การกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

นางสาวฐาปณีย์ รติจารุภัทร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2555

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

บทคัดย่อและแฟ้มข้อมูลฉบับเต็มของวิทยานิพนธ์ตั้งแต่ปีการศึกษา 2554 ที่ให้บริการในคลังปัญญาจุฬาฯ (CUIR)
เป็นแฟ้มข้อมูลของนิสิตเจ้าของวิทยานิพนธ์ที่ส่งผ่านทางบัณฑิตวิทยาลัย
The abstract and full text of theses from the academic year 2011 in Chulalongkorn University Intellectual Repository(CUIR)
are the thesis authors' files submitted through the Graduate School.

CRIMINALIZATION OF IDENTITY THEFT

Miss Tapanee Ratijaruphat

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Laws Program in Laws

Faculty of Law

Chulalongkorn University

Academic Year 2012

Copyright of Chulalongkorn University

หัวข้อวิทยานิพนธ์	การกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล
โดย	นางสาวฐาปณีย์ รติจารุภัทร
สาขาวิชา	นิติศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ มัทยา จิตติรัตน์

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะนิติศาสตร์
(ศาสตราจารย์ ดร.ศักดา ธนิตกุล)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(ศาสตราจารย์ วีระพงษ์ บุญโญภาส)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ มัทยา จิตติรัตน์)

.....กรรมการภายนอกมหาวิทยาลัย
(ศาสตราจารย์ (พิเศษ) ดร.จิรนิติ หะวานนท์)

.....กรรมการภายนอกมหาวิทยาลัย
(พันตำรวจเอก ญาณพล ยั่งยืน)

ฐาปณีย์ รติจารุภัทร : การกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล. (CRIMINALIZATION OF IDENTITY THEFT) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: รศ.มัทยา จิตติรัตน์, 166 หน้า.

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล คือ การใช้ข้อมูลส่วนบุคคลของบุคคลอื่นแสวงหาประโยชน์ในทางที่มิชอบเพื่อตนเอง หรือผู้อื่น โดยปัจจุบันเกิดการกระทำความผิดในลักษณะนี้เป็นจำนวนมากในหลายประเทศทั่วโลก เนื่องจากความเจริญก้าวหน้าทางเทคโนโลยีทำให้การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลกระทำได้ง่ายมากขึ้น ซึ่งการกระทำความผิดในลักษณะนี้อาจนำไปสู่การกระทำความผิดที่ร้ายแรงอย่างอื่น เช่น การก่อการร้าย การค้ายาเสพติดข้ามชาติ เป็นต้น

ประเทศไทยยังไม่มีบทกฎหมายเฉพาะที่จะนำมาบังคับใช้กับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล เมื่อเกิดการกระทำความผิดขึ้นจึงต้องนำบทบัญญัติในประมวลกฎหมายอาญาและพระราชบัญญัติที่เกี่ยวข้องอื่นๆ มาบังคับใช้ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ฯลฯ จากการศึกษาพบว่าบทกฎหมายที่นำมาปรับใช้ยังมีความไม่ครอบคลุม เช่น ถ้าเป็นเพียงการลักข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเพื่อไปกระทำความผิด ยังไม่มีกฎหมายบัญญัติให้การกระทำดังกล่าวเป็นความผิด รวมถึงการครอบครอง การจำหน่ายจ่ายโอนข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ดังนี้เมื่อศึกษาเปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกา และประเทศแคนาดา แล้วพบว่ามีบทบัญญัติกฎหมายที่มีความครอบคลุมการกระทำความผิดมากกว่ากฎหมายไทย เนื่องด้วยมีการบัญญัติฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะ ทำให้สามารถบังคับใช้กฎหมายแก่การกระทำความผิดได้ ผู้เขียนจึงขอเสนอให้มีการกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นความผิดทางอาญาในกฎหมายไทย โดยกำหนดในรูปแบบของกฎหมายเฉพาะ ซึ่งสามารถปรับใช้ได้เป็นการทั่วไป และมีความครอบคลุมได้ทุกกรณีของการกระทำความผิด ทั้งนี้โดยนำกฎหมายของประเทศสหรัฐอเมริกา ประเทศแคนาดา และประเทศสหราชอาณาจักรมาเป็นแนวทางในการกำหนดกฎหมายเพื่อให้มีความเหมาะสมกับรูปแบบของความผิดที่เกิดขึ้น

สาขาวิชา นิติศาสตร์ ลายมือชื่อนิสิต .....

ปีการศึกษา 2555 ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก .....

5485973434 : MAJOR LAWS
KEYWORDS : CRIMINALIZATION / IDENTITY THEFT / INDIVIDUAL INFORMATION

TAPANEE RATIJARUPHAT : CRIMINALIZATION OF IDENTITY THEFT.
ADVISOR : ASSOC. PROF. MATTAYA JITTIRAT, 166 pp.

Identity Theft is the stealing of another individual's information to commit fraud. Currently, advanced technologies simplify identity theft activities and lead to an increasing number of identity theft around the world. These offences may lead to other serious crimes such as terrorism and transnational drug trafficking etc.

Meanwhile, the United States and Canada have specific laws covering directly to all varieties of case relating to identity theft. Thailand has no law to deal with identity theft particularly. *The Criminal Code*, the *Computer Crime Act B.E. 2550* and *The Identity Card Act B.E. 2526* are commonly used against identity theft. However, the study finds that the present laws are insufficient to deal with identity theft crime. The author's proposal is to enact the specific law to criminalize identity theft in private sector offence. The new identity theft law should be able to deal with basic activities of identity theft as well as advanced identity theft activities. The earlier enacted law in United States, Canada and the United Kingdom can be the guidance in enacting the most suitable law against identity theft in Thailand.

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

Academic Year : 2012 Advisor's Signature .....

กิตติกรรมประกาศ

ในการจัดทำวิทยานิพนธ์ฉบับนี้ ผู้เขียนขอกราบขอบพระคุณ ท่าน รองศาสตราจารย์ มัทยา จิตติรัตน์ เป็นอย่างสูงที่ท่านได้ให้ความเมตตากรุณารับเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ โดยท่านได้คอยให้ความช่วยเหลือ ให้คำแนะนำ และกรุณาตรวจทาน แก้ไขวิทยานิพนธ์ฉบับนี้ จนทำให้ผู้เขียนสามารถจัดทำวิทยานิพนธ์ฉบับนี้ได้สำเร็จลุล่วงดั่งความมุ่งหมาย

ผู้เขียนขอกราบขอบพระคุณเป็นอย่างสูงต่อท่าน ศาสตราจารย์วีระพงษ์ บุญโญภาส ที่กรุณารับเป็นประธานกรรมการวิทยานิพนธ์ ท่านศาสตราจารย์ (พิเศษ) ดร.จิรนิติ หะวานนท์ และท่านพ.ต.อ.ญาณพล ยั่งยืน ที่กรุณารับเป็นกรรมการวิทยานิพนธ์ ทุกท่านต่างช่วยให้คำปรึกษา ชี้แนะแนวทางทำให้วิทยานิพนธ์ฉบับนี้มีความสมบรูณ์ และได้สละเวลาอันมีค่ามาเพื่อดำเนินการสอบวิทยานิพนธ์ให้แก่ผู้เขียน

ผู้เขียนขอกราบขอบพระคุณครอบครัวที่น่ารักของผู้เขียน ครอบครัวซึ่งเป็นกำลังใจสำคัญที่ทำให้ผู้เขียนมีความอดทน ตั้งใจ และพยายามจนจัดทำวิทยานิพนธ์ฉบับนี้ได้สำเร็จลุล่วงอย่างสมบรูณ์ ขอขอบคุณทุกความห่วงใย และความช่วยเหลือที่บรรดาพี่ๆ มอบให้กับผู้เขียนเสมอมา ผู้เขียนขอมอบความสำเร็จนี้ให้กับครอบครัวอันเป็นที่รัก

นอกจากนี้ผู้เขียนขอขอบคุณพี่ๆ เพื่อนๆ น้องๆ ทั้งหลายโดยเฉพาะเพื่อนๆ สายอาญา ฟ'54 ทุกคนที่คอยให้กำลังใจ ให้คำแนะนำและความช่วยเหลือกันเสมอมา ทำให้ผู้เขียนสามารถจัดทำวิทยานิพนธ์ได้สำเร็จตามความมุ่งหมาย

สุดท้ายนี้ หากวิทยานิพนธ์ฉบับนี้พอจะเป็นประโยชน์และมีคุณค่าทางวิชาการอยู่บ้าง ผู้เขียนขอกราบเป็นกตเวทิตาคุณแก่บิดามารดา คณาจารย์ และผู้มีพระคุณทุกท่าน แต่หากมีความบกพร่องไม่สมบรูณ์ประการใด ผู้เขียนขอน้อมรับไว้แต่เพียงผู้เดียว

สารบัญ

หน้า

บทคัดย่อภาษาไทย.....ง

บทคัดย่อภาษาอังกฤษ.....จ

กิตติกรรมประกาศ.....ฉ

สารบัญ.....ช

บทที่ 1 บทนำ.....1

1.1 ความเป็นมาและความสำคัญของปัญหา..... 1

1.2 วัตถุประสงค์ของการวิจัย..... 6

1.3 สมมติฐานของการวิจัย..... 6

1.4 วิธีดำเนินการวิจัย..... 7

1.5 ขอบเขตของการวิจัย.....7

1.6 ประโยชน์ที่คาดว่าจะได้รับ.....8

บทที่ 2 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล.....9

2.1 ความเป็นมาของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล.....10

2.2 ความหมายของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft).....14

หน้า

2.3 การนำข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไปใช้แสวงหาประโยชน์โดยทุจริต …….....20

2.3.1 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับการเงิน (Financial Identity Theft)…….. ……....20

2.3.1.1 การใช้ข้อมูลของเหยื่อเพื่อเปิดบัญชีใหม่ (new account fraud)…….……20

2.3.1.2 การใช้ข้อมูลของเหยื่อเพื่อสวมรอยในบัญชีที่เปิดไว้แล้ว (account takeover)…….....……21

2.3.2 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับการประกันภัย (Insurance Identity Theft)……..……....22

2.3.3 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับการแพทย์ (Medical Identity Theft)……..……....22

2.3.4 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับอาชญากรรม (Criminal Identity Theft)…….……23

2.3.5 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับใบอนุญาตขับขี่ (Driver's License Identity Theft)……..……....24

2.3.6 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับหมายเลขประกันสังคม (Social Security Identity Theft)……24

2.3.7 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของเด็ก (Child Identity Theft)……... ……24

2.3.8 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลแบบสังเคราะห์ หรือปลอม (Synthetic Identity Theft)…….……..25

2.4 ความเสียหายที่เกิดจากการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล……...25

2.4.1 ความเสียหายที่มีผลกระทบต่อด้านการเงิน (Financial Effects)……..…… ……....26

หน้า

2.4.2 ความเสียหายที่มีผลกระทบต่อการบันทึกประวัติอาชญากรรม (Criminal Effects)……26

2.4.3 ความเสียหายที่มีผลกระทบด้านความรู้สึก อารมณ์ หรือจิตใจ (Emotional Effects)……..……..…27

2.4.4 ความเสียหายที่ส่งผลกระทบในด้านอื่นๆ (Additional Effects)……..……...27

2.5 การคุ้มครองข้อมูลส่วนบุคคลกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล…....28

2.6 สาเหตุและปัญหาการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่เกิดขึ้นในประเทศไทย….....36

บทที่ 3 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลตามกฎหมายต่างประเทศและกฎหมายไทย……..……41

3.1 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลตามกฎหมายต่างประเทศ……...41

3.1.1 กฎหมายเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของประเทศสหรัฐอเมริกา…….....42

3.1.1.1 พระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998)……43

3.1.1.2 พระราชบัญญัติว่าด้วยการรายงานข้อมูลเครดิตอย่างยุติธรรม ค.ศ.1970 (The Fair Credit Reporting Act 1970)……50

หน้า

3.1.2 กฎหมายการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของประเทศแคนาดา……..……51

3.1.3 กฎหมายเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของประเทศสหราชอาณาจักร……...….57

3.1.3.1 พระราชบัญญัติการลักทรัพย์ ค.ศ. 1968 (The Theft Act of 1968)…… ……..57

3.1.3.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998 (The Data Protection Act of 1998)……..….59

3.1.3.3 พระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 (The Identity Card Act of 2006)…… …....…61

3.1.3.4 พระราชบัญญัติการฉ้อโกง ค.ศ. 2006 (The Fraud Act of 2006)…… ……65

3.2 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลตามกฎหมายไทย……....67

3.2.1 การกระทำความผิดตามประมวลกฎหมายอาญาที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล……..……....….67

3.2.1.1 ความผิดเกี่ยวกับการปกครองที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล……67

3.2.1.2 ความผิดเกี่ยวกับเอกสารที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล……69

หน้า

3.2.1.3 ความผิดเกี่ยวกับทรัพย์ที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล……..……78

3.2.2 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลกับฐานความผิดตามพระราชบัญญัติอื่นๆ……..……85

3.2.2.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550……..86

3.2.2.2 พระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ……..…91

3.2.2.3 ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.... 94

บทที่ 4 วิเคราะห์เปรียบเทียบกฎหมายของประเทศไทยและของต่างประเทศในเรื่องการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล……..……..98

4.1 บทวิเคราะห์เปรียบเทียบกฎหมายที่เกี่ยวข้องกับการกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล……..……..98

4.1.1 ประเภทของกฎหมายที่กำหนดฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล……..99

4.1.2 การกำหนดคำนิยามสำหรับความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล……..……100

4.1.3 การกำหนดฐานความผิด และองค์ประกอบของความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล.....……..102

หน้า

4.1.3.1 การได้มาซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล……103
4.1.3.2 การจัดทำขึ้นซึ่งเอกสารแสดงเอกลักษณ์บุคคลปลอม……..105
4.1.3.3 การมีไว้ในความครอบครองซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล……..106
4.1.3.4 การจำหน่าย หรือการโอนซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล…….....107
4.1.3.5 การทำขึ้น โอน และครอบครองเครื่องมือทำเอกสารแสดงตัวบุคคลหรือเอกสารแสดงตัวบุคคลปลอม……..108
4.1.3.6 การกำหนดถึงเหตุจูงใจที่กระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล……..109
4.1.4 ผู้เสียหายในความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล…..110
4.1.5 การกำหนดโทษ และการเยียวยาผู้เสียหายในความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล…….....113
4.2 ตารางสรุปการเปรียบเทียบกฎหมายที่เกี่ยวข้องกับการกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล……117
4.3 ความเหมาะสมในการนำแนวทางการบัญญัติกฎหมายของต่างประเทศในความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลมาบังคับใช้ในประเทศไทย…….....124
บทที่ 5 บทสรุปและข้อเสนอแนะ……128
5.1 บทสรุป……..128
5.2 ข้อเสนอแนะ……138

หน้า

รายการอ้างอิง.....143

ภาคผนวก.....148

ภาคผนวก ก.....149

ภาคผนวก ข.....155

ภาคผนวก ค.....158

ภาคผนวก ง.....162

ประวัติผู้เขียนวิทยานิพนธ์.....166

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล หมายถึง การที่บุคคลใดๆ ใช้ข้อมูลส่วนตัวของบุคคลอื่น เช่น ชื่อ นามสกุล หมายเลขบัตรประกันสังคม และหมายเลขประจำตัวประชาชน ฯลฯ โดยไม่ได้รับอนุญาตเพื่อแสวงหาประโยชน์อันมิชอบ อาทิ เพื่อไปกระทำความผิดฉ้อโกงหรือกระทำความผิดเกี่ยวกับอาชญากรรมอื่นๆ[1]

ปัจจุบันได้มีการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไปเพื่อแสวงหาประโยชน์โดยมิชอบ ซึ่งการโจรกรรมข้อมูลนี้เกิดขึ้นในหลายรูปแบบ ทั้งการโจรกรรมข้อมูลในรูปแบบทั่วไป โดยใช้วิธีการลักทรัพย์ หรือชิงทรัพย์ อาทิ ลักบัตรประจำตัวประชาชนของผู้เสียหาย หรืออาจเป็นกรณีที่ข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้ปรากฏอยู่ในที่สาธารณะอาจโดยเป็นความตั้งใจของผู้เป็นเจ้าของข้อมูลเองหรืออาจโดยความไม่ตั้งใจ เช่น ข้อมูลส่วนบุคคลต่างๆ ที่ผู้เป็นเจ้าของระบุไว้บนเว็ปไซต์หรือบนหน้าเพจของตนเองเพื่อเป็นการสื่อให้บุคคลอื่นๆ ได้ทราบว่าตนเป็นใครเพื่อประโยชน์ในการติดต่อ สื่อสาร หรือกรณีที่หน่วยเลือกตั้งมีการระบุรายละเอียดข้อมูลส่วนบุคคลของผู้มีสิทธิเลือกตั้ง หรือกรณีที่เป็นการได้มาซึ่งข้อมูลโดยการค้นข้อมูลจากเอกสารที่มีข้อมูลสำคัญต่างๆ ที่ผู้เสียหายทิ้งลงถังขยะในสถานที่สาธารณะทั่วไปหรือกระทั่งที่บ้านของผู้เสียหายเอง เหล่านี้ล้วนเป็นเรื่องที่ผู้เป็นเจ้าของข้อมูลมิได้มีเจตนาที่จะสละสิทธิในข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของตนให้ผู้อื่นสามารถนำไปแสวงหาประโยชน์ใดๆ โดยมิชอบแต่อย่างใด ผู้ที่นำข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นไปใช้โดยมิได้รับความยินยอมจึงสมควรมีความผิด เนื่องจากข้อมูลส่วนบุคคลย่อมได้รับการคุ้มครองตามหลักที่บัญญัติไว้ในรัฐธรรมนูญถึงสิทธิส่วนบุคคล (Right to

[1] Mohamed Chawki & Mohamed S. Abdel Wahab, “Identity Theft in Cyberspace: Issues and Solutions,” Lex Electronica Vol.11, 1 (Spring 2006): 2.

Privacy) กล่าวคือบุคคลอื่นไม่มีสิทธิที่จะนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้ไม่ว่าในทางใดๆ โดยที่มิได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูล ตลอดไปจนถึงวิธีการโจรกรรมแบบต้องอาศัยความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศเป็นพิเศษ กล่าวคือใช้โปรแกรมคอมพิวเตอร์มาเป็นเครื่องมือช่วยในการโจรกรรมข้อมูล โดยวิธีการนี้ในบางกรณีผู้เสียหายที่ถูกโจรกรรมข้อมูลไปไม่อาจจะรู้ถึงการโจรกรรมข้อมูลของตน ยังผลให้ผู้กระทำความผิดสามารถโจรกรรมข้อมูลได้อย่างสะดวก และง่ายดายโดยเหยื่อมิอาจรู้ตัวหรือกระทำการขัดขวางใดๆ ได้ อาจกล่าวได้ว่าโลกยุคเทคโนโลยีสารสนเทศอย่างในปัจจุบันนี้ ทำให้มีความสะดวก รวดเร็ว ในการติดต่อทำธุรกรรมต่างๆ มากขึ้น มีการจัดเก็บข้อมูลในรูปแบบอิเล็กทรอนิกส์ มีการติดต่อทำธุรกิจค้าขาย การซื้อขายและการชำระราคาสินค้า ผ่านทางเทคโนโลยีสารสนเทศมากขึ้น เช่น มีบัตรประจำตัวประชาชนแบบสมาร์ทการ์ด ซึ่งเก็บข้อมูลส่วนบุคคลต่างๆ ของบุคคลคนหนึ่งไว้อย่างละเอียด มีบัตรประจำตัวประชาชนเพียงใบเดียวก็สามารถที่จะรู้ข้อมูลสำคัญต่างๆของบุคคลคนนั้นได้อย่างง่ายดาย เช่น ประวัติด้านสุขภาพ การศึกษา อาชีพ ประวัติการย้ายที่อยู่ ฯลฯ มีหนังสือเดินทางอิเล็กทรอนิกส์ การโอนเงินออนไลน์ผ่านทางอินเตอร์เน็ต การใช้บัตรเครดิตชำระราคาสินค้าแทนการใช้เงินสดในการซื้อสินค้าตามสถานที่ห้างร้านต่างๆ ซึ่งสิ่งเหล่านี้หากนำมาใช้ในด้านดีล้วนทำให้การดำเนินชีวิตประจำวันของมนุษย์เป็นไปโดยรวดเร็ว สะดวก สบายมากขึ้น แต่หากเกิดมีการใช้ช่องโอกาสจากเทคโนโลยีเหล่านี้ไปในทางที่ผิด ในลักษณะของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไปเพื่อแสวงหาประโยชน์โดยมิชอบแล้วก็จะก่อให้เกิดปัญหาอย่างมากต่อระบบเศรษฐกิจ และกระทบต่อความเชื่อมั่นของประชาชนต่อองค์กรหรือสถาบันทางการเงินที่เข้ามามีความเชื่อมโยงกับการกระทำความผิด กล่าวคือหากมีบุคคลที่ไม่ประสงค์ดีได้ลักเอาข้อมูลต่างๆ เช่น บัตรประจำตัวประชาชน หมายเลขประจำตัวประชาชน หมายเลขบัตรประกันสังคม หมายเลขบัตรเครดิต ฯลฯ ของบุคคลคนหนึ่งไป เพื่อใช้ในการแสวงหาประโยชน์ส่วนตัวในทางที่ผิด โดยการแอบอ้าง หรือปลอมตัวสวมรอยเป็นบุคคลนั้นๆ แล้วกระทำการใดๆ อันเป็นผลเสียหายต่อบุคคลที่เป็นเจ้าของข้อมูลที่แท้จริงนั้น ตัวอย่างเช่น การลักเอาข้อมูลหมายเลขบัตรเครดิตของบุคคลหนึ่งไปใช้จ่ายซื้อสินค้าที่มีราคาสูง โดยบุคคลผู้เป็นเจ้าของที่แท้จริงมิได้ยินยอม หรือรับรู้ถึงการกระทำนั้น ซึ่งในบางกรณีผู้กระทำความผิดได้กระทำการนั้นซ้ำหลายครั้งจนยอดการใช้จ่ายผ่านบัตรเครดิตเป็นจำนวนเงินสูงมาก กว่าเจ้าของบัตรเครดิตจะรู้ถึงการถูกนำข้อมูลไปใช้ปลอมตัว หรือแอบอ้าง

นั้น ความเสียหายก็ได้เกิดขึ้นมากแล้ว ซึ่งกฎหมายที่เกี่ยวข้องกับการกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในลักษณะนี้ คือ ประมวลกฎหมายอาญาในความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ แต่บทบัญญัตินี้ไม่อาจใช้บังคับได้กับทุกกรณีความผิดที่เกิดขึ้นหรือการลักเอาบัตรประจำตัวประชาชนของบุคคลอื่นมา แล้วนำมาใช้เป็นหลักฐานในการขอสินเชื่อกับธนาคารหรือสถาบันการเงิน ซึ่งกฎหมายที่เกี่ยวข้องกับการกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในลักษณะนี้ คือ ประมวลกฎหมายอาญาในความผิดฐานลักทรัพย์ ซึ่งหากเป็นกรณีผู้กระทำจดจำเพียงข้อมูลบนบัตรโดยมิได้ลักเอาตัวบัตรประจำตัวประชาชนไปด้วยแต่อย่างใด บทบัญญัติความผิดฐานลักทรัพย์ก็มิอาจนำมาบังคับใช้ได้

ปัญหาการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่ยังไม่มีบทบัญญัติกฎหมายที่จะนำมาใช้บังคับเหล่านี้ ทำให้เกิดความเสียหายแก่บุคคลผู้เป็นเจ้าของข้อมูลตัวจริง และต่อองค์กรที่ต้องเข้ามาเกี่ยวข้องด้วยทั้งสิ้น ยิ่งไปกว่านั้นในบางกรณีการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลนี้เป็นฐานสำคัญที่นำไปสู่การประกอบอาชญากรรมร้ายแรงอื่นๆ ด้วย ตัวอย่างเช่น การปลอมตัวเป็นบุคคลอื่นเพื่อให้ตนสามารถเดินทางเข้าออกประเทศหนึ่งๆ ได้เพื่อวางแผนการก่อการร้าย ซึ่งหากเกิดการก่อการร้ายขึ้นในประเทศใดจะสร้างความเสียหายอย่างมากทั้งต่อชีวิตของประชาชน กระทบต่อความมั่นคงและระบบเศรษฐกิจของประเทศ ไม่มีนักธุรกิจใดอยากมาลงทุนทำธุรกิจภายในประเทศทำให้ระบบเศรษฐกิจภายในประเทศไม่เกิดการพัฒนา การฟอกเงินซึ่งหากประเทศใดกลายเป็นแหล่งฟอกเงินแล้วย่อมเป็นการนำสู่การประกอบอาชญากรรมอื่นอีกมาก หรือการประกอบอาชญากรรมร้ายแรงอื่นๆ ในรูปแบบองค์กรอาชญากรรมข้ามชาติ ซึ่งการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลนี้ในบางประเทศมีกรณีการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้ที่เสียชีวิตไปแล้วด้วย โดยเข้าสวมรอยว่าตนเป็นบุคคลที่เสียชีวิตไปแล้วนั้น กรณีดังนี้หากผู้เสียชีวิตที่ถูกสวมรอยนั้นเป็นบุคคลที่ไม่เป็นที่รู้จัก หรืออาจเป็นที่รู้จักเฉพาะในกลุ่มคนแคบๆ อาจทำให้ไม่มีผู้ใดรับรู้ในข้อเท็จจริงว่าบุคคลนั้นได้ถูกสวมรอยโดยบุคคลอื่นและอาจไม่มีผู้เสียหายที่จะออกมาดำเนินการทางกฎหมาย

ดังนั้นจึงอาจกล่าวได้ว่าข้อมูลส่วนบุคคลที่แสดงถึงเอกลักษณ์ของบุคคลนั้นเป็นสิ่งที่มีค่าและสมควรได้รับการคุ้มครอง ในหลายประเทศทั่วโลกต่างได้ตระหนักถึงปัญหาและความสำคัญ

ในการคุ้มครองข้อมูลเอกลักษณ์บุคคลนี้ เนื่องจากเป็นสิทธิที่มนุษย์ทุกคนย่อมมี เพราะมนุษย์ทุกคนเมื่อคลอดแล้วอยู่รอดเป็นทารก ย่อมมีสภาพบุคคล และได้สิทธิของบุคคลติดตัวมาตามธรรมชาติ ตามแนวความคิดของสำนักกฎหมายธรรมชาติ ซึ่งต่อมาสิทธิของบุคคลได้มีการบัญญัติรับรองไว้เป็นมาตรฐานสากลครั้งแรกในราวกลางศตวรรษที่ 19 ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 (Universal Declaration of Human Right 1948) ซึ่งได้บัญญัติให้การรับรองและคุ้มครองไว้ในข้อ 12 ดังนี้ “บุคคลย่อมไม่ถูกแทรกแซงโดยพลการในความเป็นอยู่ส่วนตัว ในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือไม่อาจถูกลบหลู่ในเกียรติยศและชื่อเสียง ทั้งนี้ บุคคลทุกคนย่อมมีสิทธิที่จะได้รับการปกป้องคุ้มครองโดยกฎหมายอันเนื่องจากการก้าวล่วงในสิทธินั้น”[2] จากบทบัญญัติดังกล่าวเห็นได้ว่าสิทธิของบุคคล คือ ความเป็นอิสระหรือเสรีภาพในความเป็นอยู่ส่วนตัวโดยปราศจากการสอดเข้าเกี่ยวข้องจากบุคคลอื่น ในสิทธิของบุคคลสามารถแยกออกได้เป็นหลายประการ เช่น สิทธิในความเป็นอยู่ส่วนตัว สิทธิในครอบครัว สิทธิในชื่อเสียงเกียรติยศ ฯลฯ ดังนี้ย่อมแสดงให้เห็นถึงสิทธิในข้อมูลส่วนบุคคลด้วย เนื่องจากเป็นสิ่งเฉพาะตัวและไม่อาจถูกสอดเข้าเกี่ยวข้องโดยบุคคลอื่นโดยที่มิได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูลได้

ประเทศสหรัฐอเมริกาซึ่งเป็นประเทศแรกที่กำหนดให้การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) เป็นความผิด[3] ได้ให้ความสำคัญในเรื่องนี้เป็นอย่างมาก มีการบัญญัติกฎหมายเฉพาะขึ้นสำหรับความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล คือ พระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) ซึ่งเป็นกฎหมายในระดับรัฐบาลกลาง (Federal State) กฎหมายฉบับนี้ทำให้เกิดการแก้ไขประมวลกฎหมายอาญาของสหรัฐอเมริกา (U.S. Code) ในหมวดที่ 18 มาตรา 1028 ซึ่งได้ให้ความหมายของการกระทำความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้ดังนี้ ผู้ใดโดยเจตนากระทำการโอน ครอบครอง หรือใช้ประโยชน์จากข้อมูลเอกลักษณ์ของบุคคลอื่นโดยไม่ได้รับอนุญาต เพื่อกระทำการผิดกฎหมายของสหรัฐอเมริกา

---

[2] สราวุธ ปิติยาศักดิ์, กฎหมายเทคโนโลยีสารสนเทศ (กรุงเทพมหานคร: สำนักพิมพ์นิติธรรม, 2555), หน้า 241.

[3] Martin T. Biegelman, Identity Theft Handbook Detection,Prevention,and Security (New Jersey: John Wiley & Sons, Inc, 2009), p.xix.

หรือได้ให้ความช่วยเหลือ หรือให้การสนับสนุนในการกระทำที่ผิดกฎหมายดังกล่าว อันก่อให้เกิดการละเมิดกฎหมายหรือก่อให้เกิดความผิดอาญาร้ายแรงภายใต้กฎหมายของมลรัฐใด หรือภายใต้กฎหมายท้องถิ่นใดที่มีผลใช้บังคับอยู่ ผู้นั้นสมควรได้รับโทษตามกฎหมาย และในประเทศแคนาดาก็ได้มีการบัญญัติให้การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นความผิดด้วยเช่นกัน โดยบัญญัติไว้ในประมวลกฎหมายอาญา

ในประเทศไทยยังไม่มีการบัญญัติกฎหมายเฉพาะในความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ดังนี้เมื่อเกิดการกระทำความผิดขึ้นจึงได้เพียงนำบทกฎหมายที่มีความเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลมาใช้บังคับเท่านั้นซึ่งไม่อาจบังคับใช้ได้ครอบคลุมในทุกกรณีของความผิดที่เกิดขึ้น เช่น ประมวลกฎหมายอาญาในความผิดเกี่ยวกับเอกสาร อาทิ ความผิดฐานปลอมเอกสาร ปลอมบัตรอิเล็กทรอนิกส์ ไม่อาจนำมาบังคับใช้ได้ในกรณีที่เพียงแต่นำข้อมูลไปใช้เท่านั้น มิได้มีการทำเอกสารปลอมใดๆ ขึ้น ในความผิดเกี่ยวกับทรัพย์ อาทิ ความผิดฐานลักทรัพย์ ความผิดฐานฉ้อโกง ไม่อาจนำมาบังคับใช้ได้ในกรณีที่เพียงแต่จดจำและนำข้อมูลไปใช้โดยมิได้มีการลักเอาตัวทรัพย์ไปด้วย และในกฎหมายอื่นที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในความผิดฐานเข้าถึงระบบ หรือข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ไม่อาจนำมาบังคับใช้ได้ในกรณีที่มิได้กระทำความผิดผ่านระบบคอมพิวเตอร์ หรือกรณีที่ระบบคอมพิวเตอร์นั้นมิได้มีระบบป้องกันการเข้าถึงไว้ พระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ในความผิดฐานเข้าถึงข้อมูล หรือเปิดเผยข้อมูลที่ถูกบันทึกไว้ในหน่วยความจำของบัตรประจำตัวประชาชนแบบเอนกประสงค์ เป็นการให้ความคุ้มครองแก่ข้อมูลที่ถูกบันทึกอยู่ในหน่วยความจำของบัตรเท่านั้น ไม่ได้ให้ความคุ้มครองถึงข้อมูลที่ปรากฏอยู่บนตัวบัตร และพระราชบัญญัติฉบับนี้ใช้บังคับเฉพาะกับบัตรประจำตัวประชาชนเท่านั้น ไม่รวมถึงเอกสารข้อมูลส่วนบุคคลอื่น เป็นต้น

ดังนั้นด้วยข้อจำกัดในการบังคับใช้กฎหมายของประเทศไทยในปัจจุบัน และประสบการณ์ของประเทศสหรัฐอเมริกาที่เมื่อบัญญัติกฎหมายเฉพาะแล้วทำให้จำนวนการกระทำความผิดลดลง กล่าวคือ จากการสำรวจในปีค.ศ. 2003 ถึงปี ค.ศ. 2006 เหยื่อที่ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลมีจำนวนลดลง และมูลค่าความเสียหายก็ลดลงด้วยจาก 47.6 พันล้านเหรียญ

สหรัฐในปี ค.ศ. 2003 ลดลงเหลือ 15.6 พันล้านเหรียญสหรัฐในปีค.ศ. 2006[4] จึงควรบัญญัติกฎหมายเฉพาะให้การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นความผิด เพื่อเป็นการป้องกันและควบคุมมิให้ปัญหาการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่เกิดขึ้นอยู่ในประเทศไทยปัจจุบันนี้ได้มีโอกาสทวีความรุนแรงเพิ่มขึ้นอันจะเป็นการยากลำบากต่อการปราบปราม

1.2 วัตถุประสงค์ของการวิจัย

1.) เพื่อศึกษาลักษณะของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในประเทศไทย ประเทศสหรัฐอเมริกา ประเทศแคนาดาและประเทศสหราชอาณาจักร

2.) เพื่อศึกษาความเหมาะสมของกฎหมายไทยที่นำมาปรับใช้กับกรณีการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในปัจจุบัน

3.) เพื่อเปรียบเทียบกฎหมายเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของประเทศไทยกับประเทศสหรัฐอเมริกา ประเทศแคนาดา และประเทศสหราชอาณาจักร

4.) เพื่อค้นหาแนวทางการกำหนดกฎหมายในการป้องกันและปราบปรามการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่เหมาะสมกับประเทศไทย

1.3 สมมติฐานของการวิจัย

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นการลักข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นไปใช้เพื่อแสวงหาประโยชน์โดยมิชอบ ผู้กระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลหากกระทำการลักเอกสารจะมีความผิดเมื่อการกระทำนั้นครบองค์ประกอบของการกระทำความผิดตามที่กฎหมายบัญญัติเป็นความผิดไว้ เช่น ความผิดฐานลักทรัพย์ ฉ้อโกง ปลอมเอกสาร เป็นต้น แต่ถ้าเป็นการลักเพียงข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเพื่อไปกระทำความผิด ยังไม่มีกฎหมายบัญญัติให้การกระทำดังกล่าวเป็นความผิด รวมถึงการครอบครอง การจำหน่ายจ่ายโอนข้อมูลซึ่งแสดงเอกลักษณ์บุคคล จึงสมควรบัญญัติให้การได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

[4] Identity Theft [Online], February 2013. Available from http://en.wikipedia.org/wiki/Identity_theft.

โดยชอบแต่มีเจตนานำข้อมูลไปใช้แสวงหาประโยชน์โดยทุจริตก็ดี การครอบครองและการจำหน่ายจ่ายโอนข้อมูลซึ่งแสดงเอกลักษณ์บุคคลโดยไม่ได้รับความยินยอมก็ตามเป็นความผิดเฉพาะตามที่ในหลายประเทศได้มีการบัญญัติไว้แล้ว เช่น ประเทศสหรัฐอเมริกาและประเทศแคนาดาเป็นต้น

1.4 วิธีดำเนินการวิจัย

ศึกษาวิจัยโดยวิธีวิจัยเอกสารทั้งในภาษาไทยและภาษาต่างประเทศ จากแหล่งข้อมูลทั้งที่เป็นตำรากฎหมาย วารสารกฎหมาย บทความ รายงานวิจัย รายงานสถิติ และวิทยานิพนธ์กฎหมาย ตลอดจนข้อมูลจากสื่ออิเล็กทรอนิกส์ในเรื่องที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ทั้งในประเทศไทยและต่างประเทศ

1.5 ขอบเขตของการวิจัย

วิทยานิพนธ์ฉบับนี้มุ่งศึกษาถึงที่มา นิยาม แนวความคิด รูปแบบ กฎหมายและปัญหาที่เกิดขึ้นของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในประเทศไทย โดยศึกษาเฉพาะในส่วนของประมวลกฎหมายอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 และร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.... เท่านั้น ในส่วนของต่างประเทศจะศึกษากฎหมายของประเทศสหรัฐอเมริกา ประเทศแคนาดา และประเทศสหราชอาณาจักร เพื่อนำมาวิเคราะห์แนวทางในการกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในประเทศไทย และศึกษาเฉพาะข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่อยู่ในรูปของข้อมูลที่ทำให้สามารถระบุตัวบุคคลได้ชัดเจน และการโจรกรรมข้อมูลนั้นรวมถึงการได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคลโดยชอบด้วยกฎหมาย แต่มีเจตนานำข้อมูลที่ได้มานั้นไปแสวงหาประโยชน์โดยทุจริตด้วย

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.) ทำให้รู้ เข้าใจ ในลักษณะของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของประเทศไทย ประเทศสหรัฐอเมริกา ประเทศแคนาดา และประเทศสหราชอาณาจักร

2.) ทำให้ทราบถึงบทกฎหมายของไทยที่นำมาปรับใช้กับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในปัจจุบัน

3.) ทำให้ทราบถึงความแตกต่างของกฎหมายที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของประเทศไทยกับกฎหมายสหรัฐอเมริกา แคนาดา และสหราชอาณาจักร

4.) เพื่อเป็นแนวทางในการปรับปรุง แก้ไข หรือเพิ่มเติมกฎหมายในอนาคต ที่จะกำหนดฐานความผิดและระวางโทษที่เหมาะสมสำหรับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

บทที่ 2

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล หมายถึง การที่บุคคลใดๆ ใช้ข้อมูลส่วนตัวของบุคคลอื่น เช่น ชื่อ นามสกุล หมายเลขบัตรประกันสังคม หมายเลขประจำตัวประชาชน ฯลฯ โดยไม่ได้รับอนุญาตเพื่อแสวงหาประโยชน์อันมิชอบ เช่น เพื่อไปกระทำความผิดฉ้อโกงหรือกระทำความผิดเกี่ยวกับอาชญากรรมอื่นๆ[1] ในการติดต่อ ทำการค้า หรือทำธุรกรรมต่างๆ ในชีวิตประจำวันล้วนต้องใช้ข้อมูลส่วนบุคคลเพื่อยืนยันตัวบุคคลทั้งสิ้น และเนื่องจากปัจจุบันด้วยความก้าวหน้าทางเทคโนโลยีทำให้มีการจัดทำ และเก็บข้อมูลส่วนบุคคลต่างๆ ในรูปข้อมูลอิเล็กทรอนิกส์มากขึ้น ทำให้สามารถเข้าถึงข้อมูลส่วนบุคคลได้โดยง่าย และสะดวก อีกทั้งหากข้อมูลส่วนบุคคลอิเล็กทรอนิกส์ถูกโจรกรรมไปผู้เป็นเจ้าของข้อมูลก็มิอาจล่วงรู้ได้ การโจรกรรมข้อมูลนี้จึงเกิดขึ้นได้ในหลายรูปแบบ ทั้งการโจรกรรมข้อมูลในรูปแบบทั่วไป โดยใช้วิธีการลักทรัพย์หรือชิงทรัพย์ ตลอดไปจนถึงวิธีการโจรกรรมแบบต้องอาศัยความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศเป็นพิเศษ กล่าวคือใช้โปรแกรมคอมพิวเตอร์มาเป็นเครื่องมือช่วยในการโจรกรรมข้อมูล การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลนอกจากทำไปเพื่อแสวงหาประโยชน์ทางการเงินแล้วยังเป็นการกระทำความผิดที่เป็นฐานสำคัญนำไปสู่การประกอบอาชญากรรมร้ายแรงอื่นๆ ด้วย ตัวอย่างเช่น การปลอมตัวเป็นบุคคลอื่นเพื่อให้ตนสามารถเดินทางเข้าออกประเทศหนึ่งๆ ได้เพื่อวางแผนการก่อการร้าย ซึ่งหากเกิดการก่อการร้ายขึ้นในประเทศใดจะสร้างความเสียหายอย่างมากทั้งต่อชีวิตของประชาชน กระทบต่อความมั่นคงและระบบเศรษฐกิจของประเทศ ไม่มีนักธุรกิจใดอยากมาลงทุนทำธุรกิจภายในประเทศทำให้ระบบเศรษฐกิจภายในประเทศไม่เกิดการพัฒนา การฟอกเงินซึ่งหากประเทศใดกลายเป็นแหล่งฟอกเงินแล้วย่อมเป็นการนำสู่การประกอบ

---

[1] Mohamed Chawki & Mohamed S. Abdel Wahab, “Identity Theft in Cyberspace: Issues and Solutions,” Lex Electronica Vol.11, 1 (Spring 2006): 2.

อาชญากรรมอื่นอีกมาก หรือการประกอบอาชญากรรมร้ายแรงอื่นๆ ในรูปแบบองค์กรอาชญากรรมข้ามชาติ จึงควรมีการศึกษาถึงความหมายและพัฒนาการ

2.1 ความเป็นมาของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในระยะเริ่มแรกได้เกิดขึ้นในประเทศสหรัฐอเมริกาเป็นจำนวนมาก ต่อมาการโจรกรรมได้เกิดขึ้นในประเทศต่างๆ ทั่วโลก จึงเป็นปัญหาที่นับวันจะยิ่งทวีจำนวนมากขึ้น เนื่องมาจากมีการปรับเปลี่ยนรูปแบบในการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลอยู่เสมอตามยุคสมัยตั้งแต่สมัยก่อนยุคเทคโนโลยีสารสนเทศจนถึงยุคเทคโนโลยีสารสนเทศที่มีการพัฒนา และเจริญก้าวหน้า ในระยะแรกการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล มีชื่อเรียกแตกต่างกันไปขึ้นอยู่กับลักษณะของการกระทำความผิด กล่าวคือยังไม่มีการเรียกชื่อฐานความผิดรวม แต่แยกเรียกชื่อการกระทำความผิดตามข้อเท็จจริงที่เกิดขึ้น เช่น การฉ้อโกงบัตรเครดิต (Credit card fraud) การฉ้อโกงชื่อจริง (true name fraud) การฉ้อโกงเอกลักษณ์บุคคล (Identity fraud)[2] เมื่อประมาณปี คริสตศักราช 1980 ถึงช่วงกลางปีคริสตศักราช 1990 จึงมีการใช้ชื่อเรียกความผิดที่กระทำโดยโจรกรรมข้อมูลส่วนบุคคลของผู้อื่นมาแสวงหาประโยชน์โดยมิชอบโดยรวมว่า การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) ซึ่งในช่วงเริ่มต้นการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลกระทำโดยอาศัยวิธีการโจรกรรมธรรมดา ซึ่งแหล่งที่เกิดการขโมยข้อมูลมากในช่วงเวลานั้น คือ การค้น หรือเก็บหลักฐานที่มีรายละเอียดสำคัญๆ เกี่ยวกับเอกลักษณ์บุคคลจากถังขยะ (dumpster diving) ภายในธนาคาร สำนักงานเครดิต และที่ทำการไปรษณีย์ รวมทั้งเอกสารจากกล่องรับจดหมาย อาชญากรรมการฉ้อโกงบัตรเครดิตได้เพิ่มจำนวนสูงขึ้นควบคู่ไปกับจำนวนของผู้ใช้บัตรเครดิต ตั้งแต่ช่วงต้นปีคริสตศักราช 1970 ผู้คนเริ่มให้การยอมรับ และนิยมใช้บัตรเครดิตในตลาดการค้า และการธนาคารกันเป็นจำนวนมาก จึงเสมือนเป็นการขยายช่องทางการขโมยข้อมูลของอาชญากร ต่อมาเมื่อ

[2] Martin T. Biegelman, Identity Theft Handbook Detection,Prevention,and Security (New Jersey: John Wiley & Sons, Inc, 2009), p.3.

เทคโนโลยีสารสนเทศเจริญก้าวหน้าขึ้น การใช้งานอินเตอร์เน็ตจึงมีมากขึ้น ซึ่งการใช้อินเตอร์เน็ตนั้นมีข้อดีในด้านความประหยัดค่าใช้จ่าย และประหยัดเวลา ทำให้การทำธุรกรรมใดๆ เป็นไปได้โดยสะดวก รวดเร็วขึ้น จึงทำให้ผู้ประกอบการธุรกิจ รวมทั้งบุคคลธรรมดาหันมาใช้อินเตอร์เน็ตกันอย่างแพร่หลาย อาชญากรที่ทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลจึงปรับเปลี่ยนรูปแบบในการขโมยข้อมูลของเหยื่อด้วยเช่นกัน กล่าวคือ มีการใช้โปรแกรมคอมพิวเตอร์ต่างๆ มาเป็นเครื่องมือในการขโมยข้อมูล เช่น spam, phishing, pharming, vishing, hacking และการใช้เทคโนโลยีอื่นๆ[3] เพื่อบุกเข้าไปขโมยข้อมูลที่สำคัญๆ ของเหยื่อในระบบคอมพิวเตอร์ เช่น รหัสผ่านเข้าระบบต่างๆ ของเหยื่อ ข้อมูลทางการเงิน ฯลฯ

ช่วงต้นปีคริสตศักราช 1980 ผู้ที่ตกเป็นเหยื่อส่วนมากคือ ผู้ประกอบวิชาชีพเหล่านี้ ทนายความ นายหน้าซื้อขายหุ้น แพทย์ ฯลฯ เนื่องจากเป็นบุคคลที่มีเครดิตดี เนื่องจากการใช้บัตรเครดิตในระยะแรกๆ วงเงินของบัตรเครดิตจะจำกัดไว้ ต่อมาทางธนาคารก็จะดูประวัติการใช้บัตรเครดิตหากมีประวัติทางการเงินดี ชำระตรงเวลาสม่ำเสมอ ธนาคารก็จะทำการเพิ่มวงเงินบัตรเครดิตให้ ซึ่งมีการเพิ่มวงเงินให้จนถึงขั้นที่วงเงินไม่มีจำกัด[4] จากลักษณะของการโจรกรรมการที่อาชญากรขโมยเพียงข้อมูลจึงไม่เป็นที่สังเกตเห็นของผู้ถูกขโมยข้อมูล เนื่องจากไม่มีทรัพย์สินสิ่งของที่เป็นรูปธรรมใดๆ หายไป เมื่ออาชญากรได้ข้อมูลมาจะทำการส่งผ่านข้อมูลไปยังผู้สมรู้ร่วมคิดเพื่อให้ไปกระทำการฉ้อโกงในเมืองอื่น ในปีคริสตศักราช 1985 อาชญากรได้แทรกซึมอยู่ในสำนักงานข่าวบริษัทซีบีเอสบรอดแคสติ้ง (CBS Broadcasting Inc.) ในนิวยอร์ก และได้ขโมยข้อมูลส่วนบุคคลของพนักงานบริษัทซีบีเอส กว่าหนึ่งร้อยคน รวมถึงผู้ประกาศข่าวชื่อดังอย่างวอล์เตอร์ คอนไคน์ (Walter Cronkite) และเอ็ด แบรดลีย์ (Ed Bradley) ด้วยซึ่งก่อให้เกิดความเสียหายเป็นอย่างมากแก่สำนักงานข่าว อาชญากรรมในรูปแบบนี้เริ่มทวีจำนวนมากขึ้น โดยเฉพาะในช่วงกลางปีคริสตศักราช 1980 อาชญากรรมประเภทนี้เกิดขึ้นเป็นจำนวนมาก มีผู้เสียหายมาร้องเรียน

[3] รู้ทันเทคนิคการขโมยข้อมูล[ออนไลน์], พฤศจิกายน 2555. แหล่งที่มา http://foh9.blogspot.com/2012/04/blog-post_04.html.

[4] Martin T. Biegelman, Identity Theft Handbook Detection,Prevention,and Security, p.6.

