? [Online]. Available from: https://uk.practicallaw.thomsonreuters.com/w-010-5346?transitionType=Default&contextData=(sc.Default)&firstPage=true [17 October 2020]

HOUSE OF REPRESENTATIVES. Do the Payment Card Industry Data Standards Reduce Cybercrime? [Online]. Available from: https://www.govinfo.gov/content/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm [8 November 2020]

———. Identity Theft Penalty Enhancement Act [Online]. Available from: https://www.govinfo.gov/content/pkg/CRPT-108hrpt528/html/CRPT-108hrpt528.html [20 October 2020]

Hua Hin Today. Call Center Scam [Online]. Available from: https://www.huahintoday.com/sports/call-center-scam/ [25 July 2020]

Information Commisoner's Office. What Are 'Controllers' and 'Processors'? [Online]. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/ [17 October 2020]

Insurance information instatute. Facts + Statistics: Identity Theft and Cybercrime [Online]. Available from: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1)/ [8 November 2020]

Kagan, J. Skimming [Online]. Available from: https://www.investopedia.com/terms/s/skimming.asp [15 October 2020]

Kleut, J. v. d. Identity Theft: What Is It and How to Avoid It [Online]. Available from: https://us.norton.com/internetsecurity-id-theft-what-is-identity-theft.html [10 October 2020]

Knieff, B. 2016 Global Consumer Card Fraud: Where Card Fraud Is Coming From [Online]. Available from: https://www.paymentscardsandmobile.com/wp-content/uploads/2016/07/2016-Global-Consumer-Card-Fraud-Where-Card-Fraud-Is-Coming-From.pdf [25 October 2020]

Krebs, B. Gas Theft Gangs Fuel Pump Skimming Scams [Online]. Available from: https://krebsonsecurity.com/tag/gas-pump-skimmers/ [25 July 2020]

———. Simple but Effective Point-of-Sale Skimmer [Online]. Available from: https://krebsonsecurity.com/tag/pos-skimmer/ [25 July 2020]

Krebsonsecurity. Gas Theft Gangs Fuel Pump Skimming Scams [Online]. Available from: https://krebsonsecurity.com/tag/gas-pump-skimmers/ [2 February 2020]

———. Romanian Skimmer Gang in Mexico Outed by Krebsonsecurity Stole $1.2 Billion [Online]. Available from: https://krebsonsecurity.com/category/all-about-skimmers/ [8 November 2020]

Legislation.gov.uk. Criminal Justice Act 1982 [Online]. Available from: https://www.legislation.gov.uk/ukpga/1982/48/section/37 [15 October 2020]

———. Data Protection Act 2018 [Online]. Available from: https://www.legislation.gov.uk/ukpga/1982/48/section/37 [8 November 2020]

———. Data Protection Act 2018 Legal Background [Online]. Available from: https://www.legislation.gov.uk/ukpga/2018/12/notes/division/4/index.htm [17 October 2020]

———. Data Protection Act 2018 Overview of the Act [Online]. Available from: https://www.legislation.gov.uk/ukpga/2018/12/notes/division/2/index.htm [17 October 2020]

———. Fraud Act 2006 Background [Online]. Available from: https://www.legislation.gov.uk/ukpga/2006/35/notes/division/3 [15 October 2020]

———. Fraud Act 2006 Explanatory Notes [Online]. Available from: https://www.legislation.gov.uk/ukpga/2006/35/notes/division/5/8 [15 October 2020]

———. Fraud Act 2006 Explanatory Notes [Online]. Available from: https://www.legislation.gov.uk/ukpga/2006/35/notes/division/5/2 [15 October 2020]

———. Fraud Act 2006 Explanatory Notes [Online]. Available from: https://www.legislation.gov.uk/ukpga/2006/35/notes/division/5/6 [15 October 2020]

———. Serious Crime Act 2015 Explanatory Notes [Online]. Available from: from: https://www.legislation.gov.uk/ukpga/2015/9/notes/division/3/2/2/2 [16 October 2020]

Limsamarnphun, N. Sharp Rise in Credit-Card Fraud Tipped [Online]. Available from: https://www.nationthailand.com/business/30264690 [8 November 2020]

Los Angeles and Southern California News. How to Spot a Gas Pump Skimmer [Online]. Available from: https://abc7chicago.com/gas-skimmer-pump-credit-card-quick-tip/5413649/ [25 July 2020]

Lozusic, R. Fraud and Identity Theft [Online]. Available from: https://www.parliament.nsw.gov.au/researchpapers/Documents/fraud-and-identity-theft/08-03.pdf [8 November 2020]

Office of the Attorney General. S.I. No. 537/2019 - Data Protection Act 2018 (Section 60(6)) (Central Bank of Ireland) Regulations 2019 [Online]. Available from: http://www.irishstatutebook.ie/eli/2019/si/537/made/en/print [17 October 2020]

Official Journal of the European Union. Directive 2013/40/Eu of the European Parliament and of the Council [Online]. Available from: https://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF [16 October 2020]

Oxford Learner's Dictionaries. Obtain [Online]. Available from: https://www.oxfordlearnersdictionaries.com/definition/english/obtain?q=obtain [7 October 2020]