กับทางสถาบันการเงิน และหน่วยงานที่บังคับใช้กฎหมายเพิ่มขึ้นเรื่อยๆ[5] ทำให้ในปีคริสตศักราช 1982 และปีคริสตศักราช 1984 รัฐสภาของสหรัฐอเมริกาได้ออกกฎหมายเกี่ยวกับการเข้าถึงข้อมูลโดยมิชอบ การฉ้อโกงบัตรเครดิต และบัตรเดบิตให้เป็นอาชญากรรมเฉพาะขึ้น หน่วยงานแรกที่ได้รับมอบหมายให้ดำเนินการตรวจสอบการเข้าถึงข้อมูลโดยมิชอบเพื่อการฉ้อโกงนี้ คือ หน่วยงานให้บริการด้านความลับแห่งประเทศสหรัฐอเมริกา (The United States Secret Service) หน่วยงานผู้ตรวจสอบเกี่ยวกับไปรษณีย์ที่เคยทำงานในหน้าที่ดำเนินการตรวจสอบการเข้าถึงข้อมูลโดยมิชอบนี้ในช่วงปี คริสตศักราช 1960 จึงเข้ารวมกับตัวแทนของหน่วยงานให้บริการด้านความลับ (Secret Service)[6]

อาจกล่าวได้ว่าในปัจจุบันอาชญากรรมประเภทนี้เกิดขึ้นเป็นจำนวนมาก เนื่องจากการเข้าถึงข้อมูลส่วนบุคคลของเหยื่อนั้นง่ายขึ้น และอาชญากรรมการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลนี้ยังเข้าไปเกี่ยวข้องกับอาชญากรรมประเภทอื่นๆ อีกด้วย เช่น การก่อการร้าย การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่ก่อให้เกิดเหตุการณ์ก่อการร้ายที่มีความรุนแรงมาก และเป็นกรณีที่ทำให้บุคคลผู้เกี่ยวข้องหันมาให้ความสำคัญกับความผิดนี้มากขึ้น คือ เหตุการณ์ก่อการร้ายที่เกิดขึ้นเมื่อวันที่ 11 กันยายน 2011 ที่กลุ่มอัลกออิดะห์จี้อากาศยานเพื่อพุ่งชนตึกเวิร์ดเทรดเซ็นเตอร์ในนครนิวยอร์ก ประเทศสหรัฐอเมริกา ซึ่งลักษณะของการกระทำ คือ ผู้ก่อการร้ายจะใช้ข้อมูลส่วนตัวของบุคคลอื่นเพื่อทำการเช่าห้องพัก (apartment) เช่าสำนักงาน (office space) เช่าตู้ไปรษณีย์ (post office boxes) เช่ายานพาหนะ (vehicles) และตู้เก็บของ (storage lockers) เปิดใช้บริการโทรศัพท์เคลื่อนที่ และการให้บริการสาธารณูปโภคอื่นๆ ในนามของบุคคลที่ถูกโจรกรรมข้อมูลมา ตัวอย่างเช่น กลุ่มก่อการร้ายอัลเคด้า (al-Qaeda) ในประเทศสเปนใช้บัตรเครดิต ของบุคคลอื่นเพื่อใช้จ่ายในการดำเนินการต่างๆ ใช้โทรศัพท์เคลื่อนที่ของบุคคลอื่นที่ตนลักมาเพื่อใช้ติดต่อกลับไปยังสมาชิกกลุ่มในต่างประเทศ เช่น ประเทศปากีสถาน ประเทศอัฟกานิสถาน ประเทศเลบานอน ฯลฯ ใช้หนังสือเดินทางปลอมเพื่อเป็นหลักฐานในการเปิดบัญชี

---

[5] The Bureau of Justice Assistance, Preventing Identity Theft: a Guide for Consumers, (Washington DC, 2005), p.3.

[6] Martin T. Biegelman, Identity Theft Handbook Detection,Prevention,and Security, p.4.

ธนาคาร เพื่อทำการโอนเงินเข้า ออกประเทศเพื่อใช้จ่ายในการวางแผนการก่อการร้าย[7] การกระทำความผิดอาญาร้ายแรงในรูปแบบขององค์กรอาชญากรรม อาชญากรรมข้ามชาติ เป็นต้น ประเทศสหรัฐอเมริกาที่ถือเป็นประเทศแรก ที่เกิดการกระทำความผิดในลักษณะที่มีความรุนแรง และเกิดความผิดขึ้นเป็นจำนวนมาก จึงเกิดแนวความคิดในการกำหนดให้การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นความผิด และได้บัญญัติกฎหมายเฉพาะขึ้นมาเพื่อป้องกันและปราบปรามการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล มิให้ทวีจำนวนมากขึ้นหรือสร้างความเสียหายแก่ประเทศชาติ สังคมและประชาชนไปมากกว่าที่เป็นอยู่ กฎหมายปัจจุบันที่ประเทศสหรัฐอเมริกาใช้บังคับกับการโจรกรรมเอกลักษณ์บุคคล คือ พระราชบัญญัติยับยั้งและสันนิษฐานการขโมยข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998)

ในประเทศแคนาดา การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเริ่มทวีจำนวนมากขึ้น จากข้อมูลของหน่วยวิเคราะห์สำนักงานตำรวจแห่งชาติ (Royal Canadian Mounted Police) รายงานว่าในปี ค.ศ. 2006 มีชาวแคนาดาเป็นเหยื่อของการโจรกรรมข้อมูลเอกลักษณ์บุคคลถึง 212,859 ราย ซึ่งมีมูลค่าความเสียหายรวม 15,731,000 เหรียญ รัฐบาลตระหนักถึงปัญหาที่สร้างความเสียหายอย่างมากนี้ จึงมีการออกกฎหมายเมื่อวันที่ 21 พฤศจิกายน 2007 เพื่อเป็นการหยุดยั้งอาชญากรรมประเภทนี้ โดยมีการแก้ไขประมวลกฎหมายอาญาเพิ่มเติมฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลขึ้นเป็นการเฉพาะ[8]

ในประเทศสหราชอาณาจักร ได้มีการประมาณการความเสียหายที่เกิดจากการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลต่อระบบเศรษฐกิจอยู่ที่ประมาณ 3.4 พันล้านเหรียญต่อปี ซึ่งถูกจัดเป็นอาชญากรรมที่มีจำนวนเพิ่มสูงขึ้นอย่างรวดเร็วที่สุดในปี ค.ศ. 2007 จากการสำรวจเหตุผลที่ทำให้เกิดการกระทำความผิดในลักษณะนี้เป็นจำนวนมากเนื่องจากประชาชนส่วนใหญ่ไม่รู้วิธีที่เหมาะสมในการป้องกันข้อมูลของตนเอง และไม่รู้ว่าควรปฏิบัติตัวอย่างไรเมื่อตกเป็นเหยื่อ กล่าวคือ จากการสำรวจร้อยละ 25 ของประชาชนจะไม่แจ้งความหากหนังสือเดินทางของตนสูญ

---

[7] Ibid, p.227.

[8] Identity Theft in Canada [online], February 2013. Available from: http://www.spamlaws.com/id-theft-can.html.

หาย และร้อยละ 80 ไม่รู้ว่าควรปฏิบัติตนอย่างไรเมื่อใบสูติบัตร (birth certificate) สูญหาย ผู้กระทำการโจรกรรมข้อมูลส่วนมาก คือ บุคคลภายในสถาบันการเงิน เพื่อนบ้าน หรือเพื่อนที่สามารถเข้าถึงข้อมูลส่วนบุคคลของเหยื่อได้ ซึ่งเมื่อได้ข้อมูลมาแล้วจะนำไปแสวงหาประโยชน์แก่ตนเองในรูปแบบต่างๆ เช่น เปิดบัญชีเครดิต ทำสัญญากู้ยืม ซื้อสินค้าผ่านทางออนไลน์ โดยความเสียหายเฉลี่ยต่อบุคคลอยู่ที่ประมาณ 16,000 เหรียญ ในปีค.ศ. 2007 หน่วยงานบริการให้คำแนะนำด้านการเงิน (The Financial Services Advisory หรือ FSA) ได้รับแจ้งและทำการสืบสวนคดีการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นจำนวน 56 คดี[9] ซึ่งในปัจจุบันประเทศสหราชอาณาจักรยังไม่มีการบัญญัติกฎหมายเฉพาะ แต่มีกฎหมายหลักที่สามารถนำมาปรับใช้กับการกระทำความผิดได้ คือ พระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 (The Identity Card Act of 2006) พระราชบัญญัติการฉ้อโกง ค.ศ. 2006 (The Fraud Act of 2006) เป็นต้น

ดังนี้เห็นได้ว่าปัจจุบันการโจรกรรมเอกลักษณ์บุคคลได้แผ่ขยายไปในหลายประเทศทั่วโลก ความรุนแรง และลักษณะของการกระทำความผิดก็แตกต่างกันไปตามสภาพสังคม วัฒนธรรม และเศรษฐกิจของประเทศนั้น แต่ในหลักสำคัญของการกระทำความผิดมีความเหมือนกัน คือ การนำข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นมาใช้เพื่อแสวงหาประโยชน์อันมิชอบเพื่อตนเอง หรือผู้อื่น และทำให้บุคคลอื่นเข้าใจว่าตัวอาชญากรนั้นเป็นบุคคลที่ถูกโจรกรรมข้อมูลมา

2.2 ความหมายและลักษณะของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

เนื่องจากประเทศไทยยังไม่มีการบัญญัติฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้โดยตรง จึงยังไม่มีการนิยามความหมายไว้ว่าคำว่าโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล หรือที่ต่างประเทศเรียกกันว่า Identity Theft นั้นครอบคลุมความหมายกว้างเพียงใด ดังนี้จึงต้องอาศัยแปลความหมายตามความหมายในพจนานุกรม และอ้างอิงจากความหมายที่ได้ให้ไว้เกี่ยวกับลักษณะของความผิดนี้ในกฎหมายของต่างประเทศ โดยเฉพาะจากประเทศสหรัฐอเมริกาที่เป็นประเทศเริ่มแรกที่เกิดความผิดประเภทนี้ขึ้นเป็นจำนวนมาก

---

[9] Martin T. Biegelman, Identity Theft Handbook Detection,Prevention,and Security, p.223.

การให้ความหมายของคำว่า “เอกลักษณ์ (Identity)” หมายถึงลักษณะเฉพาะตัว ลักษณะที่เหมือนกันหรือมีร่วมกัน หรือลักษณะที่แสดงความเป็นอย่างเดียวกันของคนในสังคมหนึ่งๆ ซึ่งแตกต่างจากลักษณะร่วมของคนในสังคมอื่น หรือหมายถึงลักษณะเฉพาะที่มีหนึ่งเดียว[10] เช่น ภาษาไทยเป็นเอกลักษณ์ของชาติไทย การใช้คำว่าเอกลักษณ์จึงต้องเข้าใจว่าจะใช้ในระดับใด เอกลักษณ์ของใคร คำว่าเอกลักษณ์ บัญญัติให้ตรงกับคำภาษาอังกฤษคือคำว่า identity[11] ดังนี้ หากใช้ว่า “เอกลักษณ์บุคคล” จึงหมายถึงลักษณะเฉพาะตัวที่แสดงถึงความเป็นตัวตนของบุคคลหนึ่งๆ ที่ไม่เหมือนกับบุคคลอื่นๆ

อย่างไรก็ตามเพื่อความเข้าใจและความชัดเจนถึงขอบเขตของข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ผู้เขียนขออธิบายถึงความแตกต่างระหว่าง “ข้อมูลส่วนบุคคล” (Personal Information) กับ “ข้อมูลซึ่งแสดงเอกลักษณ์บุคคล” (Identity) ดังนี้ กฎหมายไทยปัจจุบันได้มีการให้คำนิยามของคำว่าข้อมูลส่วนบุคคลไว้ในพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540 ในมาตรา 4 “ข้อมูลข่าวสารส่วนบุคคล หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย” และในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ในมาตรา 3 ให้คำนิยามของ “ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม บรรดาที่มีชื่อของบุคคลนั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย” เห็นได้ว่าการให้คำนิยามของกฎหมายสองฉบับนี้มีความเหมือนกัน ในส่วนของคำว่า “ข้อมูลซึ่งแสดงเอกลักษณ์

---

[10] ราชบัณฑิตยสถาน, พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. 2542 (กรุงเทพมหานคร: นานมีบุ๊คพับลิเคชั่นส์, 2546).

[11] กาญจนา นาคสกุล, ความหมายของคำที่น่าสนใจ [ออนไลน์], พฤศจิกายน 2555, แหล่งที่มา http://www.blog.prachyanun.com/view.php?article_id=1175.

บุคคล (Identity)" กฎหมายไทยปัจจุบันยังไม่มีการบัญญัติให้คำนิยามไว้ จึงต้องอาศัยการแปลความหมายตามพจนานุกรม และกฎหมายของต่างประเทศเป็นแนวทาง ดังนี้เมื่อเอกลักษณ์ หมายถึง ลักษณะเฉพาะตัว ข้อมูลซึ่งแสดงเอกลักษณ์บุคคล จึงคือ ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคลที่ไม่เหมือนกับบุคคลอื่นโดยข้อมูลหนึ่งๆ อาจอยู่โดยลำพังแล้วสามารถระบุตัวบุคคลได้ เช่น ลายพิมพ์นิ้วมือ รหัสพันธุกรรม (DNA) ม่านตา หมายเลขบัตรเครดิต หมายเลขบัตรประกันสังคม ฯลฯ หรือข้อมูลที่เมื่อรวมกันกับข้อมูลอื่นแล้ว สามารถระบุตัวบุคคลได้ เช่น ชื่อ นามสกุล ที่อยู่ วันเดือนปีเกิด ฯลฯ ดังนี้จึงอาจกล่าวได้ว่าข้อมูลส่วนบุคคลถือเป็นส่วนหนึ่งของข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ทั้งนี้โดยข้อมูลส่วนบุคคลประเภทหนึ่งๆ จะเป็นข้อมูลซึ่งแสดงเอกลักษณ์บุคคลหรือไม่ ขึ้นอยู่กับว่าข้อมูลนั้นจะมีความชัดเจน เฉพาะเจาะจงมากเพียงพอที่จะสามารถระบุตัวบุคคลได้หรือไม่ เช่น หากเป็นชื่อบุคคล อาจมีบุคคลหลายคนที่มีชื่อซ้ำกันได้ ดังนี้ยังไม่สามารถระบุตัวบุคคลได้ จึงไม่ถือเป็นข้อมูลซึ่งแสดงเอกลักษณ์บุคคล แต่เมื่อนำข้อมูลชื่อนั้นรวมเข้ากับนามสกุล วันเดือนปีเกิด ที่อยู่อาศัย อาจทำให้สามารถระบุตัวบุคคลได้ ดังนี้ข้อมูลรวมกันทั้งหมดนี้จึงเป็นข้อมูลซึ่งแสดงเอกลักษณ์บุคคล กล่าวคือต้องเป็นบุคคลคนนี้เพียงคนเดียวเท่านั้นไม่อาจเป็นบุคคลอื่นไปได้ เป็นต้น

การให้ความหมายของคำว่า "โจรกรรม (Theft)" หมายถึง การลัก การขโมย การปล้น[12] ดังนี้การโจรกรรมเอกลักษณ์บุคคล จึงหมายถึง การขโมยลักษณะเฉพาะตัวของบุคคลหนึ่งที่แสดงถึงความเป็นตัวตนของบุคคลนั้นโดยเฉพาะ ไม่อาจเป็นลักษณะของบุคคลอื่นไปได้ เช่น ชื่อตัว ชื่อสกุล ที่อยู่ ใบสูติบัตร หมายเลขประจำตัวประชาชน หมายเลขประกันสังคม หมายเลขบัตรเครดิต เป็นต้น อย่างไรก็ตามการ "โจรกรรม" ในกรณีทั่วไปอาจหมายถึง การขโมย แต่สำหรับการโจรกรรมตามความหมายของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) นี้ "การโจรกรรม" หมายความถึง การได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในกรณีที่ได้มาโดยชอบด้วยกฎหมาย โดยมีวัตถุประสงค์จะนำข้อมูลซึ่งแสดงเอกลักษณ์บุคคลนั้นไปแสวงหาประโยชน์โดยมิชอบด้วยกฎหมาย คือ มีเจตนาทุจริตด้วย อาทิเช่น ผู้เป็นเจ้าของข้อมูลเป็นผู้มอบข้อมูลให้อาจเพื่อทำการติดต่อใดๆ เช่น ยื่นเอกสารสมัครงาน โดยผู้ที่ได้ข้อมูลมามีเจตนาที่จะนำข้อมูลซึ่ง

[12] ราชบัณฑิตยสถาน, พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. 2542.

แสดงเอกลักษณ์บุคคลที่ได้มานั้นไปดำเนินการแสวงหาประโยชน์โดยมิชอบเพื่อตน เช่น นำไปใช้เป็นเอกสารหลักฐานในการขอสินเชื่อกับสถาบันการเงิน ฯลฯ เพื่อความชัดเจนผู้เขียนขออธิบายถึงลักษณะของการได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ดังนี้

1.) การได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคลโดยชอบด้วยกฎหมาย หมายถึงการที่บุคคลได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นได้โดยชอบด้วยกฎหมาย อาจเนื่องมาจากเป็นผู้มีสิทธิรับรู้ เข้าถึงข้อมูลนั้น หรือเป็นกรณีการได้มาซึ่งข้อมูลจากการติดต่อ ค้าขาย หรือทำธุรกรรมใดๆ ระหว่างกัน เช่น การที่ผู้สมัครงานกรอกข้อมูลและมอบเอกสารส่วนบุคคลต่างๆ ไว้ให้แก่ผู้รับสมัครงาน ตัวอย่างที่เกิดขึ้น เช่น กรณีของนางสาวยุพา หีบทอง เข้าร้องทุกข์ต่อนางปวีณา หงสกุล เพื่อขอความเป็นธรรมหลังถูกกลุ่มมิจฉาชีพนำเอกสารสำเนาบัตรประจำตัวประชาชน สำเนาทะเบียนบ้านไปจดทะเบียนห้างหุ้นส่วนจำกัดเพรสซิเด้นท์ โฮมแคร์ เซ็นเตอร์ โดยใส่ชื่อตนเป็นหุ้นส่วนและผู้จัดการ จนได้รับผลกระทบจากการถูกฟ้องร้องต่อศาลในคดีฐานฉ้อโกงไม่จ่ายเงินเดือนแก่พนักงาน ซึ่งเอกสารสำคัญที่ถูกนำมาแอบอ้างนั้น คาดว่าเมื่อ 2 ปีก่อนได้นำเอกสารไปสมัครงานที่บริษัทแห่งหนึ่งในตำแหน่งพนักงานแจกใบปลิว โดยได้เซ็นชื่อกำกับสำเนาถูกต้องแต่ไม่ได้เขียนกำกับการใช้งาน จึงคาดว่าถูกเอกสารดังกล่าวจึงถูกนำไปใช้จดทะเบียนห้างหุ้นส่วนซึ่งก่อความเสียหายดังกล่าว[13]

อย่างไรก็ตามการได้ข้อมูลมาโดยวิธีการที่ชอบด้วยกฎหมายอาจเกิดขึ้นในลักษณะที่ผู้เป็นเจ้าของข้อมูลมิได้มีความประสงค์ที่จะให้ข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของตนเองแก่ผู้อื่นแต่อย่างใด แต่เกิดจากการที่ผู้อื่นแสวงหาข้อมูลของบุคคลอื่นด้วยวิธีการต่างๆ ซึ่งวิธีการเหล่านั้นไม่มีกฎหมายบัญญัติเป็นความผิด เช่น การได้ข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นมาจากการค้นถังขยะ (Dumpster Diving) คือ การค้นขยะเพื่อค้นหาเอกสารที่มีข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นเพื่อนำไปใช้แสวงหาผลประโยชน์โดยมิชอบ ทั้งนี้การค้นถังขยะในที่สาธารณะไม่เป็น

[13] ทีมข่าวภูมิภาค, 2 สาวร้อง ปวีณา ถูกมิจฉาชีพใช้สำเนาบัตรตระเวนฉ้อโกง [ออนไลน์], 8 เมษายน 2555. แหล่งที่มา : http://www.thairath.co.th/content/region/306214.

ความผิดแต่อย่างใด ในประเทศสหรัฐอเมริกาได้มีคดี California V. Greenwood.[14] ตัดสินวางหลักไว้ว่าการได้ข้อมูลหรือหลักฐานใดๆ จากถังขยะไม่เป็นการละเมิดเนื่องจากผู้ทิ้งได้มีเจตนาสละสิทธิในขยะเหล่านั้นแล้ว เป็นต้น ดังนี้การได้มาซึ่งข้อมูลโดยชอบด้วยกฎหมายจะเป็นความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลต่อเมื่อมีวัตถุประสงค์ที่จะนำข้อมูลที่ได้มาไปใช้แสวงหาผลประโยชน์โดยมิชอบ หรือนำไปกระทำความผิดอื่นๆ กล่าวคือมีเจตนาทุจริต หากเป็นการได้มาซึ่งข้อมูลโดยชอบด้วยกฎหมายแล้วผู้ได้มาซึ่งข้อมูลไม่มีเจตนาทุจริต ที่จะนำข้อมูลไปใช้แสวงหาผลประโยชน์โดยมิชอบเพื่อตนเอง หรือเพื่อผู้อื่นแล้ว บุคคลผู้ได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นนั้นก็ไม่มีความผิดในฐานการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

2.) การได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคลโดยไม่ชอบด้วยกฎหมาย คือ การได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นโดยไม่มีสิทธิ เช่น ลักทรัพย์ ฉ้อโกง การเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ชอบ ฯลฯ การได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคลโดยมิชอบนั้นจะเป็นความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ต่อเมื่อมีการได้มาซึ่งข้อมูลแล้วนำข้อมูลนั้นมาแอบอ้าง สวมรอย หรือใช้เพื่อแสวงหาประโยชน์โดยมิชอบ หรือมีเจตนาทุจริต ตัวอย่างที่เกิดขึ้น กรณีของนายแนบ ซึ่งเป็นแก๊งขโมยบัตรประจำตัวประชาชนของคนไทยเพื่อนำไปปลอมแปลงบัตรประจำตัว ประชาชน แล้วจำหน่ายให้กับแรงงานต่างด้าวทั้งผิดกฎหมายและถูกกฎหมาย นายแนบจะนำบัตรที่ลักได้มาส่งต่อให้กับเพื่อนร่วมแก๊งที่เปิดร้านถ่ายเอกสารไปปรับเปลี่ยนรูปใหม่ให้ตรงกับรูปใบหน้าของลูกค้า และปรับเปลี่ยนวันออกบัตร วันหมดอายุบัตร แล้วนำไปให้ลูกค้าตามที่สั่ง[15] เป็นต้น

การให้ความหมายของคำว่าการโจรกรรมเอกลักษณ์บุคคล (Identity Theft) ของคณะกรรมการการค้าแห่งชาติ (Federal Trade Commission) ของประเทศสหรัฐอเมริกา คือ การที่บุคคลใดๆ ใช้ข้อมูลส่วนตัวของบุคคลอื่น เช่น ชื่อ นามสกุล หมายเลขบัตรประกันสังคม และ

---

[14] California V. Greenwood [online], April 2013. Available from : http://en.wikipedia.org/wiki/California_v._Greenwood.

[15] แรงงานต่างด้าวสัญชาติลาวหลบหนีเข้าเมืองผิดกฎหมายและปลอมแปลงเอกสารทางราชการ [ออนไลน์], 8 เมษายน 2555. แหล่งที่มา : http://atcloud.com/discussions/18474.

หมายเลขประจำตัวประชาชน ฯลฯ โดยไม่ได้รับอนุญาตเพื่อแสวงหาประโยชน์อันมิชอบ อาทิ เพื่อไปกระทำความผิดฉ้อโกงหรือกระทำความผิดเกี่ยวกับอาชญากรรมอื่นๆ[16] และในรายงานของกองบังคับงานการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (The President's Identity Theft Task Force) ที่จัดทำขึ้นในช่วงปีคริสตศักราช 2007 ได้พูดถึง การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) ไว้ว่า การให้ความหมายของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลนี้มีในหลายรูปแบบ แต่โดยส่วนสำคัญ อาจกล่าวได้ว่าเป็นการนำเอาข้อมูลส่วนบุคคลของผู้อื่นไปใช้ในทางที่ผิด นำไปกระทำการฉ้อโกง[17] และในรายงานยังระบุอีกว่าอาชญากรขโมยข้อมูลเอกลักษณ์บุคคลด้วยวิธีปกติ ไม่ได้ใช้เทคโนโลยี คือ การขโมยจดหมาย หรือจากบันทึกในที่ทำงาน หรือจากการค้นในถังขยะ ตลอดไปจนถึงการใช้เทคโนโลยีเป็นเครื่องมือในการขโมย เช่น การเจาะเข้าโปรแกรมคอมพิวเตอร์ของผู้อื่นโดยผิดกฎหมาย[18] เป็นต้น จากความหมายเหล่านี้จึงสามารถสรุปได้ว่าข้อมูลเอกลักษณ์ของบุคคลนั้นมีหลากหลายประเภท ดังนั้นการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลจึงเกิดขึ้นได้หลายวิธีด้วยเช่นกัน และผู้ที่ทำการโจรกรรมข้อมูลมาก็สามารถที่จะนำข้อมูลนั้นไปกระทำความผิดได้ในหลายรูปแบบทั้งการฉ้อโกง หรือการประกอบอาชญากรรมอื่นๆ ที่ผิดกฎหมาย ทั้งนี้ขึ้นอยู่กับความเชี่ยวชาญและความต้องการของผู้ที่กระทำการขโมยข้อมูล ความผิดในฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลจึงมีหลากหลายประเภท แต่ความผิดที่เกิดขึ้นมากจากการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล คือ การสวมรอยบุคคลไปเปิดบัญชีเพื่อขอสินเชื่อกับทางสถาบันการเงิน หรือนำหมายเลขบัตรเครดิตที่โจรกรรมมาไปใช้จ่ายซื้อสินค้าต่างๆ ซึ่งโดยมากมักจะใช้ซื้อสินค้าที่มีราคาสูง ฯลฯ

---

[16] Mohamed Chawki & Mohamed S. Abdel Wahab, "Identity Theft in Cyberspace: Issues and Solutions," Lex Electronica Vol.11, 1 (Spring 2006): 2.

[17] The President's Identity Theft Task Force: Identity Theft means although identity theft is defined in many different ways, it is, fundamentally, the misuse of another individual's personal information to commit fraud"

[18] Martin T. Biegelman, Identity Theft Handbook Detection,Prevention,and Security, p.2.

2.3 การนำข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไปใช้แสวงหาประโยชน์โดยทุจริต (Types of Identity Theft)

การโจรกรรมข้อมูลจากที่ได้กล่าวมาแล้ว คือ การได้มาซึ่งข้อมูลแสดงเอกลักษณ์บุคคลทั้งที่ได้มาโดยไม่ชอบด้วยกฎหมาย และการได้มาโดยชอบด้วยกฎหมายแต่มีเจตนานำข้อมูลมาใช้เพื่อแสวงหาประโยชน์โดยทุจริต ดังนี้การนำข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไปใช้แสวงหาประโยชน์โดยทุจริตนั้นสามารถเกิดขึ้นได้ในหลายรูปแบบ เนื่องจากอาชญากรมักปรับเปลี่ยนรูปแบบของการโจรกรรมข้อมูลอยู่เสมอ ตามสถานการณ์ของสังคม เศรษฐกิจ และกฎหมายที่เปลี่ยนแปลงไป ซึ่งทำให้การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลมีการพัฒนา เกิดรูปแบบใหม่ๆ อยู่เสมอ จึงอาจแบ่งแยกรูปแบบของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่มีอยู่ในปัจจุบันนี้ได้เป็น 8 รูปแบบ[19] คือ

2.3.1 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับการเงิน (Financial Identity Theft)

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับการเงินนี้เป็นอาชญากรรมรูปแบบเริ่มแรกของการเกิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล และเป็นรูปแบบที่เกิดความผิดขึ้นเป็นจำนวนมากที่สุด การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับการเงินนี้ คือโดยส่วนมากอาชญากรจะขโมยข้อมูลบัตรเครดิตของเหยื่อ แล้วนำไปแสวงหาประโยชน์เสมือนหนึ่งตนเป็นเจ้าของบัญชีการเงินนั้นจริงๆ ซึ่งสามารถแบ่งออกได้เป็น 2 ประเภทใหญ่ๆ[20] คือ

2.3.1.1 การใช้ข้อมูลของเหยื่อเพื่อเปิดบัญชีใหม่ (new account fraud)

การกระทำความผิดในลักษณะนี้ คือ อาชญากรจะทำการเปิดบัญชีกับสถาบันการเงินโดยใช้ข้อมูลส่วนบุคคลของผู้อื่น ที่ตนได้ขโมยมา ซึ่งรูปแบบของการเปิดบัญชี

---

[19] Jake Stroup, The 8 Types of Identity Theft [online], November 2012. Available from http://idtheft.about.com/od/Basics/a/The-8-Types-Of-Identity-Theft.htm.

[20] Chris Jay Hoofnagle, "Identity Theft: Making The Known Unknowns Known," Harvard Journal of Law & Technology Vol.21, No.1 (Fall 2007): pp. 100-104.

(open lines of credit) เป็นไปได้ทั้งกรณีเปิดบัญชีบัตรเครดิตใหม่ ทำสัญญาจำนอง หรือกระทำการใดๆ โดยอาชญากรจะใช้หมายเลขประกันสังคมของเหยื่อ ทำให้เหยื่อได้รับความเสียหายจากการที่มีประวัติทางการเงินที่ไม่ดี ยากต่อการจะขอสินเชื่อใหม่ในอนาคต อีกทั้งประวัติที่เสียหายนั้นอาจเป็นตัวการขัดขวางการถูกจ้างงานของเหยื่อได้ด้วย โดยการใช้ข้อมูลส่วนตัวของเหยื่อเพื่อเปิดบัญชีใหม่นี้อาชญากรอาจกระทำโดยไม่ได้ใช้ชื่อจริงของเหยื่อก็ได้ หรือที่เรียกกันว่าการสร้างประวัติทางการเงินปลอม หรือ synthetic theft ซึ่งได้จัดเป็นการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลอีกรูปแบบหนึ่งต่างหาก ซึ่งจะกล่าวถึงต่อไปในรูปแบบที่ 8

2.3.1.2 **การใช้ข้อมูลของเหยื่อเพื่อสวมรอยในบัญชีที่เปิดไว้แล้ว** (account takeover)

การกระทำความผิดในลักษณะนี้ คือ อาชญากรจะใช้บัญชีที่เหยื่อมีอยู่แล้วด้วยการขโมยข้อมูลรหัสผ่าน หรือการลวงให้เหยื่อเปิดเผยรหัสผ่าน หรือข้อมูลส่วนตัวของเหยื่อจนทำให้อาชญากรได้ข้อมูลที่มากพอ เพื่อทำการเข้าถึงข้อมูลและทำการเปลี่ยนแปลงบัญชีของเหยื่อ ปัญหาที่พบบ่อยในกรณีนี้ คือ การโกงบัตรเครดิตด้วยวิธีการ phishing[21] เหยื่อที่อาชญากรจะเลือกลงมือมักเป็นเหยื่อที่มีบัญชีออมทรัพย์ หรือมีการชำระเงินผ่านระบบหรือใช้บริการประมูลซื้อสินค้าทางอินเตอร์เน็ต เช่น PayPal หรือ eBay เป็นต้น การสวมรอยใช้บัญชีของเหยื่อที่มีอยู่แล้วนั้น อาจเกิดความเสียหายแก่เหยื่อไม่มากนักหากทางสถาบันการเงินนั้นมีการจำกัดความรับผิดเอาไว้ และเมื่อเหยื่อได้รับใบแจ้งหนี้จากสถาบันการเงินก็อาจโต้แย้งในความถูกต้องของรายการที่เรียกเก็บได้ หรือการที่เหยื่อมีเงินอยู่ในบัญชีออมทรัพย์อย่างร้ายที่สุด คือ เหยื่อสูญเสียเงินทั้งหมดที่มีอยู่ในบัญชี

---

[21] Phishing หรือฟิชชิ่ง เป็นเทคนิคการหลอกลวงโดยอาชญากรจะสร้างหน้าเว็บไซต์ปลอมของธนาคาร หรือสถาบันการเงิน หรือร้านค้าออนไลน์ขึ้นมา โดยหน้าเว็บไซต์ดังกล่าวจะมีความคล้ายคลึงกับเว็บไซต์ต้นฉบับเป็นอย่างมาก จนบางครั้งถ้าไม่สังเกตให้ดีก็จะไม่เห็นความแตกต่าง หลังจากนั้นอาชญากรจะส่งอีเมล์สแปมให้เหยื่อ แจ้งเหยื่อว่าบัญชีของเหยื่อมีปัญหา ให้เหยื่อเข้าไปยังเว็บไซต์ปลอมเพื่ออัพเดตข้อมูลบัญชีธนาคารของเหยื่อ หากเหยื่อหลงเชื่อและกรอกข้อมูลส่วนตัวของเหยื่อลงในเว็บไซต์ปลอมดังกล่าวก็จะทำให้ เหยื่อสูญเสียข้อมูลการเข้าถึงเว็บไซต์ที่แท้จริงของธนาคาร และบางครั้งอาจจะถูกสวมรอยทำธุรกรรมด้านการเงินของเหยื่อด้วย

2.3.2 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับการประกันภัย (Insurance Identity Theft)

การกระทำความผิดในลักษณะนี้ เป็นการใช้ข้อมูลของบุคคลอื่นเพื่อให้ตนได้รับการรักษาหรือการบริการทางการแพทย์ เหยื่อจะถูกแอบอ้างใช้สิทธิไป อาจเห็นได้ว่าการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลรูปแบบเกี่ยวกับการประกันภัยนี้ มีความใกล้เคียงกับรูปแบบทางการเงินและเกี่ยวกับรูปแบบทางการแพทย์มาก แต่ที่เห็นสมควรแยกออกเป็นอีกรูปแบบหนึ่งต่างหาก เพราะได้สร้างปัญหาให้กับเหยื่อในอีกระบบหนึ่งต่างหาก คือไม่ใช่การสูญเสียเงิน หรือการไม่ได้รับการบริการทางการแพทย์โดยตรง แต่จะทำให้ประวัติการประกันภัยของเหยื่อเสียหาย[22] เช่น อาจเกิดกรณีเหยื่อประสบอุบัติเหตุรถยนต์อยู่รัฐหนึ่ง แต่ในขณะเดียวกันกลับปรากฏข้อมูลว่าเหยื่ออยู่ที่โรงพยาบาลในอีกรัฐหนึ่ง เหยื่อจะถูกปฏิเสธการประกันภัย และมีประวัติที่ไม่ดี บริษัทประกันภัยอื่นๆ ก็ไม่อยากจะเข้ามาเสี่ยงด้วยโดยการรับประกันภัย เป็นต้น

2.3.3 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับการแพทย์ (Medical Identity Theft)

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในรูปแบบนี้ คือ อาชญากรจะนำข้อมูลส่วนบุคคลของเหยื่อไปใช้ในการเข้าทำการรักษาทางการแพทย์ เสมือนตนเป็นเจ้าของข้อมูลที่แท้จริง ทำให้ผู้เป็นเจ้าของข้อมูลที่แท้จริงถูกเรียกเก็บค่ารักษาพยาบาลนั้น และทำให้ประวัติทางการแพทย์เสียหาย คือ ไม่ถูกต้อง หรือตรงกับความเป็นจริง เช่น ผู้เป็นเจ้าของข้อมูลได้รับใบเรียกเก็บค่ารักษาพยาบาลการผ่าตัดอวัยวะ ทั้งที่ในความจริงผู้นั้นมิเคยเข้าทำการรักษาแต่อย่างใด หรือกรณีพบว่าในประวัติการรักษาพยาบาลของตนมีการระบุว่าเป็นโรคเบาหวาน ซึ่งเกิดขึ้นเนื่องจากถูกอาชญากรนำข้อมูลไปใช้ ผู้ที่อยู่ในกลุ่มเสี่ยงถูกโจรกรรมข้อมูลทางการแพทย์ คือ บุคคลที่มีอายุมากกว่า 50 ปีขึ้นไปเนื่องจากส่วนมากจะมีระบบประกันสุขภาพของรัฐ

---

[22] Jake Stroup, Insurance Identity Theft: The New Type of Identity Theft [online], November 2012. Available from http://idtheft.about.com/od/identitytheft101/a/Insurance-Identity-Theft.htm.

(government-issued insurance)[23] การกระทำความผิดในลักษณะนี้จึงมีความเป็นอันตรายต่อชีวิตของเหยื่อมาก เนื่องจากประวัติการรักษาเป็นข้อมูลสำคัญที่แพทย์จะใช้เป็นแนวทางในการรักษาผู้ป่วย การโจรกรรมเกี่ยวกับการแพทย์นี้อาจเกิดจากอาชญากร แพทย์ พยาบาล ลูกจ้างในโรงพยาบาล หรือในปัจจุบันเริ่มมีการกระทำของผู้ที่เชี่ยวชาญในวงจรอาชญากรรมโดยเฉพาะด้วย ทั้งนี้เมื่อเกิดเหตุโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลทางการแพทย์เกิดขึ้นแล้ว เหยื่อสมควรได้รับการเยียวยา แก้ไขประวัติทางการแพทย์ด้วย[24] เพื่อความปลอดภัยของเหยื่อต่อไปในอนาคต

2.3.4 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับอาชญากรรม (Criminal Identity Theft)

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับอาชญากรรมนี้ คือการนำเอาชื่อของผู้บริสุทธิ์ไปใช้ประกอบอาชญากรรม ซึ่งอาชญากรรมประเภทนี้แก้ไขปัญหาได้ยากพอๆ กับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลทางการแพทย์ เพราะอาชญากรรมมีหนทางที่จะกลับมาก่อกวนและสร้างความเสียหายให้ได้อีก เมื่อรู้ตัวว่าถูกโจรกรรมข้อมูลไปจึงควรรีบแจ้งความให้เจ้าหน้าที่ตำรวจช่วยดำเนินคดีทันที เพราะหากปล่อยช้าไปผู้ที่ถูกดำเนินคดีอาจกลายเป็นตัวของเหยื่อเสียเอง เนื่องจากอาชญากรทุกประเภทที่เกิดขึ้น เมื่อถูกจับกุมตัวได้ก็มักจะปฏิเสธว่าตนมิได้เป็นผู้กระทำความผิด ซึ่งกว่าเหยื่อจะสามารถพิสูจน์ตัวเองได้อาจใช้เวลานาน และอาจไม่ทันการณ์ ทำให้เหยื่อต้องตกอยู่ภายใต้การดำเนินกระบวนการยุติธรรมทางอาญาในฐานะผู้ต้องหา[25] ได้

---

[23] Martin T. Biegelman, Identity Theft Handbook Detection,Prevention,and Security, p.97.

[24] Pam Dixon, “Medical Identity Theft: The Information Crime that Can Kill You,” The World Privacy Forum (May 2006):p.2.

[25] Jake Stroup, The 8 Types of Identity Theft [online], November 2012. Available from http://idtheft.about.com/od/Basics/a/The-8-Types-Of-Identity-Theft.htm.

2.3.5 **การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับใบอนุญาตขับขี่** (Driver's License Identity Theft)

การโจรกรรมในรูปแบบนี้เกิดขึ้นได้ง่าย อาจเกิดโดยการถูกขโมยกระเป๋าเงิน อาชญากรเมื่อได้ใบอนุญาตขับขี่ของเหยื่อมาแล้วก็จะขายใบอนุญาตนั้นต่อให้บุคคลอื่นที่มีหน้าตาคล้ายกับเหยื่อ แล้วผู้ที่ซื้อใบอนุญาตขับขี่ที่ถูกโจรกรรมมานั้นสามารถที่จะนำหลักฐานใบขับขี่ของเหยื่อนี้ไปใช้เพื่อขอออกหลักฐานอื่นๆ ต่อไปได้ในนามของเหยื่อ การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในรูปแบบนี้จึงมักมีความเชื่อมโยงต่อกับการประกอบอาชญากรรมอื่น

2.3.6 **การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับหมายเลขประกันสังคม** (Social Security Identity Theft)

หมายเลขประกันสังคมของประชาชนในอเมริกานั้นมีความสำคัญมาก เมื่อรู้เพียงเลขประกันสังคมก็สามารถจะรับรู้ถึงรายละเอียดข้อมูลส่วนบุคคลต่างๆ ได้อย่างง่ายดาย เนื่องจากฐานข้อมูลมีความเชื่อมโยงกัน และในการทำธุรกรรมใด ทางหน่วยงานนั้นๆ จะขอให้กรอกข้อมูลเลขประกันสังคมอยู่เสมอๆ ผู้ที่มักกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับหมายเลขประกันสังคมนี้ คือ บุคคลที่ไม่อยากจะจ่ายภาษีให้กับรัฐ หรืออาจเป็นพวกหลบหนีเข้าเมืองโดยผิดกฎหมาย หรือพวกชอบหนีหนี้ หรืออาจจะเป็นผู้กระทำความผิดที่ติดทัณฑ์บนอยู่ที่ต้องการจะเปลี่ยนแปลงประวัติของตัวเอง เป็นต้น

2.3.7 **การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของเด็ก** (Child Identity Theft)

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของเด็กเริ่มมีจำนวนเพิ่มมากขึ้นเรื่อยๆ เนื่องจากเด็กต่างมีหมายเลขประกันสังคม ใบสูติบัตร ที่สามารถจะทำธุรกรรมใดได้ แต่ในวัยเด็กมักจะยังไม่มีการทำธุรกรรมใด จนกว่าเด็กนั้นจะเติบโตพอที่จะเริ่มมีการติดต่อทำธุรกรรมโดย

อาศัยข้อมูลเอกลักษณ์ส่วนบุคคลของตนเอง ซึ่งผ่านไปเป็นเวลานานแล้วที่เอกลักษณ์บุคคลของตนนั้นถูกขโมยแล้วนำไปใช้ทำเรื่องเสื่อมเสียต่างๆ ทำให้ประวัติเครดิตของเด็กผู้บริสุทธิ์นั้นต้องด่างพร้อย ด้วยส่วนใหญ่อาชญากรที่ขโมยข้อมูลเอกลักษณ์บุคคลของเด็กไปก็จะนำไปขายให้กับผู้หลบหนีเข้าเมืองมาโดยผิดกฎหมาย เพื่อให้บุคคลเหล่านั้นนำไปใช้เปิดบัญชีธนาคาร หรือขอทำใบอนุญาตขับขี่ ฯลฯ[26]

2.3.8 **การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลแบบสังเคราะห์ หรือปลอม** (Synthetic Identity Theft)

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในรูปแบบนี้เป็นรูปแบบที่เกิดขึ้นล่าสุด โดยอาชญากรจะขโมยข้อมูลเอกลักษณ์บุคคลของเหยื่อหลายๆ คน แล้วนำมาปะปนกันให้เกิดเป็นบุคคลอีกคนหนึ่งขึ้นมา ดังนี้เมื่อมีการใช้ข้อมูลนั้นๆ ก็จะเกิดผลกระทบกับเหยื่อทุกๆ รายด้วย หรืออาจกล่าวได้ว่าอาชญากรจะนำข้อมูลของหลายๆ คนมาใช้โดยไม่ได้เจาะจงว่าตนเป็นเหยื่อคนใดคนหนึ่ง แต่เพียงพยายามทำให้ผู้อื่นเข้าใจว่าตนคือคนอื่นที่มิใช่เป็นบุคคลที่อาชญากรเป็นอยู่จริง[27]

2.4 **ความเสียหายที่เกิดจากการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล**

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล คือ การลักข้อมูลส่วนบุคคลของบุคคลอื่นไปใช้แสวงหาประโยชน์โดยมิชอบเพื่อตนเอง หรือผู้อื่น ซึ่งการกระทำนั้นย่อมมีผลกระทบ และเกิดความเสียหายแก่ผู้เป็นเจ้าของข้อมูล ยิ่งไปกว่านั้นย่อมส่งผลกระทบต่อระบบเศรษฐกิจ และความเชื่อมั่นของประชาชนต่อสถาบันทางการเงิน หรือองค์กรต่างๆ ที่ต้องเข้ามามีส่วนเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลด้วย เช่น บริษัทบัตรเครดิต ทั้งนี้บุคคลที่ได้รับผลกระทบมากที่สุด คือ บุคคลผู้เป็นเจ้าของข้อมูล

---

[26] Martin T. Biegelman, Identity Theft Handbook Detection,Prevention,and Security, p172.

[27] Jake Stroup, The 8 Types of Identity Theft [online], November 2012. Available from http://idtheft.about.com/od/Basics/a/The-8-Types-Of-Identity-Theft.htm.

2.4.1 **ความเสียหายที่มีผลกระทบต่อด้านการเงิน** (Financial Effects)

เมื่อถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลปัญหาร้ายแรง ความเสียหายอันดับต้นๆ ของเหยื่อมักจะเป็นปัญหาทางด้านการเงิน คือ มีประวัติที่ไม่ดีในทางการเงิน อาจทำให้เหยื่อต้องจ่ายดอกเบี้ยแพงในการประกันภัย หรือถูกปฏิเสธการขอสินเชื่อ หรือคำขอทำบัตรเครดิต อันเนื่องมาจากสิ่งที่ตัวเหยื่อเองมิได้เป็นผู้กระทำ ความผิดที่เกิดขึ้นบ่อยและสร้างปัญหาทางการเงินให้เหยื่อ เช่น กรณีอาชญากรที่โจรกรรมข้อมูลเหยื่อไปจะใช้ข้อมูลนั้นไปเปลี่ยนแปลงที่อยู่ในการส่งใบรายงานการใช้เครดิตการ์ดของเหยื่อ ให้ส่งไปที่อื่นแทน ดังนี้กว่าเหยื่อจะรู้ตัวว่าถูกนำข้อมูลไปใช้ประโยชน์อาชญากรก็ได้สร้างความเสียหายไว้เป็นจำนวนมากแล้ว และเมื่อทางสถาบันการเงินส่งเอกสารมาทวงถามการชำระเงิน เหยื่อก็จะไม่รู้ ทำให้ประวัติเครดิตเสียหาย หรือกรณีอาชญากรเอาข้อมูลเหยื่อไปเปิดบัญชีบัตรเครดิตขึ้นใหม่ในชื่อของเหยื่อ เมื่อไม่มีการชำระเงินก็เกิดประวัติทางการเงินที่ไม่ดี หรือกรณีเอาชื่อของเหยื่อไปเปิดบัญชีและมีการสั่งจ่ายเช็คในชื่อของเหยื่อ ซึ่งเมื่อเงินในบัญชีไม่มีจ่ายเหยื่อก็อาจถูกออกหมายจับได้ หรือกรณีมีการออกเช็คปลอม บัตรเครดิตปลอม บัตรเดบิตปลอม เพื่อเข้าถึงบัญชีของเหยื่อ ถอนเงินออกจากบัญชีของเหยื่อจนหมด เป็นต้น

2.4.2 **ความเสียหายที่มีผลกระทบต่อการบันทึกประวัติอาชญากรรม** (Criminal Effects)

เมื่อมีการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกิดขึ้น อาชญากรจำนวนไม่น้อยได้นำข้อมูลเอกลักษณ์บุคคลนั้นไปประกอบอาชญากรรมเพื่อให้ตนไม่ต้องถูกจับดำเนินคดี เช่น วงจรการค้ายาเสพติด เมื่อมีหลักฐานว่าชื่อของเหยื่อนั้นมีการกระทำความผิด แล้วไม่มีผู้กระทำความผิดตัวจริงไปยังศาล ก็จะมีการออกหมายจับ เหยื่อก็จะเดือดร้อน เสียหายกับสิ่งที่ตนมิได้เป็นคนสร้างขึ้น หรือถ้ากรณีเป็นการกระทำความผิดเล็กน้อย เช่น ทำผิดกฎจราจร ก็จะมีการบันทึกไว้ซึ่งตัวเหยื่อเองก็จะไม่รับรู้ กว่าเหยื่อจะรู้ว่ามีการอ้างใช้ชื่อเหยื่อกระทำความผิด เหยื่อก็อาจได้รับการปฏิบัติประหนึ่งเหยื่อเป็นอาชญากร และจะมีประวัติอาชญากรนั้นๆ ติดตามไปตลอด และในเรื่องการพิสูจน์ความบริสุทธิ์ว่าเหยื่อมิได้เป็นผู้กระทำความผิดนั้นๆ ก็เป็นเรื่องยาก อาจต้องเสียเวลาและค่าใช้จ่ายเป็นจำนวนมากด้วย

2.4.3 **ความเสียหายที่มีผลกระทบด้านความรู้สึก อารมณ์ หรือจิตใจ** (Emotional Effects)

เนื่องจากการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นการก่ออาชญากรรมที่ล่วงล้ำเข้ามาในข้อมูลเอกลักษณ์บุคคลของเหยื่อ เหยื่อต้องมามีประวัติที่ไม่ดี ต้องเสียเวลา เสียค่าใช้จ่ายในการต่อสู้ดำเนินคดี เพื่อพิสูจน์ความบริสุทธิ์ในสิ่งที่ตนมิได้เป็นผู้ก่อ หรือมีส่วนร่วมเลยแม้แต่น้อย สิ่งเหล่านี้จะทำให้อารมณ์ และจิตใจ ของเหยื่อตกต่ำ เกิดความรู้สึกเครียด ความไม่พอใจที่ตนต้องมาวุ่นวาย ไม่ได้ใช้ชีวิตตามปกติ เนื่องจากต้องมาดำเนินการ ดำเนินคดีเพื่อแก้ไขประวัติของตนเอง และเพื่อนำตัวอาชญากรที่กระทำความผิดตัวจริงมารับผิดชอบในความเสียหายที่เกิดขึ้น ความรู้สึกพ่ายแพ้ ความสับสน ความหวาดกลัวว่าตนจะถูกกระทำความผิดในลักษณะเช่นนี้อีกหรือไม่ หรือมีประวัติไม่ดีหรือความผิดอื่นๆ ที่กระทำลงโดยใช้ชื่อเหยื่ออีกหรือไม่ และในบางกรณีหากข้อมูลเอกลักษณ์บุคคลที่อาชญากรโจรกรรมไปได้ เนื่องมาจากความไม่ระมัดระวังของเหยื่อเป็นส่วนสำคัญแล้ว เหยื่อก็จะมีความรู้สึกโทษ โกรธตัวเองด้วย หรือในกรณีที่อาชญากรที่โจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของเหยื่อนั้นเป็นบุคคลที่สนิท ใกล้ชิดกับเหยื่อ เหยื่อก็จะมีความรู้สึกถูกทรยศหักหลังจากบุคคลนั้นๆ ซึ่งความสะเทือนใจต่างๆ เหล่านี้ของเหยื่อเป็นสิ่งที่ไม่สมควรเกิดขึ้น ดังนี้หากมีหน่วยงานเฉพาะเข้ามาให้การช่วยเหลือเหยื่ออาจช่วยลดความตึงเครียดของเหยื่อลงได้

2.4.4 **ความเสียหายที่ส่งผลกระทบในด้านอื่นๆ** (Additional Effects)

เมื่ออาชญากรโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลใดๆ ได้แล้ว ก็จะนำข้อมูลนั้นไปกระทำความผิดในหลายลักษณะ ทำให้เกิดผลกระทบกับเหยื่อในอีกหลายๆ ด้าน เช่น

- เหยื่อถูกปฏิเสธการจ้างงาน หรือการเลื่อนตำแหน่ง (Denial of Employment or Promotion) เนื่องจากในบริษัทบางแห่ง หรืองานในบางตำแหน่ง การจะรับบุคคลใดเข้าทำงาน หรือทำการเลื่อนตำแหน่งจะมีการตรวจสอบประวัติของบุคคลก่อน ดังนี้เมื่อบริษัทตรวจสอบพบประวัติที่ไม่ดีของเหยื่อ ไม่ว่าจะเป็นประวัติทางการเงิน หรือประวัติอาชญากรรม บริษัทก็จะปฏิเสธการจ้างงาน หรือการเลื่อนตำแหน่ง และบริษัท

ส่วนมากก็จะไม่บอกเหตุผลที่แท้จริงให้เหยื่อทราบ ทำให้เหยื่อต้องสูญเสียโอกาสดีๆ ในชีวิตไป

- ชื่อของเหยื่อปรากฏในรายชื่อบุคคลเฝ้าระวัง เป็นเรื่องที่กระทบต่อสถานะทางสังคมของเหยื่อเป็นอย่างมาก หากอาชญากรได้กระทำให้ชื่อของเหยื่อไปปรากฏที่รายชื่อผู้กระทำความผิดเกี่ยวกับเพศ หรือความผิดเกี่ยวกับการก่อการร้าย เหยื่อต้องได้รับความอับอายและอาจสูญเสียสิทธิ หรือเสรีภาพในบางเรื่อง เช่น อาจถูกห้ามเดินทางออกนอกประเทศ หรือเมื่อเหยื่อมีการย้ายบ้าน และเพื่อนบ้านใหม่ได้รับรู้ หรือตรวจสอบรายชื่อบุคคลที่กระทำความผิดเกี่ยวกับเพศ หรือความผิดอื่นๆ โดยที่เพื่อนบ้านใหม่นั้นไม่ได้รู้จักตัวเหยื่อมาก่อนจึงอาจก่อความเข้าใจผิด ระแวงสงสัย และไม่คบหาสมาคมกับเหยื่อได้
- เหยื่อถูกปฏิเสธการทำประกันสุขภาพ ในกรณีที่อาชญากรใช้ชื่อเหยื่อในการเข้ารับการตรวจรักษา และอาชญากรนั้นเป็นโรคร้ายแรง เช่น เป็นโรค HIV ประวัตินี้ก็จะถูกบันทึกไว้เมื่อเหยื่อมีคำขอทำประกันสุขภาพก็จะถูกปฏิเสธ
- ขาดคุณสมบัติในการทำใบอนุญาตขับขี่ใหม่ หรือต่ออายุในอนุญาต ในกรณีที่อาชญากรได้สร้างประวัติที่ไม่ดีไว้ให้เหยื่อ เช่น ได้รับใบสั่งหลายครั้งและมิได้ทำการชำระค่าปรับ หรือมีการกระทำผิดกฎหมายจราจรหลายครั้ง ทำให้เหยื่อไม่สามารถขอทำใบขับขี่ใหม่ หรือทำการต่ออายุใบอนุญาตขับขี่ได้ ฯลฯ

2.5 **การคุ้มครองข้อมูลส่วนบุคคลกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล**

ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะทางการเงินประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรมบรรดาที่มีชื่อของบุคคลนั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้ความหมายรวมถึงข้อมูลที่เกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย[28] กล่าวโดยสรุปข้อมูลส่วนบุคคล คือ ข้อเท็จจริง

[28] อ้างอิงคำนิยาม "ข้อมูลข่าวสารส่วนบุคคล" จากพระราชบัญญัติข้อมูลข่าวสารของข้าราชการ พ.ศ. 2540 มาตรา 4.

เกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม ข้อมูลส่วนบุคคลนี้ถือเป็นเรื่องสิทธิ และเสรีภาพของบุคคล

“สิทธิ” หมายความถึง อำนาจที่กฎหมายรับรองคุ้มครองให้แก่บุคคลในอันที่จะเรียกร้องให้บุคคลอื่นกระทำการอย่างใดอย่างหนึ่ง สิทธิจึงก่อให้เกิดหน้าที่แก่บุคคลอื่นด้วย[29]

“เสรีภาพ” หมายความถึง สภาพการณ์ที่บุคคลมีอิสระในการที่จะกระทำการอย่างใดอย่างหนึ่งตามความประสงค์ของตน[30]

เมื่อมนุษย์ทุกคนเกิดมาเมื่อมีสภาพบุคคลย่อมได้รับการคุ้มครองในสิทธิ และเสรีภาพ ซึ่งสิทธิ เสรีภาพพื้นฐานของมนุษย์สามารถแบ่งออกได้ 5 ประเภท[31] คือ

1.) เสรีภาพในชีวิตร่างกาย โดยความมั่นคงปลอดภัยในชีวิตร่างกายถือเป็นพื้นฐานของเสรีภาพอื่นๆ ทั้งหมด

2.) เสรีภาพในชีวิตส่วนตัว คือ บุคคลแต่ละคนมีอิสระที่จะปฏิเสธไม่ให้คนอื่นมาล่วงรู้เรื่องของตนได้ หรือกล่าวคือสิทธิเสรีภาพที่บุคคลจะเลือกมีชีวิตตามที่ต้องการ โดยปราศจากการรบกวนจากบุคคลอื่น เสรีภาพในชีวิตส่วนตัว ได้แก่ เสรีภาพในเคหสถาน เสรีภาพในการติดต่อสื่อสาร เสรีภาพในความลับของบุคคล เสรีภาพในข้อมูลส่วนบุคคล และรวมไปถึงการเคารพในการแสดงออกซึ่งบุคลิกลักษณะของบุคคล

3.) เสรีภาพในตัวบุคคล เป็นเสรีภาพที่บุคคลสามารถกระทำอะไรกับเนื้อตัวร่างกายของตนเองได้ภายใต้กรอบของกฎหมาย บุคคลอื่นจะก้าวล่วงเข้ามาขัดขวางการเคลื่อนไหวทางกายภาพของบุคคลไม่ได้ เช่น เสรีภาพในการเดินทางของบุคคล

4.) เสรีภาพทางปัญญาและศีลธรรม กล่าวคือ มนุษย์สามารถแสดงออกถึงสิ่งที่ตนเองคิดและมีความเชื่อได้อย่างเสรี

5.) เสรีภาพทางด้านเศรษฐกิจสังคม เป็นเสรีภาพที่มีลักษณะพิเศษในการประกอบอาชีพในทางเศรษฐกิจ

---

[29] วรพจน์ วิศรุตพิชญ์, สิทธิและเสรีภาพตามรัฐธรรมนูญ (กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, 2538), หน้า 21.

[30] เรื่องเดียวกัน, หน้า 22.

[31] เกรียงไกร เจริญธนาวัฒน์, หลักกฎหมายว่าด้วยสิทธิเสรีภาพ (กรุงเทพมหานคร: วิญญูชน, 2547), หน้า 26-30.

สิทธิในข้อมูลส่วนบุคคล จึงถือเป็นสิทธิพื้นฐานของมนุษย์ตามความหมายในข้อ2.) บุคคลทุกคนจึงมีสิทธิที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคล มิให้บุคคลอื่นสอดเข้าเกี่ยวข้องได้ อย่างไรก็ตาม เมื่อได้มีการบัญญัติรับรองเสรีภาพในข้อมูลส่วนบุคคลไว้ตามกฎหมาย ในฐานะที่เป็น สิทธิขั้นพื้นฐานหรือสิทธิตามธรรมชาติของมนุษย์ ซึ่งหมายถึงเป็นสิทธิประจำตัวของบุคคล ที่ได้รับการคุ้มครองจากกฎหมายมิให้ผู้อื่นมาล่วงล้ำสิทธิ เนื่องจากเป็นสิทธิที่จะไม่ถูกรบกวนแทรกแซงในชีวิตเกียรติยศ ชื่อเสียง เสรีภาพ ความเสมอภาค การดำรงชีวิต การทำงาน รวมถึงประโยชน์ส่วนตัวของบุคคล เช่น สิทธิที่จะไม่ถูกรบกวนความสงบสุข สิทธิในความลับของบุคคล วิชาชีพ การค้า สิทธิในชื่อ ในข้อมูลส่วนตัวที่จะไม่ถูกเปิดเผย หรือนำไปใช้ในทางที่ก่อความเสียหาย เมื่อบุคคลมีสิทธิดังกล่าว ก็จะก่อให้เกิดหน้าที่แก่บุคคลอื่นที่จะไม่กระทำการละเมิดสิทธิของบุคคลอื่น และถือเป็นอำนาจที่บุคคลหนึ่งจะปกป้องรักษาสิทธิของตน มีสิทธิเรียกร้องมิให้มีบุคคลอื่นมาแทรกแซงในชีวิตความเป็นอยู่ส่วนตัว หรือนำข้อมูลส่วนตัวของบุคคลไปใช้แสวงหาประโยชน์อันมิชอบ[32]

สิทธิในข้อมูลส่วนบุคคล เป็นสิทธิตามธรรมชาติจึงมิได้มีการบัญญัติรับรองไว้ แต่ต่อมาเมื่อสังคมขยายตัวมากขึ้น ทุกคนมีสิทธิ เสรีภาพในการจะกระทำการใดๆ ก็ได้ แต่การนั้นต้องไม่ละเมิดสิทธิ เสรีภาพของบุคคลอื่นๆ ด้วย เพื่อขจัดปัญหาการละเมิดสิทธิ เสรีภาพของกันและกัน จึงต้องมีกฎหมายบัญญัติชัดเจนถึงขอบเขตของสิทธิ และเสรีภาพของบุคคล โดยประเทศต่างๆ ก็ได้บัญญัติรับรองสิทธิในข้อมูลส่วนบุคคลไว้ในกฎหมายภายในของประเทศตน ในส่วนของกฎหมายระหว่างประเทศที่ถือเป็นหลักกฎหมายสากล ก็มีบัญญัติรับรองสิทธินี้ไว้เช่นกัน ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 ขององค์การสหประชาชาติ (Universal Declaration of Human Rights 1948) ในข้อ 12 ว่า “บุคคลใดๆ ย่อมไม่ถูกแทรกแซงโดยพลการในความเป็นอยู่ส่วนตัว ในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือไม่อาจถูกลบหลู่ในเกียรติยศและชื่อเสียง ทั้งนี้ บุคคลทุกคนย่อมมีสิทธิที่จะได้รับการปกป้องคุ้มครองโดยกฎหมายอันเนื่องจากการก้าวล่วงในสิทธินั้น”[33] กล่าวคือข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของสิทธิในความเป็นอยู่ส่วนตัว จึงถือเป็นสิ่งที่ได้รับการคุ้มครองตามปฏิญญานี้ด้วย นอกจากนั้นในกติการะหว่าง

---

[32] ชูชีพ ปิณฑะสิริ,”การละเมิดสิทธิส่วนตัว,” (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์), หน้า4.

[33] สราวุธ ปิติยาศักดิ์, กฎหมายเทคโนโลยีสารสนเทศ (กรุงเทพมหานคร: สำนักพิมพ์นิติธรรม, 2555), หน้า 241.

ประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights-ICCPR) ซึ่งมีผลบังคับในปี ค.ศ. 1976 ในข้อ 17 ได้กำหนดให้ประเทศภาคีสมาชิกมีพันธะผูกพันในการให้ความเคารพต่อสิทธิในข้อมูลส่วนบุคคลด้วย[34] ซึ่งประเทศไทยเข้าร่วมเป็นภาคีสมาชิกเมื่อวันที่ 29 ตุลาคม พ.ศ. 2539 และมีผลใช้บังคับเมื่อวันที่ 30 มกราคม พ.ศ. 2540[35] กล่าวคือข้อมูลส่วนบุคคลจะต้องได้รับการคุ้มครอง ข้อมูลส่วนบุคคลต้องไม่ถูกเปิดเผยหรือละเมิดเว้นแต่กรณีที่มีความจำเป็นอย่างยิ่งเท่านั้น

สิทธิในความเป็นส่วนตัวหรือ สิทธิส่วนบุคคล(Right to privacy) ที่ประชุม ICJ (International Commission of Jurists) ได้ให้ความหมายไว้ในการประชุมเมื่อปี 1967 ที่กรุงสต็อกโฮล์มประเทศสวีเดน ว่าเป็น “สิทธิที่จะอยู่โดยลำพังโดยมีการรบกวนการแทรกแซงในระดับที่น้อยที่สุด”ซึ่งมีการขยายความว่า หมายถึงสิทธิของปัจเจกชนที่จะดำเนินชีวิตโดยได้รับการคุ้มครองจากสิ่งเหล่านี้ คือ

1. การแทรกแซงในชีวิตความเป็นส่วนตัว ครอบครัว และเคหะสถาน

2. การแทรกแซงในทางกายภาพ หรือในทางจิตใจ หรือศีลธรรมและเสรีภาพในทางความคิด

3. การกระทำต่อเกียรติยศและชื่อเสียง

4. การไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนความจริง ซึ่งทำให้เป็นที่เสื่อมเสียในสายตาของสาธารณชน

5. การเปิดเผยข้อเท็จจริงที่ไม่ถูกต้องอันเป็นที่น่าอับอายเกี่ยวกับชีวิตความเป็นส่วนตัว

6. การใช้ชื่อหรือเครื่องหมายชี้เฉพาะหรือภาพโดยไม่มีอำนาจ

7. การสืบความลับ การสอดรู้สอดเห็น การติดตามเฝ้าดู และการรบกวน

8. การแทรกแซงการติดต่อสื่อสารระหว่างกัน

---

[34] International Covenant on Civil and Political Rights Article 17

“1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks”

[35] กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง [ออนไลน์], พฤศจิกายน 2555, แหล่งที่มา http://www.mfa.go.th/humanrights/images/stories/iccprt.pdf.

9. การเปิดเผยข้อมูลข่าวสารที่เป็นความลับ ซึ่งผู้กระทำได้รับมาอันเนื่องมาจากการประกอบวิชาชีพนั้น

10. การใช้งานในทางที่มิชอบซึ่งการติดต่อสื่อสารส่วนบุคคล

ดังนั้น อาจกล่าวได้ว่าขอบเขตที่บุคคลควรได้รับการคุ้มครองและการเคารพในสิทธิความเป็นส่วนตัวก็คือการดำรงชีวิตอย่างเป็นอิสระ มีสิทธิที่จะแสวงหาความสุขในชีวิตตามวิถีทางที่อาจเป็นไปได้และเป็นความพอใจตราบเท่าที่ไม่ขัดต่อกฎหมาย ไม่ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชนและไม่เป็นการล่วงละเมิดสิทธิเสรีภาพของผู้อื่น

สิทธิความเป็นส่วนตัว (Right to Privacy) สามารถจำแนกออกได้เป็น 4 ประเภท ดังนี้

1. ความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลหรือข้อมูลส่วนตัว (Information Privacy)
2. ความเป็นส่วนตัวเกี่ยวกับเนื้อตัวและร่างกาย (Bodily Privacy)
3. ความเป็นส่วนตัวในการติดต่อสื่อสาร (Privacy of Communication)
4. ความเป็นส่วนตัวในการอยู่หรือพักอาศัย (Territorial Privacy)

สิทธิในข้อมูลซึ่งแสดงเอกลักษณ์บุคคลอยู่ในส่วนที่เกี่ยวกับข้อมูลส่วนบุคคล (Information Privacy) ดังนี้ผู้เขียนจึงขออธิบายรายละเอียดเฉพาะสิทธิส่วนบุคคลในส่วนที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ดังนี้

ความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลหรือข้อมูลส่วนตัว (Information Privacy) เป็นการให้ความคุ้มครองข้อมูลส่วนบุคคลโดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคลทั้งนี้ ความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลหรือข้อมูลส่วนตัวนั้น มีหลักการสากลที่เป็นกรอบในการคุ้มครองข้อมูลส่วนบุคคล (Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data) ขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) ซึ่งหลักเกณฑ์ดังกล่าว ประกอบด้วย

(ก.) หลักข้อจำกัดในการเก็บรวบรวมข้อมูล สาระสำคัญ คือ ในการเก็บรวบรวมข้อมูลนั้นต้องชอบด้วยกฎหมายและต้องใช้วิธีการที่เป็นธรรมและเหมาะสมโดยในการเก็บรวบรวมข้อมูลนั้นต้องให้เจ้าของข้อมูลรู้เห็น รับรู้หรือได้รับความยินยอมจากเจ้าของข้อมูล

(ข.) หลักคุณภาพของข้อมูล สาระสำคัญคือ ข้อมูลที่เก็บรวบรวมนั้นต้องเกี่ยวข้องกับวัตถุประสงค์ที่กำหนดขึ้นว่า“จะนำไปใช้ทำอะไร” และเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ใน

การดำเนินงานของหน่วยงานตามที่กฎหมายกำหนดนอกจากนั้นข้อมูลดังกล่าวจะต้องถูกต้องสมบูรณ์หรือทำให้เป็นปัจจุบันหรือทันสมัยอยู่เสมอ

(ค.)หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ สาระสำคัญ คือต้องกำหนดวัตถุประสงค์ว่าข้อมูลที่มีการเก็บรวบรวมนั้นเก็บรวมรวมไปเพื่ออะไรพร้อมทั้งกำหนดระยะเวลาที่เก็บรวบรวมหรือรักษาข้อมูลนั้นตลอดจนกรณีที่จำเป็นต้องมีการเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวมข้อมูลเช่นว่านั้นไว้ให้ชัดเจน

(ง.) หลักข้อจำกัดในการนำไปใช้ สาระสำคัญคือ ข้อมูลส่วนบุคคลนั้นจะต้องไม่มีการเปิดเผย ทำให้มี หรือปรากฏในลักษณะอื่นใดซึ่งไม่ได้กำหนดไว้โดยชัดแจ้งในวัตถุประสงค์ของการเก็บรวบรวมข้อมูลเว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลหรือโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

(จ.) หลักการรักษาความมั่นคงปลอดภัยข้อมูล สาระสำคัญ คือจะต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมเพื่อป้องกันความเสี่ยงภัยใดๆ ที่อาจจะทำให้ข้อมูลนั้นสูญหาย เข้าถึง ทำลาย ใช้ ดัดแปลงแก้ไข หรือเปิดเผยโดยมิชอบ

(ฉ.) หลักการเปิดเผยข้อมูล สาระสำคัญ คือ ควรมีการประกาศนโยบาย ให้ทราบโดยทั่วกัน หากมีการปรับปรุงแก้ไขหรือพัฒนาแนวนโยบายหรือแนวปฏิบัติที่เกี่ยวกับข้อมูลส่วนบุคคลก็ควรเปิดเผยหรือประกาศไว้ให้ชัดเจน รวมทั้งให้ข้อมูลใดๆที่สามารถระบุเกี่ยวกับหน่วยงานของรัฐผู้ให้บริการ ที่อยู่ ผู้ควบคุมข้อมูลส่วนบุคคลด้วย

(ช.) หลักการมีส่วนร่วมของบุคคล สาระสำคัญ คือให้บุคคลซึ่งเป็นเจ้าของข้อมูลได้รับแจ้งหรือยืนยันจากหน่วยงานของรัฐที่เก็บรวบรวมหรือจัดเก็บข้อมูลทราบว่า“หน่วยงานของรัฐนั้นๆได้รวบรวมข้อมูลหรือจัดเก็บข้อมูลส่วนบุคคลดังกล่าวหรือไม่ภายในระยะเวลาที่เหมาะสม”

(ซ.) หลักความรับผิดชอบ สาระสำคัญคือ ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล[36]

สำหรับประเทศไทยสิทธิในข้อมูลส่วนบุคคล เป็นสิทธิที่ได้รับการรับรอง และคุ้มครองตามกฎหมายรัฐธรรมนูญแห่งราชอาณาจักรไทย โดยในรัฐธรรมนูญฉบับปัจจุบันได้บัญญัติรับรองสิทธิไว้ในมาตรา 35 ความว่า

---

[36] บรรเจิด สิงคะเนติ และคณะ, รายงานวิจัยฉบับสมบูรณ์ เรื่อง ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Right to Privacy) (กรุงเทพมหานคร: สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ), หน้า 3 - 6.

“สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง

การกล่าว หรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว จะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ”

จากการที่มีกฎหมายสูงสุดของประเทศได้บัญญัติรับรอง และให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคลไว้แบบกว้างๆ เช่น ในสิทธิความเป็นส่วนตัว สิทธิในการได้รับความคุ้มครองข้อมูลส่วนบุคคล คือข้อมูลส่วนบุคคลต้องไม่ถูกนำไปแสวงหาประโยชน์โดยมิชอบ หรือถูกเปิดเผย เว้นแต่มีกฎหมายบัญญัติให้เปิดเผยได้ ดังนี้ในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้มีการบัญญัติคุ้มครองข้อมูลข่าวสารส่วนบุคคลไว้ ในส่วนของการจัดเก็บและเปิดเผยข้อมูลข่าวสารส่วนบุคคล ดังนี้ หน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคลดังต่อไปนี้

1. ต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้อง และจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น และยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น

2. พยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น
3. จัดให้มีการตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับสิ่งดังต่อไปนี้

   (ก) ประเภทของบุคคลที่มีการเก็บข้อมูลไว้

   (ข) ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล

(ค) ลักษณะการใช้ข้อมูลตามปกติ

(ง) วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล

(จ) วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล

(ฉ) แหล่งที่มาของข้อมูล

4. ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ

5. จัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคล ตามความเหมาะสม เพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

ในกรณีที่เก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบล่วงหน้าหรือพร้อมกับการขอข้อมูลถึงวัตถุประสงค์ที่จะนำข้อมูลมาใช้ ลักษณะการใช้ข้อมูลตามปกติ และกรณีที่ขอข้อมูลนั้นเป็นกรณีที่อาจให้ข้อมูลได้โดยความสมัครใจหรือเป็นกรณีมีกฎหมายบังคับ และหน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้ เว้นแต่เป็นไปตามลักษณะการใช้ข้อมูลตามปกติ ซึ่งโดยหลักแล้วหน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่เป็นการเปิดเผยดังต่อไปนี้

1. การเปิดเผยต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตน เพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น

2. การใช้ข้อมูลเป็นไปตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น

3. การเปิดเผยต่อหน่วยงานของรัฐที่ทำงานด้วยการวางแผน หรือการสถิติ หรือสำมะโนต่างๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

4. การเปิดเผยเพื่อประโยชน์ในการศึกษาวิจัย โดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด

5. การเปิดเผยต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐเพื่อการตรวจดูคุณค่าในการเก็บรักษา

6. การเปิดเผยต่อเจ้าหน้าที่ของรัฐ เพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม

7. การเปิดเผยเป็นการซึ่งจำเป็น เพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

8. การเปิดเผยต่อศาล และเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว

ดังนี้เห็นได้ว่ากฎหมายไทยที่มีอยู่ในปัจจุบันมีการบัญญัติให้ความคุ้มครองข้อมูลส่วนบุคคลไว้ โดยการกำหนดวิธีจัดเก็บ และการนำข้อมูลไปใช้ของหน่วยงานของรัฐ แต่มิได้มีการบัญญัติเอาผิดแก่บุคคลที่โจรกรรมข้อมูลของบุคคลอื่นไปใช้โดยมิชอบแต่อย่างใด ผู้เขียนจึงมีความเห็นว่าควรนำหลักการการให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลนี้ ไปใช้เป็นหลักในการบัญญัติความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

2.6 สาเหตุและปัญหาการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่เกิดขึ้นในประเทศไทย

ปัจจุบันอาจกล่าวได้ว่าการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้เกิดขึ้นเป็นจำนวนมากกว่าในอดีต อาจเนื่องมาจากความเจริญก้าวหน้าทางเทคโนโลยีที่ทำให้การโจรกรรมข้อมูลเกิดได้ง่ายขึ้น โดยลักษณะของการกระทำความผิดคือการขโมยข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของบุคคลอื่นไป แล้วนำไปใช้ในทางที่มิชอบเพื่อแสวงหาประโยชน์ในรูปแบบต่างๆ ทั้งนี้ อาจแบ่งเป็นสาเหตุหลักได้ 3 หลักใหญ่ๆ ดังนี้

1. **การเกิดแรงจูงใจในด้านต่าง ๆ ให้กระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล**

(ก) แรงจูงใจด้านผลประโยชน์ตอบแทนหรือทรัพย์สิน กล่าวคือ ผู้โจรกรรมข้อมูลตัดสินใจกระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเนื่องมาจากคำนึงถึงผลตอบแทนทางการเงินที่ตนจะได้รับ เช่น ผู้โจรกรรมข้อมูลมีปัญหาทางการเงิน ด้วยฐานะของตนไม่อาจใช้จ่ายเพื่อซื้อสิ่งของต่างๆ ที่ตนต้องการได้และเห็นว่าการกระทำความผิดจะทำให้ตนได้รับผลตอบแทนสูง ตัวอย่างคดีที่เกิดขึ้น เช่น กองปราบจับเซลส์บัตรเครดิตอดีตหนุ่มธนาคาร เอาหลักฐานส่วนตัวของลูกค้ากว่า 100 ราย ไปขอทำบัตรเครดิตกับธนาคารอื่น แล้วนำบัตรไปกดเงินสดเพื่อนำเงินไปใช้ส่วนตัว สร้างความเสียหายให้ธนาคารหลายแห่ง รวมมูลค่าความเสียหายกว่า 5 ล้านบาท หลังจากถูกจับ ได้ประกันตัวไป และในระหว่างศาลพิจารณาคดี ผู้ต้องหากลับไปก่อคดีซ้ำอีก มูลค่าความเสียหายอีก 5 ล้านบาท จนสุดท้ายถูกตำรวจจับได้ ยอมรับสารภาพโดยให้เหตุผลว่าที่ตนกระทำความผิดไปเนื่องจากตนไม่มีรายได้ เพราะไม่มีงานทำ[37]หรือแรงจูงใจในการเลียนแบบพฤติกรรมของคนที่ตนคบหาสมาคมด้วย เมื่อเห็นบุคคลอื่นสามารถกระทำความผิดสำเร็จ และได้ผลประโยชน์ตอบแทนเป็นจำนวนเงินสูงมาก จึงเกิดความคิดที่จะกระทำเลียนแบบ

(ข) แรงจูงใจด้านความรู้สึก ความภาคภูมิใจ กล่าวคือ ผู้โจรกรรมข้อมูลตัดสินใจกระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเนื่องมาจากคิดว่าตนเป็นบุคคลที่มีทักษะในการโจรกรรมข้อมูลสูง หรือกล่าวคือมีทักษะของอาชญากร (criminal skills)[38] คิดว่าการกระทำความผิดเป็นงานที่ท้าทายเมื่อตนทำได้สำเร็จจะเกิดความภาคภูมิใจ เช่น บุคคลที่มีความเชี่ยวชาญด้านระบบคอมพิวเตอร์ที่มีความซับซ้อนจะเกิดความภาคภูมิใจเมื่อตนสามารถเข้าไปโจรกรรมข้อมูลในระบบคอมพิวเตอร์ของผู้อื่นได้

---

[37] อดีตหนุ่มแบงก์แสบ สวมรอยบัตรลูกค้า รูดปรื๊ดนับสิบล้าน, หนังสือพิมพ์ไทยรัฐ [ออนไลน์], วันที่ 21 มิถุนายน 2554, แหล่งที่มา http://www.thairath.co.th/today/view/180573.

[38] ปกรณ์ มณีปกรณ์, อาชญาวิทยาและทัณฑวิทยา, พิมพ์ครั้งที่ 2 (กรุงเทพมหานคร: เอ็ม.ที.เพรส, 2553), หน้า 218.

2. **ความเจริญก้าวหน้าทางด้านเทคโนโลยี ทำให้การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลกระทำได้ง่าย และสะดวกมากขึ้น**

ในอดีตช่วงที่เทคโนโลยียังไม่มีความเจริญอย่างเช่นในปัจจุบัน การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลต้องกระทำโดยวิธีสามัญทั่วไป คือ การลักทรัพย์ ซึ่งการกระทำความผิดในลักษณะนี้มีความเสี่ยงสูงในการโดนจับกุม ดำเนินคดี การกระทำความผิดจึงยังคงเกิดขึ้นเป็นจำนวนไม่มากนัก แต่เมื่อเทคโนโลยีมีความเจริญก้าวหน้ามากขึ้น วิธีการโจรกรรมข้อมูลก็ทำได้ง่ายขึ้น เนื่องจากมีโปรแกรมคอมพิวเตอร์ต่างๆ เป็นเครื่องมือช่วยให้สามารถโจรกรรมข้อมูลได้สะดวกมากขึ้น และยากต่อการถูกติดตามจับกุมดำเนินคดีด้วย ทำให้การกระทำความผิดทวีจำนวนมากยิ่งขึ้น

3. **การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่มีความเกี่ยวข้องกับกระบวนการอาชญากรรม**

(ก) กระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเพื่อไปกระทำความผิดที่ร้ายแรงอื่นๆ เช่น การก่อการร้าย ขบวนการค้ายาเสพติดข้ามชาติ ฯลฯ ตัวอย่างกรณีการก่อการร้ายที่เกิดขึ้นในต่างประเทศ เช่น เหตุการณ์ก่อการร้ายที่เกิดขึ้นเมื่อวันที่ 11 กันยายน 2011 ที่กลุ่มอัลกออิดะห์จี้อากาศยานเพื่อพุ่งชนตึกเวิร์ด เทรดเซ็นเตอร์ในนครนิวยอร์ก ประเทศสหรัฐอเมริกา ซึ่งลักษณะของการกระทำ คือ ผู้ก่อการร้ายจะใช้ข้อมูลส่วนตัวของบุคคลอื่นเพื่อทำการเช่าห้องพัก (apartment) เช่าสำนักงาน (office space) เช่าตู้ไปรษณีย์ (post office boxes) เช่ายานพาหนะ (vehicles) และตู้เก็บของ (storage lockers) เปิดใช้บริการโทรศัพท์เคลื่อนที่ และการให้บริการสาธารณูปโภคอื่นๆ ในนามของบุคคลที่ถูกโจรกรรมข้อมูลมา เพื่อดำเนินการต่างๆ ตามแผนการก่อการร้าย[39] หรือกรณีที่เกิดขึ้นในประเทศไทย คือการใช้ข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นในการเปิดหมายเลขโทรศัพท์เคลื่อนที่เพื่อใช้เป็นเครื่องมือในการวางระเบิด หรือการดำเนินการก่อการร้าย ฯลฯ

(ข) กระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเพื่อต้องการลบล้างประวัติที่ไม่ดีของตน และไม่ต้องการให้ผู้อื่นรู้ว่าตนเคยมีประวัติไม่ดีมาก่อน เช่น ประวัติอาชญากรรม

---

[39] Martin T. Biegelman, Identity Theft Handbook Detection,Prevention,and Security, p 227.

(ค) กระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลโดยถือเป็นการทำธุรกิจอย่างหนึ่ง คือ ทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นมา แล้วนำไปจำหน่ายจ่ายโอนต่อไป เพื่อหวังผลประโยชน์ทางด้านทรัพย์สินเงินทอง

การเปลี่ยนแปลงทางสังคมมีผลต่อการเกิดอาชญากรรม ไม่ว่าจะเป็นการเปลี่ยนแปลงเนื่องมาจากสาเหตุใด[40] เช่น การเพิ่มของจำนวนประชากรก็ทำให้สังคมมีความซับซ้อนมากขึ้น และการที่มีประชากรเพิ่มขึ้นทำให้เกิดปัญหาต่างๆ ตามมา เช่น ปัญหาที่อยู่อาศัย การประกอบอาชีพ การว่างงาน ปัญหาเศรษฐกิจ ซึ่งความยากจนอาจเป็นปัญหาสำคัญที่ทำให้ทุกคนต่างต้องดิ้นรนต่อสู้เพื่อความอยู่รอด ซึ่งบางคนอาจหาทางออกด้วยการกระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่เกี่ยวข้องกับผลประโยชน์ทางทรัพย์สิน ทำให้เกิดปัญหาอาชญากรรม หรืออาจเกิดจากการเปลี่ยนแปลงทางเทคโนโลยี โลกในยุคโลกาภิวัฒน์มีการเปลี่ยนแปลงทางเทคโนโลยีมาก มีนวัตกรรมใหม่ๆ เกิดขึ้นอยู่เสมอๆ เช่น คอมพิวเตอร์ ระบบอินเตอร์เน็ต ซึ่งสิ่งเหล่านี้เมื่อนำไปใช้ในทางที่ผิดก็จะทำให้เกิดปัญหาอาชญากรรมได้ เช่น นำเทคโนโลยีมาเป็นเครื่องมือช่วยในการโจรกรรมข้อมูล มีการสร้างเครื่องมือที่ใช้ในการปลอมบัตรอิเล็กทรอนิกส์[41] ฯลฯ ปัญหาอาชญากรรมเหล่านี้จะลดลง หรือถูกปราบปรามได้ก็ด้วยการมีกฎหมายที่สามารถนำมาบังคับใช้ได้อย่างมีประสิทธิภาพ ดังนี้ปัญหาที่เกิดขึ้น คือ ประเทศไทยยังไม่มีบทกฎหมายเฉพาะที่จะนำมาบังคับใช้กับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล กฎหมายที่เกี่ยวข้องที่นำมาบังคับใช้ก็ไม่มีความครอบคลุมในทุกลักษณะของความผิดที่เกิดขึ้น ทำให้ในบางกรณีไม่อาจนำตัวผู้กระทำการโจรกรรมข้อมูลมาลงโทษตามกฎหมายได้ ทำให้เกิดปัญหาการกระทำความผิดเพิ่มมากขึ้นด้วยอันเนื่องมาจากปัญหาทางพยานหลักฐาน ด้วยลักษณะของการกระทำความผิดเป็นการยากที่จะติดตามหาตัวผู้กระทำความผิด โดยเฉพาะกรณีที่กระทำการโจรกรรมข้อมูลโดยใช้เทคโนโลยีเป็นเครื่องมือ เนื่องจากกว่าผู้ถูกโจรกรรมจะรับรู้ถึงการถูกนำข้อมูลส่วนบุคคลไปใช้ในทางที่มิชอบ ความเสียหายก็ได้เกิดขึ้นมาเป็นเวลานานแล้ว การสืบหาพยานหลักฐานต่างๆ เพื่อ

---

[40] โสภา ชปีลมันน์, อาชญากรรม: ปัญหาที่ควรแก้ไขในสังคมปัจจุบัน, (กรุงเทพมหานคร: โรงพิมพ์ไทยวัฒนาพานิช), หน้า 22.

[41] นวลจันทร์ ทัศนชัยกุล, อาชญากรรม การป้องกัน: การควบคุม, พิมพ์ครั้งที่ 2 (นนทบุรี: พรทิพย์การพิมพ์, 2548), หน้า 21-23.

จะนำตัวผู้กระทำความผิดมาลงโทษจึงกระทำได้ยาก อีกทั้งผู้กระทำความผิดอาจโอน หรือจำหน่ายข้อมูลที่โจรกรรมมาต่อไปหลายทอดยิ่งทำให้ยากต่อการติดตามจับกุมผู้กระทำความผิดทั้งหมด

บทที่ 3

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลตามกฎหมายต่างประเทศและกฎหมายไทย

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล หากเป็นการลักเอาตัวเอกสาร หรือลักข้อมูลไปแล้วทำการปลอมเอกสารใดๆ ขึ้น เพื่อนำไปใช้แสวงหาผลประโยชน์อันมิชอบ การกระทำเช่นนั้นอาจเป็นความผิดตามประมวลกฎหมายอาญาในความผิดฐานปลอมเอกสาร ลักทรัพย์ และเป็นความผิดประกอบการกระทำในความผิดฐานฉ้อโกง หรือเป็นความผิดตามกฎหมายฉบับอื่นๆ ได้ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ฯลฯ แต่ในบางลักษณะความผิดของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไม่มีกฎหมายบัญญัติเป็นความผิด เช่น การจดจำหมายเลขบัตรเครดิตของผู้อื่นไปใช้โดยมิชอบ ซึ่งแตกต่างจากกฎหมายของต่างประเทศที่มีการบัญญัติฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะ เช่น พระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ. 1998 ของประเทศสหรัฐอเมริกา และในประมวลกฎหมายอาญาของประเทศแคนาดา จึงเห็นควรศึกษาเปรียบเทียบกฎหมายต่างประเทศและกฎหมายไทยในปัจจุบันเพื่อจะได้นำมาวิเคราะห์และเสนอแนะแนวทางในการบัญญัติกฎหมายที่เหมาะสมกับประเทศไทยต่อไป

3.1 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลตามกฎหมายต่างประเทศ

วิทยานิพนธ์ฉบับนี้ศึกษากฎหมายเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของ 3 ประเทศ โดยประเทศที่มีการบัญญัติให้การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) เป็นความผิดเฉพาะ คือ ประเทศสหรัฐอเมริกา และประเทศแคนาดา อย่างไรก็

ตามแม้ประเทศ สหราชอาณาจักรจะมิได้มีการบัญญัติฐานความผิดเฉพาะสำหรับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้โดยเฉพาะ แต่มีกฎหมายที่เกี่ยวข้องหลายฉบับที่สามารถนำมาปรับใช้กับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้ในบางกรณี จึงควรศึกษาเปรียบเทียบกฎหมายของแต่ละประเทศเพื่อให้เห็นความแตกต่าง เพื่อเป็นแนวทางในการกำหนดความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่เหมาะสมสำหรับประเทศไทยต่อไป

3.1.1 กฎหมายเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาถือเป็นประเทศแรกๆ ที่ได้กำหนดให้การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นความผิดอาญา เนื่องจากได้พบการกระทำความผิดในรูปแบบนี้เกิดขึ้นก่อนประเทศอื่น และมีการกระทำความผิดในลักษณะนี้เป็นจำนวนมาก ซึ่งก่อความเสียหายอย่างมากต่อระบบเศรษฐกิจของประเทศสหรัฐอเมริกา[1] ตัวอย่างกรณีการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่เกิดขึ้นในประเทศสหรัฐอเมริกาเป็นครั้งแรก คือ ในช่วงปีคริสตศักราช 1935 ได้มีการประกาศใช้พระราชบัญญัติการรักษาความปลอดภัยทางสังคม (Social Security Act) ทำให้เกิดการใช้หมายเลขประกันสังคมกันอย่างแพร่หลายในประเทศสหรัฐอเมริกา บริษัทผลิตกระเป๋าเฟอร์รี่ในเมืองนิวยอร์ก (Ferree Company of Lockport, New York) ได้ออกแบบกระเป๋าให้มีช่องใส่บัตรประกันสังคม (Social Security Card) โดยได้ทำสำเนาบัตรของพนักงานตนเพื่อใช้เป็นบัตรตัวอย่าง คือบัตรของนางฮิลด้า วิชเชอร์ (Hilda Whitcher) กระเป๋าได้ถูกจำหน่ายออกไปเป็นจำนวนมาก จนในปี 1943 พบว่ามีคนใช้หมายเลขประกันสังคมของนางฮิลด้าถึง 5,700 คน หน่วยงานรักษาความปลอดภัยทางสังคม (Social Security Administration, SSA) จึงต้องทำการออกหมายเลขประกันสังคมให้กับนางฮิลด้าใหม่เพื่อแก้ไขปัญหาที่ถูกบุคคลอื่นนำหมายเลขประกันสังคมไปใช้โดยไม่ชอบด้วยกฎหมาย ในช่วงที่เกิดปัญหานี้เป็นช่วงที่ยังไม่มีการใช้บัตร

[1] Martin T. Biegelman, Identity Theft Handbook Detection,Prevention,and Security (New Jersey: John Wiley & Sons, Inc, 2009), p.xix.

เครดิตที่แพร่หลาย ทำให้ความเสียหายยังเกิดขึ้นไม่มากนัก[2] แต่ต่อมาเมื่อสภาพสังคมเปลี่ยนแปลงไป รูปแบบการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลก็ได้พัฒนาอย่างต่อเนื่องจนกระทั่งในปี 1998 ประเทศสหรัฐอเมริกาจึงได้มีการบัญญัติกฎหมายขึ้นเพื่อบังคับใช้กับฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลโดยเฉพาะ เพื่อเป็นการปราบปราม และป้องกันมิให้มีการกระทำความผิดเช่นนี้ต่อไป หรือเพิ่มจำนวนสูงขึ้น หรือทวีความร้ายแรงมากขึ้น ซึ่งเป็นกฎหมายในระดับรัฐบาลกลาง (Federal Law) ได้แก่กฎหมายที่มีชื่อว่า พระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) ซึ่งเมื่อมีการบังคับใช้กฎหมายนี้ จำนวนอาชญากรรมการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลก็มีจำนวนลดน้อยลง[3] ผู้เขียนจึงขออธิบายถึงการกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในกฎหมายฉบับนี้ และกฎหมายอื่น ที่มีความเกี่ยวข้องเชื่อมโยงกับการกระทำความผิด ดังนี้

3.1.1.1 **พระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ. 1998 (The Identity Theft and Assumption Deterrence Act of 1998)**

วัตถุประสงค์หลักของพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) มี 4 ข้อ คือ

1.) กำหนดให้ผู้ที่ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (ผู้เป็นเจ้าของข้อมูล) เป็นผู้เสียหาย ซึ่งเดิมมีเพียงบริษัทผู้ออกบัตรเครดิตเท่านั้นที่เป็นผู้เสียหาย

2.) ให้อำนาจแก่หน่วยงานของรัฐ เช่น หน่วยงาน FBI และหน่วยงานอื่นๆ ที่บังคับใช้กฎหมายมีอำนาจสอบสวนคดีในความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

3.) หากมีการตัดสินว่ามีการกระทำความผิดเกิดขึ้นจริง ให้สิทธิแก่ผู้เสียหายในการเรียกร้องค่าเสียหาย หรือมีมาตรการต่างๆ ในการเยียวยาผู้เสียหาย

---

[2] Ibid, p.14.

[3] Identity Theft [online] November 2012, Available from http://en.wikipedia.org/wiki/Identity_theft.

4.) กำหนดให้หน่วยงานคณะกรรมาธิการการค้าของรัฐบาลกลาง (The Federal Trade Commission หรือ FTC) เป็นหน่วยงานเฉพาะที่ทำหน้าที่รับเรื่องราวร้องทุกข์ และดำเนินการต่างๆ ที่เกี่ยวข้องกับการกระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

พระราชบัญญัติฉบับนี้เมื่อบัญญัติออกมายังผลให้เกิดการแก้ไขประมวลกฎหมายของสหรัฐอเมริกา (U.S. Code) ในหมวดที่ 18 มาตรา 1028 ซึ่งได้ให้ความหมายของการกระทำความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้ดังนี้ ผู้ใดโดยเจตนากระทำการโอน ครอบครอง หรือใช้ประโยชน์จากข้อมูลเอกลักษณ์บุคคลของบุคคลอื่นโดยไม่ได้รับอนุญาต เพื่อกระทำการผิดกฎหมายของสหรัฐอเมริกา (กฎหมายรัฐบาลกลางหรือ federal law) หรือได้ให้ความช่วยเหลือ หรือให้การสนับสนุนในการกระทำที่ผิดกฎหมายดังกล่าว อันก่อให้เกิดการละเมิดกฎหมายหรือก่อให้เกิดความผิดอาญาร้ายแรงภายใต้กฎหมายของมลรัฐใด หรือภายใต้กฎหมายท้องถิ่นใดที่มีผลใช้บังคับอยู่ ผู้นั้นสมควรได้รับโทษตามกฎหมาย[4] และพระราชบัญญัติฉบับนี้ยังได้มีการกำหนดหน่วยงานที่รับผิดชอบโดยตรงเกี่ยวกับการกระทำความผิดนี้ด้วย คือ คณะกรรมาธิการการค้าของรัฐบาลกลาง (The Federal Trade Commission หรือ FTC) ให้ทำการบันทึก เก็บรวบรวมข้อมูลความผิดที่เกิดขึ้นและประเมินความเสียหาย มีหน้าที่รับคำร้องเรียนจากบุคคลทั่วไปที่ยื่นหนังสือโดยมีเหตุผลอันน่าเชื่อ (reasonable belief) ว่าตนได้ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล[5] โดยต้องทำให้หน่วยงานคณะกรรมาธิการการค้าของรัฐบาลกลางเชื่อว่าตนได้ตกเป็นผู้เสียหายที่แท้จริงในการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล เนื่องจากผู้ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไม่อาจเป็นผู้ยื่นฟ้องร้องด้วยตนเองได้ แต่ต้องให้หน่วยงานคณะกรรมาธิการการค้าของรัฐบาลกลางเป็นผู้ยื่นฟ้องให้ ดังนี้การยื่นหนังสือร้องเรียนต่อหน่วยงานจึงเป็นเพียงข้อสันนิษฐานของกฎหมายว่าบุคคลผู้นั้นเป็น

---

[4] Identity Theft and Assumption Deterrence Act of 1998 [online] November 2012, Available from http://www.ckfraud.org/title_18.html.

[5] Identity Theft and Assumption Deterrence Act of 1998 [online] 10 December 2012, Available from http://itlaw.wikia.com/wiki/Identity_Theft_and_Assumption_Deterrence_Act_of_1998.

ผู้เสียหายในการถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล[6] และในพระราชพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 ยังมีการยอมรับให้บุคคลที่ถูกโจรกรรมข้อมูลเอกลักษณ์บุคคลหรือผู้ที่ตกเป็นเหยื่อของอาชญากรนั้นเป็นผู้เสียหายที่แท้จริง เป็นผู้ที่จะได้รับความคุ้มครองตามกฎหมาย

รายละเอียดของพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 ในส่วนที่สำคัญมี ดังนี้

(ก) คำนิยาม คำนิยามของคำที่เกี่ยวข้องกับความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้ในมาตรา 1028(c) เพื่อความเข้าใจฐานความผิดนี้ได้มากขึ้นจึงได้มีการอธิบายคำต่างๆ เหล่านี้ไว้ คือ

"เครื่องมือทำเอกสาร" (document-making implement) หมายถึง อุปกรณ์เครื่องมือ รอยประทับตรา อุปกรณ์อิเล็กทรอนิกส์ใดๆหรือโปรแกรมคอมพิวเตอร์ต่างๆ ที่สามารถใช้ในการจัดทำเอกสารแสดงตัวบุคคล เอกสารแสดงตัวบุคคลปลอม หรือเอกสารอื่นใด

"เอกสารแสดงตัวบุคคล" (identification document) หมายถึง เอกสารที่ออกหรือจัดทำขึ้นโดยอำนาจของรัฐบาลกลาง มลรัฐ หน่วยงานทางปกครองของรัฐ รัฐบาลต่างประเทศหรือองค์กรระหว่างประเทศที่สามารถออกเอกสารที่มีผลสมบูรณ์ และระบุตัวบุคคลได้เฉพาะเจาะจง

"สิ่งซึ่งแสดงตัวบุคคล" (means of identification) หมายถึง ชื่อ หรือตัวเลขใดๆ ที่สามารถใช้โดยลำพัง หรือร่วมกับข้อมูลอื่นๆ แล้วสามารถระบุตัวบุคคลได้ รวมถึง

- ชื่อ หมายเลขประกันสังคม วันเดือนปีเกิด ใบอนุญาตขับขี่ที่ออกโดยรัฐบาล หมายเลขประจำตัวประชาชน หมายเลขทะเบียนบุคคลต่างด้าว หมายเลขหนังสือเดินทาง หมายเลขประจำตัวลูกจ้างหรือหมายเลขผู้เสียภาษี

---

[6] Jake Stroup, The Identity Theft and Assumption Deterrence Act of 1998 [online] 10 December 2012, Available from http://idtheft.about.com/od/glossary/a/ITADA.htm.