Parliament of Australia. Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill 2004 [Online]. Available from: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd0405/05bd013 [13 October 2020]

———. Cybercrime Bill 2001 [Online]. Available from: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd0102/02bd048 [12 October 2020]

Pwchk.com. Atm Fraud: Do You Know If Your Customer's Card Data Has Been Compromised? [Online]. Available from: https://www.pwchk.com/en/risk-assurance/ra-atm-fraud-aug2016.pdf [25 November 2017]

Rouse, M. Storage Medium (Storage Media) [Online]. Available from: https://searchstorage.techtarget.com/definition/storage-medium [16 October 2020]

Sancho, D. Atm Malware on the Rise [Online]. Available from: https://blog.trendmicro.com/trendlabs-security-intelligence/atm-malware-on-the-rise/?_ga=2.110755589.1613302766.1580972794-179933209.1580972794 [2 February 2020]

Segura, J. Web Skimmer Phishes Credit Card Data Via Rogue Payment Service Platform [Online]. Available from: https://blog.malwarebytes.com/web-threats/2019/11/web-skimmer-phishes-credit-card-data-via-rogue-payment-service-platform/ [2 February 2020]

Seidle, N. Gas Pump Skimmers [Online]. Available from: https://learn.sparkfun.com/tutorials/gas-pump-skimmers/all [8 November 2020]

Siciliano, R. Point of Sale Skimming Attacks and Pci Standards [Online]. Available from: https://www.thebalance.com/what-are-point-of-sale-skimming-attacks-and-pci-1947471 [25 July 2020]

Steele, J. Payment Method Statistics [Online]. Available from: https://www.creditcards.com/credit-card-news/payment-method-statistics-1276/ [1 November 2020]

The Australian Law Reform Commission. Criminalising Identity Theft [Online]. Available from: https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/12-identity-theft/criminalising-identity-theft/ [29 October 2020]

The Crown Prosecution Service. Computer Misuse Act [Online]. Available from: https://www.cps.gov.uk/legal-guidance/computer-misuse-act [16 October 2020]

———. The Fraud Act 2006 [Online]. Available from: https://www.cps.gov.uk/legal-guidance/fraud-act-2006 [15 October 2020]

The Nilson Report. Top 50 Card Issuers in Asia-Pacific [Online]. Available from: https://nilsonreport.com/upload/content_promo/The_Nilson_Report_Issue_1164.pdf [1 November 2020]

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA. Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004 Explanatory Memoranda [Online]. Available from: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr2131_ems_c79a0bd1-87a4-42e4-be65-485ba6850273%22 [12 October 2020]

The World Bank. Percent People with Credit Cards - Country Rankings [Online]. Available from: https://www.theglobaleconomy.com/rankings/people_with_credit_cards/ [1 November 2020]

———. Percent People with Debit Cards - Country Rankings [Online]. Available from: https://www.theglobaleconomy.com/rankings/people_with_debit_cards/ [1 November 2020]

Trulioo.com. 100,000 Years of Identity Verification: An Infographic History [Online]. Available from: https://www.trulioo.com/blog/infographic-the-history-of-id-verification [25 October 2020]

Tubeza, P. C. P507m Lost to Credit Card Fraud in 2016 [Online]. Available from: https://newsinfo.inquirer.net/882963/p507m-lost-to-credit-card-fraud-in-2016 [25 October 2020]

Wall, D. S. Future Identities: Changing Identities in the Uk – the Next 10 Years [Online]. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/275784/13-521-identity-related-crime-uk.pdf [25 October 2020]

Wikia.org. Cybercrime Act 2001 [Online]. Available from: https://itlaw.wikia.org/wiki/Cybercrime_Act_2001 [12 October 2020]

Wikipedia. Fraud Act 2006 [Online]. Available from: https://en.wikipedia.org/wiki/Fraud_Act_2006 [15 October 2020]

Yapp, P. The 30-Year-Old Computer Misuse Act Is Not Fit for Purpose [Online]. Available from: https://www.scl.org/articles/10854-the-30-year-old-computer-misuse-act-is-not-fit-for-purpose [17 October 2020]

ประวัติผู้เขียน

ชื่อ-สกุล	นายโปลิต สุขสว่าง
วัน เดือน ปี เกิด	13 ตุลาคม 2535
สถานที่เกิด	จังหวัดนราธิวาส
วุฒิการศึกษา	- ระดับประถมศึกษา โรงเรียนอนุบาลสงขลา - ระดับมัธยมศึกษาตอนต้น โรงเรียนมหาวชิราวุธ จังหวัดสงขลา - ระดับมัธยมศึกษาตอนปลาย โรงเรียน มอ.วิทยานุสรณ์ จังหวัดสงขลา - ระดับปริญญาตรี นิติศาสตรบัณฑิต เกียรตินิยมอันดับสอง จุฬาลงกรณ์มหาวิทยาลัย ปีการศึกษา 2557 - หลักสูตรวิชาว่าความของสำนักฝึกอบรมวิชาว่าความ สภาทนายความในพระบรมราชูปถัมภ์ รุ่นที่ 45 - เนติบัณฑิตไทย สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภาในพระบรมราชูปถัมภ์ สมัยที่ 70