- ข้อมูลเอกลักษณ์ทางชีวภาพของบุคคล เช่น ลายพิมพ์นิ้วมือ เสียง เยื่อชั้นในม่านตา หรือเอกลักษณ์ทางกายภาพอื่นๆ ที่แสดงออก
- หมายเลขอิเล็กทรอนิกส์ที่เป็นเอกลักษณ์ ที่อยู่ รหัสผ่าน
- ข้อมูลจากการสื่อสารโดยเทคโนโลยีที่สามารถระบุตัวบุคคลได้

"บัตรแสดงตัวบุคคล" (personal identification card) หมายถึง เอกสารที่แสดงตัวบุคคลที่ออกโดยรัฐบาลโดยมีวัตถุประสงค์เพื่อระบุเอกลักษณ์เฉพาะบุคคล

"การจัดทำ" (produce) รวมถึงการปรับเปลี่ยน แก้ไข การรับรองว่าเป็นเอกสารจริง หรือการนำมาประกอบกับสิ่งอื่นด้วย

จากคำนิยามเหล่านี้ทำให้กล่าวได้ว่าข้อมูลหรือสิ่งที่กฎหมายฉบับนี้มุ่งให้ความคุ้มครอง คือ ชื่อ หรือตัวเลขใดๆ ที่สามารถใช้โดยลำพัง หรือร่วมกับข้อมูลอื่นๆ แล้วสามารถระบุตัวบุคคลได้ เช่น หมายเลขประกันสังคม ใบอนุญาตขับขี่ที่ออกโดยรัฐบาล หมายเลขประจำตัวประชาชน หมายเลขทะเบียนบุคคลต่างด้าว หมายเลขหนังสือเดินทาง หมายเลขประจำตัวลูกจ้าง หรือหมายเลขผู้เสียภาษี และข้อมูลเอกลักษณ์ทางชีวภาพของบุคคลด้วย เช่น ลายพิมพ์นิ้วมือ เสียง เยื่อชั้นในม่านตา และรวมถึงข้อมูลที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ต่างๆ ที่สามารถระบุตัวบุคคลได้ด้วย

(ข) องค์ประกอบความผิด ในกฎหมายฉบับนี้ได้กำหนดฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้ในมาตรา 1028[7] ดังนี้

1.) ผู้ใดกระทำโดยรู้ และปราศจากอำนาจตามกฎหมายจัดทำขึ้นซึ่งเอกสารแสดงตัวบุคคลหรือเอกสารแสดงตัวบุคคลปลอม

2.) ผู้ใดกระทำโดยรู้ และเจตนาโอนซึ่งเอกสารแสดงตัวบุคคลหรือเอกสารแสดงตัวบุคคลปลอม โดยรู้อยู่ว่าเอกสารดังกล่าวได้มาจากการโจรกรรมหรือถูกทำขึ้นโดยปราศจากอำนาจตามกฎหมาย

[7] The Identity Theft and Assumption Deterrence Act of 1998 Article 1028 (โปรดดูภาคผนวก)

3.) ผู้ใดกระทำโดยรู้ และครอบครองโดยเจตนาจะใช้กระทำผิดกฎหมาย หรือโอนโดยผิดกฎหมายซึ่งเอกสารแสดงตัวบุคคลหรือเอกสารแสดงตัวบุคคลปลอมตั้งแต่ห้าฉบับขึ้นไป (นอกเหนือจากเอกสารที่ออกโดยชอบด้วยกฎหมายให้แก่ผู้ครอบครอง)

4.) ผู้ใดกระทำโดยรู้ และครอบครองเอกสารแสดงตัวบุคคล (นอกเหนือจากเอกสารที่ออกโดยชอบด้วยกฎหมายให้แก่ผู้ครอบครอง) หรือเอกสารแสดงตัวบุคคลปลอม โดยมีเจตนาจะใช้เอกสารนั้นเพื่อฉ้อโกงสหรัฐอเมริกา

5.) ผู้ใดกระทำโดยรู้ เจตนาทำ โอนหรือครอบครองเครื่องมือทำเอกสารแสดงตัวบุคคลหรือเอกสารแสดงตัวบุคคลปลอม หรือสิ่งใดๆ ที่ก่อให้เกิดผลได้เช่นเดียวกัน

6.) ผู้ใดกระทำโดยรู้ และครอบครองเอกสารแสดงตัวบุคคลที่เป็นเอกสารของสหรัฐอเมริกา โดยรู้ว่าเป็นเอกสารที่ถูกโจรกรรมมาหรือถูกทำขึ้นโดยปราศจากอำนาจตามกฎหมาย

7.) ผู้ใดกระทำโดยรู้ โอนหรือใช้โดยปราศจากอำนาจตามกฎหมายซึ่งเอกสารแสดงตัวบุคคลของบุคคลอื่น โดยเจตนาจะกระทำความผิด หรือให้ความช่วยเหลือ หรือสนับสนุนการกระทำใดๆ ที่เป็นความผิดตามกฎหมายของรัฐบาลกลาง หรือเป็นความผิดตามกฎหมายของมลรัฐใดที่สามารถนำมาปรับใช้ได้

ในฐานความผิดนี้มีการบัญญัติเอาความผิดกับการพยายาม และการสมคบกันกระทำความผิดด้วย โดยจะลงโทษเท่ากับกรณีเป็นความผิดสำเร็จ และรับผิดเท่ากับตัวการ ในฐานความผิดนั้นๆ

เมื่อพิจารณาถ้อยบัญญัติในพระราชบัญญัติฉบับนี้แล้ว เห็นได้ว่ากฎหมายได้บัญญัติการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นความผิดกับการจัดทำขึ้น การโอน การครอบครอง และการใช้ซึ่งเอกสารแสดงตัวบุคคลปลอม ทั้งนี้กฎหมายได้บัญญัติครอบคลุมไปถึงเอกสารแสดงตัวบุคคลที่เป็นเอกสารที่แท้จริงด้วย ทั้งบัญญัติครอบคลุมไปถึงบุคคลผู้ทำ โอนหรือครอบครองเครื่องมือที่ใช้ในการจัดทำเอกสารแสดงเอกลักษณ์บุคคลปลอมด้วย รวมถึงมีการ

บัญญัติให้ผู้ที่ร่วมสมคบกันกระทำความผิดต้องรับผิดเสมือนตัวการ และหากเป็นกรณีพยายามกระทำความผิดกฎหมายได้บัญญัติให้รับโทษเท่ากับความผิดสำเร็จ เนื่องจากเห็นว่าหากมีการกระทำความผิดสำเร็จเกิดขึ้นจะก่อความเสียหายเป็นอย่างมาก ดังนี้การพิจารณาว่าการกระทำใดเป็นการกระทำความผิดตามฐานความผิดเหล่านี้หรือไม่ ฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลสามารถแยกองค์ประกอบความผิดได้ ดังนี้

<u>องค์ประกอบภายนอก</u>

1. ผู้ใด
2. (ก) จัดทำขึ้นซึ่งเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอม
   (ข) โอนซึ่งเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอม
   (ค) ครอบครองซึ่งเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอม
   (ง) ใช้ซึ่งเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอม
   (จ) ทำ โอน หรือครอบครองเครื่องมือที่ใช้ทำเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอม

<u>องค์ประกอบภายใน</u> คือ เจตนา

(ค) การกำหนดโทษ การกำหนดบทลงโทษสำหรับผู้กระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลมีดังนี้

1.) โทษปรับหรือโทษจำคุกไม่เกิน 15 ปี หรือทั้งจำทั้งปรับ ในความผิดดังนี้

(ก) การจัดทำ หรือโอนซึ่งเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอมที่

- เป็นเอกสารแสดงตัวบุคคลที่ออกโดยหรืออยู่ภายใต้อำนาจของรัฐบาลกลาง หรือ
- เป็นเอกสารสูติบัตร หรือใบอนุญาตขับขี่ หรือบัตรประจำตัวประชาชน

(ข) การจัดทำ หรือโอนซึ่งเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอม จำนวนตั้งแต่ห้าฉบับขึ้นไป

(ค) การกระทำความผิดตามมาตรา 1028 (a)(5) หรือ

(ง) การกระทำความผิดตามมาตรา 1028 (a)(7) ที่เกี่ยวข้องกับการโอน หรือใช้ลักษณะเฉพาะบุคคลตั้งแต่หนึ่งครั้งขึ้นไป และผลของการกระทำนั้นทำให้ได้ผลตอบแทนรวมตั้งแต่ 1,000 เหรียญสหรัฐขึ้นไป ภายในระยะเวลา 1 ปี

2.) โทษปรับหรือโทษจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับ ในความผิดดังนี้

(ก) การจัดทำ หรือใช้สิ่งที่ใช้ระบุตัวบุคคล เอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอม หรือ

(ข) การกระทำความผิดตามมาตรา 1028 (a)(3) และมาตรา 1028 (a)(7)

3.) โทษปรับหรือโทษจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ ในความผิดดังนี้

(ก) กระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเพื่อทำให้สะดวกขึ้นในการกระทำความผิดเกี่ยวกับการค้ายาเสพติด

(ข) กระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเพื่อเป็นการกระทำที่เชื่อมโยงกับการกระทำความผิดอาญาที่ใช้ความรุนแรง หรือ

(ค) การกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลซ้ำ และคดีก่อนถึงที่สุดแล้ว

4.) โทษปรับ หรือโทษจำคุกไม่เกิน 25 ปี หรือทั้งจำทั้งปรับ ถ้าเป็นการกระทำความผิดที่เป็นการให้ความสะดวกแก่การก่อการร้ายระหว่างประเทศ

5.) ทุกกรณีความผิดภายใต้มาตรา 1028 (a) ให้ยึดทรัพย์สินของบุคคลที่ใช้ หรือที่มีไว้เพื่อใช้ในการกระทำความผิด

6.) โทษปรับ หรือโทษจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ สำหรับความผิดฐานอื่นๆ

3.1.1.2 **พระราชบัญญัติว่าด้วยการรายงานข้อมูลเครดิตอย่างยุติธรรม ค.ศ.**1970 (The Fair Credit Reporting Act 1970)

พระราชบัญญัติว่าด้วยการรายงานข้อมูลเครดิตอย่างยุติธรรม ค.ศ. 1970 เป็นกฎหมายเกี่ยวกับเครดิตที่มีการกำหนดมาตรการในการให้ความคุ้มครองแก่ผู้เสียหาย(ลูกค้าผู้เปิดเครดิต) กล่าวคือ มีระบบการแจ้งเตือนการถูกฉ้อโกง (fraud alerts) โดยเกิดจากการร้องขอโดยตรงจากเจ้าของเครดิต หรือตัวแทน ว่าตนอาจตกเป็นเหยื่อการฉ้อโกง หรือการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ทางหน่วยงานก็จะแจ้งเตือนลงในบัญชีเครดิตทุกอันของลูกค้าผู้เปิดเครดิต และมีมาตรการระงับเครดิตที่เกิดจากการถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (block of information resulting from identity theft) ทางหน่วยงานจะระงับเครดิตเมื่อมีหลักฐานแสดงตัวตนของผู้เปิดเครดิตที่ชัดเจน มีสำเนารายงานการถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล มีเอกสารชี้แจงข้อมูลจากผู้เปิดเครดิตว่าตนมิได้ทำธุรกรรมนั้นๆ แต่ทั้งนี้หน่วยงานมีสิทธิที่จะปฏิเสธการระงับเครดิตได้ในกรณีที่ข้อมูลที่ร้องขอให้ระงับโดยผู้เปิดเครดิตนั้นผิดพลาด หรือมีการบิดเบือนความจริง หรือกรณีผู้เปิดเครดิตได้สินค้าไว้ในครอบครองจากการทำธุรกรรมที่ถูกระงับนั้น และในพระราชบัญญัติฉบับนี้ยังมีมาตรการเยียวยาผู้เสียหายจากการถูกโจรกรรมข้อมูลด้วย คือ เปิดโอกาสให้ผู้ที่ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่ประวัติเครดิตถูกอาชญากรทำให้เสียหาย ได้มีโอกาสแก้ไขประวัติให้กลับดีเหมือนเดิมได้ เพื่อเป็นการคุ้มครอง และเยียวยาผู้เสียหาย ที่ต้องมาเสียประวัติทางเครดิตทั้งๆ ที่ตนมิได้มีส่วนในการกระทำความผิดใดๆ[8]

การจากศึกษากฎหมายของประเทศสหรัฐอเมริกาพบว่าได้มีการให้คำจำกัดความของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) ไว้ในพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) คือ ผู้ใดโดยเจตนากระทำการโอน ครอบครอง หรือใช้ประโยชน์จากข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นโดยไม่ได้รับอนุญาต เพื่อกระทำการผิดกฎหมายของสหรัฐอเมริกา (กฎหมายรัฐบาลกลางหรือ federal law) หรือได้ให้ความช่วยเหลือ หรือให้การสนับสนุนในการ

[8] The Fair Credit Reporting Act [online], February 2013. Available from http://www.ftc.gov/os/statutes/031224fcra.pdf.

กระทำที่ผิดกฎหมายดังกล่าว อันก่อให้เกิดการละเมิดกฎหมายหรือก่อให้เกิดความผิดอาญาร้ายแรงภายใต้กฎหมายของมลรัฐใด หรือภายใต้กฎหมายท้องถิ่นใดที่มีผลใช้บังคับอยู่ ผู้นั้นสมควรได้รับโทษตามกฎหมาย ซึ่งฐานความผิดที่บัญญัติไว้ครอบคลุมการกระทำตั้งแต่ การจัดทำขึ้น การโอน การครอบครอง และการใช้ซึ่งเอกสารแสดงตัวบุคคลปลอม และมีการบัญญัติบทลงโทษตามความร้ายแรงของความผิดที่เกิดขึ้นด้วย กล่าวคือ หากกระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเพื่อไปกระทำความผิดอย่างอื่นที่ร้ายแรง เช่น การก่อการร้าย หรือเป็นขบวนการค้ายาเสพติด ฯลฯ ผู้กระทำความผิดนั้นต้องรับโทษหนักขึ้น อีกทั้งยังมีมาตรการเยียวยาผู้ที่ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลด้วย คือ ในพระราชบัญญัติว่าด้วยการรายงานข้อมูลเครดิตอย่างยุติธรรม ค.ศ.1970 (The Fair Credit Reporting Act 1970) บัญญัติให้ผู้ที่ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลสามารถขอให้มีการแก้ไขประวัติเครดิตของตนเองให้กลับดีเหมือนเดิมก่อนถูกโจรกรรมข้อมูลไปใช้โดยมิชอบได้

3.1.2 กฎหมายการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของประเทศแคนาดา

ประเทศแคนาดามีการบัญญัติกฎหมายในฐานความผิดเกี่ยวกับสิ่งซึ่งแสดงเอกลักษณ์บุคคล (Identity) ไว้เป็น 2 ประเภท คือ การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) และการฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Fraud) ซึ่งความแตกต่างของสองฐานความผิดนี้ คือ มีการแบ่งการกระทำความผิดเกี่ยวกับเอกลักษณ์บุคคลไว้เป็นสองขั้นตอน ขั้นตอนที่หนึ่ง คือ การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล หรืออาจกล่าวได้ว่าเป็นขั้นตอนของการขโมยเพื่อให้ได้มา หรือมีไว้ในครอบครองซึ่งข้อมูลเอกลักษณ์ของผู้อื่น เมื่อมีผู้กระทำความผิดในลักษณะนี้ก็จะเป็นความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) ขั้นตอนที่สอง คือ การนำข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นไปใช้ฉ้อโกง หรือแสวงหาผลประโยชน์โดยมิชอบเพื่อตนเอง หรือผู้อื่น เมื่อมีผู้กระทำความผิดในลักษณะนี้ก็จะผิดฐานฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Fraud) ดังนี้จะเห็นได้ว่าผู้กระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล กับผู้กระทำความผิดฐานฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

อาจเป็นบุคคลคนเดียวกันหรือต่างบุคคลก็ได้ และในการกระทำความผิดครั้งหนึ่ง อาจเป็นการกระทำความผิดเพียงฐานหนึ่งฐานใดหรือทั้งสองฐานความผิดก็ได้ ประเทศแคนาดาได้บัญญัติฐานความผิดเหล่านี้ไว้เป็นการเฉพาะในประมวลกฎหมายอาญา โดยได้แบ่งเป็น 2 มาตรา ในส่วนแรกฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) มาตรา 402 ได้แบ่งย่อยออกเป็น 2 มาตรา คือมาตรา 402.1 จะบัญญัติเกี่ยวกับคำนิยามและมาตรา 402.2 บัญญัติเกี่ยวกับองค์ประกอบของฐานความผิด และส่วนที่สองฐานฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Fraud) ในมาตรา 403 ดังรายละเอียดต่อไปนี้

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft)

(ก) คำนิยาม ได้มีการบัญญัติคำนิยามของคำว่า “ข้อมูลซึ่งแสดงเอกลักษณ์บุคคล” (Identity Information) ไว้ในมาตรา 402.1[9] ว่าหมายถึง ข้อมูลใดๆ รวมทั้งทางชีววิทยาหรือข้อมูลชีวภาพที่ใช้โดยลำพัง หรือร่วมกับข้อมูลอื่นๆ เพื่อระบุตัวบุคคล หรืออ้างถึงตัวบุคคล รวมถึงลายพิมพ์นิ้วมือ เสียง เยื่อชั้นในลูกตา ม่านตา ประวัติดีเอ็นเอ ชื่อ ที่อยู่ วันเดือนปีเกิด ลายเซ็น ลายเซ็นอิเล็กทรอนิกส์ ลายเซ็นดิจิทัล (digital signature) ชื่อผู้ใช้ (user name) หมายเลขบัตรเครดิต หมายเลขบัตรเดบิต หมายเลขบัญชีสถาบันไฟแนนซ์ หมายเลขหนังสือเดินทาง หมายเลขประกันสังคม หมายเลขประกันสุขภาพ หมายเลขใบอนุญาตขับขี่ หรือรหัสผ่าน

จากการเปรียบเทียบคำนิยามข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ. 1998 กฎหมายของประเทศสหรัฐอเมริกาแล้วเห็นได้ว่าประมวลกฎหมายของประเทศแคนาดามีการให้คำนิยามไว้ในลักษณะที่คล้ายคลึงกัน กล่าวคือ หมายความถึงข้อมูลทุกชนิดที่ทำให้สามารถจะระบุตัวบุคคลได้ รวมถึงข้อมูลที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ด้วย ทำให้บทบัญญัติของกฎหมายสามารถให้ความคุ้มครอง และบังคับใช้แก่ข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้ครอบคลุมทุกประเภท

[9] Canadian Criminal Code Article 402.1 (โปรดดูภาคผนวก)

(ข) องค์ประกอบความผิด

ฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) มาตรา 402.2[10] มีองค์ประกอบความผิด ดังนี้

(1) ผู้ใดกระทำโดยเจตนา ได้มาหรือครอบครองข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่น โดยมีไว้เพื่อกระทำความผิดอาญาอุกฉกรรจ์ รวมถึงมีการฉ้อโกง หลอกลวง หรือกล่าวเท็จรวมอยู่ในองค์ประกอบความผิดนั้นด้วย

(2) ผู้ใดกระทำการถ่ายทอด ทำให้สามารถเข้าถึง แจกจ่าย ขาย หรือเสนอขายข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่น หรือมีไว้ในครอบครองเพื่อจุดประสงค์ดังที่กล่าวมา ไม่ว่าโดยเจตนาหรือประมาท ใช้ข้อมูลนั้นเพื่อกระทำความผิดอาญาอุกฉกรรจ์ รวมถึงมีการฉ้อโกง หลอกลวง หรือกล่าวเท็จรวมอยู่ในองค์ประกอบความผิดนั้นด้วย

(3) การกระทำความผิดตามข้อ (1) และ ข้อ (2) นั้นหากกระทำความผิดในฐานความผิดดังต่อไปนี้ให้ถือเป็นความผิดอาญาอุกฉกรรจ์

(ก.) การปลอมแปลงหนังสือเดินทาง (มาตรา 57)

(ข.) ฉ้อโกงโดยใช้หนังสือรับรองการเป็นพลเมือง (มาตรา 58)

(ค.) แสดงตนเป็นเจ้าพนักงาน (มาตรา 130)

(ง.) ให้การเท็จ (มาตรา 131)

(จ.) ขโมย หรือปลอมแปลงบัตรเครดิต (มาตรา 342)

(ฉ.) ปลอมรายงานการเงิน (มาตรา 362)

(ช.) ปลอมแปลง (มาตรา 366)

---

[10] Canadian Criminal Code Article 402.2 (โปรดดูภาคผนวก)

(ฆ.) ใช้ จำหน่าย ครอบครองเอกสารปลอม (มาตรา 368)

(ฌ.) ฉ้อโกง (มาตรา 380)

(ญ.) ฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (มาตรา 403)

(4) ผู้ต้องหาที่กระทำความผิดตามข้อ (1) หรือข้อ (2) สามารถถูกลงโทษได้โดยศาลที่มีเขตอำนาจในสถานที่ที่เกิดการกระทำความผิดขึ้น หรือสถานที่ที่พบการกระทำความผิด หรือสถานที่ที่ผู้กระทำความผิดถูกจับ หรืออยู่ในอำนาจการคุมขัง

การพิจารณาว่าการกระทำใดเป็นการกระทำความผิดตามฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลหรือไม่ ต้องพิจารณาถึงองค์ประกอบของความผิด ดังนี้

<u>องค์ประกอบภายนอก</u>

1. ผู้ใด

2. (ก) ได้มา เพื่อกระทำความผิดอาญา หรือ

(ข) ครอบครอง เพื่อกระทำความผิดอาญา หรือ

(ค) โอน หรือกระทำการใดที่ทำให้บุคคลอื่นสามารถเข้าถึง

3. ข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่น

<u>องค์ประกอบภายใน</u> คือ เจตนา

ฐานความผิดฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Fraud) มาตรา 403 ผู้ใดกระทำการโดยเจตนาฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่น ไม่ว่าจะเป็นของบุคคลที่มีชีวิตอยู่หรือของผู้ที่เสียชีวิตไปแล้ว เพื่อวัตถุประสงค์ดังกล่าวนี้ถือเป็นการกระทำความผิดฐานฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

(ก) กระทำเพื่อแสวงหาประโยชน์เพื่อตนเอง หรือผู้อื่น

(ข) กระทำเพื่อให้ตนได้รับทรัพย์สิน หรือผลประโยชน์อย่างอื่นในทรัพย์สิน

(ค) กระทำเพื่อให้ผู้เป็นเจ้าของข้อมูลหรือผู้อื่นเกิดความเสียหาย

(ง) กระทำเพื่อหลบหนีการจับกุม การดำเนินคดี หรือเพื่อขัดขวางกระบวนการยุติธรรม

การพิจารณาว่าการกระทำใดเป็นการกระทำความผิดตามฐานความผิดฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคลนี้หรือไม่ ต้องพิจารณาถึงองค์ประกอบของความผิด ดังนี้

<u>องค์ประกอบภายนอก</u>

1. ผู้ใด
2. ใช้ข้อมูลซึ่งแสดงเอกลักษณ์บุคคล
3. ของผู้อื่น หรือของผู้ที่ถึงแก่กรรมแล้ว
4. เพื่อ (ก) แสวงหาประโยชน์เพื่อตนเอง หรือผู้อื่น
   (ข) ให้ตนได้รับทรัพย์สิน หรือผลประโยชน์อย่างอื่นในทรัพย์สิน
   (ค) ทำให้ผู้เป็นเจ้าของข้อมูลหรือผู้อื่นเกิดความเสียหาย
   (ง) หลบหนีการจับกุม การดำเนินคดี หรือเพื่อขัดขวางกระบวนการยุติธรรม

<u>องค์ประกอบภายใน</u> คือ เจตนา

จากการเปรียบเทียบฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ. 1998 กฎหมายของประเทศสหรัฐอเมริกาแล้วเห็นได้ว่าในประมวลกฎหมายอาญาของประเทศแคนาดามีการบัญญัติที่แตกต่าง โดยมีการให้รายละเอียด และมีความครอบคลุมถึงการได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นมากกว่า กล่าวคือ กฎหมายของแคนาดาแบ่งความผิดออกเป็นสองมาตรา คือ ส่วนการได้มา ครอบครอง และจำหน่ายจ่ายโอนข้อมูลซึ่งแสดงเอกลักษณ์บุคคล บัญญัติเป็นความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) และในส่วนที่สอง คือ ส่วนที่นำ

ข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นไปใช้เพื่อแสวงหาประโยชน์โดยมิชอบเพื่อตนเอง หรือผู้อื่น บัญญัติเป็นความผิดฐานฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Fraud) ซึ่งมีความแตกต่างจากกฎหมายของประเทศสหรัฐอเมริกาที่บัญญัติความผิดในทั้งสองลักษณะนี้อยู่ในมาตราเดียวกันซึ่งก็สามารถนำมาปรับใช้กับความผิดที่เกิดขึ้นได้เช่นเดียวกัน แต่ทั้งนี้กฎหมายของประเทศแคนาดาได้บัญญัติชัดเจนถึงการได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคลว่าให้รวมถึงกรณีที่เป็นการได้มาโดยการฉ้อโกง หลอกลวงด้วย และการได้มาซึ่งข้อมูลนั้นจะเป็นความผิดก็ต่อเมื่อผู้ได้ข้อมูลนั้นมีเจตนาที่จะนำข้อมูลที่ได้มาไปกระทำความผิด

(ค) การกำหนดโทษ บทกำหนดโทษสำหรับผู้ใดกระทำความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) เป็นความผิดอาญาอุกฉกรรจ์ โทษจำคุกสำหรับความผิดนั้นไม่เกิน 5 ปี หรือมีความผิดลงโทษตามการตัดสินอย่างรวบรัด (summary conviction)

บทกำหนดโทษสำหรับผู้ใดกระทำความผิดการฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Fraud) บทกำหนดโทษสำหรับผู้กระทำความผิดตามมาตรานี้ คือ ผู้กระทำความผิดมีโทษจำคุกไม่เกิน 10 ปี หรือมีความผิดลงโทษตามการตัดสินอย่างรวบรัด (summary conviction) และมีมาตรการเยียวยาผู้เสียหายด้วย โดยให้ผู้เสียหายได้รับชดใช้ค่าเสียหายที่เกิดขึ้น รวมถึงค่าใช้จ่ายในการดำเนินการแก้ไขประวัติข้อมูลเอกลักษณ์บุคคลให้ถูกต้องด้วย เช่น การดำเนินการแก้ไขประวัติเครดิต

การจากศึกษากฎหมายของประเทศแคนาดามีการบัญญัติความผิดเกี่ยวกับการโจรกรรมและการฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้ในประมวลกฎหมายอาญา โดยแบ่งเป็นสองมาตรา คือ มาตรา 402.2 บัญญัติถึงการขโมยเพื่อให้ได้มา หรือมีไว้ในครอบครองซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่น เมื่อมีผู้กระทำความผิดในลักษณะนี้ก็จะเป็นความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) มาตรา 403 บัญญัติถึงการนำข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นไปใช้ฉ้อโกง หรือแสวงหาผลประโยชน์โดยมิชอบเพื่อตนเอง หรือผู้อื่น เมื่อมีผู้กระทำความผิดในลักษณะนี้ก็จะเป็นความผิดฐานฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Fraud) และมีการบัญญัติคำนิยามของข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้ครอบคลุมถึง

ข้อมูลส่วนบุคคลต่างๆ ไม่ว่าโดยลำพังหรือเมื่อรวมเข้ากับข้อมูลอื่นๆ แล้วสามารถระบุตัวบุคคลได้ รวมถึงข้อมูลที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ด้วย ซึ่งเป็นการบัญญัติคำนิยามได้ครอบคลุมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลทุกประเภทเช่นเดียวกันกับกฎหมายของประเทศสหรัฐอเมริกา

3.1.3 กฎหมายเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของประเทศสหราชอาณาจักร

ประเทศสหราชอาณาจักรก็มีปัญหาอาชญากรรมการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกิดขึ้นจำนวนมากเช่นกัน หน่วยงานบริการป้องกันการฉ้อโกงของสหราชอาณาจักร (The UK's Fraud Prevention Service) ได้แสดงสถิติของจำนวนผู้ที่ตกเป็นเหยื่อของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้ว่า ในปี 2010 ในประเทศสหราชอาณาจักรมีผู้ตกเป็นเหยื่อของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นจำนวน 89,000 ราย ซึ่งจำนวนเหยื่อได้เพิ่มสูงขึ้นจากเมื่อปี 2009 ที่มีเหยื่อจำนวน 85,000 ราย[11] กล่าวคือมีจำนวนเหยื่อเพิ่มมากขึ้นถึง 4,000 ราย ประเทศสหราชอาณาจักรจึงให้ความสำคัญกับการกระทำความผิดเช่นนี้อยู่มาก แต่ในปัจจุบันกฎหมายที่เกี่ยวข้องกับการกระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของประเทศสหราชอาณาจักรยังกระจัดกระจาย มิได้มีการออกกฎหมายเฉพาะอย่างเช่นในประเทศสหรัฐอเมริกา และประเทศแคนาดา ดังนี้ผู้เขียนจึงขออธิบายกฎหมายที่มีส่วนเกี่ยวข้องกับความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ดังนี้

3.1.3.1 **พระราชบัญญัติการลักทรัพย์ ค.ศ.** 1968 (The Theft Act of 1968)

อาชญากรที่ใช้ข้อมูลส่วนตัวของบุคคลอื่นเพื่อทำการขโมยสินค้า หรือทรัพย์สินอื่นๆ อาจมีความผิดตามกฎหมายฉบับนี้ได้

[11] Identity Theft [online] November 2012, Available from http://en.wikipedia.org/wiki/Identity_theft.

(ก) คำนิยาม พระราชบัญญัติฉบับนี้ได้ให้คำนิยามของคำว่า โจร (Theft) ไว้คือ บุคคลที่ไม่ซื่อสัตย์มีเจตนาที่จะเอาทรัพย์สินของผู้อื่นมาเป็นของตนโดยการขโมย และให้คำนิยามของคำว่า ทรัพย์สิน (Property) ไว้อย่างกว้างมาก กล่าวคือ ให้หมายความรวมถึงเงิน และทรัพย์สินอื่นๆ รวมทั้งสิ่งที่อยู่ในระหว่างการดำเนินการ และทรัพย์สินที่ไม่มีรูปร่างด้วย ดังนี้การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลจึงสามารถนำกฎหมายนี้มาปรับใช้ได้

(ข) องค์ประกอบความผิด ฐานความผิดเกี่ยวข้องที่สำคัญๆ[12] คือ

ความผิดเกี่ยวกับการได้ทรัพย์สินมาโดยการหลอกลวง ซึ่งได้บัญญัติกฎหมายไว้กว้างๆ คือ การหลอกลวงเพื่อให้ได้ไปซึ่งทรัพย์สินใดๆ เป็นความผิดอาญาทั้งสิ้น โดยมีโทษจำคุกไม่เกิน 10 ปี[13]เนื่องจากการโจรกรรมข้อมูลซึ่งเอกลักษณ์บุคคลเป็นเสมือนการหลอกลวงบุคคลอื่นว่าตนเป็นบุคคลผู้มีสิทธินั้นๆ จริงจึงอาจปรับเข้าบทกฎหมายนี้ได้

ความผิดเกี่ยวกับการคงไว้ซึ่งเครดิตที่ผิดกฎหมาย[14] กล่าวคือผู้ที่มีหน้าที่เกี่ยวข้องกับการจัดทำเครดิตมีเจตนาไม่ยกเลิกเครดิตนั้นโดยผิดกฎหมาย ซึ่งเครดิตที่ผิดกฎหมายนั้น อาจเกิดจากการโจรกรรม การกรรโชก ฉ้อโกง หรือรับของโจร

(ค) การกำหนดโทษ ความผิดเกี่ยวกับการได้ทรัพย์สินมาโดยการหลอกลวง มีโทษจำคุกไม่เกิน 10 ปี

ความผิดเกี่ยวกับการคงไว้ซึ่งเครดิตที่ผิดกฎหมายผู้กระทำความผิดฐานนี้มีโทษจำคุกไม่เกิน 10 ปี

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลสามารถปรับใช้กับบทบัญญัติในพระราชบัญญัติการลักทรัพย์ ค.ศ. 1968 ได้เนื่องมาจากพระราชบัญญัติฉบับนี้ได้ให้คำนิยามของทรัพย์สิน (Property) ไว้อย่างกว้างมาก กล่าวคือ ให้หมายความรวมถึงเงิน ทรัพย์สินอื่นๆ รวมทั้ง

---

[12] Theft Act 1968[Online], February 2013. Available from http://www.legislation.gov.uk/ukpga/1968/60/contents.

[13] Theft Act 1968 Section 15 (โปรดดูภาคผนวก)

[14] Theft Act 1968 Section 24A (โปรดดูภาคผนวก)

ทรัพย์สินที่ไม่มีรูปร่างด้วย ดังนั้นการลักข้อมูลซึ่งแสดงเอกลักษณ์บุคคลจึงอาจเป็นความผิดฐานลักทรัพย์ตามกฎหมายฉบับนี้ได้ และยังมีการบัญญัติฐานความผิดการหลอกลวงให้ได้ไปซึ่งทรัพย์สินของบุคคลอื่นด้วย การนำข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นไปใช้เพื่อฉ้อโกงจึงเป็นความผิดตามกฎหมายฉบับนี้ด้วยเช่นกัน แต่อย่างไรก็ตามในกรณีการฉ้อโกงนี้บุคคลที่กฎหมายมุ่งคุ้มครอง คือบุคคลที่ถูกหลอกลวงไปซึ่งทรัพย์สินมิได้มีเจตนารมณ์ที่จะคุ้มครองผู้ที่ถูกลักข้อมูลซึ่งแสดงเอกลักษณ์บุคคลแต่อย่างใด

3.1.3.2 **พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ.** 1998 (The Data Protection Act of 1998)

กฎหมายฉบับนี้ให้การคุ้มครองข้อมูลส่วนบุคคล สิ่งที่เป็นเอกลักษณ์ที่สามารถระบุถึงตัวบุคคลได้ เช่น ประวัติครอบครัว การนับถือศาสนา รสนิยมทางเพศ ประวัติทางการเงิน บันทึกสุขภาพ เป็นต้น องค์กรที่เก็บรวบรวมข้อมูลต้องเก็บรักษาข้อมูลอย่างดี และต้องมีความมั่นใจว่ามีวิธีการ หรือเทคโนโลยีที่ทันสมัย และดีเพียงพอที่จะเก็บรักษาข้อมูลไว้อย่างเป็นความลับ

(ก) คำนิยาม พระราชบัญญัติฉบับนี้ได้ให้ความหมายของข้อมูลส่วนบุคคล (personal data) ว่าหมายความถึง ข้อมูลเกี่ยวกับความเป็นอยู่ของบุคคลซึ่งสามารถระบุตัวบุคคลได้จากข้อมูลนั้นเอง หรือจากข้อมูล ข่าวสารที่อยู่ในการควบคุมของผู้ควบคุมข้อมูล (data controller) และรวมถึงการแสดงความคิดเห็น คำบอกกล่าวใดๆ ที่เกี่ยวกับบุคคลซึ่งผู้อื่น หรือบุคคลที่สามได้กล่าวถึงเจ้าของข้อมูลส่วนบุคคลนั้น

(ข) องค์ประกอบความผิด ฐานความผิดที่มีความเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล คือ การได้รับข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย มาตรา 55[15] บุคคลใดๆ ต้องไม่เจตนา หรือประมาท ได้มาหรือเปิดเผยซึ่งข้อมูลส่วนบุคคลของผู้อื่น โดยปราศจากความยินยอมของผู้ควบคุมข้อมูล ยกเว้นแต่การได้มาหรือการเปิดเผยข้อมูลนั้น

[15] The Data Protection Act of 1998 Article 55 (โปรดดูภาคผนวก)

ก. เปิดเผยโดยความจำเป็นเพื่อการป้องกันหรือสืบหาอาชญากรรม

ข. เปิดเผยเนื่องจากถูกร้องขอโดยผู้มีอำนาจภายใต้กฎหมาย หรือคำสั่งศาล

ค. บุคคลนั้นเชื่อโดยมีเหตุผลว่าตนมีสิทธิที่จะได้รับหรือเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลอื่นได้

ง. บุคคลนั้นเชื่อโดยมีเหตุผลว่าตนจะได้รับความยินยอมจากผู้ควบคุมข้อมูลหากผู้ควบคุมข้อมูลทราบถึงการนั้น

จ. การได้รับหรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อประโยชน์สาธารณะ

ผู้ที่มีความผิดในฐานนี้นอกเหนือจากผู้ซึ่งได้รับหรือเปิดเผยข้อมูลส่วนบุคคลแล้ว ยังรวมถึงผู้ที่เสนอขายข้อมูลส่วนบุคคลของตนเอง และขายข้อมูลส่วนบุคคลของผู้อื่นที่ได้มาโดยการฝ่าฝืนกฎหมายด้วย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998 เป็นกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลโดยหลักการสำคัญของกฎหมายเน้นถึงการบัญญัติถึงหน้าที่ เพื่อบังคับใช้แก่ผู้ควบคุมข้อมูล (data controller) ในการจัดเก็บ ดูแล ควบคุมและใช้ข้อมูลส่วนบุคคลเป็นหลัก ในพระราชบัญญัติฉบับนี้ได้ให้คำนิยามของข้อมูลส่วนบุคคล (personal data) ว่าหมายความถึง ข้อมูลเกี่ยวกับความเป็นอยู่ของบุคคลซึ่งสามารถระบุตัวบุคคลได้จากข้อมูล ซึ่งจากความหมายนี้เองอาจสรุปได้ว่ามีความใกล้เคียงกับข้อมูลซึ่งแสดงเอกลักษณ์บุคคล กล่าวคือเป็นข้อมูลที่ทำให้สามารถระบุตัวบุคคลได้อย่างเฉพาะเจาะจง ดังนี้ข้อมูลซึ่งแสดงเอกลักษณ์บุคคลจึงได้รับความคุ้มครองตามพระราชบัญญัติฉบับนี้ด้วย โดยมีฐานความผิดที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล คือ ความผิดฐานการได้มาหรือเปิดเผยข้อมูลส่วนบุคคลของผู้อื่นโดยมิชอบ

3.1.3.3 **พระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ.** 2006 (The Identity Card Act of 2006)

กฎหมายฉบับนี้ได้จัดตั้งสถาบันทะเบียนเอกลักษณ์บุคคลแห่งชาติ (The Institution of the National Identity Register) เพื่อทำการออกบัตรประจำตัวและหนังสือเดินทาง มีหน้าที่ในการตรวจสอบความถูกต้องของข้อมูล และประวัติของประชาชนที่ถูกเก็บรวบรวมไว้ เพราะกฎหมายต้องการที่จะหาวิธีป้องกันการฉ้อโกง และการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล หน่วยงานสามารถเก็บรวบรวมข้อมูลเกี่ยวกับอาชญากรรมที่มีความเกี่ยวข้องกับบัตรประจำตัวประชาชนได้

การออกกฎหมายฉบับนี้รัฐบาลเห็นว่าจะสามารถช่วยป้องกันการละเมิดข้อมูลส่วนบุคคลได้ เนื่องมาจาก

1. กฎหมายมีข้อจำกัดในการจัดเก็บข้อมูลอย่างเคร่งครัด กล่าวคือ จัดเก็บได้เพียงข้อมูลที่จำเป็นเท่านั้น

2. การขอตรวจสอบหลักฐานข้อมูลซึ่งแสดงเอกลักษณ์บุคคล จะกระทำได้เมื่อได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูลเท่านั้น แต่อาจมีข้อยกเว้นโดยกฎหมายได้

3. กฎหมายไม่ได้บังคับให้เจ้าของบัตรประจำตัวประชาชนจะต้องพกบัตรติดตัวตลอดเวลา

4. หากมีการนำข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นไปใช้โดยมิชอบต้องได้รับโทษทางอาญาตามกฎหมาย

5. กฎหมายได้กำหนดข้อมูลที่สามารถจัดเก็บได้ไว้ท้ายพระราชบัญญัติอย่างชัดเจน ซึ่งแบ่งข้อมูลออกเป็น 9 กลุ่ม[16] ดังนี้

1.) ข้อมูลเกี่ยวกับตัวบุคคล เช่น ชื่อตัว ชื่ออื่นที่บุคคลมีหรือเป็นที่รู้จัก วันเดือนปีเกิด สถานที่เกิด เพศ ฯลฯ

2.) ข้อมูลที่ใช้ระบุตัวบุคคล เช่น รูปภาพถ่าย ลายมือชื่อ ลายพิมพ์นิ้วมือ ฯลฯ

[16] รายละเอียดท้ายพระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 โปรดดูภาคผนวก

3.) ข้อมูลเกี่ยวกับสถานะ เช่น สัญชาติ สิทธิในการพำนักภายในประเทศสหราชอาณาจักร ฯลฯ

4.) หมายเลขอ้างอิงที่เกี่ยวกับตัวบุคคล เช่น หมายเลขประจำตัวประชาชน หมายเลขประจำตัวอื่นที่รัฐบาลออกให้ หมายเลขประกันภัย หมายเลขที่เกี่ยวกับเอกสารการเข้าเมือง หมายเลขหนังสือเดินทางของประเทศสหราชอาณาจักร ตลอดจนหมายเลขเอกสารที่ใช้แทนหนังสือเดินทาง ฯลฯ

5.) บันทึกประวัติข้อมูล เช่น ข้อมูลใดๆ ที่บันทึกในครั้งก่อนๆ รายละเอียดของการเปลี่ยนแปลงข้อมูล วันมรณะ

6.) ประวัติเกี่ยวกับการลงทะเบียน และบัตรประจำตัว เช่น วันที่มีคำขอลงทะเบียน เหตุผลของการไม่บันทึกข้อมูล ฯลฯ

7.) ข้อมูลที่ใช้ในการตรวจสอบความถูกต้องสมบรูณ์ เช่น ข้อมูลที่ใช้ในการเปลี่ยนแปลงรายละเอียดทางทะเบียนในการออกบัตรประจำตัว รายละเอียดเกี่ยวกับขั้นตอนในการตรวจสอบความถูกต้อง ความสมบรูณ์ทางทะเบียน ฯลฯ

8.) ข้อมูลที่ใช้ในการรักษาความปลอดภัยของข้อมูล เช่น หมายเลขเอกลักษณ์ประจำตัวบุคคล รหัสผ่าน หรือวิธีตั้งรหัสผ่านอื่น คำถาม และคำตอบที่ใช้ยืนยันตัวบุคคล

9.) ประวัติการให้ข้อมูล เช่น รายละเอียดเกี่ยวกับข้อมูลที่จัดให้แก่บุคคล รายละเอียดเกี่ยวกับบุคคลที่ให้ข้อมูล ฯลฯ

(ก) คำนิยาม มาตรา 26[17] ได้ให้คำนิยามของคำว่า “เอกสารแสดงข้อมูลเอกลักษณ์บุคคล” (identity document) ไว้ว่า เอกสารใดๆ ที่มีความหมายเหมือน

[17] Identity Card Act 2006 Article 26 (โปรดดูภาคผนวก)

ก. บัตรประจำตัวประชาชน

ข. เอกสารที่เกี่ยวกับชื่อ หรือยศ

ค. เอกสารการเข้าเมือง

ง. หนังสือเดินทางของประเทศสหราชอาณาจักร

จ. หนังสือเดินทางที่ออกโดยผู้มีอำนาจในประเทศหรือนอกอาณาเขตประเทศสหราชอาณาจักรหรือโดยองค์กรระหว่างประเทศ

ฉ. เอกสารที่สามารถใช้แทนหนังสือเดินทางได้ (ในบางสถานการณ์หรือทุกสถานการณ์)

ช. ใบอนุญาตขับขี่ของประเทศสหราชอาณาจักร

ซ. ใบอนุญาตขับขี่ที่ออกโดยผู้มีอำนาจในประเทศหรือนอกอาณาเขตประเทศสหราชอาณาจักร

(ข) องค์ประกอบความผิด มาตรา 25[18] การครอบครองเอกสารปลอมแสดงข้อมูลเอกลักษณ์บุคคลของบุคคลอื่น โดยรู้หรือเชื่อว่าเป็นของปลอม หรือได้มาโดยไม่ถูกต้อง โดยมีเจตนาจะใช้เอกสารนั้นเพื่อลงทะเบียนข้อเท็จจริงเกี่ยวกับตนเอง หรืออนุญาตเพื่อให้บุคคลอื่นใช้ข้อมูลเพื่อสืบ หรือตรวจสอบข้อเท็จจริงเกี่ยวกับตนเองหรือเกี่ยวกับบุคคลอื่น

ในมาตรานี้ยังเอาผิดแก่ผู้ที่จัดทำ หรือมีเครื่องมือ อุปกรณ์ที่สามารถนำมาใช้ทำเอกสารปลอม เพื่อนำเอกสารไปใช้ยืนยันตัวบุคคล

มาตรา 28[19] การให้ข้อมูลเท็จแก่บุคคลอื่น ทั้งกรณีโดยเจตนา คือรู้ว่าข้อมูลเป็นเท็จ หรือประมาท

ก. เกี่ยวกับความปลอดภัย เพื่อการแก้ไขข้อมูลในการลงทะเบียน

---

[18] Identity Card Act 2006 Article 25 (โปรดดูภาคผนวก)

[19] Identity Card Act 2006 Article 28 (โปรดดูภาคผนวก)

ข. เพื่อยืนยัน (มีหรือไม่มีการเปลี่ยนแปลง) ในเนื้อหาหรือรายละเอียดของการลงทะเบียน

ค. เพื่อให้ตนเองได้แก้ไขหรือได้รับบัตรประจำตัวประชาชน

(ค) การกำหนดโทษ ผู้กระทำความผิดฐานครอบครองเอกสารปลอมแสดงข้อมูลเอกลักษณ์บุคคลของบุคคลอื่น โดยรู้หรือเชื่อว่าเป็นของปลอม หรือได้มาโดยไม่ถูกต้อง โดยมีเจตนาจะใช้เอกสารนั้นเพื่อลงทะเบียนข้อเท็จจริงเกี่ยวกับตนเอง หรืออนุญาตเพื่อให้บุคคลอื่นใช้ข้อมูลเพื่อสืบ หรือตรวจสอบข้อเท็จจริงเกี่ยวกับตนเองหรือเกี่ยวกับบุคคลอื่น มีโทษปรับ หรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ

พระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 (The Identity Card Act of 2006) ได้ให้คำนิยามของ“เอกสารแสดงข้อมูลเอกลักษณ์บุคคล” (identity document) ไว้ว่า เอกสารใดๆ ที่มีความหมายเหมือน บัตรประจำตัวประชาชน เอกสารการเข้าเมือง หนังสือเดินทางของประเทศสหราชอาณาจักร ใบอนุญาตขับขี่ของประเทศสหราชอาณาจักร ฯลฯ ซึ่งจากคำนิยามนี้เองทำให้เห็นว่าแม้ชื่อของพระราชบัญญัติจะเป็นพระราชบัญญัติบัตรประจำตัวประชาชน แต่เนื้อหาในกฎหมายได้ให้ความคุ้มครองแก่เอกสารอื่นๆ นอกเหนือจากบัตรประจำตัวประชาชนด้วย เช่น หนังสือเดินทาง ในอนุญาตขับขี่ เป็นต้น ทำให้พระราชบัญญัติฉบับนี้สามารถให้ความคุ้มครองเอกสารที่แสดงข้อมูลเอกลักษณ์บุคคลได้หลายประเภทมิใช่ให้ความคุ้มครองเพียงบัตรประจำตัวประชาชนเท่านั้น ซึ่งแตกต่างจากพระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ของประเทศไทยที่แม้จะมีชื่อกฎหมายที่เหมือนกันแต่กฎหมายไทยให้ความคุ้มครองเอกสารเพียงชนิดเดียว คือบัตรประจำตัวประชาชน ฐานความผิดในพระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 ที่มีความเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล คือ การครอบครองเอกสารปลอมที่แสดงข้อมูลเอกลักษณ์บุคคลของผู้อื่น หรือได้มาโดยไม่ถูกต้องซึ่งเอกสารแสดงข้อมูลเอกลักษณ์บุคคลของผู้อื่น โดยมีเจตนาจะใช้เอกสารเพื่อแสวงหาผลประโยชน์โดยมิชอบ

3.1.3.4 **พระราชบัญญัติการฉ้อโกง ค.ศ.** 2006 (The Fraud Act of 2006)

กฎหมายฉบับนี้ อาจนำไปปรับใช้กับการกระทำความผิดที่มีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศเป็นเครื่องมือช่วยในการกระทำความผิดได้ เช่น การฟิชชิ่ง (Phishing) การฟามมิ่ง (Pharming) เพื่อแอบอ้างใช้ข้อมูลส่วนตัวของบุคคลอื่น เนื่องจากได้มีการบัญญัติการฉ้อโกงไว้แบบกว้างๆ และไม่จำต้องพิสูจน์ถึงการหลอกลวงหรือการได้มาซึ่งทรัพย์สินซึ่งต่างจากกฎหมายเดิม

(ก) คำนิยาม กฎหมายฉบับนี้ได้กำหนดนิยามและแบ่งรูปแบบการฉ้อโกงออกเป็น 3 ประเภทใหญ่ๆ คือ

1. การฉ้อโกงโดยเป็นตัวแทนปลอมหรือฉ้อโกงโดยแสดงตนอันเป็นเท็จ (fraud by false representation) คือ บุคคลใดไม่ซื่อสัตย์แสดงตนเป็นตัวแทนทำให้ผู้อื่นเข้าใจผิด เพื่อแสวงหาประโยชน์สำหรับตนเองหรือผู้อื่น เป็นเหตุให้บุคคลอื่นเกิดความเสียหาย หรือความเสี่ยงที่จะเสียหาย

2. การฉ้อโกงโดยการเปิดเผยข้อมูล (fraud by failing to disclose information) คือ บุคคลผู้มีหน้าที่ตามกฎหมายในการเปิดเผยข้อมูล ได้เปิดเผยข้อมูลโดยไม่ชอบแก่บุคคลอื่นเพื่อแสวงหาประโยชน์สำหรับตนเองหรือผู้อื่น เป็นเหตุให้บุคคลอื่นเกิดความเสียหาย หรือความเสี่ยงที่จะเสียหาย

3. การฉ้อโกงโดยละเมิดหน้าที่ (fraud by abuse of position) คือ เจ้าหน้าที่ผู้มีหน้าที่เกี่ยวข้องกับผลประโยชน์ทางการเงินของบุคคลอื่น ทุจริตในหน้าที่ เพื่อแสวงหาประโยชน์สำหรับตนเองหรือผู้อื่น เป็นเหตุให้บุคคลอื่นเกิดความเสียหาย หรือความเสี่ยงที่จะเสียหาย การกระทำนั้นรวมถึงการละเลยเพิกเฉยต่อหน้าที่ด้วย

(ข) องค์ประกอบความผิด มาตรา 7[20] กำหนดความผิดในการจัดทำขึ้น หรือจำหน่ายของที่ใช้เพื่อการฉ้อโกงโดยผู้นั้นมีความผิดถ้าได้ ทำขึ้น ดัดแปลง จำหน่าย หรือเสนอขายสิ่งของใดๆ โดยรู้ว่าของนั้นถูกทำ หรือดัดแปลงสำหรับใช้ในการฉ้อโกง

(ค) การกำหนดโทษ ในคดีความผิดเล็กน้อย โทษจำคุกไม่เกิน 12 เดือน หรือปรับไม่เกินที่กฎหมายกำหนด หรือทั้งจำทั้งปรับ กรณีความผิดร้ายแรง โทษจำคุกไม่เกิน 10 ปี หรือปรับ หรือทั้งจำทั้งปรับ

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล คือการลักข้อมูลส่วนบุคคลของผู้อื่นไปใช้เพื่อแสวงหาประโยชน์โดยมิชอบ การฉ้อโกงก็เป็นการกระทำความผิดรูปแบบหนึ่งที่เกิดขึ้นเนื่องจากการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล กล่าวคือการนำข้อมูลไปใช้ฉ้อโกง โดยในพระราชบัญญัติการฉ้อโกง ค.ศ. 2006 นี้ได้แบ่งแยกลักษณะของการฉ้อโกงออกเป็น 3 ลักษณะ คือ ฉ้อโกงโดยแสดงตนอันเป็นเท็จ การฉ้อโกงโดยการเปิดเผยข้อมูล และการฉ้อโกงโดยละเมิดหน้าที่ การบัญญัติความผิดฐานฉ้อโกงของพระราชบัญญัติการฉ้อโกงนี้จึงมีความเหมือนกับกฎหมายการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของประเทศแคนาดาในส่วนฐานความผิดการฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Fraud)

---

[20] The Fraud Act of 2006 Article 7 Making or supplying articles for use in frauds

(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article—

(a) knowing that it is designed or adapted for use in the course of or in connection with fraud, or

(b) intending it to be used to commit, or assist in the commission of, fraud.

(2) A person guilty of an offence under this section is liable—

(a) on summary conviction, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum (or to both);

(b) on conviction on indictment, to imprisonment for a term not exceeding 10 years or to a fine (or to both).

3.2 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลตามกฎหมายไทย

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นการลักข้อมูลส่วนตัวของบุคคลอื่นไปใช้เพื่อแสวงหาประโยชน์อันมิชอบ อาทิ เพื่อไปกระทำความผิดฉ้อโกงหรือกระทำความผิดเกี่ยวกับอาชญากรรมอื่นๆ เช่น การแอบดู และจดจำรายละเอียดข้อมูลที่อยู่บนบัตรอิเล็กทรอนิกส์ของผู้อื่นเพื่อนำไปใช้แสวงหาประโยชน์โดยมิชอบ ถ้าเป็นการลักข้อมูลที่เป็นเอกสารอาจเป็นความผิดฐานลักทรัพย์ แต่บางกรณีการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไม่เป็นความผิดฐานลักทรัพย์ เพราะ ผู้กระทำมิได้ลักเอาตัวทรัพย์ไป ลักเพียงข้อมูลเท่านั้น จึงมีบางกรณีที่มาสามารถนำกฎหมายไทยที่มีอยู่ในปัจจุบันมาบังคับใช้กับการกระทำความผิดได้ จึงเห็นควรศึกษากฎหมายไทยปัจจุบันที่นำมาปรับใช้กับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลว่ามีข้อจำกัดประการใดบ้าง เพื่อให้สามารถนำเสนอแนวทางการกำหนดกฎหมายสำหรับความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้อย่างเหมาะสมกับลักษณะของความผิด

3.2.1 การกระทำความผิดตามประมวลกฎหมายอาญาที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

เมื่อเกิดมีการกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลขึ้น บทบัญญัติกฎหมายที่เกี่ยวข้องที่สามารถนำมาบังคับใช้กับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้ในบางกรณี คือ ประมวลกฎหมายอาญา ฐานความผิดที่มีบทบัญญัติเกี่ยวข้องกับรูปแบบของการกระทำความผิดมีดังนี้

3.2.1.1 ความผิดเกี่ยวกับการปกครองที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

ความผิดเกี่ยวกับการปกครอง ในประมวลกฎหมายอาญา ลักษณะ 2 ความผิดต่อเจ้าพนักงาน หมวด 1

ฐานความผิดในหมวดความผิดต่อเจ้าพนักงานที่มีความเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล คือ ความผิดที่ราษฎรกระทำผิดต่อเจ้าพนักงาน ฐานแจ้งความเท็จต่อเจ้าพนักงานในมาตรา 137 การกระทำใดจะเป็นความผิดต่อเมื่อการกระทำนั้นครบองค์ประกอบความผิด[21] ดังนี้

<u>องค์ประกอบภายนอก</u>

1. แจ้งข้อความ
2. อันเป็นเท็จ
3. แก่เจ้าพนักงาน
4. ซึ่งอาจทำให้ผู้อื่น หรือประชาชนเสียหาย

<u>องค์ประกอบภายใน</u> เจตนา

การกระทำความผิดฐานแจ้งความเท็จต่อเจ้าพนักงานนี้ต้องเป็นการกระทำต่อเจ้าพนักงานผู้มีหน้าที่รับแจ้งความในเรื่องนั้นๆ หากเป็นการแจ้งความเท็จแก่บุคคลทั่วไป หรือเจ้าพนักงานผู้ไม่มีหน้าที่ หรือไม่มีส่วนเกี่ยวข้องแล้ว การกระทำนั้นก็จะไม่เป็นความผิด และในการแจ้งความตามความหมายในมาตรานี้รวมถึงการแจ้งโดยวิธีกรอกข้อความเท็จลงในเอกสารแล้วยื่นให้แก่เจ้าพนักงานด้วย ดังนี้การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นมาแล้วนำข้อมูลมาแจ้งแก่เจ้าพนักงานเพื่อขอให้ออกเอกสาร หรือกระทำการติดต่อใดๆ ผู้กระทำการนั้นย่อมมีความผิดฐานแจ้งความเท็จ เนื่องจากครบองค์ประกอบความผิด กล่าวคือมีการกระทำโดยการนำข้อมูลของบุคคลอื่นมาแจ้งหรือกรอกข้อความว่าเป็นข้อมูลของตนเองย่อมเป็นความเท็จ และอาจทำให้ผู้อื่นเสียหาย คือผู้ที่เป็นเจ้าของข้อมูลอาจได้รับความเสียหาย แต่อย่างไรก็ตามฐานความผิดนี้ยังมีข้อจำกัด คือ ต้องเป็นการแจ้งความเท็จแก่เจ้าพนักงานผู้มีหน้าที่รับแจ้งความเท่านั้นและผู้ที่

[21] ทวีเกียรติ มีนะกนิษฐ, <u>คำอธิบายกฎหมายอาญา ภาคความผิดและลหุโทษ</u>, พิมพ์ครั้งที่ 3 (กรุงเทพมหานคร: วิญญูชน, 2549), หน้า 259-262.

เป็นผู้เสียหายในความผิดฐานนี้ คือ เจ้าพนักงาน มิใช่ผู้ที่ถูกลักข้อมูลซึ่งแสดงเอกลักษณ์บุคคลมาใช้แต่อย่างใด

3.2.1.2 **ความผิดเกี่ยวกับเอกสารที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล**

ความผิดเกี่ยวกับเอกสาร ในประมวลกฎหมายอาญา ลักษณะ 7 ความผิดเกี่ยวกับการปลอมและการแปลง หมวด 3

การจะพิจารณาว่าการกระทำใดๆ จะครบองค์ประกอบของฐานความผิดในหมวดนี้หรือไม่ ย่อมต้องพิจารณาก่อนว่า “เอกสาร” ตามความในหมวดนี้นั้นมีความหมายว่าอย่างไร

ประมวลกฎหมายอาญาได้ให้คำนิยามของคำว่า “เอกสาร” ไว้ในมาตรา 1(7) ว่า “เอกสาร หมายความว่า กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ถ่ายภาพหรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น” จากคำนิยามนี้สิ่งใดจะจัดเป็นเอกสารต้องมีสาระสำคัญ 4 ประการ[22] คือ

1.) ต้องเป็นสิ่งที่มีรูปร่าง เพื่อให้มีความมั่นคงพอควร เนื่องจากเอกสารมีความสำคัญในการใช้เป็นหลักฐาน

2.) ต้องมุ่งแสดงความหมาย คือ สื่อถึงความคิดของผู้กระทำ มีเจตนาที่จะแสดงความหมาย แม้ผู้อื่นจะไม่เข้าใจก็ตาม[23]

3.) ต้องสามารถมองเห็นได้ด้วยตาเปล่า เพื่อสามารถใช้เป็นพยานหลักฐาน หากไม่สามารถเห็นได้ด้วยตาเปล่าก็ไม่ใช่เอกสาร เช่น แถบแม่เหล็กในบัตรเครดิต บาร์โค้ด บัตรที่ใช้คลื่นวิทยุ หรือไมโครชิพต่างๆ แม้จะสามารถเก็บข้อมูลต่างๆ ได้มากมายก็ตาม แต่จะต้องอ่าน

---

[22] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, คำอธิบายความผิดเกี่ยวกับ การปลอมและการแปลง ตามประมวลกฎหมายอาญา (กรุงเทพมหานคร: วิญญูชน, 2555), หน้า 108.

[23] ทวีเกียรติ มีนะกนิษฐ, คำอธิบายกฎหมายอาญา ภาคความผิดและลหุโทษ, พิมพ์ครั้งที่ 3 (กรุงเทพมหานคร: วิญญูชน , 2549), หน้า 372.

ข้อมูลจากระบบอื่นๆ ซึ่งไม่สามารถเห็นได้ด้วยตาเปล่า ไม่ถือเป็นเอกสารตามมาตรา 1(7) แต่อาจเป็นบัตรอิเล็กทรอนิกส์ตามความหมายในมาตรา 1(14) ได้ การมองเห็นด้วยตาเปล่านี้อาจทำให้ปรากฏบนวัตถุต่างๆ ด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่นก็ได้ เช่น ชื่อ นามสกุล วันเดือนปีเกิด ในบัตรประจำตัวประชาชน ผังที่ดินในหน้าโฉนดที่ดิน ฯลฯ

4.) ไม่จำกัดรูปแบบในการทำเอกสาร เช่น โดยการพิมพ์ การถ่ายภาพ หรือวิธีอื่นๆ เช่น ป้ายทะเบียนรถยนต์

ในความผิดฐานปลอมเอกสาร มาตรา 264 มีองค์ประกอบความผิด[24] ดังนี้

<u>องค์ประกอบภายนอก</u>

1. ผู้ใด

2. (ก) ทำเอกสารปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด

(ข) เติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใดๆ ในเอกสารที่แท้จริง หรือ

(ค) ประทับตราปลอม หรือลงลายมือชื่อปลอมในเอกสาร

3. โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น หรือประชาชน

<u>องค์ประกอบภายใน</u>

1.เจตนา

2.เจตนาพิเศษ เพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารที่แท้จริง

ความผิดฐานปลอมเอกสารสิทธิ มาตรา 265 มีองค์ประกอบความผิดเช่นเดียวกับการปลอมเอกสารมาตรา 264 กล่าวคือเป็นบทฉกรรจ์ที่ผู้กระทำความผิดต้องรับโทษหนักขึ้น หากเอกสารที่ปลอมนั้นเป็นเอกสารสิทธิหรือเอกสารราชการ

---

[24] เกียรติขจร วัจนะสวัสดิ์, <u>กฎหมายอาญา ภาคความผิด เล่ม2</u>, พิมพ์ครั้งที่ 5 (กรุงเทพมหานคร: จิรรัชการพิมพ์, 2550), หน้า 126.

ความผิดฐานใช้เอกสารปลอม มาตรา 268 คือผู้ใดใช้หรืออ้างเอกสารที่ปลอมขึ้นตามมาตรา 264 หรือมาตรา 265 ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษดังที่บัญญัติไว้ในมาตรานั้นๆ

เมื่อพิจารณาจากองค์ประกอบความผิดฐานปลอมเอกสารนี้แล้ว เห็นได้ว่าสามารถปรับใช้กับการกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้ในบางกรณี เช่น กรณีที่ผู้กระทำความผิดนำเอกลักษณ์บุคคล ชื่อ และหมายเลขบัญชีธนาคารของผู้เสียหายมาใช้เพื่อกระทำความผิด คือนำข้อมูลนั้นมาปลอมใบถอนเงิน เพื่อทำการถอนเงินออกจากบัญชีของผู้เสียหาย ตัวอย่างคดีจากคำพิพากษาฎีกาที่ 1104/2545[25] จากข้อเท็จจริง คือ จำเลยเป็นพนักงานธนาคาร ได้รู้ข้อมูลบัญชีของผู้เสียหาย จึงทำการปลอมใบถอนเงิน จนถอนเงินจากบัญชีของผู้เสียหายได้สำเร็จ ซึ่งกระทำการเช่นนี้ถึง 11 ครั้งได้เงินของผู้เสียหายไปเป็นจำนวนสามล้านกว่าบาท ศาลฎีกาวินิจฉัยไว้ว่า การกระทำของ จำเลยมีความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญา มาตรา 335(11) วรรคแรก และมีความผิดฐานเป็นผู้ปลอมเอกสารสิทธิและใช้เอกสารสิทธิปลอม ตามประมวลกฎหมายอาญามาตรา 265, 268 วรรคแรก ประกอบด้วยมาตรา 265

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลกับความผิดฐานปลอมเอกสาร เอกสาร มีหมายความว่า กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ถ่ายภาพหรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น ข้อมูลซึ่งแสดงเอกลักษณ์บุคคลจึงย่อมมีปรากฏอยู่บนเอกสารใดๆ ได้ เช่น บัตรประจำตัวประชาชน บัตรเครดิต ใบสูติบัตร ฯลฯ ดังนี้หากผู้โจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้ลักเอาตัวเอกสารที่มีข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นไป แล้วนำข้อมูลนั้นมาทำเอกสารปลอมขึ้น เช่น ลักบัตรประจำตัวประชาชนของผู้อื่นมาแล้วนำมาปรับแก้ไขชื่อ หรือข้อมูลอื่นๆ บนบัตร ผู้กระทำย่อมมีความผิดฐานปลอมเอกสาร แต่หากเป็นกรณีการลักข้อมูลซึ่งแสดงเอกลักษณ์บุคคลมาแล้วแต่ยังไม่ได้กระทำการใดๆ กับตัวเอกสาร หรือยังไม่ได้ทำเอกสารปลอม

[25] ฎีกาตัดสินเกี่ยวกับปัญหาข้อกฎหมาย [ออนไลน์], พฤศจิกายน 2555 แหล่งที่มา www.law-community.com/newsdata/file_data/1304306256.doc.

ใดๆ ขึ้น ผู้กระทำนั้นก็ยังไม่มีความผิดฐานปลอมเอกสาร ซึ่งถือเป็นข้อจำกัดของฐานความผิดนี้ กล่าวคือ หากเป็นกรณีที่มีผู้โจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นไปโดยมีเจตนาจะนำไปใช้แสวงหาประโยชน์โดยมิชอบด้วยกฎหมาย แต่ยังไม่มีการจัดทำปลอมขึ้นซึ่งเอกสาร การกระทำนั้นจะยังไม่เป็นความผิด ยกตัวอย่างเช่น พนักงานธนาคารได้เก็บเอกสารที่มีข้อมูลส่วนบุคคลของลูกค้าไว้ เพื่อหวังที่จะนำข้อมูลของลูกค้าไปกรอกแบบฟอร์มเพื่อถอนเงินออกจากบัญชีของลูกค้า ดังนี้การเก็บข้อมูลของลูกค้าไว้ ยังไม่ถือเป็นการกระทำความผิดฐานปลอมเอกสาร หรือฐานใช้เอกสารปลอมแต่อย่างใด เป็นต้น

ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ในประมวลกฎหมายอาญา ลักษณะ 7 ความผิดเกี่ยวกับการปลอมและการแปลง หมวด 4

การจะพิจารณาว่าการกระทำใดๆ จะครบองค์ประกอบของฐานความผิดในหมวดนี้หรือไม่ ย่อมต้องพิจารณาก่อนว่า “บัตรอิเล็กทรอนิกส์” นั้นมีความหมายว่าอย่างไร ประมวลกฎหมายอาญาได้ให้คำนิยามของคำว่า “บัตรอิเล็กทรอนิกส์” ไว้ในมาตรา 1(14) ว่า

> “บัตรอิเล็กทรอนิกส์ หมายความว่า
>
> (ก) เอกสารหรือวัตถุอื่นใดไม่ว่าจะมีรูปลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใด ทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า
> (ข) ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยมิได้มีการออกเอกสารหรือวัตถุใดให้ แต่มีวิธีการใช้ในทำนองเดียวกับ (ก) หรือ
> (ค) สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ”

จากคำนิยามนี้ จึงสามารถแบ่งลักษณะของบัตรอิเล็กทรอนิกส์ได้เป็น 3 ประเภท คือ

(1 ก) ไม่จำกัดเฉพาะที่เป็นเอกสารเท่านั้น แต่รวมถึงวัตถุอื่นใดไม่ว่าจะมีลักษณะใดด้วย[26] กล่าวคือไม่จำกัดว่าต้องออกมาในรูปของบัตรเท่านั้น อย่างบัตรหลากหลายประเภทที่มีใช้กันอยู่ในปัจจุบัน จำพวกบัตรเครดิต บัตรเดบิต บัตรเอทีเอ็ม บัตรซิมการ์ด บัตรสมาร์ทการ์ด ฯลฯ แต่อาจอยู่ในรูปวัตถุอื่นใด เช่น กระดาษ หรือหีบห่อ ต่างๆ ที่ห่อหุ้มสินค้า ซึ่งระบุตัวเลขและลายเส้นต่างๆ ที่เรียกกันว่ารหัสแท่งหรือบาร์โค้ด[27] ก็ได้

(2 ข) ตามนิยามข้อ (ข) จะมุ่งเน้นที่เรื่องของ ข้อมูล รหัส หมายเลขบัญชี โดยที่ผู้ออกมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ด้วย เช่น รหัส Pin Phone รหัสเติมเงิน รหัสจองตั๋วเครื่องบิน (E-Ticket) ที่มิได้มีการออกเอกสารอื่นๆ ให้อีก

(3ค) สิ่งที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อระบุตัวบุคคล หมายถึงลักษณะเฉพาะของบุคคล (Biometric) เช่น ลายนิ้วมือ ม่านตา เสียง หรือ DNA เป็นต้น ซึ่งสิ่งเหล่านี้จะถือเป็นบัตรอิเล็กทรอนิกส์ก็ต่อเมื่อนำไปใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์[28] เช่น ลายนิ้วมือที่ใช้เปิดอุปกรณ์เครื่องคอมพิวเตอร์ ประตูรถยนต์ เสียงหรือม่านตาที่ใช้เพื่อเปิดประตูห้องหรือตู้นิรภัย เป็นต้น

เมื่อได้ทราบถึงความหมายของบัตรอิเล็กทรอนิกส์แล้ว ก็จะต้องมาพิจารณาถึงความผิดที่เกี่ยวข้องซึ่งมีอยู่ด้วยกันหลายลักษณะ แต่ในที่นี้ผู้เขียนขอกล่าวถึงเฉพาะมาตราที่เป็นฐานความผิดสำคัญ และมีอุปสรรคปัญหาในการบังคับใช้แก่การกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

---

[26] ทวีเกียรติ มีนะกนิษฐ, คำอธิบายกฎหมายอาญา ภาคความผิดและลหุโทษ, หน้า 382.

[27] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญา ภาคความผิด เล่ม2, หน้า 222.

[28] สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, คำอธิบายความผิดเกี่ยวกับ การปลอมและการแปลง ตามประมวลกฎหมายอาญา, หน้า 160.

ความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ในประมวลกฎหมายอาญามาตรา 269/1 มีองค์ประกอบความผิด[29] ดังนี้

องค์ประกอบภายนอก

1. ผู้ใด
2. (ก) ทำบัตรอิเล็กทรอนิกส์ปลอมขึ้นทั้งฉบับ หรือแต่ส่วนหนึ่งส่วนใด

(ข) เติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใดๆ ในบัตรอิเล็กทรอนิกส์ที่แท้จริง

3. โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

องค์ประกอบภายใน

1. เจตนา
2. เจตนาพิเศษ ถ้าได้กระทำ

(ก) เพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นบัตรอิเล็กทรอนิกส์ที่แท้จริง หรือ

(ข) เพื่อใช้ประโยชน์อย่างหนึ่งอย่างใด

ความผิดฐานปลอมบัตรอิเล็กทรอนิกส์นี้ ไม่อาจปรับใช้ได้กับการกระทำการโจรกรรมเอกลักษณ์บุคคลในรูปแบบที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ได้ในทุกกรณี เนื่องมาจากบ่อยครั้งที่ อาชญากรมิได้ทำการปลอมบัตรอิเล็กทรอนิกส์ของเหยื่อแต่อย่างใด แต่อาชญากรได้อาศัยข้อมูลส่วนตัวของเหยื่อทำการติดต่อกับธนาคารเพื่อขอทำบัตรเครดิตขึ้นใหม่ในชื่อของเหยื่อโดยตรงเลย ดังนี้การที่ธนาคารผู้มีอำนาจในการออกบัตรเครดิตได้ออกบัตรเครดิตให้แก่อาชญากรด้วยเชื่อว่าเป็นบุคคลเจ้าของข้อมูลตัวจริงนั้น จึงไม่ถือเป็นการปลอมบัตรอิเล็กทรอนิกส์ตามมาตรา 269/1 เนื่องจากเป็นการออกบัตรเครดิตให้โดยธนาคาร หรือสถาบันการเงินที่มีอำนาจในการออกบัตรเครดิตอย่างถูกต้อง กรณีหากมีการจับกุมผู้กระทำการคัดลอกข้อมูลเอกลักษณ์บุคคล

[29] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญา ภาคความผิด เล่ม2,หน้า 231.

ต่างๆ ของเหยื่อไปเป็นจำนวนมาก แต่ยังมิได้มีการลงมือทำการปลอมบัตรเครดิตหรือใช้บัตรเครดิตปลอม ผู้กระทำการนั้นอาจไม่ต้องรับผิดในทางอาญา เพราะการลอกเอาข้อมูลส่วนตัวของเหยื่อนั้นยังไม่อาจถือว่าเป็นความผิดฐานลักทรัพย์ เพราะข้อมูลมิใช่ทรัพย์

ความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ตามประมวลกฎหมายอาญามาตรา 269/5 เมื่อนำฐานความผิดนี้มาใช้กับกรณีการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลจะเกิดปัญหา คือ ไม่อาจปรับใช้มาตรานี้เพื่อเอาผิดแก่ผู้กระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในกรณีเกี่ยวกับการจดจำหมายเลขบัตรเครดิตหรือข้อมูลต่างๆ บนบัตรเครดิตแล้วนำไปใช้แสวงหาประโยชน์โดยมิชอบต่างๆ ได้ เนื่องจากปัญหาความหมายของบัตรอิเล็กทรอนิกส์ที่กล่าวมาในข้อ (ข) ที่ว่าจะเป็นบัตรอิเล็กทรอนิกส์ในความหมายนี้ได้ต้องเป็นข้อมูลเลขรหัส หรือหมายเลขต่างๆ ที่ผู้ออกมิได้ออกเอกสารหรือวัตถุอื่นใดให้ ในกรณีหมายเลขบนบัตรเครดิต รวมทั้งวันหมดอายุ หรือข้อมูลต่างๆ ที่ปรากฏอยู่บนบัตรเครดิต จึงไม่เข้าความหมายในข้อ (ข) ดังนี้เฉพาะหมายเลขบัตรเครดิตแต่เพียงอย่างเดียวจึงมิใช่ “บัตรอิเล็กทรอนิกส์” จึงเกิดปัญหาว่าหากมีการจดจำและนำเฉพาะหมายเลขและวันหมดอายุของบัตรเครดิตของผู้อื่นไปใช้โดยมิชอบโดยมิได้นำตัวบัตรเครดิตของผู้อื่นไปใช้ด้วย ผู้กระทำนั้นก็จะไม่มีความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/5 เพราะหมายเลขบัตรและวันหมดอายุดังกล่าวไม่ใช่บัตรอิเล็กทรอนิกส์ ซึ่งปัญหานี้สามารถเกิดขึ้นได้จริงในทางปฏิบัติเนื่องจากในปัจจุบันการชำระค่าสินค้า หรือค่าอาหารต่างๆ สามารถกระทำได้โดยเพียงบอกหมายเลขบัตรเครดิต เช่น การโทรสั่งอาหารดิลิเวอรี่หรือสั่งซื้อสินค้าออนไลน์ ทั้งเมื่อกรณีเกิดการกระทำความผิดขึ้นจะนำความผิดในมาตรานี้มาอนุโลมใช้ก็มิน่าจะกระทำได้ เนื่องจากการตีความกฎหมายอาญาในการลงโทษบุคคลใดนั้นจะต้องตีความโดยเคร่งครัด[30]

หมวดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์นี้ได้มีการบัญญัติฐานความผิดสำหรับบุคคลที่ทำเครื่องมือ หรือวัตถุสำหรับใช้ในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ไว้ด้วยในมาตรา 269/2 ซึ่งแตกต่างจากฐานความผิดอื่นๆ ในลักษณะความผิดเกี่ยวกับการปลอมและการแปลง

[30] เรื่องเดียวกัน, หน้า 260.

บัตรอิเล็กทรอนิกส์ คือ เอกสารที่แสดงข้อมูลซึ่งแสดงเอกลักษณ์บุคคลประเภทหนึ่ง เนื่องจากข้อมูลในบัตรอิเล็กทรอนิกส์นั้นสามารถระบุตัวบุคคลได้ และเป็นข้อมูลของบุคคลคนนั้นเพียงคนเดียว เป็นข้อมูลเฉพาะซึ่งจะไม่เหมือนกับของบุคคลอื่น ดังนั้นการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเมื่อได้ข้อมูลมาแล้วนำมาทำการปลอมบัตรอิเล็กทรอนิกส์ขึ้น แล้วนำบัตรอิเล็กทรอนิกส์ปลอมไปใช้ หรือลักบัตรอิเล็กทรอนิกส์ของผู้อื่นมาใช้ ผู้กระทำจึงมีความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ใช้บัตรอิเล็กทรอนิกส์ปลอม หรือใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบได้ ข้อจำกัดของความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ คือ หากเป็นกรณีที่ไม่ได้มีการลักเอาบัตรอิเล็กทรอนิกส์ไป เพียงแต่จดจำหมายเลขบัตร หรือข้อมูลอื่นๆ ที่อยู่บนบัตรไปใช้เพื่อแสวงหาประโยชน์แต่เพียงอย่างเดียว ผู้กระทำนั้นไม่มีความผิดฐานปลอมบัตรอิเล็กทรอนิกส์หรือใช้บัตรอิเล็กทรอนิกส์ปลอมแต่อย่างใด เนื่องจากข้อมูลที่ปรากฏอยู่บนตัวบัตรไม่ถือบัตรอิเล็กทรอนิกส์

ความผิดเกี่ยวกับหนังสือเดินทาง ในประมวลกฎหมายอาญาลักษณะ 7 ความผิดเกี่ยวกับการปลอมและการแปลง หมวด 5

การจะพิจารณาว่าการกระทำใดๆ จะครบองค์ประกอบของฐานความผิดในหมวดนี้หรือไม่ ย่อมต้องพิจารณาก่อนว่า “หนังสือเดินทาง” ตามความในหมวดนี้นั้นมีความหมายว่าอย่างไร

ประมวลกฎหมายอาญาได้ให้คำนิยามของคำว่า “หนังสือเดินทาง” ไว้ในมาตรา 1(15) ว่า “หนังสือเดินทาง” หมายความว่า เอกสารสำคัญประจำตัวไม่ว่าจะมีรูปลักษณะใดที่รัฐบาลไทย รัฐบาลต่างประเทศ หรือองค์การระหว่างประเทศออกให้แก่บุคคลใด เพื่อใช้แสดงตนในการเดินทางระหว่างประเทศ และให้หมายความรวมถึงเอกสารใช้แทนหนังสือเดินทางและแบบหนังสือเดินทางที่ยังไม่ได้กรอกข้อความเกี่ยวกับผู้ถือหนังสือเดินทางด้วย

ในความผิดฐานปลอมหนังสือเดินทางในมาตรา 269/8 มีองค์ประกอบความผิดเหมือนกับการปลอมเอกสารในมาตรา 264 กล่าวคือ มีองค์ประกอบความผิด ดังนี้

องค์ประกอบภายนอก

1. ผู้ใด

2. (ก) ทำหนังสือเดินทางปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด

(ข) เติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใดๆ ในหนังสือเดินทางที่แท้จริง หรือ

(ค) ประทับตราปลอม หรือลงลายมือชื่อปลอมในหนังสือเดินทาง

3. โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น หรือประชาชน

องค์ประกอบภายใน

1.เจตนา

2.เจตนาพิเศษ เพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นหนังสือเดินทางที่แท้จริง

การปลอมหนังสือเดินทางมีองค์ประกอบของความผิดเช่นเดียวกันกับการปลอมเอกสาร เนื่องจากหนังสือเดินทางก็เป็นเอกสารที่แสดงความหมายอย่างหนึ่งแต่ที่มีการกำหนดไว้เป็นความผิดเฉพาะแยกออกจากความผิดฐานปลอมเอกสาร เนื่องมาจากหนังสือเดินทางถือเป็นเอกสารที่มีความสำคัญมากเป็นพิเศษ จึงเห็นควรมีการกำหนดโทษสำหรับความผิดฐานปลอมหนังสือเดินทางนั้นหนักกว่าการปลอมเอกสาร และการปลอมเอกสารราชการ เนื่องจากการตระหนักถึงปัญหาการก่อการร้าย และอาชญากรรมข้ามชาติในปัจจุบันที่ได้ทวีความรุนแรงมากขึ้น มีการใช้หนังสือเดินทางเป็นเครื่องมือในการกระทำความผิดซึ่งเป็นเรื่องที่ส่งผลกระทบต่อความมั่นคงภายในประเทศ และกระทบต่อความสัมพันธ์ระหว่างประเทศด้วย จึงมีการบัญญัติเพิ่มเติมและขยายขอบเขตของการกระทำความผิดเกี่ยวกับหนังสือเดินทางให้กว้างมากขึ้น นอกเหนือไปจากความผิดฐานปลอมเอกสารธรรมดาอีก กล่าวคือ กำหนดความผิดขึ้นใหม่กรณี “มีไว้เพื่อใช้” “จำหน่าย” “มีไว้เพื่อจำหน่าย” และมีการกำหนดข้อสันนิษฐานการมีไว้เพื่อจำหน่าย ใน

มาตรา 269/9 กำหนดความผิดฐาน “นำเข้าใน” หรือ “ส่งออกนอก” ราชอาณาจักรซึ่งหนังสือเดินทางปลอม ในมาตรา 269/10 และกำหนดความผิดฐาน “ใช้หนังสือเดินทางของผู้อื่นโดยมิชอบ” และ “จัดหาหนังสือเดินทาง” ในมาตรา 269/11[31] เนื่องจากความผิดเกี่ยวกับหนังสือเดินทางนี้เป็นฐานความผิดที่เพิ่งกำหนดขึ้นใหม่ มีผลใช้บังคับเมื่อ วันที่ 16 สิงหาคม 2550 ทำให้การบัญญัติกฎหมายนั้นครอบคลุมได้มากกว่าความผิดฐานปลอมเอกสารธรรมดา หนังสือเดินทางถือเป็นเอกสารที่มีข้อมูลซึ่งแสดงเอกลักษณ์บุคคลปรากฏอยู่ ดังนั้นการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไปแล้วทำการปลอมหนังสือเดินทาง หรือใช้หนังสือเดินทางปลอม จึงเป็นความผิดฐานปลอมหนังสือเดินทางหรือใช้หนังสือเดินทางปลอมได้

3.2.1.3 **ความผิดเกี่ยวกับทรัพย์ที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล**

ความผิดฐานลักทรัพย์ ในประมวลกฎหมายอาญาลักษณะ 12 ความผิดเกี่ยวกับทรัพย์ หมวด 1

การจะพิจารณาว่าการกระทำใดๆ จะครบองค์ประกอบของฐานความผิดนี้หรือไม่ ย่อมต้องพิจารณาถึงองค์ประกอบความผิดและความหมายขององค์ประกอบแต่ละส่วนก่อนว่ามีความหมายอย่างไร องค์ประกอบความผิดฐานลักทรัพย์มาตรา 334[32] มีดังนี้

<u>องค์ประกอบภายนอก</u>

1. ผู้ใด (ผู้กระทำ)
2. เอาไป (การกระทำ)
3. ทรัพย์ของผู้อื่น หรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วย (วัตถุแห่งการกระทำ)

<u>องค์ประกอบภายใน</u>

---

[31] เรื่องเดียวกัน, หน้า 264-267.

[32] เกียรติขจร วัจนะสวัสดิ์, <u>กฎหมายอาญา ภาคความผิด เล่ม3</u> (กรุงเทพมหานคร: จิรรัชการพิมพ์, 2550), หน้า 1.

1. เจตนา (เจตนาธรรมดา คือ ประสงค์ต่อผล หรือเล็งเห็นผล)
2. เจตนาพิเศษ คือ “โดยทุจริต”

องค์ประกอบความผิดหรือคำที่มีความสำคัญ และมักก่อให้เกิดปัญหาในการตีความในฐานความผิดนี้ คือ คำว่า “ทรัพย์” และการ ”เอาไป”

“ทรัพย์” นั้นมีความหมายว่าอย่างไร ตามประมวลกฎหมายลักษณะอาญา ร.ศ. 127 มาตรา 6(10) ได้ให้นิยามคำว่าทรัพย์ไว้ว่า “ทรัพย์นั้น ท่านหมายความว่าบรรดาสิ่งของอันบุคคลสามารถมีกรรมสิทธิ์หรือถืออำนาจเป็นเจ้าของได้ เป็นต้นว่า เงินตรา และบรรดาสิ่งของอันพึงเคลื่อนจากที่ได้ก็ดีและเคลื่อนที่ไม่ได้ก็ดี ท่านก็นับว่าเป็นทรัพย์อันกล่าวมาในข้อนี้” แต่ในประมวลกฎหมายอาญาฉบับปัจจุบันมิได้มีการบัญญัติคำนิยามของทรัพย์ไว้ ดังนั้นการจะทราบความหมายของคำว่าทรัพย์ในปัจจุบันคงต้องดูจากประมวลกฎหมายแพ่งและพาณิชย์ เป็นไปตามหลักที่ว่ากฎหมายย่อมเกี่ยวข้องซึ่งกันและกันอยู่เว้นแต่ตามบทบัญญัตินั้นๆ จะแสดงว่าไม่ประสงค์จะให้มีความหมายดังปรากฏตามกฎหมายอื่น[33] ประมวลแพ่งและพาณิชย์ได้ให้ความหมายของคำว่า ”ทรัพย์” ไว้ในมาตรา 137 ว่า “ทรัพย์” หมายความว่า วัตถุมีรูปร่าง จากความหมายของทรัพย์นี้เองที่ทำให้เกิดปัญหาในการจะนำบทบัญญัติความผิดฐานลักทรัพย์มาใช้กับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่กระทำการผ่านเครื่องคอมพิวเตอร์หรือสื่ออิเล็กทรอนิกส์ต่างๆ เคยมีคำพิพากษาศาลฎีกาที่ 5161/2547 ได้วินิจฉัยไว้ว่า ข้อมูล ตามพจนานุกรมให้ความหมายว่า ข้อเท็จจริงหรือสิ่งที่ถือหรือยอมรับว่าเป็นข้อเท็จจริง สำหรับใช้เป็นหลักอนุมานหาความจริงหรือการคำนวณ ส่วนข้อเท็จจริง หมายความว่า ข้อความแห่งเหตุการณ์ที่เป็นมาหรือที่เป็นอยู่จริง ข้อความหรือเหตุการณ์ที่จะต้องวินิจฉัยว่าเท็จหรือจริง ดังนั้นข้อมูลจึงไม่นับเป็นวัตถุมีรูปร่าง สำหรับตัวอักษร ภาพ แผนผัง และตราสารเป็นเพียงสัญลักษณ์ที่ถ่ายทอดความหมายของข้อมูลออกจากแผ่นบันทึกข้อมูล โดยอาศัยเครื่องคอมพิวเตอร์ มิใช่รูปร่างของข้อมูล เมื่อประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 137 บัญญัติว่า ทรัพย์ หมายความว่า วัตถุมี

[33] หยุด แสงอุทัย, กฎหมายอาญา ภาค 2-3 พิมพ์ครั้งที่ 7 (กรุงเทพมหานคร: มหาวิทยาลัยธรรมศาสตร์, 2538), หน้า 433.

รูปร่าง ข้อมูลในแผ่นบันทึกข้อมูลจึงไม่ถือเป็นทรัพย์ การที่จำเลยนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลจากแผ่นบันทึกข้อมูลของโจทก์ร่วม จึงไม่เป็นความผิดฐานลักทรัพย์ จากตัวอย่างคำพิพากษาฎีกานี้เห็นได้ว่า ข้อมูลในเครื่องคอมพิวเตอร์แม้จะมีราคา และอาจถือเอาได้ แต่ไม่ใช่วัตถุมีรูปร่าง (tangible property) กล่าวคือ เป็นวัตถุไม่มีรูปร่าง (intangible property) จึงไม่ถือว่าเป็นทรัพย์ หากมีการขโมยข้อมูลไปย่อมไม่มีความผิดฐานลักทรัพย์ ดังนั้นกรณีการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลการขโมยข้อมูลส่วนบุคคลของเหยื่อผ่านทางอินเตอร์เน็ต ย่อมไม่เป็นการลักทรัพย์ เนื่องจากข้อมูลนั้นมิใช่ทรัพย์ ผู้กระทำจึงไม่มีความผิดฐานลักทรัพย์[34] ตามประมวลกฎหมายอาญามาตรา 334

นอกจากการพิจารณาว่าสิ่งที่ลักนั้นเป็นทรัพย์ตามความหมายที่กล่าวมาหรือไม่แล้ว ย่อมต้องดูมาถึงความหมายของคำว่า “เอาไป” ด้วย เนื่องจากในความผิดฐานลักทรัพย์นี้กฎหมายมุ่งคุ้มครองกรรมสิทธิ์ในตัวทรัพย์ และการครอบครองตัวทรัพย์ด้วย ดังนั้นการเอาไป ต้องเป็นกรณีที่ทรัพย์อยู่ในความครอบครองของผู้อื่น แล้วมีการเข้าแย่งการครอบครอง โดยพาเอาทรัพย์นั้นไปในลักษณะที่ตัดกรรมสิทธิ์ด้วย[35] ดังนี้กรณีการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลโดยการขโมยข้อมูลของเหยื่อผ่านทางอินเตอร์เน็ต ย่อมไม่เป็นการเอาไปเนื่องจากไม่ได้มีการแย่งการครอบครองและไม่ได้ตัดกรรมสิทธิ์ใดๆ ของเจ้าของด้วย เคยมีคำพิพากษาศาลฎีกาที่ 1147/2546[36] ได้วินิจฉัยไว้ว่าการใช้ประโยชน์จากข้อมูลของผู้อื่นจนครบถ้วนขั้นตอนด้วยการแสดงรายการเท็จจนทำให้มีการเปิดบัญชีเงินฝากปลอมในจำนวนเงินที่ทำรายการแล้วอาจจะยังไม่มีความผิดฐานลักทรัพย์จนกว่าจะมีการเบิกถอนเงินสดออกไปเสียก่อน[37] ตามองค์ประกอบความผิด

---

[34] ผาสุก เจริญเกียรติ,”Identity Theft อาชญากรรมใกล้ตัว,” ดุลพาห ปีที่ 56, เล่มที่ 1 (มกราคม-เมษายน 2552): 172.

[35] เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญา ภาคความผิด เล่ม3, หน้า 2.

[36] คำพิพากษาศาลฎีกาที่ 1147/2546 การที่จำเลยซึ่งเป็นพนักงานของธนาคารโจทก์ร่วมทำบันทึกข้อมูลรายการขายลดเช็คอันเป็นเท็จเป็นเพียงการใช้กลอุบายว่า มีลูกค้านำเช็คไปขายลดให้แก่โจทก์ร่วมแม้จะได้รับใบเสร็จรับเงินจากการขายลดเช็คแล้วนำไปเปิดบัญชีเงินฝากชื่อบัญชี ป. ซึ่งเป็นบัญชีปลอมที่ธนาคารโจทก์ร่วมเพื่อพักเงินที่จะลักไว้แต่จำนวนเงินตามใบเสร็จรับเงินหรือในบัญชีเงินฝากปลอมยังเป็นกรรมสิทธิ์และอยู่ในความครอบครองของโจทก์ร่วม โดยเฉพาะบัญชีเงินฝากเป็นหลักฐานควบคุมการฝากและถอนเงินของเจ้าของบัญชีเท่านั้น และการถอนเงินแต่ละครั้งจำต้องทำรายการถอนในแบบพิมพ์ใบถอนเงิน ตราบใดที่ยังไม่มีการถอนเงินไปจากโจทก์ร่วม การเอาทรัพย์ไปก็ยังไม่เกิดขึ้น แม้จะเปิดบัญชีเป็นเท็จไว้ก็ยังถือไม่ได้ว่า การลักเงินสดสำเร็จแล้ว”

[37] ผาสุก เจริญเกียรติ,”Identity Theft อาชญากรรมใกล้ตัว,” ดุลพาห ปีที่ 56, เล่มที่ 1 (มกราคม-เมษายน 2552): 173.

ในส่วนของการเอาไป ดังนี้หากต้องรอให้มีการเบิกถอนเงินสดออกไปก่อนเสียจึงจะมีความผิดฐานลักทรัพย์ ย่อมก่อให้เกิดความเสียหายมาก และในส่วนของบุคคลผู้ถูกนำชื่อไปใช้ย่อมได้รับความเสียหายแล้ว อาจเสียชื่อเสียง เสียเวลาหรือเสียค่าใช้จ่ายในการดำเนินคดี หากมีกฎหมายเรื่องการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลโดยเฉพาะการกระทำเช่นนี้ย่อมถือเป็นความผิดสำเร็จนับตั้งแต่มีการนำชื่อหรือข้อมูลซึ่งแสดงเอกลักษณ์บุคคลอื่นๆ ของบุคคลอื่นไปใช้เพื่อแสวงหาประโยชน์แล้ว

การโจรกรรมทรัพย์สินโดยปกติถือเป็นความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญาอยู่แล้ว เนื่องจากบทบัญญัติความผิดฐานลักทรัพย์มีเจตนารมณ์ให้ความคุ้มครองกรรมสิทธิ์ และการครอบครองตัวทรัพย์ ดังนี้ข้อมูลซึ่งแสดงเอกลักษณ์บุคคลอาจอยู่ในรูปเอกสารหรือเป็นเพียงข้อมูลที่ไม่มีตัวเอกสารรองรับ ดังนี้หากเป็นการลักเอาตัวเอกสารไปผู้กระทำย่อมมีความผิดฐานลักทรัพย์ เนื่องจากเป็นการแย่งกการครอบครอง และแย่งกรรมสิทธิ์ในตัวทรัพย์นั้นไปจากผู้เป็นเจ้าของ แต่หากเป็นการลักซึ่งข้อมูลเพียงอย่างเดียวโดยมิได้ลักเอกสารใดๆ มาด้วย เช่น การจดจำหมายเลขบัตรเครดิตของผู้อื่นแล้วนำไปใช้ ฯลฯ ผู้กระทำไม่มีความผิดฐานลักทรัพย์ หรือหากเป็นกรณีการได้มาซึ่งเอกสารโดยชอบด้วยกฎหมาย เช่น ผู้สมัครงานได้มอบเอกสารให้ไว้ แม้ผู้ได้ข้อมูลมาจะมีเจตนานำเอกสารนั้นไปใช้ในทางที่มิชอบ หรือเพื่อแสวงหาผลประโยชน์โดยทุจริตก็ไม่มีความผิดฐานลักทรัพย์ แต่ทั้งนี้อาจเป็นความผิดตามฐานความผิดอื่นๆ ได้ เช่น การฉ้อโกง การปลอมเอกสาร เป็นต้น

ความผิดฐานฉ้อโกง ในประมวลกฎหมายอาญาลักษณะ 12 ความผิดเกี่ยวกับทรัพย์ หมวด 3

องค์ประกอบความผิดฐานฉ้อโกงในประมวลกฎหมายอาญา มาตรา 341[38] มีดังนี้

<u>องค์ประกอบภายนอก</u>

1. ผู้ใด

[38] เกียรติขจร วัจนะสวัสดิ์, <u>กฎหมายอาญา ภาคความผิด เล่ม3</u>, หน้า 197.

2. หลอกลวงด้วยการ (ก) แสดงข้อความอันเป็นเท็จ

(ข) ปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง

3. ผู้อื่น
4. โดยการหลอกลวงดังว่านั้น (ก) ได้ไปซึ่งทรัพย์สินของผู้ถูกหลอกลวง หรือบุคคลที่สามหรือ

(ข) ทำให้ผู้ถูกหลอกลวง หรือบุคคลที่สาม ทำ ถอน หรือทำลายเอกสารสิทธิ

<u>องค์ประกอบภายใน</u>

1. เจตนา (เจตนาธรรมดา คือ ประสงค์ต่อผล หรือเล็งเห็นผล)
2. เจตนาพิเศษ คือ “โดยทุจริต”

จากองค์ประกอบความผิดนี้การหลอกลวง คือ การทำให้เข้าใจผิด ซึ่งสามารถกระทำได้ 2 วิธี คือ การแสดงข้อความอันเป็นเท็จ และการปกปิดข้อความจริงซึ่งควรบอกให้แจ้ง สามารถปรับบทบัญญัตินี้กับการกระทำผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้ในบางกรณี และการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลนี้ก็เข้าข่ายที่ผู้กระทำความผิดต้องรับโทษหนักขึ้นกว่ากรณีการฉ้อโกงธรรมดาด้วย กล่าวคือในฐานความผิดฉ้อโกงนี้มีเหตุเพิ่มโทษ หรือบทฉกรรจ์ด้วย คือในมาตรา 342(1) ผู้กระทำจะต้องรับโทษหนักขึ้น ถ้ากระทำการฉ้อโกงโดยการแสดงตนเป็นคนอื่น ซึ่งการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์ย่อมเป็นการแสดงตนเป็นคนอื่น หรือหลอกลวงผู้อื่นเพื่อให้ตนได้ทรัพย์สิน ในนามของบุคคลอื่น ทำให้ผู้อื่นเข้าใจว่าตนเป็นบุคคลอื่น ตัวอย่างเช่น กรณีผู้กระทำนำเอาข้อมูล รหัสต่างๆ ของบุคคลอื่นมาใช้แสดงตนว่าตนนั้นเป็นบุคคลผู้ทรงสิทธิตามเอกสารดังกล่าว ทำให้ผู้อื่นเข้าใจผิดไป แล้วเข้าทำธุรกรรมต่างๆ นั้น เพื่อให้ตนได้รับผลประโยชน์ไป ถือเป็นการแสดงข้อความอันเป็นเท็จหรือการปกปิดความจริงที่ควรแจ้งให้ทราบ ผู้กระทำการนั้นมีความผิดฐานฉ้อโกงโดยแสดงตนเป็นคนอื่นตามมาตรา 342(1) สามารถเทียบเคียงได้กับคำพิพากษาศาลฎีกาที่ 816/2487 ที่วินิจฉัยว่าการที่จำเลยแอบอ้างนำบัตร

อนุญาตลาของทหารมาใช้แสดงตนเพื่อใช้สิทธิขอซื้อตั๋วโดยสารในอัตราครึ่งราคา จนพนักงานขายตั๋วหลงเชื่อ จำเลยมีความผิดฐานฉ้อโกง แต่ทั้งนี้ไม่สามารถที่จะนำบทบัญญัติความผิดฐานฉ้อโกงโดยการแสดงตนเป็นคนอื่นนั้นมาปรับใช้กับทุกความผิดของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้ เนื่องมาจากในการกระทำความผิดฐานฉ้อโกงนั้นต้องมีบุคคลที่ถูกหลอกลวงตามองค์ประกอบของความผิด ซึ่งโดยทั่วไปต้องเป็นมนุษย์ เพราะสัตว์ สิ่งของ หรือสิ่งไม่มีชีวิตอื่นๆ ไม่สามารถที่จะรับรู้ถึงการแสดงเจตนาได้ แต่ปัจจุบันการทำธุรกรรมบางประเภทมักกระทำผ่านทางเครือข่ายระบบคอมพิวเตอร์ เช่น เครื่องรับฝากถอนเงินอัตโนมัติ (ATM) เครื่องรูดบัตรเครดิต หรือระบบฐานข้อมูลออนไลน์ต่างๆ ซึ่งเป็นเครื่องจักรกลมิใช่มนุษย์จึงไม่อาจถูกหลอกลวงได้ ผู้กระทำจึงอาจไม่มีความผิดฐานฉ้อโกง และหากเป็นกรณีที่การหลอกลวงของผู้กระทำนั้นมิได้ทำให้ได้รับไปซึ่งทรัพย์สิน แต่ได้รับไปซึ่งผลประโยชน์อย่างอื่น เช่น การสามารถเข้า-ออกในสถานที่ใดๆ ได้ ซึ่งประโยชน์เช่นนี้ไม่ถือเป็นทรัพย์สิน ดังนี้ผู้กระทำก็อาจไม่มีความผิดฐานฉ้อโกงด้วยเช่นเดียวกัน และความผิดฐานฉ้อโกงเป็นความผิดที่ต้องมีผลปรากฏด้วย[39] กล่าวคือหากมีแต่เพียงการหลอกลวงเกิดขึ้นด้วยการแสดงข้อความอันเป็นเท็จ แต่ยังไม่มีผลปรากฏ คือ ยังมิได้มีการได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวง เช่นนี้ความผิดฐานฉ้อโกงก็ยังไม่เป็นความผิดสำเร็จ ซึ่งหากเป็นกรณีมีฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นการเฉพาะ ย่อมเป็นความผิดสำเร็จนับแต่ผู้กระทำได้ใช้ข้อมูลของบุคคลอื่นมาแอบอ้างแล้ว และอุปสรรค ปัญหาของความผิดฐานฉ้อโกงอีกอย่างหนึ่งที่ทำให้ฐานความผิดนี้ไม่เหมาะสมกับการกระทำความผิดโดยการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล คือ ในเรื่องของบุคคลที่ได้รับการคุ้มครองโดยกฎหมายในฐานความผิด หรือคือเรื่องประเด็นผู้เสียหายในความผิดฐานฉ้อโกง ความผิดตามประมวลกฎหมายอาญาผู้ที่มีสิทธิฟ้องคดี หรือร้องทุกข์เพื่อให้มีการดำเนินคดีนั้นต้องเป็นผู้เสียหายเท่านั้นจึงจะสามารถกระทำได้ ประมวลกฎหมายวิธีพิจารณาความอาญาได้บัญญัติถึงคำนิยามของคำว่า “ผู้เสียหาย” ไว้ในมาตรา 2(4) ว่า “หมายความถึงบุคคลผู้ได้รับความเสียหายเนื่องจากการกระทำผิดฐานใดฐานหนึ่ง รวมทั้งบุคคลอื่นที่มีอำนาจจัดการแทนได้ ดั่งบัญญัติไว้ในมาตรา 4, 5 และ 6”

[39] เรื่องเดียวกัน, หน้า 244.

จากคำนิยามนี้จึงสามารถแยกผู้เสียหายได้เป็น 2 ประเภท คือ ผู้เสียหายที่แท้จริง และผู้มีอำนาจจัดการแทนผู้เสียหายที่แท้จริง ในที่นี้ขอกล่าวถึงเพียงประเด็นผู้เสียหายที่แท้จริง

หลักเกณฑ์ของการเป็นผู้เสียหายที่แท้จริง[40] มีดังนี้

1. มีการกระทำผิดอาญาเกิดขึ้น
2. บุคคลนั้นได้รับความเสียหายเนื่องจากการกระทำผิดนั้น
3. บุคคลนั้นต้องเสียหายโดยนิตินัย

กรณีของบุคคลได้รับความเสียหายเนื่องจากการกระทำผิดนั้นต้องดูว่าบุคคลนั้นเป็นบุคคลประเภทที่กฎหมายในฐานความผิดนั้นๆ ประสงค์จะคุ้มครองหรือไม่ ในบางกรณีของการฉ้อโกงโดยแสดงตนเป็นคนอื่น ผู้เสียหายที่กฎหมายมุ่งคุ้มครองไม่ใช่บุคคลที่ถูกแอบอ้างชื่อหรือบุคคลที่ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไปใช้ จึงทำให้เหยื่อผู้ถูกแอบอ้างชื่อไม่สามารถฟ้องร้องคดีได้ เคยมีคำพิพากษาศาลฎีกาที่ 2193/2534[41] วินิจฉัยไว้ว่าจำเลยเอาเช็คไปปลอมลายมือชื่อของผู้รับเงินสลักหลังโอนให้จำเลย แล้วนำไปหลอกลวงธนาคารให้จ่ายเงินเป็นการกระทำต่อธนาคาร ไม่ได้กระทำต่อผู้รับเงิน ดังนี้ธนาคารและเจ้าหน้าที่ธนาคารที่ถูกหลอกลวงเป็นผู้เสียหายในความผิดฐานฉ้อโกง ส่วนผู้ที่มีชื่อเป็นผู้รับเงินตามเช็คไม่ใช่ผู้เสียหายในความผิดฐานฉ้อโกงนี้[42] หรือในคำพิพากษาฎีกาที่ 12582/2547 วินิจฉัยไว้ว่าจำเลยปลอมบัตรเครดิตวีซ่าของธนาคาร ท. โดยระบุชื่อ ส. แล้วนำไปซื้อสินค้าที่ร้านค้า ห. โดยอ้างว่าจำเลย คือ ส. ธนาคาร ท. จ่ายเงินค่าสินค้าให้แก่ร้าน ห. ดังนี้ ผู้เสียหายในความผิดฐานฉ้อโกงนั้น ปรากฏว่าจำเลยได้แสดงตนว่าเป็น ส. แก่ร้าน ห. จึงเป็นการแสดงข้อความอันเป็นเท็จแก่พนักงานขายของของร้าน ห. การที่

---

[40] คะนึง ฦาไชย, กฎหมายวิธีพิจารณาความอาญา เล่ม1 พิมพ์ครั้งที่ 9 (กรุงเทพมหานคร: โรงพิมพ์เดือนตุลา, 2551), หน้า 20.

[41] คำพิพากษาฎีกาที่ 2193/2534 การที่จำเลยนำเช็คที่บริษัท ก. สั่งจ่ายโจทก์ร่วม ซึ่งจำเลยได้ปลอมลายมือชื่อของโจทก์ร่วมแล้วสลักหลังให้จำเลย แล้วนำไปแสดงต่อเจ้าหน้าที่ฝ่ายการเงินของธนาคาร ช. เพื่อเรียกเก็บเงินเข้าบัญชีของจำเลย แม้จะเป็นการหลอกลวงโดยแสดงข้อความอันเป็นเท็จหรือปกปิดความจริงที่ควรบอกให้แจ้งก็ตาม แต่ก็เป็นการกระทำต่อธนาคาร ช. และเจ้าหน้าที่ฝ่ายการเงินของธนาคารนั้นโดยตรง ไม่อาจถือได้ว่าเป็นการกระทำต่อโจทก์ร่วม หากโจทก์ร่วมจะได้รับความเสียหายเพราะเสียสิทธิที่จะได้รับเงินตามเช็คดังกล่าวไป ก็เป็นความเสียหายที่โจทก์ร่วมได้รับในความผิดฐานปลอมเอกสาร หาใช่ความเสียหายจากการหลอกลวงของจำเลยไม่ โจทก์ร่วมจึงมิใช่ผู้เสียหายในความผิดฐานฉ้อโกง

[42] วิเชียร ดิเรกอุดมศักดิ์, วิ.อาญาพิสดาร เล่ม1 (กรุงเทพมหานคร: แสงจันทร์การพิมพ์, 2554), หน้า 10.

พนักงานร้านส่งมอบสินค้าให้จำเลย ถือว่าเจ้าของร้านค้าเป็นผู้เสียหายในความผิดฐานฉ้อโกง ส่วนธนาคาร ท. และ ส. ผู้ถูกระบุชื่อเป็นเจ้าของบัตรเครดิตปลอม มิได้ถูกจำเลยหลอกลวงด้วย จึงมิใช่ผู้เสียหายในความผิดฐานฉ้อโกง กล่าวคือธนาคารเป็นเพียงผู้ได้รับความเสียหายทางแพ่งเท่านั้น[43]

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลมีความเกี่ยวข้องกับการฉ้อโกง คือ เป็นการนำข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นมาใช้เพื่อหลอกลวงบุคคลอื่นเพื่อให้ตนได้มาซึ่งทรัพย์สิน แต่ข้อจำกัดของความผิดฐานฉ้อโกง คือ การฉ้อโกงต้องทำให้ได้ไปซึ่งทรัพย์สิน ซึ่งไม่รวมถึงผลประโยชน์อย่างอื่น เช่น การได้รับสิทธิเข้า-ออกในสถานที่ ฯลฯ และผู้เสียหายที่กฎหมายมุ่งคุ้มครอง คือ บุคคลที่ถูกหลอกลวงไปซึ่งทรัพย์สิน กฎหมายไม่ได้มีเจตนารมณ์ที่จะให้ความคุ้มครองผู้ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลแต่อย่างใด ซึ่งกรณีนี้ทำให้แตกต่างจากการที่มีกฎหมายบัญญัติฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะอย่างในกฎหมายของประเทศสหรัฐอเมริกา และประเทศแคนาดา ที่จะบัญญัติให้ความคุ้มครองแก่ผู้ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะ

3.2.2 การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลกับฐานความผิดตามพระราชบัญญัติอื่นๆ

นอกเหนือจากประมวลกฎหมายอาญาที่มีฐานความผิดที่เกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลแล้ว ยังมีกฎหมายอื่นๆ ที่มีความเกี่ยวข้องด้วย ดังนี้

[43] เกียรติขจร วัจนะสวัสดิ์, คำอธิบายหลักกฎหมายวิธีพิจารณาความอาญา ว่าด้วยการดำเนินคดีในขั้นตอนก่อนการพิจารณา พิมพ์ครั้งที่ 7 (กรุงเทพมหานคร: พลสยามพริ้นติ้ง, 2553), หน้า 129.

3.2.2.1 **พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.**2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นี้เข้ามามีความเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเนื่องมาจาก ปัจจุบันในการดำเนินชีวิตประจำวัน การประกอบธุรกิจ หรือการทำธุรกรรมใดๆ ของบุคคล มีเทคโนโลยีสารสนเทศเข้ามาเกี่ยวข้องด้วยมาก เนื่องจากมนุษย์ชอบความสะดวกสบาย จึงมีการพัฒนาเทคโนโลยีใหม่ๆ ขึ้นเสมอๆ เพื่อให้สามารถตอบสนองความต้องการต่างๆ ของมนุษย์ได้อย่างมีประสิทธิภาพมากขึ้น ซึ่งเทคโนโลยีก็เหมือนกับหลายๆ สิ่งที่มีทั้งข้อดีและข้อเสีย ขึ้นอยู่กับบุคคลที่นำไปใช้ จึงเป็นที่แน่นอนว่ามีบุคคลกลุ่มหนึ่งนำเทคโนโลยีมาเป็นเครื่องมือในการกระทำความผิดเพื่อแสวงหาประโยชน์ในรูปแบบต่างๆ อาจกล่าวได้ว่า การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หมายถึง การกระทำความผิดโดยเจตนาต่อระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ รวมถึงการกระทำความผิดโดยใช้ระบบคอมพิวเตอร์ และเครือข่ายอินเตอร์เน็ตเป็นเครื่องมือในการกระทำความผิด[44]

บทบัญญัติในพระราชบัญญัตินี้ที่มีความเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล คือ ในความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5) และความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา7) ซึ่งคำที่มีความสำคัญ และต้องทำความเข้าใจเพื่อจะนำไปสู่การปรับใช้กฎหมายได้ถูกต้องตามฐานความผิดเหล่านี้ คือ คำว่า “ระบบคอมพิวเตอร์” และ “ข้อมูลคอมพิวเตอร์” ซึ่งพระราชบัญญัตินี้ได้ให้คำนิยามไว้ในมาตรา 3 ดังนี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบคอมพิวเตอร์จึงได้แก่ ฮาร์ดแวร์และซอฟต์แวร์ที่พัฒนาขึ้นเพื่อประมวลผลข้อมูลดิจิทัล (digital data) อันประกอบด้วยเครื่องคอมพิวเตอร์ และอุปกรณ์รอบข้าง (peripheral) ต่างๆ ในการรับเข้าหรือป้อนข้อมูล (input) นำออกหรือแสดงผลข้อมูล (output) และบันทึกหรือ

[44] สราวุธ ปิติยาศักดิ์, กฎหมายเทคโนโลยีสารสนเทศ (กรุงเทพมหานคร: นิติธรรม, 2555), หน้า 267.

เก็บข้อมูล (store and record) ดังนั้นระบบคอมพิวเตอร์จึงอาจเป็นอุปกรณ์เพียงเครื่องเดียว หรือหลายเครื่องอันมีลักษณะเป็นชุดเชื่อมต่อกัน ทั้งนี้โดยอาจเชื่อมต่อกันผ่านระบบเครือข่าย และมีลักษณะการทำงานโดยอัตโนมัติตามโปรแกรมที่กำหนดไว้ และไม่มีการแทรกแซงโดยตรงจากมนุษย์ ส่วนโปรแกรมคอมพิวเตอร์จะหมายถึงชุดคำสั่งที่ทำหน้าที่สั่งการให้คอมพิวเตอร์ทำงาน[45]

ตามความหมายของ “ระบบคอมพิวเตอร์” นี้จะเห็นได้ว่า คอมพิวเตอร์นั้นต้องมีการเชื่อมการทำงานเข้าด้วยกัน ดังนี้จึงไม่ครอบคลุมไปถึงคอมพิวเตอร์ที่ไม่ได้เชื่อมต่อกับโครงข่าย เช่น หากคอมพิวเตอร์นั้นเราใช้พิมพ์งาน หรือเก็บข้อมูลแต่เพียงอย่างเดียวโดยไม่ได้มีการเชื่อมต่อกับระบบใดๆ คอมพิวเตอร์นั้นก็จะไม่อยู่ในความหมายของระบบคอมพิวเตอร์นี้ อีกทั้งไม่ครอบคลุมถึงเทคโนโลยีที่มีอยู่ในปัจจุบันด้วย เนื่องจากปัจจุบันมิใช่มีเพียงแต่คอมพิวเตอร์เท่านั้นที่จะสามารถใช้ระบบประมวลผลและส่งข้อมูลได้ ยังมีอุปกรณ์ เครื่องมือตัวอื่นๆ อีกที่สามารถทำงานได้อย่างคอมพิวเตอร์ เช่น โทรศัพท์มือถือแบบสมาร์ทโฟนที่เป็นที่นิยมอย่างมากในปัจจุบัน จึงเกิดปัญหาว่าความผิดเกี่ยวกับคอมพิวเตอร์ตามพระราชบัญญัติฉบับนี้เป็นความผิดอาญา ดังนั้นตามหลักพื้นฐานของกฎหมายอาญาต้องตีความโดยเคร่งครัด จะไปตีความในทางขยายความเพื่อให้เพิ่มความรับผิดในทางอาญาไปเกินกว่าที่ตัวบทกฎหมายกำหนดไว้ไม่ได้[46]

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย ตัวอย่างของ ”ข้อมูล” เช่น ข้อมูลซึ่งเป็นรหัสผ่าน หรือลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น แต่แม้ข้อมูลจะมีลักษณะหลากหลาย แต่ข้อมูลคอมพิวเตอร์ในความหมายของพระราชบัญญัติฉบับนี้ต้องมีลักษณะสำคัญประการหนึ่ง คือ ต้องเป็นข้อมูลดิจิทัลเท่านั้น และหมายความถึงเฉพาะข้อมูลที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้เท่านั้นจึงจะได้รับความ

---

[45] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ... และร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ... (กรุงเทพมหานคร: โรงพิมพ์เดือนตุลา, 2544), หน้า 101.

[46] มานิตย์ จุมปา, คำอธิบายกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (กรุงเทพมหานคร: วิญญูชน, 2553), หน้า 47.

คุ้มครองตามพระราชบัญญัตินี้ ส่วนข้อมูลที่ถูกจัดเก็บในรูปแบบอื่น เช่น แผ่นดิสก์ หรืออุปกรณ์อื่นใดที่ไม่มีการเชื่อมต่อกับระบบคอมพิวเตอร์ หากมีผู้ใดมากระทำให้เกิดความเสียหาย หรือมีการนำข้อมูลนั้นไปจากเจ้าของข้อมูลย่อมไม่เป็นความผิดตามประมวลกฎหมายอาญาในความผิดฐานลักทรัพย์ หรือทำให้เสียทรัพย์ และไม่มีความผิดตามพระราชบัญญัตินี้ด้วย[47] จึงยังมีช่องว่างในการนำพระราชบัญญัติฉบับนี้ ไปปรับใช้กับการกระทำความผิดเกี่ยวกับการโจรกรรมเอกลักษณ์บุคคล เนื่องจากจะใช้พระราชบัญญัตินี้บังคับได้ ต้องเป็นการกระทำความผิดผ่านทางระบบคอมพิวเตอร์ที่มีการเชื่อมต่อ หรือทำต่อข้อมูลคอมพิวเตอร์เท่านั้น กล่าวคือการให้คำจำกัดความ หรือประเภทของสื่อที่ใช้ในการกระทำความผิดยังไม่ครอบคลุมเพียงพอ แต่ในบางกรณีผู้กระทำการโจรกรรมเอกลักษณ์บุคคลก็กระทำความผิดเข้าองค์ประกอบของพระราชบัญญัติฉบับนี้ ผู้เขียนจึงขออธิบายถึงฐานความผิดต่างๆ ที่สำคัญที่มีความเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ดังนี้

ความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ มาตรา 5 มีองค์ประกอบความผิดอาญา ดังนี้

<u>องค์ประกอบภายนอก</u>

1. ผู้ใด
2. เข้าถึงโดยมิชอบ
3. ซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน

<u>องค์ประกอบภายใน</u> คือ เจตนาธรรมดา คือ ประสงค์ต่อผล หรือเล็งเห็นผล (ตามประมวลกฎหมายอาญามาตรา 59)

[47] เรื่องเดียวกัน, หน้า 48.

เอกสารที่ใช้ประกอบการนำเสนอร่างกฎหมายฉบับนี้ ซึ่งจัดทำโดยสำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ได้ให้คำอธิบายคำว่า “เข้าถึง” (access) ไว้ว่าหมายถึง การเข้าถึงไม่ว่าจะโดยทางกายภาพ เช่น การเข้าถึงตัวคอมพิวเตอร์แล้วหาทางผ่านเข้าไปใช้คอมพิวเตอร์ซึ่งมีการกำหนดรหัสผ่านเพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้คอมพิวเตอร์นั้น หรือการเข้าถึงที่แม้อยู่ห่างไกลจากเครื่องคอมพิวเตอร์แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ได้ และความหมายของคำว่า “มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน” หมายถึง ระบบคอมพิวเตอร์นั้นได้มีการสร้างมาตรการป้องกันการเข้าถึงไว้ เพื่อป้องกันไม่ให้บุคคลอื่นที่ไม่มีสิทธิเข้าถึงระบบคอมพิวเตอร์ ดังนั้นหากเป็นกรณีที่คอมพิวเตอร์มิได้มีการสร้างมาตรการป้องกันการเข้าถึงเอาไว้ ผู้ที่เข้าไปย่อมไม่มีความผิด ซึ่งปกติบุคคลทั่วไปก็มิได้จัดให้เครื่องคอมพิวเตอร์ของตนมีระบบการป้องกันการเข้าถึงเอาไว้

ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ มาตรา 7 มีองค์ประกอบความผิดอาญา ดังนี้

<u>องค์ประกอบภายนอก</u>

1. ผู้ใด
2. เข้าถึงโดยมิชอบ
3. ซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

<u>องค์ประกอบภายใน</u> คือ เจตนาธรรมดา คือ ประสงค์ต่อผล หรือเล็งเห็นผล (ตามประมวลกฎหมายอาญามาตรา 59)

ฐานความผิดนี้มีองค์ประกอบทุกอย่างเหมือนกับความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ มีข้อแตกต่างเพียงจุดเดียว คือ เป็นการเข้าถึงข้อมูล โดยข้อมูลนั้นต้องเป็นข้อมูลที่มีการเก็บหรือส่งด้วยวิธีการทางอิเล็กทรอนิกส์ ซึ่งไม่ได้หมายความถึงระบบคอมพิวเตอร์ เพราะระบบคอมพิวเตอร์ไม่สามารถเก็บหรือส่งได้ ดังนี้ในบางครั้งการกระทำความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบนี้ อาจไม่จำเป็นต้องมีการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบก่อน เช่น การเข้าถึงข้อมูลที่บรรจุไว้ในแผ่นบันทึกข้อมูลที่มีระบบการป้องกันการเข้าถึงไว้ เป็นต้น[48]

บทบัญญัติฐานความผิดมาตราอื่นๆ ที่อาจปรับใช้กับการกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้ คือ กำหนดความผิดสำหรับบุคคลที่กระทำด้วยประการใดๆ โดยมิชอบด้วยกฎหมายด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ (มาตรา 8) และการกำหนดความผิดสำหรับผู้ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (มาตรา 9)

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในปัจจุบันมีรูปแบบที่เปลี่ยนแปลงและพัฒนาไปเป็นอย่างมาก มีการใช้เทคโนโลยีเป็นเครื่องมือช่วยในการโจรกรรมข้อมูล จึงอาจนำพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาปรับใช้กับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้ในบางกรณีที่ผู้โจรกรรมได้ใช้วิธีการเข้าถึงข้อมูล หรือระบบคอมพิวเตอร์ของผู้อื่นที่มีระบบป้องกันการเข้าถึงไว้โดยมิชอบ แต่พระราชบัญญัติฉบับนี้ยังมีข้อจำกัด คือ นำมาบังคับใช้ได้เฉพาะกรณีที่การโจรกรรมข้อมูลนั้นกระทำผ่านระบบคอมพิวเตอร์และมีการตั้งระบบการป้องกันการเข้าถึงข้อมูลไว้เท่านั้น ผู้เข้าถึงข้อมูลหรือระบบคอมพิวเตอร์จึงจะมีความผิด

[48] เรื่องเดียวกัน, หน้า 67.

3.2.2.2 **พระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ.** 2526

พระราชบัญญัติบัตรประจำตัวประชาชนเป็นกฎหมายอีกฉบับหนึ่งที่มีความเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล เนื่องมาจากบัตรประจำตัวประชาชนนับเป็นเอกสารสำคัญส่วนบุคคลที่บุคคลทุกคนต้องมี เมื่อถึงเกณฑ์อายุตามที่กฎหมายบัญญัติ โดยปัจจุบันกฎหมายได้บัญญัติให้บุคคลที่มีอายุตั้งแต่เจ็ดปีบริบูรณ์ต้องมีบัตรประจำตัวประชาชน ซึ่งวัตถุประสงค์ในการจัดทำบัตรประจำตัวประชาชนก็เพื่อใช้ในการพิสูจน์และยืนยันตัวบุคคล เพื่อทำการติดต่อ เพื่อแสดงสิทธิ หรือเพื่อทำธุรกรรมต่างๆ[49] เช่น การขอสินเชื่อจากธนาคาร การสมัครงาน การขอใบอนุญาตขับขี่ การใช้สิทธิเลือกตั้ง ฯลฯ หรืออาจกล่าวได้ว่า ในการทำธุรกรรมที่สำคัญต่างๆ ในชีวิตประจำวันล้วนต้องใช้บัตรประจำตัวประชาชน เพื่อเป็นหลักฐานซึ่งแสดงตัวบุคคล ดังนี้บัตรประจำตัวประชาชน ข้อมูลที่อยู่ในบัตร และรวมถึงข้อมูลที่ถูกจัดเก็บ หรือบันทึกไว้ในหน่วยความจำของบัตรประชาชนแบบเอนกประสงค์ (smart card) นั้นจึงเป็นเป้าหมายสำคัญของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

บัตรประจำตัวประชาชนเป็นเอกสารหรือบัตรที่ทางราชการออกให้แก่ผู้ถือ อันเป็นหลักฐานแสดงว่าผู้ถือบัตรมีสัญชาติไทย และมีรายละเอียดเกี่ยวกับบุคคลนั้น เช่น ชื่อตัว ชื่อสกุล วันเดือนปีเกิด ภูมิลำเนา ฯลฯ เพื่อใช้ยืนยันตัวบุคคล

บทบัญญัติในพระราชบัญญัตินี้ที่มีความเกี่ยวข้อง หรือสามารถนำมาปรับใช้กับกรณีการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล มีดังนี้ คือ

ความผิดฐานเข้าถึงข้อมูลหรือเปิดเผยข้อมูลที่ถูกบันทึกไว้ในหน่วยความจำของบัตรประจำตัวประชาชนแบบเอนกประสงค์ (มาตรา 12[50]) ข้อจำกัดของมาตรานี้คือ บัญญัติถึงเพียงแต่ข้อมูลที่อยู่ในรูปของอิเล็กทรอนิกส์หรือข้อมูลที่ถูกเก็บไว้ในหน่วยความจำของบัตร

---

[49] สมคิด เลิศไพฑูรย์ และคณะ, รายงานวิจัยฉบับสมบูรณ์ การคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในบัตรประจำตัวประชาชนแบบอเนกประสงค์ (กรุงเทพมหานคร: สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์), หน้า 26.

[50] มาตรา 12 "ผู้ใดเข้าถึงข้อมูลหรือเปิดเผยข้อมูลที่บันทึกไว้ในหน่วยความจำตามมาตรา 7/1 อันมิใช่ข้อมูลทั่วไปที่ปรากฏอยู่บนบัตรตามมาตรา 7 โดยมิได้รับความยินยอมจากผู้ถือบัตร ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ เว้นแต่เป็นการเข้าถึงข้อมูลหรือเปิดเผยตามมาตรา 10 หรือตามคำสั่งศาล หรือเข้าถึงข้อมูลระหว่างหน่วยงานของรัฐที่จำเป็นต้องใช้ข้อมูลนั้นในการปฏิบัติหน้าที่"

ประจำตัวประชาชนแบบเอนกประสงค์ (smart card) เท่านั้น จึงไม่ครอบคลุมถึงข้อมูลที่ปรากฏอยู่บนตัวบัตร

ความผิดฐานยื่นคำขอมีบัตรประจำตัวประชาชนอันเป็นเท็จ มาตรา 14 ผู้ใด

(1) ยื่นคำขอมีบัตรโดยมิได้มีสัญชาติไทย ด้วยการแสดงหลักฐานอันเป็นเท็จหรือปกปิดข้อความจริงต่อพนักงานเจ้าหน้าที่ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงห้าปี หรือปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(2) แจ้งข้อความหรือแสดงหลักฐานอันเป็นเท็จต่อพนักงานเจ้าหน้าที่ ในการขอมีบัตรตามมาตรา 6 หรือการขอมีบัตรใหม่ตามมาตรา 6 ตรี หรือการขอมีบัตรใหม่หรือขอเปลี่ยนบัตรตามมาตรา 6 จัตวา อันมิใช่เป็นกรณีตาม (1) ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

(3) ปลอมบัตรหรือใบรับหรือใบแทนใบรับ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี หรือปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท หรือทั้งจำทั้งปรับ

(4) ใช้หรือแสดงบัตรหรือใบรับหรือใบแทนใบรับ อันเกิดจากการกระทำความผิดตาม (1) (2)หรือ (3) ต้องระวางโทษตามที่กำหนดไว้สำหรับความผิดนั้น

ถ้าผู้กระทำความผิดตาม (4) เป็นผู้กระทำความผิดตาม (1) (2) หรือ (3) ให้ลงโทษตาม (1) (2) หรือ (3) แล้วแต่กรณี แต่กระทงเดียว

ถ้าผู้กระทำความผิดหรือผู้ใช้หรือผู้สนับสนุนการกระทำความผิดตาม (1) (2) (3) หรือ (4) เป็นเจ้าพนักงานออกบัตร เจ้าพนักงานตรวจบัตร หรือเจ้าพนักงานเจ้าหน้าที่ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

บทบัญญัตินี้เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล คือ การลักข้อมูล หรือเอกสารส่วนบุคคลของผู้อื่นมาแล้วนำมาแจ้งแก่พนักงานเจ้าหน้าที่เพื่อขอออกบัตรประจำตัวประชาชน ถือเป็นความผิดฐานแจ้งความเท็จ หรือแสดงหลักฐานอันเป็นเท็จต่อพนักงาน

เจ้าหน้าที่ ซึ่งบทบัญญัตินี้สามารถปรับใช้ได้กับกรณียื่นคำขอเท็จในการขอให้ออกบัตรประจำตัวประชาชนเท่านั้น แต่จากลักษณะการกระทำความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล มีการนำข้อมูลของบุคคลอื่นไปแอบอ้างทำเอกสารอื่นอีกหลายประเภท เช่น บัตรเครดิต บัตรเดบิต หนังสือเดินทาง เป็นต้น

ความผิดฐานใช้บัตร ใบรับ หรือใบแทนใบรับของผู้อื่นว่าเป็นของตน มาตรา 15 ผู้ใดนำบัตรหรือใบรับหรือใบแทนใบรับของผู้อื่นไปใช้แสดงว่าตนเป็นเจ้าของบัตรหรือใบรับหรือใบแทนใบรับ ต้องระวางโทษจำคุกตั้งแต่หกเดือนถึงห้าปี และปรับตั้งแต่หนึ่งหมื่นบาทถึงหนึ่งแสนบาท

ความผิดฐานเอาไปเสียหรือยึดไว้ซึ่งบัตร หรือใบรับหรือใบแทนใบรับบัตรประจำตัวประชาชนของผู้อื่น เพื่อประโยชน์สำหรับตนเอง หรือผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินหกเดือนและปรับไม่เกินหนึ่งหมื่นบาท (มาตรา15 ทวิ)

ดังนี้จะเห็นได้ว่าพระราชบัญญัติฉบับนี้ยังมีข้อจำกัดอยู่หลายประการที่จะสามารถนำมาปรับใช้กับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้ในทุกกรณี กล่าวคือ พระราชบัญญัตินี้สามารถบังคับใช้ได้เฉพาะแก่บัตรประจำตัวประชาชนเท่านั้น ไม่รวมถึงบัตรแสดงข้อมูลส่วนบุคคลอื่นๆ ที่อาจจะมีข้อมูลเช่นเดียวกันกับข้อมูลในบัตรประจำตัวประชาชน เช่น บัตรนักศึกษาที่มีหมายเลขประจำตัวประชาชน คือ กฎหมายยังบัญญัติคุ้มครองแค่การนำตัวบัตรประจำตัวประชาชนของบุคคลอื่นไปใช้ แต่มิได้บัญญัติครอบคลุมไปถึงการที่นำเพียงข้อมูลในบัตรไปใช้ ดังนี้หากมีการนำหมายเลขประจำตัวประชาชนของบุคคลอื่นไปใช้เพื่อแสวงหาประโยชน์ใดๆ โดยมิชอบ หรือการนำบัตรอื่นใดที่มีข้อมูลเช่นเดียวกันกับบัตรประจำตัวประชาชนไปใช้ พระราชบัญญัติฉบับนี้จะยังไม่สามารถนำมาบังคับใช้เพื่อลงโทษแก่ผู้กระทำนั้นๆ ได้ ซึ่งมีความแตกต่างจากกฎหมายของประเทศสหราชอาณาจักรในพระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 (Identity Card Act of 2006) เนื่องจากในพระราชบัญญัติบัตรประจำตัวประชาชนของประเทศสหราชอาณาจักรให้ความคุ้มครองรวมถึงเอกสารอื่นนอกเหนือจากบัตรประจำตัวประชาชนด้วย เช่น หนังสือเดินทาง ในอนุญาตขับขี่ ฯลฯ เนื่องมาจากในบทบัญญัติกฎหมายใช้คำ

ว่า เอกสารแสดงข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Document) ซึ่งให้หมายความรวมถึงเอกสารใดๆ ที่มีความหมายเหมือนกับบัตรประจำตัวประชาชน เอกสารการเข้าเมือง หนังสือเดินทาง ใบอนุญาตขับขี่ เป็นต้น ดังนี้พระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 ของประเทศสหราชอาณาจักรจึงบัญญัติครอบคลุมเอกสารซึ่งแสดงเอกลักษณ์บุคคลได้มากกว่าพระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ของไทย

3.2.2.3 ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

เมื่อพิจารณาเนื้อหากฎหมายของร่างพระราชบัญญัติฉบับนี้แล้ว สามารถสรุปหลักการสำคัญในการให้ความคุ้มครองข้อมูลส่วนบุคคลในร่างพระราชบัญญัติฉบับนี้ได้ ดังนี้

1.) หลักข้อจำกัดในการเก็บข้อมูล กล่าวคือ ในการจัดเก็บข้อมูลส่วนบุคคล ข้อมูลที่จัดเก็บจะต้องได้มาโดยวิธีการที่ถูกต้องและชอบด้วยกฎหมาย โดยจะต้องให้บุคคลที่เป็นเจ้าของข้อมูลรับทราบและยินยอมในการจัดเก็บข้อมูลนั้น โดยที่ผู้ที่มีอำนาจในการจัดเก็บและประมวลข้อมูลจะต้องกระทำอย่างจำกัดเท่าที่จำเป็น

2.) หลักคุณภาพของข้อมูล กล่าวคือ ข้อมูลส่วนบุคคลที่จัดเก็บควรมีความเกี่ยวข้องกับวัตถุประสงค์ในการใช้งาน และต้องเป็นข้อมูลที่ถูกต้องสมบูรณ์ และปรับปรุงให้ตรงตามความเป็นจริงอยู่เสมอ

3.) หลักการกำหนดวัตถุประสงค์ กล่าวคือ ต้องมีการกำหนดวัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคลก่อนที่จะมีการจัดเก็บข้อมูลนั้น หรือในเวลาที่ทำการประมวลผล ฉะนั้นการใช้ข้อมูลส่วนบุคคลในภายหลังสามารถกระทำได้เฉพาะเพื่อให้สำเร็จตามวัตถุประสงค์ หรือไม่ขัดกับวัตถุประสงค์ของการจัดเก็บข้อมูลเท่านั้น

4.) หลักการใช้ข้อมูลอย่างจำกัด กล่าวคือ การใช้ข้อมูลจะกระทำโดยขัดต่อวัตถุประสงค์ในการจัดเก็บมิได้ เว้นแต่ได้รับความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูล หรือได้รับอนุญาตตามเงื่อนไขที่กฎหมายกำหนด

5.) หลักการรักษาความปลอดภัย กล่าวคือ ต้องจัดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูลเพื่อป้องกันความเสี่ยง การเข้าถึง การทำลาย การใช้ เปลี่ยนแปลง แก้ไข หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

6.) หลักการเปิดเผยข้อมูล กล่าวคือ ต้องกำหนดวิธีการทั่วไปในการเปิดเผยข้อมูล รูปแบบของการเปิดเผยข้อมูล หลักเกณฑ์ในการขอให้มีการเปิดเผยข้อมูล ซึ่งต้องไม่เป็นการกระทบต่อความเป็นอยู่ส่วนตัวของเจ้าของข้อมูล

7.) หลักการมีส่วนร่วมของเจ้าของข้อมูล กล่าวคือ มีการกำหนดให้เจ้าของข้อมูลมีสิทธิต่างๆ ดังต่อไปนี้

- ได้รับการแจ้งว่ามีข้อมูลของตนจัดเก็บอยู่

- ตรวจสอบข้อมูลของตนที่มีผู้จัดเก็บ

- ขอให้แก้ไขข้อมูลที่ไม่ถูกต้อง

- ปฏิเสธในการจัดเก็บข้อมูลของตน

8.) หลักความรับผิด กล่าวคือ มีการกำหนดความรับผิดในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล

9.) หลักข้อจำกัดในการส่งหรือโอนข้อมูลส่วนบุคคลให้แก่บุคคลอื่นข้ามพรมแดน กล่าวคือ เป็นการป้องกันการโอนข้อมูลส่วนบุคคลไปยังประเทศที่มิได้มีกฎหมาย และวิธีปฏิบัติที่สามารถให้หลักประกันและคุ้มครองข้อมูลส่วนบุคคลได้อย่างดีเพียงพอ เว้นแต่จะได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูล

จากหลักการและสาระสำคัญของร่างพระราชบัญญัติฉบับนี้จะเห็นได้ว่ากฎหมายฉบับนี้เน้นการบังคับใช้กับการจัดเก็บข้อมูล การกำหนดหน้าที่ควบคุม ดูแลข้อมูลของผู้ควบคุมข้อมูลมิให้ทำการเปิดเผยข้อมูลส่วนบุคคลใดๆ ได้ตามอำเภอใจ ในส่วนบทบัญญัติที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลจึงมีอยู่เพียงมาตราเดียวที่อาจนำมาปรับใช้ได้ คือ

ความผิดฐานกระทำการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันไม่ชอบด้วยกฎหมาย ซึ่งบัญญัติไว้ในมาตรา 58

มาตรา 58 “ผู้ใดกระทำการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันไม่ชอบด้วยกฎหมาย หรือเพื่อให้ผู้อื่นเสียหาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่งเป็นการเผยแพร่ข้อมูลส่วนบุคคลทางสิ่งพิมพ์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หรือสื่ออิเล็กทรอนิกส์อื่น ผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

การบัญญัติฐานความผิดเพื่อคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 58 นี้ผู้เขียนมีความเห็นว่ายังมีการบัญญัติที่มีขอบเขตกว้างมากเกินไป ทำให้ขาดความชัดเจน อาจทำให้เกิดความไม่ชัดเจน แน่นอนในการนำมาบังคับใช้ จึงเห็นควรมีการแก้ไข ปรับปรุง เพิ่มเติม เพื่อให้บทบัญญัติกฎหมายมีความชัดเจนมากยิ่งขึ้น โดยศึกษาเปรียบเทียบกับกฎหมายต่างประเทศเพื่อนำมาใช้เป็นแนวทางในการบัญญัติกฎหมายให้มีความเหมาะสมกับลักษณะของการกระทำความผิดมากขึ้น

ร่างพระราชบัญญัติฉบับนี้ได้กำหนดคำนิยามของคำว่า ข้อมูลส่วนบุคคล ไว้ในมาตรา 3 ว่า “ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม บรรดาที่มีชื่อของบุคคลนั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย” ซึ่งสิ่งต่างๆ เหล่านี้เป็นข้อมูลส่วนบุคคลที่อาจเป็นข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้ คือ อาจเป็นข้อมูลที่ใช้เพียงลำพังก็เป็นสิ่งซึ่งแสดงเอกลักษณ์บุคคลได้ เช่น ลายพิมพ์นิ้วมือ หรืออาจเป็นกรณีการรวมกันของข้อมูลส่วนบุคคลหลายๆ ข้อมูลแล้วจึงเกิดเป็นข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่สามารถระบุตัวบุคคลได้แน่นอน

เฉพาะเจาะจง เช่น ชื่อ โดยลำพังอาจไม่เป็นสิ่งซึ่งแสดงเอกลักษณ์บุคคลเนื่องจากบุคคลอาจมีชื่อซ้ำกันได้ แต่เมื่อนำชื่อ ไปรวมกับข้อมูลอื่นๆ เช่น นามสกุล วันเดือนปีเกิด ที่อยู่ ฯลฯ แล้วทำให้สามารถระบุตัวบุคคลได้ ข้อมูลส่วนบุคคลเหล่านี้ก็จะกลายเป็นข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

อย่างไรก็ตามจากการเปรียบเทียบการบัญญัติคำนิยามข้อมูลส่วนบุคคลในต่างประเทศโดยเฉพาะกฎหมายของประเทศสหรัฐอเมริกา และประเทศแคนาดา พบว่ามีการบัญญัตินิยามครอบคลุมถึงข้อมูลทางอิเล็กทรอนิกส์ด้วย ซึ่งผู้เขียนเห็นว่ามีความเหมาะสมกับสถานการณ์ในปัจจุบันที่มีการใช้ข้อมูลทางอิเล็กทรอนิกส์กันแพร่หลายมากขึ้น มีการทำธุรกรรมต่างๆ ผ่านทางอินเตอร์เน็ตมากขึ้น เช่น การทำธุรกรรมทางการเงิน การโอนเงินผ่านทางระบบคอมพิวเตอร์ออนไลน์ ฯลฯ และในส่วนคำนิยามของไทยมีบัญญัติรวมถึงข้อมูลส่วนบุคคลของผู้ที่ถึงแก่กรรมไปแล้วด้วย ผู้เขียนเห็นว่ามีความเหมาะสมเนื่องจากสามารถช่วยแก้ไขปัญหาการสวมรอยบุคคลของคนต่างด้าวที่เข้าประเทศมาโดยมิชอบด้วยกฎหมายที่ใช้ช่องโอกาสจากข้อมูลของผู้ที่เสียชีวิตไปแล้วได้ จาการศึกษาร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ผู้เขียนเห็นว่าบทบัญญัติในหลักการสำคัญได้มีการบัญญัติให้ความคุ้มครองข้อมูลส่วนบุคคลไว้เป็นพื้นฐานแล้ว หากได้มีการแก้ไข ปรับปรุง เพิ่มเติมบทบัญญัติในบางส่วน จะช่วยให้สามารถบังคับใช้กับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล และสามารถอำนวยความยุติธรรมได้มากยิ่งขึ้น

บทที่ 4

วิเคราะห์เปรียบเทียบกฎหมายของประเทศไทยและของต่างประเทศ ในเรื่องการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

ปัจจุบันประเทศไทยยังไม่มีบทกฎหมายเฉพาะที่จะนำมาบังคับใช้กับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล จึงได้แต่เพียงนำบทกฎหมายที่มีความเกี่ยวข้อง หรือใกล้เคียงมาปรับใช้กับการกระทำความผิด ซึ่งทำให้เกิดช่องว่างในการบังคับใช้กฎหมายขึ้น เนื่องจากในบางกรณีของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ไม่มีบทกฎหมายใดที่จะสามารถนำมาบังคับใช้แก่ผู้กระทำความผิดได้ เช่น ในกรณีที่มีการรวบรวมเก็บข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เพื่อจะนำไปใช้แสวงหาประโยชน์โดยมิชอบ หรือกรณีการจดจำหมายเลขบัตรเครดิต บัตรประจำตัวประชาชนไปใช้ ฯลฯ ดังนี้เมื่อศึกษากฎหมายของต่างประเทศที่มีความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกิดขึ้นเป็นจำนวนมากแล้ว พบว่าในบางประเทศมีการบัญญัติกฎหมายสำหรับฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะ ประเทศที่ผู้เขียนศึกษา คือ ประเทศสหรัฐอเมริกา และประเทศแคนาดา ในบางประเทศก็มิได้มีการบัญญัติบทกฎหมายไว้เฉพาะเช่นเดียวกันกับประเทศไทย ประเทศที่ผู้เขียนทำการศึกษา คือ ประเทศสหราชอาณาจักร ดังนี้ผู้เขียนจึงเห็นควรเปรียบเทียบบทกฎหมายของประเทศไทยและต่างประเทศในส่วนที่เกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

4.1 บทวิเคราะห์เปรียบเทียบกฎหมายที่เกี่ยวข้องกับการกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

ในการจะพิจารณาว่าการกระทำใดเป็นความผิดทางอาญาหรือไม่ ต้องดูเรื่องโครงสร้างความรับผิดทางอาญา และสาระสำคัญของกฎหมาย คือ เมื่อมีผู้กระทำการฝ่าฝืนกฎหมาย ย่อมต้องรับโทษ ดังนี้ผู้เขียนจึงเปรียบเทียบกฎหมายโดยแบ่งเป็นประเด็นย่อย ดังนี้

4.1.1 ประเภทของกฎหมายที่กำหนดฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

ในทุกระบบกฎหมาย หรือในทุกประเทศทั่วโลก กฎหมายที่จะนำมาใช้บังคับกับประชาชนพลเมืองย่อมมีหลากหลายประเภท ซึ่งกฎหมายแต่ละประเภทอาจมีลำดับศักดิ์ ขอบเขตของการบังคับใช้ไม่เท่ากัน จึงเกิดการแบ่งประเภทของกฎหมายขึ้น ดังนี้ในความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในแต่ละประเทศจะอยู่ในกฎหมายประเภทใด จึงเป็นประเด็นที่ต้องเปรียบเทียบเพื่อให้เห็นถึงความสำคัญ และเพื่อเป็นแนวทางในการปรับปรุง แก้ไข หรือกำหนดบทกฎหมายของประเทศไทยต่อไป

ประเทศสหรัฐอเมริกา มีการบัญญัติฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะในพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) ซึ่งพระราชบัญญัติฉบับนี้ทำให้เกิดการแก้ไขประมวลกฎหมายอาญาของสหรัฐอเมริกาในหมวดที่ 18 มาตรา 1028 ว่าด้วยการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

ประเทศแคนาดา มีการบัญญัติฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะในประมวลกฎหมายอาญามาตรา 402 และมาตรา 403

ประเทศสหราชอาณาจักร ไม่มีการบัญญัติฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะ แต่มีกฎหมายที่เกี่ยวข้อง และมีความใกล้เคียงที่สามารถนำมาบังคับใช้ได้อยู่หลายบทกฎหมาย ซึ่งอาจทำให้เกิดความสับสน ยุ่งยากในการบังคับใช้กับความผิดและไม่ครอบคลุมในทุกกรณีของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ซึ่งกฎหมายฉบับที่อาจนำมาปรับใช้ได้จัดอยู่ในประเภทพระราชบัญญัติ

ประเทศไทย ไม่มีการบัญญัติฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะ แต่มีกฎหมายที่เกี่ยวข้อง และมีความใกล้เคียงที่สามารถนำมาบังคับใช้ได้อยู่

หลายบทกฎหมาย ซึ่งอาจทำให้เกิดความสับสน ยุ่งยากในการบังคับใช้กับความผิด และไม่ครอบคลุมในทุกกรณีของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ซึ่งกฎหมายฉบับที่อาจนำมาปรับใช้ได้อยู่ในประเภทประมวลกฎหมาย และพระราชบัญญัติ

เนื่องจากประเทศไทยและประเทศสหราชอาณาจักรไม่มีการบัญญัติบทกฎหมายเฉพาะสำหรับความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้ ในการเปรียบเทียบกฎหมายจึงต้องยึดบทกฎหมายที่มีความเกี่ยวข้อง และใกล้เคียงที่สุดที่สามารถจะนำมาเปรียบเทียบได้

4.1.2 การกำหนดคำนิยามสำหรับความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

เนื่องจากประเทศไทยและประเทศสหราชอาณาจักรไม่มีการบัญญัติบทกฎหมายเฉพาะสำหรับความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้ ผู้เขียนจึงได้นำบทกฎหมายที่เกี่ยวข้อง และมีความใกล้เคียงมาเปรียบเทียบในส่วนของการนิยามความหมายสำหรับความผิด ทั้งนี้เพื่อเป็นแนวทางในการกำหนดบทนิยามที่เหมาะสมสำหรับประเทศไทยต่อไป

ประเทศสหรัฐอเมริกา ในพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) มีการบัญญัติคำนิยาม “สิ่งซึ่งแสดงตัวบุคคล” (means of identification) ไว้ว่าหมายความถึง ชื่อ หรือตัวเลขใดๆ ที่สามารถใช้โดยลำพัง หรือร่วมกับข้อมูลอื่นๆ แล้วสามารถระบุตัวบุคคลได้ รวมถึง

- ชื่อ หมายเลขประกันสังคม วันเดือนปีเกิด ใบอนุญาตขับขี่ที่ออกโดยรัฐบาล หมายเลขประจำตัวประชาชน หมายเลขทะเบียนบุคคลต่างด้าว หมายเลขหนังสือเดินทาง หมายเลขประจำตัวลูกจ้างหรือหมายเลขผู้เสียภาษี
- ข้อมูลเอกลักษณ์ทางชีวภาพของบุคคล เช่น ลายพิมพ์นิ้วมือ เสียง เยื่อชั้นในม่านตา หรือเอกลักษณ์ทางกายภาพอื่นๆ ที่แสดงออก

- หมายเลขอิเล็กทรอนิกส์ที่เป็นเอกลักษณ์ ที่อยู่ รหัสผ่าน
- ข้อมูลจากการสื่อสารโดยเทคโนโลยีที่สามารถระบุตัวบุคคลได้

ประเทศแคนาดา ในประมวลกฎหมายอาญามีการบัญญัติคำนิยาม “ข้อมูลซึ่งแสดงเอกลักษณ์บุคคล” (Identity Information) ว่าหมายความถึง ข้อมูลใดๆ รวมทั้งทางชีววิทยาหรือข้อมูลชีวภาพที่ใช้โดยลำพัง หรือร่วมกับข้อมูลอื่นๆ เพื่อระบุตัวบุคคล หรืออ้างถึงตัวบุคคล รวมถึง ลายพิมพ์นิ้วมือ เสียง เยื่อชั้นในลูกตา ม่านตา ประวัติดีเอ็นเอ ชื่อ ที่อยู่ วันเดือนปีเกิด ลายเซ็น ลายเซ็นอิเล็กทรอนิกส์ ลายเซ็นดิจิทัล (digital signature) ชื่อผู้ใช้ (user name) หมายเลขบัตรเครดิต หมายเลขบัตรเดบิต หมายเลขบัญชีสถาบันไฟแนนซ์ หมายเลขหนังสือเดินทาง หมายเลขประกันสังคม หมายเลขประกันสุขภาพ หมายเลขใบอนุญาตขับขี่ หรือรหัสผ่าน

ประเทศสหราชอาณาจักร ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998 (The Data Protection Act of 1998) มีการบัญญัติคำนิยามของ “ข้อมูลส่วนบุคคล” (personal data) ว่าหมายความถึง ข้อมูลเกี่ยวกับความเป็นอยู่ของบุคคลซึ่งสามารถระบุตัวบุคคลได้จากข้อมูลนั้นเอง หรือจากข้อมูล ข่าวสารที่อยู่ในการควบคุมของผู้ควบคุมข้อมูล (data controller) และรวมถึงการแสดงความคิดเห็น คำบอกกล่าวใดๆ ที่เกี่ยวกับบุคคลซึ่งผู้อื่น หรือบุคคลที่สามได้กล่าวถึงเจ้าของข้อมูลส่วนบุคคลนั้น และในพระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 (The Identity Card Act of 2006) มีการให้คำนิยามของคำว่า “เอกสารแสดงข้อมูลเอกลักษณ์บุคคล” (identity document) ไว้ว่า เอกสารใดๆ ที่มีความหมายเหมือน

ก. บัตรประจำตัวประชาชน
ข. เอกสารที่เกี่ยวกับชื่อ หรือยศ
ค. เอกสารการเข้าเมือง
ง. หนังสือเดินทางของประเทศสหราชอาณาจักร
จ. หนังสือเดินทางที่ออกโดยผู้มีอำนาจในประเทศ หรือนอกอาณาเขตประเทศสหราชอาณาจักร หรือโดยองค์กรระหว่างประเทศ
ฉ. เอกสารที่สามารถใช้แทนหนังสือเดินทางได้ (ในบางสถานการณ์หรือทุกสถานการณ์)

ช. ใบอนุญาตขับขี่ของประเทศสหราชอาณาจักร

ซ. ใบอนุญาตขับขี่ที่ออกโดยผู้มีอำนาจในประเทศหรือนอกอาณาเขตประเทศสหราชอาณาจักร

ประเทศไทย ในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ได้มีการบัญญัตินิยามของคำว่า “ข้อมูลส่วนบุคคล” ว่าหมายความถึง ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม บรรดาที่มีชื่อของบุคคลนั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

ดังนี้แล้วจะเห็นได้ว่าคำนิยามของประเทศสหรัฐอเมริกา กับคำนิยามของประเทศแคนาดามีความคล้ายคลึงกันมาก และเป็นคำนิยามที่บัญญัติได้ครอบคลุมกว่าของประเทศสหราชอาณาจักรและของประเทศไทย กล่าวคือ คำนิยามของทั้งประเทศไทยและประเทศสหหราชอาณาจักรยังไม่มีการบัญญัติครอบคลุมไปถึงเรื่องข้อมูลทางอิเล็กทรอนิกส์ ซึ่งนับเป็นสิ่งจำเป็นและในปัจจุบันก็เกิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลทางอินเตอร์เน็ต หรือทางสื่ออิเล็กทรอนิกส์อยู่เป็นจำนวนมาก แต่ทั้งนี้คำนิยามของประเทศไทยมีการบัญญัติถึงข้อมูลของผู้ที่ถึงแก่กรรมแล้วด้วย ผู้เขียนเห็นว่ามีความเหมาะสม เนื่องจากปัญหาที่เกิดขึ้นในปัจจุบันก็มีการโจรกรรมข้อมูลของบุคคลซึ่งเสียชีวิตไปแล้วด้วย

4.1.3 การกำหนดฐานความผิด และองค์ประกอบของความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

ในฐานความผิดหนึ่งๆ ย่อมต้องมีการแยกองค์ประกอบความผิด เพื่อที่จะได้รู้ว่าการกระทำใดๆ จะถือเป็นการกระทำความผิดตามกฎหมายนั้นๆ ซึ่งคือ เรื่องโครงสร้างความรับผิดในทางอาญา กล่าวคือบุคคลจะต้องรับผิดในทางอาญาต่อเมื่อ

1.) การกระทำครบองค์ประกอบความผิดที่กฎหมายบัญญัติ

2.) การกระทำไม่มีกฎหมายยกเว้นความผิด

3.) การกระทำไม่มีกฎหมายยกเว้นโทษ

ในประเด็นเปรียบเทียบส่วนนี้ ก็คือ ข้อ 1.) ของโครงสร้างความรับผิดทางอาญา เรื่อง องค์ประกอบความผิดที่กฎหมายบัญญัติ ซึ่งสามารถแบ่งออกได้เป็น 4 ส่วน คือ หนึ่งส่วนของการกระทำ สององค์ประกอบภายนอก สามองค์ประกอบภายใน และสี่ผลของการกระทำสัมพันธ์กับการกระทำ สามส่วนแรกเป็นสิ่งจำเป็นที่ต้องปรากฏอยู่ในมาตราที่บัญญัติความผิด เพื่อให้เกิดความครอบคลุม และง่ายต่อความเข้าใจในการเปรียบเทียบฐานความผิด และองค์ประกอบความผิดนี้ ผู้เขียนจึงแบ่งออกเป็นประเด็นย่อย ดังนี้

4.1.3.1 การได้มาซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล

4.1.3.2 การจัดทำขึ้นซึ่งเอกสารแสดงเอกลักษณ์บุคคลปลอม

4.1.3.3 การมีไว้ในความครอบครองซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล

4.1.3.4 การจำหน่าย หรือการโอนซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล

4.1.3.5 การทำขึ้น โอน และครอบครองเครื่องมือทำเอกสารแสดงตัวบุคคลหรือเอกสารแสดงตัวบุคคลปลอม

4.1.3.6 การกำหนดถึงเหตุจูงใจที่กระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

4.1.3.1 **การได้มาซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล**

ในการดำเนินชีวิตประจำวัน การติดต่อ ทำธุรกรรมกับสถานที่ต่างๆ ในปัจจุบันล้วนต้องมีการให้ข้อมูลส่วนตัว เพื่อทำการยืนยันตัวบุคคลที่เป็นผู้ดำเนินการในเรื่องนั้นๆ จึงเกิดการให้และรับข้อมูลส่วนบุคคลกันในหลายลักษณะ ทำให้การได้มาซึ่งข้อมูลเอกลักษณ์บุคคลนั้นสามารถแบ่งออกได้เป็น 2 ประเภท คือ หนึ่งการได้มาซึ่งข้อมูลเอกลักษณ์บุคคลโดยชอบด้วยกฎหมาย ตัวอย่างเช่น ผู้มาติดต่อสมัครงานได้กรอกรายละเอียดข้อมูลส่วนตัวลงในใบสมัครและ

มอบให้แก่บริษัทที่ตนไปสมัครงาน และสอง การได้มาซึ่งข้อมูลเอกลักษณ์บุคคลโดยมิชอบด้วยกฎหมาย เช่น การขโมยบัตรประชาชน หรือขโมยบัตรเครดิต ดังนี้ในปัจจุบันกฎหมายของประเทศไทยไม่มีการบัญญัติความผิดเกี่ยวกับการได้มาซึ่งข้อมูลเอกลักษณ์บุคคลไว้เป็นการเฉพาะ จึงได้เพียงนำกฎหมายที่มีความเกี่ยวข้อง และใกล้เคียงมาบังคับใช้เท่านั้น กล่าวคือ ความผิดฐานลักทรัพย์ ความผิดฐานฉ้อโกง ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ซึ่งฐานความผิดนี้ก็สามารถบังคับใช้ได้แค่ในส่วนที่เป็นการได้มาซึ่งข้อมูลเอกลักษณ์บุคคลโดยมิชอบด้วยกฎหมายแต่เพียงอย่างเดียว ไม่สามารถนำมาบังคับใช้กับการได้มาซึ่งข้อมูลเอกลักษณ์บุคคลโดยชอบด้วยกฎหมาย ที่ผู้ที่ได้ข้อมูลมาเจตนาจะเก็บข้อมูลนั้นไว้เพื่อนำไปแสวงหาประโยชน์ที่มิชอบแก่ตน หรือผู้อื่นในภายหลัง หรือในกรณีที่ได้มาซึ่งข้อมูลเอกลักษณ์บุคคลโดยมิชอบด้วยกฎหมาย ในบางกรณีก็ไม่มีกฎหมายที่จะนำมาบังคับใช้ ตัวอย่างเช่น การแอบดูและจดจำข้อมูลหมายเลขบัตรประจำตัวประชาชนของผู้อื่นไว้ หรือการแอบจดหมายเลขบัตรเครดิตของผู้อื่นไว้ หรือการเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นซึ่งคอมพิวเตอร์นั้นมิได้มีระบบป้องกันการเข้าถึงไว้ เป็นต้น จึงกล่าวได้ว่ากฎหมายไทยปัจจุบันยังไม่ครอบคลุมเพียงพอสำหรับความผิดฐานการได้มาซึ่งข้อมูลหรือเอกสารที่แสดงเอกลักษณ์บุคคล เมื่อเปรียบเทียบกับกฎหมายของประเทศสหราชอาณาจักร พบว่าในกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998 (The Data Protection Act of 1998) มีการกำหนดฐานความผิดสำหรับผู้ที่ได้มาซึ่งข้อมูลส่วนบุคคล หรือข้อมูลที่อยู่ในส่วนบุคคลโดยที่ไม่ได้รับความยินยอมจากผู้ควบคุมข้อมูล และในประมวลกฎหมายอาญาของประเทศแคนาดา มีการกำหนดฐานความผิดสำหรับผู้ที่ได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่น โดยมีวัตถุประสงค์เพื่อจะนำไปใช้กระทำความผิดอาญา รวมถึงกรณีการได้มาโดยฉ้อโกง หลอกลวง หรือกล่าวเท็จด้วย ดังนี้ผู้เขียนจึงเห็นว่าการบัญญัติความผิดเกี่ยวกับการได้มาซึ่งข้อมูลหรือเอกสารแสดงเอกลักษณ์บุคคลของประเทศสหราชอาณาจักร และประเทศแคนาดามีความครอบคลุมมากกว่ากฎหมายไทยที่มีอยู่ในปัจจุบัน

4.1.3.2 การจัดทำขึ้นซึ่งเอกสารแสดงเอกลักษณ์บุคคลปลอม

ในการกระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์ของบุคคลนั้น สิ่งสำคัญและเกิดขึ้นมากในการกระทำความผิด คือ การจัดทำเอกสารซึ่งแสดงเอกลักษณ์บุคคลปลอมขึ้นมา เพื่อสร้างความน่าเชื่อถือในการนำไปใช้เสมือนตนเป็นเจ้าของเอกสารนั้นจริงๆ เพราะตนมีเอกสารนั้นๆ อยู่ในความครอบครอง ในปัจจุบันกฎหมายของประเทศไทยที่เกี่ยวข้องกับฐานความผิดการจัดทำขึ้นซึ่งเอกสารแสดงเอกลักษณ์บุคคลปลอมนั้นมีการบัญญัติคุ้มครองไว้เพียงเฉพาะเอกสารบางประเภทเท่านั้น กล่าวคือ ในประมวลกฎหมายอาญาลักษณะความผิดเกี่ยวกับการปลอมและการแปลง มาตรา 264 การปลอมเอกสาร มาตรา 265 การปลอมเอกสารสิทธิ มาตรา 266 การปลอมเอกสารราชการ มาตรา 269/1 การปลอมบัตรอิเล็กทรอนิกส์ มาตรา 269/8 การปลอมหนังสือเดินทาง และในกฎหมายอื่นปรากฏมีในพระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ในมาตรา 14(3) การปลอมบัตร หรือใบรับหรือใบแทนใบรับบัตรประจำตัวประชาชน ดังนี้จะเห็นได้ว่าลักษณะการบัญญัติกฎหมายของไทยเป็นแบบกำหนดการคุ้มครองเป็นประเภทๆ เอกสารไป ทำให้ยังเกิดมีช่องว่างสำหรับเอกสารแสดงเอกลักษณ์บุคคลบางประเภทที่ยังไม่ได้รับการคุ้มครอง ตัวอย่างเช่น ใบสูติบัตร หรือในส่วนของเอกสารอิเล็กทรอนิกส์ซึ่งเป็นที่นิยมใช้กันมากในปัจจุบัน และเกิดการกระทำความผิดผ่านทางอิเล็กทรอนิกส์มากขึ้นด้วย ยังไม่มีกฎหมายบัญญัติให้ความคุ้มครอง ตัวอย่างเช่น การปลอมลายมือชื่ออิเล็กทรอนิกส์ เมื่อเปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกาพบว่าในกฎหมายพระราชบัญญัติยับยั้งและสันนิษฐานการขโมยข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) มีการกำหนดความผิดสำหรับผู้ที่จัดทำขึ้นซึ่งเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอม ซึ่งเอกสารนั้นบัญญัติไว้ครอบคลุมกว่าของประเทศไทย กล่าวคือมีการบัญญัติคุ้มครองไปถึงเอกสารข้อมูลบุคคลทางชีวภาพด้วย ตัวอย่างเช่น ลายพิมพ์นิ้วมือ เสียง ม่านตา และรวมถึงที่เป็นข้อมูลทางอิเล็กทรอนิกส์ด้วย ตัวอย่างเช่น ลายมือชื่ออิเล็กทรอนิกส์ หรือรหัสผ่านทางอิเล็กทรอนิกส์ต่างๆ เป็นต้น

4.1.3.3 การมีไว้ในความครอบครองซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล

การมีไว้ในความครอบครองซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคลนี้ สามารถแบ่งแยกออกได้เป็น 2 ประเภท คือ การมีไว้ในครอบครองซึ่งเอกสารแสดงเอกลักษณ์บุคคลที่เป็นของจริง และการมีไว้ในครอบครองซึ่งเอกสารแสดงเอกลักษณ์บุคคลที่เป็นของปลอม ซึ่งปัจจุบันกฎหมายไทยก็ได้มีการบัญญัติถึงความผิดการมีไว้ในความครอบครองซึ่งเอกสารแสดงเอกลักษณ์บุคคลทั้งสองประเภท แต่เฉพาะเอกสารบางประเภทเท่านั้น คือ ในประมวลกฎหมายอาญา มาตรา 269/4 การมีไว้ในครอบครองเพื่อใช้ หรือเพื่อจำหน่ายซึ่งบัตรอิเล็กทรอนิกส์ปลอม มาตรา 269/6 การมีไว้ในครอบครองเพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่น มาตรา 269/9 การมีไว้ในครอบครองเพื่อใช้ หรือเพื่อจำหน่ายซึ่งหนังสือเดินทางปลอม และในกฎหมายอื่นปรากฏมีในพระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ในมาตรา 15 ทวิ การเอาไปเสียหรือยึดไว้ซึ่งบัตร หรือใบรับหรือใบแทนใบรับบัตรประจำตัวประชาชนของผู้อื่น เพื่อประโยชน์สำหรับตนเองหรือผู้อื่นโดยมิชอบ ดังนี้เห็นได้ว่ากฎหมายไทยยังให้ความคุ้มครองเอกสารซึ่งแสดงเอกลักษณ์บุคคลได้ไม่ครบถ้วน ตัวอย่างเช่น หนังสือเดินทางของผู้อื่น บัตรประกันสังคมของผู้อื่น ใบอนุญาตขับขี่ของผู้อื่น เป็นต้น เมื่อเปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกาพบว่าในกฎหมายพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) มีการกำหนดความผิดสำหรับผู้มีไว้ในความครอบครองซึ่งเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอมตั้งแต่ห้าฉบับขึ้นไป ดังนี้จึงมีความหมายรวมถึงเอกสารแสดงตัวบุคคลทุกประเภท และรวมทั้งที่เป็นเอกสารจริงและเอกสารปลอมด้วย และในประมวลกฎหมายอาญาของประเทศแคนาดา มีการกำหนดความผิดสำหรับผู้ที่มีไว้ในความครอบครองซึ่งข้อมูลที่แสดงเอกลักษณ์บุคคลของผู้อื่น เพื่อใช้ หรือเพื่อจำหน่าย ซึ่งมีความครอบคลุมข้อมูล และเอกสารซึ่งแสดงเอกลักษณ์บุคคลทุกประเภท ดังนี้จึงเห็นได้ว่ากฎหมายของประเทศสหรัฐอเมริกา และประเทศแคนาดามีความครอบคลุมมากกว่ากฎหมายไทย

4.1.3.4 การจำหน่าย หรือการโอนซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล

ปัจจุบันข้อมูลซึ่งแสดงเอกลักษณ์บุคคล หรือข้อมูลส่วนบุคคลนั้นได้เข้ามามีบทบาทในการติดต่อ ทำธุรกรรมซื้อขายเป็นอย่างมาก เนื่องจากในการติดต่อค้าขายใดๆ ย่อมต้องมีการให้ข้อมูลรายละเอียดเกี่ยวกับสิ่งยืนยันตัวบุคคล ตัวอย่างเช่น ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์ หมายเลขประจำตัวประชาชน เป็นต้น การทำธุรกิจปัจจุบันก็มีการแข่งขันกันสูงทำให้ผู้ประกอบการต้องใช้ทุกวิถีทางเพื่อให้ตนสามารถเข้าถึงกลุ่มลูกค้าได้มากที่สุด ทำให้เกิดการซื้อขายข้อมูลลูกค้าขึ้นมากมาย ซึ่งปัจจุบันกฎหมายไทยก็ได้มีการบัญญัติเกี่ยวกับฐานความผิดการจำหน่ายข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล คือ ในประมวลกฎหมายอาญา มาตรา 269/4 วรรคสอง ความผิดฐานจำหน่ายบัตรอิเล็กทรอนิกส์ปลอม และมาตรา 269/9 วรรคสอง ความผิดฐานจำหน่ายหนังสือเดินทางปลอม ซึ่งเห็นได้ว่ายังบัญญัติไม่ครอบคลุมถึงข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคลประเภทอื่นๆ ตัวอย่างเช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เมื่อเปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกาพบว่าในกฎหมายพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) มีการกำหนดฐานความผิดสำหรับผู้ที่เจตนาโอนซึ่งเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอม โดยรู้อยู่ว่าเอกสารดังกล่าวได้มาจากการโจรกรรม หรือถูกจัดทำขึ้นโดยปราศจากอำนาจตามกฎหมาย กฎหมายของประเทศสหรัฐอเมริกานี้จึงครอบคลุมถึงข้อมูลและเอกสารแสดงเอกลักษณ์บุคคลทุกประเภท รวมทั้งยังบัญญัติเอาผิดทั้งในกรณีที่เป็นเอกสารของจริงและในกรณีที่เป็นเอกสารของปลอมด้วย และในประมวลกฎหมายอาญาของประเทศแคนาดา มีการกำหนดฐานความผิดสำหรับผู้ที่จำหน่าย หรือเสนอขายข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคลของผู้อื่น กฎหมายของประเทศแคนาดานี้จึงครอบคลุมถึงข้อมูล และเอกสารแสดงเอกลักษณ์บุคคลทุกประเภท และในกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998 (The Data Protection Act of 1998) ของประเทศสหราชอาณาจักร ก็มีการบัญญัติเอาผิดกับการจำหน่าย หรือเสนอขายข้อมูลส่วนบุคคลโดยปราศจากความยินยอมของผู้ควบคุมข้อมูล ทั้งนี้กฎหมายฉบับนี้ได้บัญญัติเอาผิดทั้งกรณีการจำหน่ายข้อมูลส่วนบุคคลของตนเอง และกรณี

การจำหน่ายข้อมูลส่วนบุคคลของผู้อื่นด้วย ดังนี้จึงเห็นได้ว่ากฎหมายของต่างประเทศมีการบัญญัติฐานความผิดเกี่ยวกับการจำหน่าย หรือการโอนซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคลได้ครอบคลุมมากกว่าประเทศไทย

4.1.3.5 การทำขึ้น โอน และครอบครองเครื่องมือทำเอกสารแสดงตัวบุคคลหรือเอกสารแสดงตัวบุคคลปลอม

ในการจะจัดทำเอกสารซึ่งแสดงเอกลักษณ์บุคคลปลอมขึ้น สิ่งจำเป็นหนึ่งที่จะขาดไม่ได้ คือ เครื่องมือ เนื่องจากเอกสารแสดงเอกลักษณ์บุคคลส่วนมากมักจะมีการใช้วัสดุพิเศษและมีการออกแบบที่เป็นเอกลักษณ์ที่ให้ทำปลอมขึ้นได้ยาก ตัวอย่างเช่น บัตรประจำตัวประชาชน ที่จะมีลายน้ำ หรือตราประทับต่างๆ บนบัตร ตราประทับในหนังสือเดินทาง เป็นต้น แต่อย่างไรก็ตามก็ยังคงมีเครื่องมือ หรือเทคโนโลยีต่างๆ ที่สามารถจัดทำเอกสารซึ่งแสดงเอกลักษณ์บุคคลปลอมขึ้นได้ เมื่อบุคคลใดทำเครื่องมือเช่นว่าขึ้น หรือมีเครื่องมือนั้นไว้ในครอบครอง หรือโอนเครื่องมือนั้นย่อมก็ให้เกิดการปลอมเอกสารซึ่งแสดงเอกลักษณ์บุคคลได้สะดวก และเพิ่มจำนวนมากขึ้น ปัจจุบันกฎหมายไทยที่บัญญัติความผิดเกี่ยวกับการทำขึ้น โอน และครอบครองเครื่องมือทำเอกสารแสดงตัวบุคคลหรือเอกสารแสดงตัวบุคคลปลอม มีปรากฏอยู่ในประมวลกฎหมายอาญา มาตรา 269/2 ที่เอาผิดกับบุคคลใดที่ทำเครื่องมือ หรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ หรือมีเครื่องมือหรือวัตถุเช่นว่านั้น เพื่อใช้หรือเพื่อให้ได้ข้อมูลในการปลอมหรือแปลง ดังนี้จะเห็นได้ว่ากฎหมายไทยบัญญัติเพียงเครื่องมือที่ใช้ปลอมหรือแปลงบัตรอิเล็กทรอนิกส์เท่านั้น ยังไม่ครอบคลุมถึงเอกสารซึ่งแสดงเอกลักษณ์บุคคลในอีกหลายๆ ประเภท ตัวอย่างเช่น เครื่องมือทำบัตรประจำตัวประชาชนปลอม ทำบัตรอนุญาตขับขี่ปลอม เป็นต้น เมื่อเปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกาพบว่าในกฎหมายพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) มีการกำหนดฐานความผิดเกี่ยวกับเครื่องมือไว้ว่า ผู้ใดเจตนาทำ โอนหรือครอบครองเครื่องมือทำเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอม หรือสิ่งใดๆ ที่ก่อให้เกิดผลได้เช่นเดียวกันนั้นมีความผิด ดังนี้เป็นการบัญญัติกว้างๆ

สามารถรวมถึงเครื่องมือ หรือสิ่งอื่นใดที่สามารถทำเอกสารแสดงตัวบุคคลปลอมได้ในเอกสารทุกประเภท และในพระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 (The Identity Card Act of 2006) ของประเทศสหราชอาณาจักรได้มีการบัญญัติเอาผิดแก่ผู้ที่จัดทำ หรือมีเครื่องมือ อุปกรณ์ที่สามารถนำมาใช้ทำเอกสารปลอมด้วย ซึ่งเอกสารแสดงข้อมูลเอกลักษณ์บุคคลตามคำนิยามในพระราชบัญญัติฉบับนี้มีความหมายครอบคลุมกว่ากฎหมายไทย คือ รวมเอกสารใดๆ ที่มีความหมายเหมือนกับบัตรประจำตัวประชาชน หนังสือเดินทาง เอกสารคนเข้าเมือง และใบอนุญาตขับขี่ เป็นต้น จึงเห็นได้ว่ากฎหมายของประเทศสหรัฐอเมริกา และประเทศสหราชอาณาจักรมีการบัญญัติที่ครอบคลุมประเภทของเอกสารมากกว่าในกฎหมายไทย

4.1.3.6 การกำหนดถึงเหตุจูงใจที่กระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

การกระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลนั้น อาจเกิดขึ้นโดยเป็นฐานความผิดเดียวที่ผู้กระทำต้องรับผิดก็ได้ หรืออาจเป็นกรณีที่การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นเพียงฐานความผิดเริ่มแรกที่จะนำไปสู่การกระทำความผิดอื่นๆ หรืออาจกล่าวได้ว่าแท้จริงแล้วผู้กระทำความผิดนั้นต้องการที่จะกระทำความผิดอาญาฐานอื่น แต่จะกระทำความผิดอาญาฐานนั้นๆ สำเร็จได้ต้องกระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลก่อน ทั้งนี้อาจเพื่อความสะดวกในการกระทำความผิด หรือเพื่อหลีกเลี่ยงการถูกจับกุมดำเนินคดีก็ได้ ตัวอย่างเช่น การปลอมตัวเป็นบุคคลอื่นโดยอาศัยการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลมาแล้วใช้เสมือนเป็นข้อมูลของตนเองเพื่อเดินทางเข้า หรือออกประเทศที่ตัวตนที่แท้จริงไม่อาจเข้า หรือออกได้ หรือเพื่อหลีกเลี่ยงการตรวจสอบ เพื่อเข้าไปวางแผนหรือกระทำการก่อการร้าย เป็นต้น ซึ่งกฎหมายของประเทศไทยในปัจจุบันยังไม่มีการกำหนดฐานความผิดในลักษณะนี้ไว้ แต่เมื่อเปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกาแล้วพบว่าในกฎหมายพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) มีการกำหนดฐานความผิดที่เป็นแรงจูงใจให้บุคคลนั้นกระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล กล่าวคือ มีการบัญญัติโทษหนักขึ้นหากการกระทำ

ความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลนั้น ทำขึ้นเพื่อให้ความสะดวกในการกระทำความผิดเกี่ยวกับการค้ายาเสพติด หรือเป็นการกระทำที่เชื่อมโยงกับการกระทำความผิดอาญาอื่นที่ใช้ความรุนแรง หรือเป็นการให้ความสะดวกแก่การก่อการร้ายระหว่างประเทศ ดังนี้ผู้เขียนเห็นว่าเป็นการบัญญัติกฎหมายที่มีความเหมาะสมเนื่องจาก การให้ความสะดวกแก่การกระทำความผิดฐานอื่นล้วนมีความร้ายแรง หากเกิดความผิดนั้นๆ ขึ้นก็จะสร้างความเสียหายเป็นอย่างมาก ทั้งต่อประเทศที่ความผิดนั้นเกิดขึ้น และประเทศอื่นๆ ในสังคมโลกด้วย

4.1.4 ผู้เสียหายในความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

ในทุกๆ ฐานความผิดที่กฎหมายได้บัญญัติขึ้นล้วนต้องมีเจตนารมณ์เพื่อจะคุ้มครองสิ่งใดสิ่งหนึ่ง ตัวอย่างเช่น ความผิดฐานลักทรัพย์ สิ่งที่กฎหมายมุ่งจะคุ้มครอง คือ กรรมสิทธิ์ในตัวทรัพย์ของเจ้าของทรัพย์ ดังนี้ เมื่อมีผู้ใดมาแย่งการครอบครอง และกรรมสิทธิ์ในทรัพย์นั้น ผู้เป็นเจ้าของทรัพย์ย่อมเป็นผู้เสียหาย มีสิทธิร้องทุกข์ หรือดำเนินคดีได้ บุคคลอื่นที่มิใช่ผู้เสียหายในความผิดฐานนั้นๆ ก็จะไม่สามารถดำเนินการใดๆ ทางคดีเพื่อให้นำตัวผู้กระทำความผิดมาลงโทษหรือเพื่อจะให้ตนได้รับการชดใช้ เยียวยาก็มิได้ด้วย ดังนี้ประเด็นเรื่องบุคคลที่กฎหมายต้องการคุ้มครอง หรือบุคคลผู้ที่กฎหมายบัญญัติให้เป็นผู้เสียหายในความผิดเกี่ยวกับการโจรกรรมเอกลักษณ์บุคคลจึงเป็นเรื่องสำคัญที่ต้องพิจารณา

ประเทศสหรัฐอเมริกา เนื่องจากประเทศสหรัฐอเมริกามีการบัญญัติฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะ จึงมีการกำหนดไว้ในกฎหมายพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) อย่างชัดเจนว่า ผู้ที่ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นผู้เสียหาย เป็นบุคคลที่กฎหมายต้องการให้ความคุ้มครอง จึงมีสิทธิร้องทุกข์ หรือฟ้องร้องคดี อีกทั้งมีมาตรการเยียวยาผู้เสียหายด้วย โดยให้ผู้เสียหายสามารถดำเนินการแก้ไขประวัติข้อมูลเอกลักษณ์บุคคลให้ถูกต้องได้ เนื่องจากช่วงที่ถูกโจรกรรมข้อมูลไปใช้อาจทำให้เกิดมี

ประวัติที่ไม่ดีขึ้นได้ เช่น ประวัติการใช้เครดิตที่บัญญัติไว้ใน พระราชบัญญัติว่าด้วยการรายงานข้อมูลเครดิตอย่างยุติธรรม ค.ศ.1970 (The Fair Credit Reporting Act 1970) เป็นต้น

ประเทศแคนาดา เนื่องจากประเทศแคนาดามีการบัญญัติฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะ จึงมีการกำหนดไว้อย่างชัดเจนว่า ผู้ที่ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นผู้เสียหาย เป็นบุคคลที่กฎหมายต้องการให้ความคุ้มครอง มีสิทธิร้องทุกข์ หรือฟ้องร้องคดี พร้อมทั้งมีมาตรการเยียวยาผู้เสียหายด้วย โดยให้ผู้เสียหายได้รับชดใช้ค่าเสียหายที่เกิดขึ้น รวมถึงค่าใช้จ่ายในการดำเนินการแก้ไขประวัติข้อมูลเอกลักษณ์บุคคลให้ถูกต้องด้วย

ประเทศสหราชอาณาจักร เนื่องจากประเทศสหราชอาณาจักรไม่มีบทกฎหมายเฉพาะบุคคลที่ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลนั้นจะได้รับความคุ้มครองตามกฎหมายหรือไม่ จึงต้องพิจารณาแต่ละฐานความผิด ในกฎหมายแต่ละฉบับที่มีความเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล กล่าวคือ ในความผิดฐานกระทำโดยหลอกลวงผู้อื่นเพื่อให้ได้ทรัพย์สินใดๆ ไป ในพระราชบัญญัติการลักทรัพย์ ค.ศ. 1968 (The Theft Act of 1968) ผู้เสียหายหรือบุคคลที่กฎหมายมุ่งคุ้มครอง คือ ผู้ถูกหลอกลวง ซึ่งอาจเป็นได้ทั้งผู้ที่ถูกโจรกรรมข้อมูล หรือเป็นบุคคลอื่น ในความผิดฐานเปิดเผยข้อมูลส่วนบุคคลของผู้อื่นโดยมิชอบ ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998 (The Data Protection Act of 1998) ผู้เสียหายหรือบุคคลที่กฎหมายมุ่งคุ้มครอง คือ เจ้าของข้อมูลที่ถูกเปิดเผยนั้น ในความผิดฐานครอบครองเอกสารซึ่งแสดงเอกลักษณ์บุคคลปลอม โดยมีเจตนาจะใช้เอกสารเสมือนเป็นเอกสารจริงของตนเอง ในพระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 (The Identity Card Act of 2006) ผู้เสียหายหรือบุคคลที่กฎหมายมุ่งคุ้มครอง คือ ผู้ถูกใช้ข้อมูลหากผู้นั้นได้รับความเสียหายหรือคือหน่วยงานที่บุคคลที่ครอบครองเอกสารปลอมนั้นไปทำการติดต่อด้วย ในฐานความผิดการให้ข้อมูลเท็จแก่บุคคลอื่นเพื่อให้ตนได้รับเอกสารประจำตัวหรือบัตรประจำตัวประชาชน ผู้เสียหายหรือบุคคลที่กฎหมายมุ่งคุ้มครอง คือ หน่วยงานที่ได้รับการแจ้งความเท็จนั้น ในความผิดฐานฉ้อโกงโดยเป็นตัวแทนปลอมหรือฉ้อโกงโดยแสดงตนอันเป็นเท็จ (fraud by false representation) ผู้เสียหายหรือบุคคลที่กฎหมายมุ่งคุ้มครอง คือ บุคคลที่ได้รับการติดต่อจากผู้ฉ้อโกง ซึ่งย่อมไม่ใช่ผู้

เป็นเจ้าของข้อมูล ในความผิดฐานฉ้อโกงโดยการเปิดเผยข้อมูล (fraud by failing to disclose information) ผู้เสียหายหรือบุคคลที่กฎหมายมุ่งคุ้มครอง คือ บุคคลที่ถูกเปิดเผยข้อมูลที่ได้รับความเสียหาย ในความผิดฐานฉ้อโกงโดยละเมิดหน้าที่ (fraud by abuse of position) ผู้เสียหายหรือบุคคลที่กฎหมายมุ่งคุ้มครอง คือ บุคคลที่ได้รับความเสียหาย ซึ่งอาจเป็นได้ทั้งองค์กร หรือบริษัทที่ผู้กระทำการฉ้อโกงทำงานอยู่ หรืออาจเป็นบุคคลที่ถูกนำข้อมูลไปใช้ ดังนี้จะเห็นได้ว่ายังไม่มีกฎหมายเฉพาะให้ความคุ้มครองแก่ผู้ที่ถูกโจรกรรมข้อมูล ทำให้ในบางกรณีแม้ผู้ที่ถูกโจรกรรมข้อมูลจะได้รับความเสียหาย ตัวอย่างเช่น เสียชื่อเสียง เสียประวัติทางการเงิน เป็นต้น แต่ก็ไม่สามารถฟ้องร้องดำเนินคดีแก่ผู้กระทำความผิดได้

ประเทศไทย เนื่องจากประเทศไทยยังไม่มีบทกฎหมายเฉพาะ บุคคลที่ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลนั้นจะได้รับความคุ้มครองตามกฎหมายหรือไม่ จึงต้องพิจารณาแต่ละฐานความผิด ในกฎหมายแต่ละฉบับที่มีความเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล กล่าวคือ ในประมวลกฎหมายอาญา ลักษณะความผิดเกี่ยวกับการปลอมและการแปลง ความผิดฐานปลอมเอกสาร ปลอมเอกสารสิทธิ ปลอมเอกสารราชการ ปลอมบัตรอิเล็กทรอนิกส์ ปลอมหนังสือเดินทาง กฎหมายล้วนมุ่งคุ้มครองตัวเอกสาร มิได้มุ่งคุ้มครองข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่ถูกนำไปใช้ หรือคุ้มครองผู้ที่ถูกนำข้อมูลไปใช้แต่อย่างใด ลักษณะความผิดเกี่ยวกับทรัพย์ ความผิดฐานลักทรัพย์ แม้กฎหมายจะมุ่งคุ้มครองกรรมสิทธิ์ในตัวทรัพย์ของผู้เป็นเจ้าของ แต่ในหลายลักษณะของความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไม่อาจครบองค์ประกอบของความผิดฐานลักทรัพย์ได้ ความผิดฐานฉ้อโกง กฎหมายมุ่งคุ้มครองบุคคลที่ต้องเสียหายจากการถูกหลอกลวง ซึ่งโดยมากมักจะไม่ใช่ผู้ที่ถูกโจรกรรมข้อมูล ในพระราชบัญญัติอื่นๆ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ในความผิดฐานเข้าถึงระบบหรือข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ กฎหมายมุ่งคุ้มครองบุคคลผู้เป็นเจ้าของข้อมูล แต่กฎหมายฉบับนี้ก็ยังมีข้อจำกัดอยู่มาก ดังได้อธิบายไว้แล้วในบทที่ 3 พระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ในความผิดฐานปลอมบัตรประจำตัวประชาชน กฎหมายมุ่งคุ้มครองเอกสารเช่นเดียวกับความผิดฐานปลอมและแปลงในประมวลกฎหมายอาญา ในความผิดฐานใช้บัตร หรือใบรับหรือใบแทนใบรับบัตรประจำตัวประชาชนของผู้อื่นโดยมิชอบ กฎหมายมุ่ง

คุ้มครองบุคคลผู้เป็นเจ้าของบัตรประจำตัวประชาชน ความผิดฐานกระทำการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันไม่ชอบด้วยกฎหมาย ในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... กฎหมายมุ่งคุ้มครองบุคคลผู้เป็นเจ้าของข้อมูล แต่อย่างไรก็ดีกฎหมายฉบับนี้ยังไม่มีผลใช้บังคับ และฐานความผิดที่กำหนดไว้ก็ยังไม่ชัดเจน และไม่ครอบคลุม ดังนี้จะเห็นได้ว่ายังไม่มีกฎหมายเฉพาะให้ความคุ้มครองแก่ผู้ที่ถูกโจรกรรมข้อมูล ทำให้ในบางกรณีแม้ผู้ที่ถูกโจรกรรมข้อมูลจะได้รับความเสียหาย ตัวอย่างเช่น เสียชื่อเสียง เสียประวัติทางการเงิน เป็นต้น แต่ก็ไม่สามารถฟ้องร้องดำเนินคดีแก่ผู้กระทำความผิดได้

ดังนี้ผู้เขียนมีความเห็นว่าประเทศไทยควรมีการบัญญัติกฎหมายขึ้นเฉพาะเพื่อให้ความคุ้มครองแก่ข้อมูลซึ่งแสดงเอกลักษณ์บุคคล เพื่อกำหนดให้ผู้ที่ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นผู้เสียหายที่แท้จริง ที่สามารถร้องทุกข์ หรือดำเนินการฟ้องร้องคดีได้ เนื่องจากในความเป็นจริงผู้ถูกโจรกรรมข้อมูลย่อมได้รับความเสียหาย เหมือนในพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) ของประเทศสหรัฐอเมริกา และประมวลกฎหมายอาญาของประเทศแคนาดา

4.1.5 การกำหนดโทษ และการเยียวยาผู้เสียหายในความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

ในกฎหมายอาญาเมื่อมีการกำหนดว่าการกระทำใดเป็นความผิดแล้ว ย่อมต้องมีการกำหนดโทษที่จะลงแก่ผู้ที่ฝ่าฝืนด้วยเสมอ ซึ่งโทษทางอาญามีอยู่ 5 ประเภท คือ ประหารชีวิต จำคุก กักขัง ปรับ และริบทรัพย์สิน การที่กฎหมายจะบัญญัติลงโทษประเภทใด และระวางโทษเท่าใด ในฐานความความผิดย่อมต้องขึ้นอยู่กับความเหมาะสม และต้องได้สัดส่วนกับผลร้ายที่จะเกิดจากการกระทำความผิดนั้นๆ ดังนี้การเปรียบเทียบกฎหมายเพื่อเป็นแนวทางในการกำหนดความผิด จึงต้องพิจารณาเรื่องการกำหนดโทษด้วย

ประเทศสหรัฐอเมริกา มีการกำหนดโทษอยู่สองประเภท คือ โทษปรับ และโทษจำคุก โดยมีการแบ่งแยกโทษตามความร้ายแรง กล่าวคือ กรณีกระทำความผิดฐานโจรกรรมเอกลักษณ์บุคคลธรรมดา มีระวางโทษปรับ และโทษจำคุกไม่เกิน 3 ปี จนถึงโทษจำคุกไม่เกิน 15 ปี แต่กรณีที่กระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเพื่อความสะดวกในการกระทำความผิดอื่นๆ ต่อไป มีระวางโทษที่หนักขึ้น ดังนี้

ระวางโทษปรับ หรือโทษจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับในกรณี กระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

- กระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเพื่อทำให้สะดวกขึ้นในการกระทำความผิดเกี่ยวกับการค้ายาเสพติด

- กระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเพื่อเป็นการกระทำที่เชื่อมโยงกับการกระทำความผิดอาญาที่ใช้ความรุนแรง หรือ

- การกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลซ้ำ และคดีก่อนถึงที่สุดแล้ว

ระวางโทษปรับ หรือโทษจำคุกไม่เกิน 25 ปี หรือทั้งจำทั้งปรับ ในกรณี กระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเพื่อการให้ความสะดวกแก่การก่อการร้ายระหว่างประเทศ และมีมาตรการให้ยึดทรัพย์สินของบุคคลที่ใช้ หรือที่มีไว้เพื่อใช้ในการกระทำความผิดในทุกกรณีความผิดของการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลด้วย

ประเทศแคนาดา มีการกำหนดโทษเพียงประเภทเดียว คือ โทษจำคุก โดยมีการแบ่งแยกโทษตามฐานความผิด คือ ในฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ระวางโทษจำคุกไม่เกิน 5 ปี ในฐานความผิดฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ระวางโทษจำคุกไม่เกิน 10 ปี

ประเทศสหราชอาณาจักร เนื่องจากประเทศสหราชอาณาจักรไม่มีบทกฎหมายเฉพาะสำหรับความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล จึงต้องพิจารณาแต่ละฐานความผิด

ในกฎหมายแต่ละฉบับที่มีความเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล กล่าวคือ พระราชบัญญัติการลักทรัพย์ ค.ศ. 1968 ในฐานความผิดเกี่ยวกับการได้ทรัพย์สินมาโดยการหลอกลวง เป็นความผิดทางอาญา มีระวางโทษจำคุกไม่เกิน 10 ปี พระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 (The Identity Card Act of 2006) ในฐานความผิดการครอบครองเอกสารแสดงข้อมูลเอกลักษณ์บุคคลปลอมของบุคคลอื่น โดยในฐานความผิดนี้ยังเอาผิดแก่ผู้ที่จัดทำ หรือมีเครื่องมือ อุปกรณ์ที่สามารถนำมาใช้ทำเอกสารปลอม เพื่อนำเอกสารไปใช้ยืนยันตัวบุคคลด้วย มีระวางโทษปรับ หรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ พระราชบัญญัติการฉ้อโกง ค.ศ. 2006 (The Fraud Act of 2006) ในฐานความผิดทำขึ้น ดัดแปลง จำหน่าย หรือเสนอขายสิ่งของใดๆ โดยรู้ว่าของนั้นถูกทำ หรือดัดแปลงสำหรับใช้ในการฉ้อโกง ในคดีความผิดเล็กน้อย มีระวางโทษจำคุกไม่เกิน 12 เดือน หรือปรับไม่เกินที่กฎหมายกำหนด หรือทั้งจำทั้งปรับ และกรณีเป็นความผิดร้ายแรง มีระวางโทษจำคุกไม่เกิน 10 ปี หรือปรับ หรือทั้งจำทั้งปรับ เห็นได้ว่ามีการกำหนดโทษอยู่สองประเภท คือ โทษปรับ และโทษจำคุก

ประเทศไทย เนื่องจากประเทศไทยไม่มีบทกฎหมายเฉพาะสำหรับความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล จึงต้องพิจารณาแต่ละฐานความผิด ในกฎหมายแต่ละฉบับที่มีความเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล กล่าวคือ ประมวลกฎหมายอาญา ลักษณะความผิดเกี่ยวกับการปลอมและการแปลง ความผิดเกี่ยวกับเอกสาร เอกสารสิทธิ และเอกสารราชการ มีระวางโทษปรับตั้งแต่ไม่เกิน หกพันบาทจนถึงปรับไม่เกินสองแสนบาท ระวางโทษจำคุกตั้งแต่ไม่เกิน 1 ปีจนถึงจำคุกไม่เกิน 10 ปี ความผิดฐานเกี่ยวกับบัตรอิเล็กทรอนิกส์ มีระวางโทษปรับตั้งแต่ไม่เกินสองหมื่นบาทจนถึงปรับไม่เกินสองแสนบาท ระวางโทษจำคุกตั้งแต่ไม่เกิน 1 ปีจนถึงจำคุกไม่เกิน 10 ปี ความผิดเกี่ยวกับหนังสือเดินทาง มีระวางโทษปรับตั้งแต่ไม่เกินสองหมื่นบาทจนถึงปรับไม่เกินสี่แสนบาท ระวางโทษจำคุกตั้งแต่ไม่เกิน 1 ปีจนถึงจำคุกไม่เกิน 20 ปี ลักษณะความผิดเกี่ยวกับทรัพย์ ความผิดฐานลักทรัพย์ ระวางโทษปรับไม่เกินหกพันบาท ระวางโทษจำคุกไม่เกิน 3 ปี ความผิดฐานฉ้อโกงโดยแสดงตนเป็นคนอื่น ระวางโทษปรับไม่เกินหนึ่งหมื่นบาท ระวางโทษจำคุกไม่เกิน 5 ปี พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ในความผิดฐานเข้าถึงระบบหรือข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ระวางโทษ

ปรับตั้งแต่ไม่เกินหนึ่งหมื่นบาทจนถึงปรับไม่เกินสามแสนบาท ระวางโทษจำคุกตั้งแต่ไม่เกิน 6 เดือนจนถึงจำคุกไม่เกิน 15 ปี พระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ในความผิดฐานปลอมบัตรประจำตัวประชาชน หรือใช้บัตรประจำตัวประชาชนของผู้อื่น ระวางโทษปรับตั้งแต่ไม่เกินหนึ่งหมื่นบาทจนถึงปรับไม่เกินสองแสนบาท ระวางโทษจำคุกตั้งแต่ไม่เกิน 6 เดือนจนถึงจำคุกไม่เกิน 10 ปี ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ..... ในความผิดฐานกระทำการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันไม่ชอบด้วยกฎหมาย ระวางโทษปรับไม่เกินหกหมื่นบาท ระวางโทษจำคุกไม่เกิน 3 ปี เห็นได้ว่ามีการกำหนดโทษอยู่สองประเภท คือ โทษปรับ และโทษจำคุก

ดังนี้จากการเปรียบเทียบการกำหนดโทษเห็นได้ว่าทุกประเทศได้บัญญัติโทษอยู่เพียงสองประเภท คือโทษปรับและโทษจำคุก ซึ่งมีระวางโทษแตกต่างกันออกไป แต่ส่วนมากจะอยู่ในระวางโทษจำคุกตั้งแต่ 1 ปีจนถึง 20 ปี ในประเทศสหรัฐอเมริกาได้มีการแบ่งแยกระวางโทษตามความร้ายแรงของการกระทำความผิดด้วย ซึ่งผู้เขียนเห็นว่ามีความเหมาะสมเป็นอย่างยิ่ง เนื่องจากถ้าการกระทำความผิดใดสร้างความเสียหาย กระทบต่อคนจำนวนมากก็สมควรได้รับโทษหนักกว่าการกระทำความผิดที่สร้างความเสียหายที่น้อยกว่า

ตารางสรุปการเปรียบเทียบกฎหมายที่เกี่ยวข้องกับการกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลใน 5 ประเด็น ดังนี้

1. ประเภทกฎหมาย
2. คำนิยาม
3. ฐานความผิด
4. ผู้เสียหาย
5. บทกำหนดโทษ

1. **ประเภทกฎหมาย**

ประเทศ	
ประเทศสหรัฐอเมริกา	พระราชบัญญัติการยังยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ. 1998
ประเทศแคนาดา	ประมวลกฎหมายอาญา
ประเทศสหราชอาณาจักร	ไม่มีกฎหมายบัญญัติฐานความผิดไว้โดยเฉพาะ แต่มีกฎหมายที่เกี่ยวข้อง คือ - พระราชบัญญัติการลักทรัพย์ ค.ศ. 1968 - พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998 - พระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 - พระราชบัญญัติการฉ้อโกง ค.ศ. 2006
ประเทศไทย	ไม่มีกฎหมายบัญญัติฐานความผิดไว้โดยเฉพาะ แต่มีกฎหมายที่เกี่ยวข้อง คือ - ประมวลกฎหมายอาญา - พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 - พระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 - ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

สรุป ประเทศสหรัฐอเมริกา และประเทศแคนาดามีการบัญญัติความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะ ส่วนประเทศสหราชอาณาจักร และประเทศไทยไม่มีการบัญญัติฐานความผิดไว้เป็นการเฉพาะ จึงต้องปรับใช้กฎหมายที่มีความเกี่ยวข้องแก่ความผิดที่เกิดขึ้นเป็นกรณีๆ ไป

2. **คำนิยาม**

ประเทศ	เนื้อหา
ประเทศสหรัฐอเมริกา	ปรากฏในพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ. 1998 “สิ่งซึ่งแสดงตัวบุคคล” : ชื่อ หรือตัวเลขใดๆ ที่สามารถใช้โดยลำพัง หรือร่วมกับข้อมูลอื่นๆ แล้วสามารถระบุตัวบุคคลได้ รวมถึง ชื่อ หมายเลขประกันสังคม วันเดือนปีเกิด ใบอนุญาตขับขี่ที่ออกโดยรัฐบาล หมายเลขประจำตัวประชาชน หมายเลขทะเบียนบุคคลต่างด้าว รวมถึงข้อมูลทางอิเล็กทรอนิกส์ที่สามารถระบุตัวบุคคลได้
ประเทศแคนาดา	ปรากฏในประมวลกฎหมายอาญา“ข้อมูลซึ่งแสดงเอกลักษณ์บุคคล” : ข้อมูลใดๆ ทั้งที่ใช้โดยลำพัง หรือร่วมกับข้อมูลอื่นๆ เพื่อระบุตัวบุคคล หรืออ้างถึงตัวบุคคล รวมถึงลายพิมพ์นิ้วมือ ชื่อ ที่อยู่ วันเดือนปีเกิด ลายเซ็น รวมถึงข้อมูลทางอิเล็กทรอนิกส์
ประเทศสหราชอาณาจักร	ปรากฏในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998 “ข้อมูลส่วนบุคคล” : ข้อมูลเกี่ยวกับความเป็นอยู่ของบุคคลซึ่งสามารถระบุตัวบุคคลได้จากข้อมูลนั้นเอง และในพระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 “เอกสารแสดงข้อมูลเอกลักษณ์บุคคล” : เอกสารใดๆ ที่มีความหมายเหมือน บัตรประจำตัวประชาชน เอกสารการเข้าเมืองหนังสือเดินทางของประเทศสหราชอาณาจักร ใบอนุญาตขับขี่ของประเทศสหราชอาณาจักร
ประเทศไทย	ปรากฏในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... “ข้อมูลส่วนบุคคล” : ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติ

	อาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม บรรดาที่มีชื่อของบุคคลนั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

สรุป การบัญญัติคำนิยามของประเทศไทยและประเทศสหราชอาณาจักรยังไม่มีการบัญญัติครอบคลุมไปถึงเรื่องข้อมูลทางอิเล็กทรอนิกส์เหมือนอย่างของประเทศสหรัฐอเมริกา และประเทศแคนาดา แต่อย่างไรก็ตามประเทศไทยได้มีการบัญญัติคำนิยามครอบคลุมไปถึงข้อมูลของผู้ที่ถึงแก่กรรมแล้วด้วย

3. **ฐานความผิด**

ประเทศ/ฐานความผิด	**การได้มาซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล**	**การจัดทำขึ้นซึ่งเอกสารแสดงเอกลักษณ์บุคคลปลอม**	**การมีไว้ในครอบครองซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล**	**การจำหน่าย หรือการโอนซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล**	**การทำขึ้น โอน หรือครอบครองเครื่องมือทำเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอม**
ประเทศสหรัฐอเมริกา	-	การจัดทำขึ้นซึ่งเอกสารแสดงเอกลักษณ์บุคคลปลอมทุกประเภทรวมทั้งที่เป็นข้อมูลทางอิเล็กทรอนิกส์ด้วย	การครอบครองเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอมตั้งแต่ห้าฉบับขึ้นไป	การโอนซึ่งเอกสารแสดงตัวบุคคลหรือเอกสารแสดงตัวบุคคลปลอม โดยรู้ว่าเป็นเอกสารปลอม หรือได้มาโดยมิชอบ	ทำ โอนหรือครอบครองเครื่องมือทำเอกสารแสดงตัวบุคคลปลอม หรือสิ่งใดๆ ที่ก่อให้เกิดผลได้เช่นเดียวกันมีความผิด
ประเทศแคนาดา	การได้มาซึ่งข้อมูลฯ เพื่อนำไปใช้กระทำความผิดอาญา ไม่ว่าจะเป็นการได้มาโดยชอบหรือมิชอบด้วยกฎหมายก็ตาม	-	การครอบครองซึ่งข้อมูลที่แสดงเอกลักษณ์บุคคลของผู้อื่นทุกประเภท	จำหน่าย หรือเสนอขายข้อมูลหรือเอกสารแสดงเอกลักษณ์บุคคลของผู้อื่น	-
ประเทศสหราชอาณาจักร	การได้มาซึ่งข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากผู้ควบคุมข้อมูล	-	การครอบครองเอกสารแสดงเอกลักษณ์บุคคลปลอมโดยมีเจตนาจะใช้แสวงหาประโยชน์โดยมิชอบเพื่อตน	จำหน่าย หรือเสนอขายข้อมูลส่วนบุคคลโดยปราศจากความยินยอมของผู้ควบคุมข้อมูล ทั้งกรณีการจำหน่ายข้อมูลของตนเองและผู้อื่นด้วย	จัดทำ หรือมีเครื่องมืออุปกรณ์ที่สามารถนำมาใช้ทำเอกสารปลอมใดๆ ที่มีความหมายเหมือนกับบัตรประจำตัวประชาชน หนังสือ

					เดินทาง เอกสารคนเข้าเมือง ใบอนุญาตขับขี่ ฯลฯ
ประเทศไทย	มีเฉพาะกรณีการได้มาซึ่งข้อมูลฯ โดยมิชอบเท่านั้น เช่น การลักทรัพย์ การเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ชอบ ฯลฯ	มีเฉพาะการจัดทำขึ้นซึ่งเอกสารบางประเภทเท่านั้น เช่น การปลอมเอกสาร การปลอมบัตรอิเล็กทรอนิกส์ การปลอมหนังสือเดินทาง ฯลฯ	มีเฉพาะการครอบครองเอกสารบางประเภทเท่านั้น เช่น ครอบครองบัตรอิเล็กทรอนิกส์ปลอม ครอบครองหนังสือเดินทางของผู้อื่น ฯลฯ	มีเฉพาะการจำหน่ายเอกสารบางประเภทเท่านั้น เช่น จำหน่ายบัตรอิเล็กทรอนิกส์ปลอม การจำหน่ายหนังสือเดินทางปลอม ฯลฯ	มีบัญญัติเฉพาะเครื่องมือที่ใช้ทำเอกสารเพียงชนิดเดียว คือเครื่องมือหรือวัตถุที่ใช้ในการปลอมบัตรหรือแปลงบัตรอิเล็กทรอนิกส์
สรุป	ประเทศแคนาดามีการบัญญัติที่ครอบคลุมถึงการได้มาของข้อมูลซึ่งแสดงเอกลักษณ์บุคคลทั้งกรณีที่เป็นการได้มาโดยมิชอบและกรณีการได้มาโดยชอบแต่มีเจตนาจะนำข้อมูลฯ ไปใช้แสวงหาประโยชน์โดยมิชอบ	ประเทศสหรัฐอเมริกามีการบัญญัติที่ครอบคลุมถึงเอกสารแสดงเอกลักษณ์บุคคลทุกประเภท	ประเทศสหรัฐอเมริกาและประเทศแคนาดามีการบัญญัติครอบคลุมถึงการครอบครองเอกสารแสดงเอกลักษณ์บุคคลทุกประเภท	ประเทศสหรัฐอเมริกา บัญญัติครอบคลุมถึงเอกสารทุกประเภททั้งที่เป็นเอกสารจริงและเอกสารปลอมด้วย ประเทศแคนาดาบัญญัติถึงเพียงเอกสารแสดงเอกลักษณ์บุคคลของผู้อื่น แต่ประเทศสหราชอาณาจักรได้บัญญัติครอบคลุมถึงการจำหน่ายข้อมูลหรือเอกสารแสดงเอกลักษณ์บุคคลของตนเองด้วย	ประเทศสหรัฐอเมริกามีการบัญญัติครอบคลุมถึงเครื่องมือที่ใช้ในการปลอมเอกสารซึ่งแสดงเอกลักษณ์บุคคลทุกประเภท ประเทศสหราชอาณาจักรแม้จะมิได้บัญญัติถึงทุกประเภทเอกสารเช่นเดียวกับสหรัฐอเมริกา แต่ก็บัญญัติได้ครอบคลุมชนิดของเอกสารมากกว่ากฎหมายไทย

4. **ผู้เสียหาย**

ประเทศ	เนื้อหา
ประเทศสหรัฐอเมริกา	มีกฎหมายบัญญัติไว้เป็นการเฉพาะให้ความคุ้มครองแก่ผู้ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล
ประเทศแคนาดา	มีกฎหมายบัญญัติไว้เป็นการเฉพาะให้ความคุ้มครองแก่ผู้ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล
ประเทศสหราชอาณาจักร	ไม่มีกฎหมายบัญญัติไว้เป็นการเฉพาะจึงต้องพิจารณาแต่ละฐานความผิด
ประเทศไทย	ไม่มีกฎหมายบัญญัติไว้เป็นการเฉพาะจึงต้องพิจารณาแต่ละฐานความผิด

สรุป ประเทศสหรัฐอเมริกาและประเทศแคนาดา มีการบัญญัติฐานความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะ กฎหมายจึงให้ความคุ้มครองแก่ผู้ถูกโจรกรรมข้อมูลฯ อย่างชัดแจ้ง แต่ประเทศสหราชอาณาจักรและประเทศไทย ไม่มีการบัญญัติฐานความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะ จึงมีการปรับใช้กฎหมายที่เกี่ยวข้องต่างๆ จึงต้องพิจารณาแต่ละฐานความผิดว่าฐานความผิดนั้นๆ มีเจตนารมณ์อย่างไร เช่น ในความผิดฐานฉ้อโกง กฎหมายมุ่งคุ้มครองผู้ที่ถูกหลอกลวงเอาทรัพย์สินไป มิได้ให้ความคุ้มครองแก่ผู้ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ดังนี้จึงเห็นได้ว่าการไม่มีบทบัญญัติฐานความผิดเฉพาะ ในบางกรณีอาจทำให้ผู้ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไม่ได้รับความคุ้มครองตามกฎหมาย

5. **บทกำหนดโทษ**

ประเทศ	เนื้อหา
ประเทศสหรัฐอเมริกา	มีการกำหนดโทษ 2 ประเภท คือโทษปรับและโทษจำคุก โดยมีการแบ่งแยกระวางโทษตามความร้ายแรงของการกระทำความผิดด้วย คือ กระทำความผิดฐานโจรกรรมเอกลักษณ์บุคคลธรรมดา มีระวางโทษปรับ และโทษจำคุกไม่เกิน 3 ปี จนถึงโทษจำคุกไม่เกิน 15 ปี แต่กรณีที่กระทำการโจรกรรมข้อมูลซึ่งแสดง

	เอกลักษณ์บุคคลเพื่อความสะดวกในการกระทำความผิดอื่นๆ ต่อไป มีระวางโทษที่หนักขึ้น ดังนี้ ระวางโทษปรับ หรือโทษจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับในกรณี กระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล - เพื่อทำให้สะดวกขึ้นในการกระทำความผิดเกี่ยวกับการค้ายาเสพติด - เพื่อเป็นการกระทำที่เชื่อมโยงกับการกระทำความผิดอาญาที่ใช้ความรุนแรง หรือ - การกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลซ้ำ และคดีก่อนถึงที่สุดแล้ว ระวางโทษปรับ หรือโทษจำคุกไม่เกิน 25 ปี หรือทั้งจำทั้งปรับ ในกรณี กระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเพื่อการให้ความสะดวกแก่การก่อการร้ายระหว่างประเทศ
ประเทศแคนาดา	มีการกำหนดโทษประเภทเดียว คือ โทษจำคุก แบ่งเป็น 2 ฐานความผิด คือ การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ระวางโทษจำคุกไม่เกิน 5 ปี และการฉ้อโกงข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ระวางโทษจำคุกไม่เกิน 10 ปี
ประเทศสหราชอาณาจักร	มีการกำหนดโทษ 2 ประเภท คือโทษปรับและโทษจำคุก โดยพิจารณาตามฐานความผิดในพระราชบัญญัติที่มีความเกี่ยวข้องแต่ละฉบับ ดังนี้ พระราชบัญญัติการลักทรัพย์ ค.ศ. 1968 มีระวางโทษจำคุกไม่เกิน 10 ปี, พระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 ระวางโทษปรับ หรือจำคุกไม่เกิน 10 ปี, พระราชบัญญัติการฉ้อโกง ค.ศ. 2006 ระวางโทษปรับ หรือจำคุกไม่เกิน 10 ปี
ประเทศไทย	มีการกำหนดโทษ 2 ประเภท คือโทษปรับและโทษจำคุก โดยพิจารณาตามฐานความผิดในกฎหมายที่มีความเกี่ยวข้อง ดังนี้ <u>ประมวลกฎหมายอาญา</u> - ความผิดเกี่ยวกับเอกสาร มีระวางโทษปรับตั้งแต่ไม่เกินหกพันบาทถึงสี่แสนบาท โทษจำคุกไม่เกิน 1 ปีถึง 20 ปี

	- ความผิดเกี่ยวกับทรัพย์ มีระวางโทษปรับตั้งแต่ไม่เกินหกพันบาทถึงหนึ่งหมื่นบาท จำคุกไม่เกิน 3 ปีถึง 5 ปี <u>พระราชบัญญัติที่มีความเกี่ยวข้อง</u> - พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ระวางโทษปรับไม่เกินหนึ่งหมื่นบาทถึงสองแสนบาท โทษจำคุกไม่เกิน 6 เดือนถึง 10 ปี - พระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ระวางโทษปรับไม่เกินหนึ่งหมื่นบาทถึงสองแสนบาท โทษจำคุกไม่เกิน 6 เดือนถึง 10 ปี - ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... มีระวางโทษเดียว คือโทษปรับไม่เกินหกหมื่นบาท โทษจำคุกไม่เกิน 3 ปี

สรุป ทุกประเทศได้บัญญัติโทษอยู่เพียงสองประเภท คือโทษปรับและโทษจำคุก ซึ่งมีระวางโทษแตกต่างกันออกไป แต่ส่วนมากจะอยู่ในระวางโทษจำคุกตั้งแต่ 1 ปีจนถึง 20 ปี ในประเทศสหรัฐอเมริกาได้มีการแบ่งแยกระวางโทษตามความร้ายแรงของการกระทำความผิดด้วย ซึ่งผู้เขียนเห็นว่ามีความเหมาะสมเป็นอย่างยิ่ง เนื่องจากการกระทำความผิดใดสร้างความเสียหายกระทบต่อคนจำนวนมากก็สมควรได้รับโทษหนักกว่าการกระทำความผิดที่สร้างความเสียหายที่น้อยกว่า

4.3 ความเหมาะสมในการนำแนวทางการบัญญัติกฎหมายของต่างประเทศในความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลมาบังคับใช้ในประเทศไทย

จากการศึกษาการโจรกรรมเอกลักษณ์บุคคล และกฎหมายที่ใช้บังคับกับการกระทำความผิดทั้งของประเทศไทย และต่างประเทศแล้ว พบว่ากฎหมายของไทยในปัจจุบันยังไม่มีการบัญญัติฐานความผิดโจรกรรมเอกลักษณ์บุคคลไว้เป็นการเฉพาะ ทำให้เมื่อเกิดการกระทำความผิดขึ้น ต้องนำกฎหมายที่เกี่ยวข้อง หรือที่มีความใกล้เคียงมาบังคับใช้ ทำให้เกิดช่องว่างของกฎหมาย แต่ในประเทศสหรัฐอเมริกา และประเทศแคนาดา ได้มีการบัญญัติฐานความผิด

โจรกรรมเอกลักษณ์บุคคลไว้เป็นการเฉพาะ ทำให้สามารถบังคับใช้กฎหมายกับความผิดได้อย่างครอบคลุมลักษณะของความผิดที่เกิดขึ้น และมีประสิทธิภาพในการบังคับใช้กฎหมาย ผู้เขียนจึงเห็นว่าควรที่จะนำการบัญญัติกฎหมายของต่างประเทศมาเป็นแนวทางในการกำหนดความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในประเทศไทย เพื่อให้การบัญญัติกฎหมายในความผิดฐานโจรกรรมข้อมูลเอกลักษณ์บุคคลของประเทศไทยมีความครอบคลุมการกระทำความผิดได้ทั้งหมด

ประเด็นประเภทกฎหมาย ประเทศสหรัฐอเมริกา มีการบัญญัติเป็นฐานความผิดเฉพาะโดยการบัญญัติออกมาในรูปพระราชบัญญัติเพื่อให้มีการแก้ไขเพิ่มเติมในส่วนประมวลกฎหมายอาญา ประเทศแคนาดามีการบัญญัติเป็นฐานความผิดเฉพาะไว้ในประมวลกฎหมายอาญา และประเทศสหราชอาณาจักรไม่มีการบัญญัติเป็นฐานความผิดเฉพาะไว้ แต่มีพระราชบัญญัติต่างๆ ที่มีความเกี่ยวข้องที่สามารถนำมาบังคับใช้ได้ ดังนี้สำหรับประเทศไทย ขณะนี้กำลังมีการพิจารณาร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ซึ่งเป็นร่างกฎหมายที่มีการบัญญัติฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้บ้างแล้ว อีกทั้งเป็นกฎหมายเฉพาะซึ่งจะช่วยให้สามารถนำไปบังคับใช้กับการกระทำความผิดได้ครอบคลุมมากขึ้น ผู้เขียนจึงมีความเห็นว่าควรทำการแก้ไข เพิ่มเติม ฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... จะเป็นการดี และมีความเหมาะสมที่สุด

ประเด็นคำนิยาม ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ได้มีบัญญัติเอาไว้แล้วว่า “ข้อมูลส่วนบุคคล” หมายความถึง ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม บรรดาที่มีชื่อของบุคคลนั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย ซึ่งจากการศึกษาเปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกา และประเทศแคนาดาแล้วพบว่าคำนิยามในกฎหมายไทยยังมี

ความหมายไม่ครอบคลุมถึงข้อมูลทางอิเล็กทรอนิกส์ ซึ่งถือเป็นรูปแบบของข้อมูลที่ถูกโจรกรรมเป็นจำนวนมากขึ้นในยุคเทคโนโลยีสารสนเทศอย่างในปัจจุบัน

ประเด็นฐานความผิด ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ได้มีบัญญัติเอาไว้แล้วในมาตรา 58 ความว่า “ผู้ใดกระทำการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้ตนเอง หรือผู้อื่นได้รับประโยชน์อันไม่ชอบด้วยกฎหมาย หรือเพื่อให้ผู้อื่นเสียหาย ต้องระวางโทษปรับไม่เกินหกหมื่นบาท หรือจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับ” ซึ่งผู้เขียนมีความเห็นว่าเป็นการบัญญัติที่มีขอบเขตกว้างมากเกินไป ทำให้เกิดความไม่ชัดเจน อาจทำให้เกิดปัญหาในการตีความเพื่อนำมาบังคับใช้ได้ และเป็นการบัญญัติที่การกระทำความผิดในทุกลักษณะจะมีระวางโทษเท่ากันทุกการกระทำ ซึ่งผู้เขียนเห็นว่าไม่เหมาะสมเนื่องจากการบัญญัติบทลงโทษควรคำนึงถึงความได้สัดส่วนกับความร้ายแรงของการกระทำประกอบด้วย จึงเห็นควรบัญญัติฐานความผิดให้ชัดเจนมากขึ้นอย่างกฎหมายของประเทศสหรัฐอเมริกาที่มีการบัญญัติชัดเจนถึงฐานความผิดการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลถึง การได้มา การครอบครอง การใช้ การจำหน่าย รวมถึงผู้ที่มีเครื่องมือที่ใช้ในการกระทำความผิดอยู่ในความครอบครองด้วย

ประเด็นผู้เสียหาย เนื่องจากประเทศไทยยังไม่มีกฎหมายเฉพาะสำหรับความผิดฐานโจรกรรมเอกลักษณ์บุคคล มีเพียงการนำบทกฎหมายที่มีความเกี่ยวข้องมาบังคับใช้ เช่น ประมวลกฎหมายอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และพระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 จึงยังไม่มีกฎหมายที่ให้ความคุ้มครองบุคคลผู้ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล อย่างไรก็ตามในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่มีการบัญญัติความผิดฐานกระทำการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้ตนเอง หรือผู้อื่นได้รับประโยชน์อันไม่ชอบด้วยกฎหมาย หรือเพื่อให้ผู้อื่นเสียหาย ถือเป็นบทกฎหมายที่ให้ความคุ้มครองแก่บุคคลผู้ถูกโจรกรรมข้อมูล แต่ยังมิได้มีการบัญญัติมาตรการเพื่อเยียวยาผู้เสียหายอย่างในกฎหมายของประเทศสหรัฐอเมริกา และประเทศแคนาดาที่มีการบัญญัติคุ้มครองบุคคลผู้ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้ และมีการกำหนดมาตรการเยียวยาผู้เสียหาย ในเรื่องค่าเสียหายและการแก้ไขประวัติเครดิตที่ไม่ถูกต้องที่เกิดจาก

การถูกนำข้อมูลไปใช้โดยมิชอบด้วย ดังนี้ผู้เขียนจึงมีความเห็นว่าควรที่จะมีการบัญญัติมาตรการเยียวยาแก่บุคคลผู้ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้ในกฎหมายไทยด้วย

ประเด็นบทกำหนดโทษ ในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่มีการบัญญัติความผิดฐานกระทำการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้ตนเอง หรือผู้อื่นได้รับประโยชน์อันไม่ชอบด้วยกฎหมาย หรือเพื่อให้ผู้อื่นเสียหาย นั้นมีการกำหนดโทษ 2 ประเภท คือ โทษปรับ และโทษจำคุก โดยระวางโทษปรับไม่เกินหกหมื่นบาท และระวางโทษจำคุกไม่เกิน 3 ปี ซึ่งจากการเปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกา มีการกำหนดโทษ 2 ประเภท คือ โทษปรับ และโทษจำคุก โดยระวางโทษแบ่งแยกตามความร้ายแรงของลักษณะของความผิดที่เกิดขึ้น เช่น หากการกระทำความผิดมีความเกี่ยวข้องกับการค้ายาเสพติด หรือเกี่ยวข้องกับการก่อการร้าย ระวางโทษจะหนักกว่ากรณีที่กระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลธรรมดา ดังนี้ผู้เขียนเห็นว่าการแบ่งแยกระวางโทษในความผิดแต่ละลักษณะให้หนัก เบาแตกต่างกันตามความร้ายแรงของการกระทำความผิดนั้นเป็นเรื่องที่เหมาะสม เนื่องจากการกำหนดโทษทางอาญาควรลงโทษให้ได้สัดส่วนกับการกระทำความผิด

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล (Identity Theft) คือ การที่บุคคลใดๆ ใช้ข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่น เช่น หมายเลขบัตรเครดิต หมายเลขประจำตัวประชาชน หมายเลขประกันสังคม ฯลฯ โดยไม่ได้รับอนุญาตเพื่อแสวงหาประโยชน์โดยทุจริต เช่น เพื่อไปกระทำความผิดฉ้อโกงหรือกระทำความผิดเกี่ยวกับอาชญากรรมอื่นๆ ในปัจจุบันเกิดการกระทำความผิดในลักษณะนี้เป็นจำนวนมากสาเหตุเนื่องมาจากการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลกระทำได้โดยง่าย สะดวก และยากต่อการจับกุมผู้กระทำความผิดมาลงโทษ เนื่องจากในปัจจุบันประเทศไทยยังไม่มีการบัญญัติความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะ ทำให้ต้องนำบทกฎหมายที่เกี่ยวข้องมาบังคับใช้เมื่อเกิดการกระทำความผิดขึ้น จึงยังมีข้อจำกัดทางกฎหมายอยู่ กล่าวคือ

ประมวลกฎหมายอาญาในลักษณะความผิดเกี่ยวกับเอกสาร กฎหมายยังมีความไม่ครอบคลุมการกระทำความผิดอยู่หลายกรณี ตัวอย่างเช่น กรณีการแอบเก็บข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นเอาไว้ โดยมีจุดประสงค์เพื่อจะนำข้อมูลนั้นไปใช้แสวงหาประโยชน์โดยมิชอบสำหรับตนเองในอนาคต ยังไม่มีการปลอมเอกสารใดขึ้น จึงยังไม่มีความผิดฐานปลอมเอกสาร (มาตรา 264) ในความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ กรณีผู้โจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลมิได้โจรกรรมบัตรอิเล็กทรอนิกส์โดยตรง แต่ได้โจรกรรมข้อมูลส่วนบุคคลอื่นเพื่อนำไปใช้เป็นหลักฐานในการขอเปิดบัตรเครดิตขึ้นใหม่ในนามของผู้ถูกโจรกรรมข้อมูล ผู้กระทำการโจรกรรมจึงไม่มีความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ (มาตรา 269/1) แต่อย่างใด เนื่องจากเป็นการออกบัตรโดยถูกต้องของสถาบันการเงินที่มีอำนาจโดยชอบด้วยกฎหมาย ในกรณีที่มีการแอบดู และจดจำรายละเอียดข้อมูลที่อยู่บนบัตรอิเล็กทรอนิกส์เพื่อนำไปใช้แสวงหาประโยชน์โดยมิชอบ ตัวอย่างเช่น

การจดจำหมายเลขบัตรเครดิตไปใช้ชำระราคาสินค้า ผู้กระทำไม่มีความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่น เนื่องจากข้อมูลที่ปรากฏอยู่บนบัตรเครดิต ไม่ถือเป็นบัตรอิเล็กทรอนิกส์ตามคำนิยามของกฎหมาย (มาตรา 269/5)

ประมวลกฎหมายอาญาในลักษณะความผิดเกี่ยวกับทรัพย์ บทกฎหมายที่นำมาใช้บังคับกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล เช่น ความผิดฐานลักทรัพย์ สามารถใช้ได้เฉพาะกรณี กล่าวคือใช้ได้กับการโจรกรรมที่เกิดขึ้นกับทรัพย์ปกติ เช่น โจรกรรมบัตรประจำตัวประชาชน หนังสือเดินทาง ฯลฯ แต่ไม่สามารถนำมาบังคับใช้กับกรณีการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่อยู่ในสื่ออื่นๆ อย่างในคอมพิวเตอร์ได้เนื่องมาจาก ข้อมูลในเครื่องคอมพิวเตอร์แม้จะมีราคา และอาจถือเอาได้ แต่ไม่ใช่วัตถุมีรูปร่าง (tangible property) กล่าวคือ เป็นวัตถุไม่มีรูปร่าง (intangible property) จึงไม่ถือว่าเป็นทรัพย์ ดังนั้นหากมีการโจรกรรมข้อมูลไปย่อมไม่มีความผิดฐานลักทรัพย์ (มาตรา 334) อีกทั้งองค์ประกอบความผิดฐานลักทรัพย์ในส่วนของการเอาไป ต้องเป็นการเอาไปที่ตัดอำนาจกรรมสิทธิ์ของผู้เป็นเจ้าของด้วย แต่การโจรกรรมเพียงข้อมูลไปมิได้เป็นการเอาไปซึ่งกรรมสิทธิ์แต่อย่างใด ความผิดฐานฉ้อโกง ในการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่นไปแสวงหาประโยชน์โดยมิชอบนั้น เป็นการกระทำที่แสดงตนเป็นบุคคลอื่น จึงอาจมีความผิดฐานฉ้อโกงโดยแสดงตนเป็นบุคคลอื่นได้ (มาตรา 342(1)) แต่ทั้งนี้ไม่อาจปรับใช้ได้กับทุกการกระทำความผิด เนื่องจากการฉ้อโกง คือการหลอกลวงผู้อื่นเพื่อให้ได้ไปซึ่งทรัพย์สิน จึงต้องเป็นการหลอกลวงบุคคล แต่ในปัจจุบันการทำธุรกรรมบางประเภทมักกระทำผ่านทางเครือข่ายระบบคอมพิวเตอร์ซึ่งเป็นเครื่องจักรกลมิใช่มนุษย์จึงไม่อาจถูกหลอกลวงได้ และหากเป็นกรณีที่การหลอกลวงของผู้กระทำนั้นมิได้ทำให้ได้รับไปซึ่งทรัพย์สิน แต่ได้รับไปซึ่งผลประโยชน์อย่างอื่น ตัวอย่างเช่น การสามารถเข้า-ออกในสถานที่ใดๆ ได้ ซึ่งประโยชน์เช่นนี้ไม่ถือเป็นทรัพย์สิน ดังนี้ผู้กระทำอาจไม่มีความผิดฐานฉ้อโกง และประเด็นเรื่องผู้เสียหายในความผิดฐานฉ้อโกง ผู้เสียหายที่กฎหมายมุ่งคุ้มครองไม่ใช่บุคคลที่ถูกแอบอ้างชื่อ หรือบุคคลที่ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไปใช้ แต่เป็นบุคคลที่ถูกหลอกลวงซึ่งทรัพย์สินไป ทำให้ผู้ถูกโจรกรรมข้อมูลมิได้รับความคุ้มครอง

นอกเหนือจากประมวลกฎหมายอาญาที่มีฐานความผิดที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลแล้ว ยังมีกฎหมายอื่นๆ ที่มีความเกี่ยวข้องด้วย กล่าวคือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ฐานความผิดที่มีความเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล คือ ความผิดฐานเข้าถึงระบบ หรือข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (มาตรา 5 และมาตรา 7) ในฐานความผิดนี้มีข้อจำกัด คือ ต้องเป็นระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ ที่มีระบบป้องกันการเข้าถึงไว้ด้วย เมื่อมีผู้เข้าถึงจึงจะเป็นความผิด ซึ่งปกติบุคคลทั่วไปก็มิได้จัดให้เครื่องคอมพิวเตอร์ของตนมีระบบการป้องกันการเข้าถึงเอาไว้ และข้อจำกัดของพระราชบัญญัติฉบับนี้อีกประการหนึ่ง คือ จำกัดเฉพาะการกระทำความผิดโดยผ่านคอมพิวเตอร์เท่านั้น ยังไม่ครอบคลุมไปถึงอุปกรณ์ หรือเครื่องมืออิเล็กทรอนิกส์อื่นที่มีระบบการทำงานที่ใกล้เคียงกับคอมพิวเตอร์ เช่น โทรศัพท์สมาร์ทโฟน ซึ่งเป็นที่นิยมใช้กันอย่างแพร่หลายในปัจจุบัน

พระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ความผิดฐานเข้าถึงข้อมูล หรือเปิดเผยข้อมูลที่ถูกบันทึกไว้ในหน่วยความจำของบัตรประจำตัวประชาชนแบบเอนกประสงค์ (มาตรา 12) ข้อจำกัดของฐานความผิดนี้ คือ บัญญัติคุ้มครองเพียงข้อมูลที่อยู่ในรูปของอิเล็กทรอนิกส์หรือข้อมูลที่ถูกเก็บไว้ในหน่วยความจำของบัตรประจำตัวประชาชนแบบเอนกประสงค์ (smart card) เท่านั้น จึงไม่ครอบคลุมถึงข้อมูลที่ปรากฏอยู่บนตัวบัตร และข้อจำกัดอีกประการหนึ่งของพระราชบัญญัติฉบับนี้ คือ ใช้บังคับได้เฉพาะกับบัตรประจำตัวประชาชนเท่านั้น

ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ร่างกฎหมายฉบับนี้ได้มีแนวทางในการให้ความคุ้มครองข้อมูลส่วนบุคคลโดยเน้นเกี่ยวกับการกำหนดหน้าที่ควบคุม ดูแลข้อมูลของผู้ควบคุมข้อมูลเป็นหลัก มีส่วนที่เกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลคือความผิดฐานกระทำการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันไม่ชอบด้วยกฎหมาย (มาตรา 58) ซึ่งผู้เขียนมีความเห็นว่าบทบัญญัติที่มีความเกี่ยวข้องกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่กำหนดไว้ในมาตรา 58 ยังเป็นการบัญญัติที่มีขอบเขตกว้างมากเกินไป ทำให้เกิดความไม่ชัดเจน อาจทำให้เกิดปัญหาในการตีความ

เพื่อนำมาบังคับใช้ได้ และเป็นการบัญญัติที่การกระทำความผิดในทุกลักษณะจะมีระวางโทษเท่ากันทุกการกระทำ ซึ่งผู้เขียนเห็นว่ามีความไม่เหมาะสมเนื่องจากการบัญญัติบทลงโทษควรคำนึงถึงความได้สัดส่วนกับความร้ายแรงของการกระทำประกอบด้วย เมื่อผู้เขียนได้ทำการศึกษาเปรียบเทียบกับกฎหมายต่างประเทศแล้วมีความเห็นว่ากฎหมายของต่างประเทศ โดยเฉพาะประเทศสหรัฐอเมริกา และประเทศแคนาดามีการบัญญัติความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะ ทำให้สามารถนำมาบังคับใช้กับการกระทำความผิดได้ครอบคลุมกว่ากฎหมายไทย

ประเทศไทยขณะนี้กำลังมีการพิจารณาร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ซึ่งเป็นร่างกฎหมายที่มีการบัญญัติฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้บ้างแล้ว อีกทั้งเป็นกฎหมายเฉพาะซึ่งจะช่วยให้สามารถนำไปบังคับใช้กับการกระทำความผิดได้ทั่วไป และครอบคลุมมากขึ้น ผู้เขียนจึงมีความเห็นว่าควรทำการแก้ไขเพิ่มเติม ฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เป็นการดี และมีความเหมาะสมที่สุด ดังรายละเอียดต่อไปนี้ ประเด็นคำนิยาม ร่างพระราชบัญญัติฉบับนี้ ได้มีบัญญัติถึงความหมายของข้อมูลส่วนบุคคลเอาไว้ ซึ่งมีความใกล้เคียงกับกฎหมายของต่างประเทศมาก แต่ยังมีความไม่ครอบคลุม กล่าวคือ ในพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) ของประเทศสหรัฐอเมริกา และในประมวลกฎหมายอาญาของประเทศแคนาดาได้ให้คำนิยามไว้ครอบคลุมกว่า คือ ให้ความคุ้มครองข้อมูลทางอิเล็กทรอนิกส์ด้วย ซึ่งข้อมูลทางอิเล็กทรอนิกส์ถือเป็นรูปแบบของข้อมูลที่ถูกโจรกรรมเป็นจำนวนมากขึ้นในยุคเทคโนโลยีสารสนเทศอย่างในปัจจุบัน จึงเห็นควรบัญญัติเพิ่มเติมคำนิยามในกฎหมายไทยให้มีความครอบคลุมมากยิ่งขึ้น

เนื่องจากปัจจุบันประเทศไทยยังไม่มีกฎหมายเฉพาะในความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล จึงต้องอาศัยบทกฎหมายที่มีความเกี่ยวข้องกับความผิดมาบังคับใช้ ผู้เขียนได้แยกประเด็นฐานความผิด หรือองค์ประกอบของความผิดออกเป็น 6 ประเด็น ดังนี้

ความผิดฐานการได้มาซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล กฎหมายไทยที่มีความเกี่ยวข้องที่อาจนำมาบังคับใช้ คือ ความผิดฐานลักทรัพย์ ความผิดฐานฉ้อโกง ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ กรณีที่ได้มาซึ่งข้อมูลเอกลักษณ์บุคคลโดยมิชอบด้วยกฎหมายในบางกรณีไม่มีกฎหมายที่จะนำมาบังคับใช้ ตัวอย่างเช่น การแอบดูและจดจำข้อมูลหมายเลขบัตรประจำตัวประชาชนของผู้อื่นไว้ หรือการแอบจดหมายเลขบัตรเครดิตของผู้อื่นไว้ หรือการเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นซึ่งคอมพิวเตอร์นั้นมิได้มีระบบป้องกันการเข้าถึงไว้ เป็นต้น จึงกล่าวได้ว่ากฎหมายไทยปัจจุบันยังไม่ครอบคลุมเพียงพอสำหรับความผิดฐานการได้มาซึ่งข้อมูล หรือเอกสารที่แสดงเอกลักษณ์บุคคล เมื่อเปรียบเทียบกับกฎหมายของประเทศสหราชอาณาจักร พบว่าในกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998 (The Data Protection Act of 1998) มีการกำหนดฐานความผิดสำหรับผู้ที่ได้มาซึ่งข้อมูลส่วนบุคคล หรือข้อมูลที่อยู่ในส่วนบุคคลโดยที่ไม่ได้รับความยินยอมจากผู้ควบคุมข้อมูล และในประมวลกฎหมายอาญาของประเทศแคนาดา มีการกำหนดฐานความผิดสำหรับผู้ที่ได้มาซึ่งข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของผู้อื่น โดยมีวัตถุประสงค์เพื่อจะนำไปใช้กระทำความผิดอาญา รวมถึงกรณีการได้มาโดยฉ้อโกง หลอกลวง หรือกล่าวเท็จด้วย ดังนี้ผู้เขียนจึงเห็นว่าการบัญญัติความผิดเกี่ยวกับการได้มาซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคลของประเทศสหราชอาณาจักร และประเทศแคนาดามีความครอบคลุมมากกว่ากฎหมายไทยที่มีอยู่ในปัจจุบัน

ความผิดฐานการจัดทำขึ้นซึ่งเอกสารแสดงเอกลักษณ์บุคคลปลอม ในปัจจุบันกฎหมายไทยที่เกี่ยวข้องกับฐานความผิดการจัดทำขึ้นซึ่งเอกสารแสดงเอกลักษณ์บุคคลปลอมนั้นมีการบัญญัติคุ้มครองไว้เพียงเฉพาะเอกสารบางประเภทเท่านั้น กล่าวคือ ในประมวลกฎหมายอาญาลักษณะความผิดเกี่ยวกับการปลอมและการแปลง มาตรา 264 การปลอมเอกสาร มาตรา 265 การปลอมเอกสารสิทธิ มาตรา 266 การปลอมเอกสารราชการ มาตรา 269/1 การปลอมบัตรอิเล็กทรอนิกส์ มาตรา 269/8 การปลอมหนังสือเดินทาง และในกฎหมายอื่นปรากฏมีในพระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ในมาตรา 14(3) การปลอมบัตร หรือใบรับหรือใบแทนใบรับบัตรประจำตัวประชาชน ดังนี้จะเห็นได้ว่าลักษณะการบัญญัติกฎหมายของไทยเป็นแบบกำหนดการคุ้มครองเป็นประเภทๆ เอกสารไป ทำให้ยังเกิดมีช่องว่างสำหรับเอกสารแสดง

เอกลักษณ์บุคคลบางประเภทที่ยังไม่ได้รับความคุ้มครอง ตัวอย่างเช่น ใบสูติบัตร หรือในส่วนของเอกสารอิเล็กทรอนิกส์ซึ่งเป็นที่นิยมใช้กันมากในปัจจุบัน ยังไม่มีกฎหมายบัญญัติให้ความคุ้มครอง ตัวอย่างเช่น การปลอมลายมือชื่ออิเล็กทรอนิกส์ เมื่อเปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกาพบว่าในกฎหมายพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ. 1998 (The Identity Theft and Assumption Deterrence Act of 1998) มีการกำหนดความผิดสำหรับผู้ที่จัดทำขึ้นซึ่งเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอม ซึ่งเอกสารนั้นบัญญัติไว้ครอบคลุมกว่าของประเทศไทย กล่าวคือมีการบัญญัติคุ้มครองไปถึงเอกสารส่วนบุคคลทุกประเภท รวมถึงข้อมูลบุคคลทางชีวภาพด้วย ตัวอย่างเช่น ลายพิมพ์นิ้วมือ เสียง ม่านตา และยังครอบคลุมถึงที่เป็นข้อมูลทางอิเล็กทรอนิกส์ด้วย ตัวอย่างเช่น ลายมือชื่ออิเล็กทรอนิกส์ หรือรหัสผ่านทางอิเล็กทรอนิกส์ต่างๆ

การมีไว้ในความครอบครองซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคลนี้สามารถแบ่งแยกออกได้เป็น 2 ประเภท คือ การมีไว้ในครอบครองซึ่งเอกสารแสดงเอกลักษณ์บุคคลที่เป็นของจริง และการมีไว้ในครอบครองซึ่งเอกสารแสดงเอกลักษณ์บุคคลที่เป็นของปลอม ซึ่งปัจจุบันกฎหมายไทยก็ได้มีการบัญญัติถึงความผิดการมีไว้ในความครอบครองซึ่งเอกสารแสดงเอกลักษณ์บุคคลทั้งสองประเภท แต่เฉพาะในเอกสารบางประเภทเท่านั้น คือ ในประมวลกฎหมายอาญา มาตรา 269/4 การมีไว้ในครอบครองเพื่อใช้ หรือเพื่อจำหน่ายซึ่งบัตรอิเล็กทรอนิกส์ปลอม มาตรา 269/6 การมีไว้ในครอบครองเพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่น มาตรา 269/9 การมีไว้ในครอบครองเพื่อใช้ หรือเพื่อจำหน่ายซึ่งหนังสือเดินทางปลอม และในกฎหมายอื่นปรากฏมีในพระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 ในมาตรา 15 ทวิ การเอาไปเสียหรือยึดไว้ซึ่งบัตร หรือใบรับหรือใบแทนใบรับบัตรประจำตัวประชาชนของผู้อื่น เพื่อประโยชน์สำหรับตนเอง หรือผู้อื่นโดยมิชอบ ดังนี้เห็นได้ว่ากฎหมายไทยยังให้ความคุ้มครองเอกสารซึ่งแสดงเอกลักษณ์บุคคลได้ไม่ครบถ้วน ตัวอย่างเช่น หนังสือเดินทางของผู้อื่น บัตรประกันสังคมของผู้อื่น ใบอนุญาตขับขี่ของผู้อื่น เป็นต้น เมื่อเปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกาพบว่าในกฎหมายพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) มีการกำหนดความผิดสำหรับผู้มีไว้ในความ

ครอบครองซึ่งเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอมตั้งแต่ห้าฉบับขึ้นไป ดังนี้จึงมีความหมายรวมถึงเอกสารแสดงตัวบุคคลทุกประเภท และรวมทั้งที่เป็นเอกสารจริงและเอกสารปลอมด้วย และในประมวลกฎหมายอาญาของประเทศแคนาดา มีการกำหนดความผิดสำหรับผู้ที่มีไว้ในความครอบครองซึ่งข้อมูลที่แสดงเอกลักษณ์บุคคลของผู้อื่น เพื่อใช้ หรือเพื่อจำหน่าย ซึ่งมีความครอบคลุมข้อมูล และเอกสารซึ่งแสดงเอกลักษณ์บุคคลทุกประเภท ดังนี้จึงเห็นได้ว่ากฎหมายของประเทศสหรัฐอเมริกา และประเทศแคนาดามีความครอบคลุมมากกว่ากฎหมายไทย

การจำหน่าย หรือการโอนซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคล กฎหมายไทยในประมวลกฎหมายอาญา มาตรา 269/4 วรรคสอง ความผิดฐานจำหน่ายบัตรอิเล็กทรอนิกส์ปลอม และมาตรา 269/9 วรรคสอง ความผิดฐานจำหน่ายหนังสือเดินทางปลอม ซึ่งเห็นได้ว่ายังบัญญัติไม่ครอบคลุมถึงข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคลประเภทอื่นๆ ตัวอย่างเช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เมื่อเปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกาพบว่าในกฎหมายพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) มีการกำหนดฐานความผิดสำหรับผู้ที่เจตนาโอนซึ่งเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอม โดยรู้อยู่ว่าเอกสารดังกล่าวได้มาจากการโจรกรรม หรือถูกจัดทำขึ้นโดยปราศจากอำนาจตามกฎหมาย กฎหมายของประเทศสหรัฐอเมริกานี้จึงครอบคลุมถึงข้อมูล และเอกสารแสดงเอกลักษณ์บุคคลทุกประเภท รวมทั้งยังบัญญัติเอาผิดทั้งในกรณีที่เป็นเอกสารของจริงและในกรณีที่เป็นเอกสารของปลอมด้วย และในประมวลกฎหมายอาญาของประเทศแคนาดา มีการกำหนดฐานความผิดสำหรับผู้ที่จำหน่าย หรือเสนอขายข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคลของผู้อื่น กฎหมายของประเทศแคนาดานี้จึงครอบคลุมถึงข้อมูล และเอกสารแสดงเอกลักษณ์บุคคลทุกประเภท และในกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 1998 (The Data Protection Act of 1998) ของประเทศสหราชอาณาจักร ก็มีการบัญญัติเอาผิดกับการจำหน่าย หรือเสนอขายข้อมูลส่วนบุคคลโดยปราศจากความยินยอมของผู้ควบคุมข้อมูล ทั้งนี้กฎหมายฉบับนี้ได้บัญญัติเอาผิดทั้งกรณีการจำหน่ายข้อมูลส่วนบุคคลของตนเอง และกรณีการจำหน่ายข้อมูลส่วนบุคคลของผู้อื่นด้วย ดังนี้จึง

เห็นได้ว่ากฎหมายของต่างประเทศมีการบัญญัติฐานความผิดเกี่ยวกับการจำหน่าย หรือการโอน ซึ่งข้อมูล หรือเอกสารแสดงเอกลักษณ์บุคคลได้ครอบคลุมมากกว่าประเทศไทย

การทำขึ้น โอน และครอบครองเครื่องมือทำเอกสารแสดงตัวบุคคลหรือเอกสารแสดงตัวบุคคลปลอม กฎหมายไทยที่บัญญัติความผิดเกี่ยวกับการทำขึ้น โอน และครอบครองเครื่องมือทำเอกสารแสดงตัวบุคคลหรือเอกสารแสดงตัวบุคคลปลอม ปรากฏอยู่ในประมวลกฎหมายอาญา มาตรา 269/2 ที่เอาผิดกับบุคคลใดที่ทำเครื่องมือ หรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ หรือมีเครื่องมือหรือวัตถุเช่นว่านั้น เพื่อใช้หรือเพื่อให้ได้ข้อมูลในการปลอมหรือแปลง ดังนี้จะเห็นได้ว่ากฎหมายไทยบัญญัติเพียงเครื่องมือที่ใช้ปลอมหรือแปลงบัตรอิเล็กทรอนิกส์เท่านั้น ยังไม่ครอบคลุมถึงเอกสารซึ่งแสดงเอกลักษณ์บุคคลในอีกหลายๆ ประเภท ตัวอย่างเช่น เครื่องมือทำบัตรประจำตัวประชาชนปลอม ทำบัตรอนุญาตขับขี่ปลอม เป็นต้น เมื่อเปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกาพบว่าในกฎหมายพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) มีการกำหนดฐานความผิดเกี่ยวกับเครื่องมือไว้ว่า ผู้ใดเจตนาทำ โอนหรือครอบครองเครื่องมือทำเอกสารแสดงตัวบุคคล หรือเอกสารแสดงตัวบุคคลปลอม หรือสิ่งใดๆ ที่ก่อให้เกิดผลได้เช่นเดียวกันนั้นมีความผิด ดังนี้เป็นการบัญญัติขอบเขตกว้าง สามารถรวมถึงเครื่องมือ หรือสิ่งอื่นใดที่สามารถทำเอกสารแสดงตัวบุคคลปลอมได้ในเอกสารทุก ประเภท และในพระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006 (The Identity Card Act of 2006) ของประเทศสหราชอาณาจักรได้มีการบัญญัติเอาผิดแก่ผู้ที่จัดทำ หรือมีเครื่องมือ อุปกรณ์ที่สามารถนำมาใช้ทำเอกสารปลอมด้วย ซึ่งเอกสารแสดงข้อมูลเอกลักษณ์บุคคลตามคำนิยามในพระราชบัญญัติฉบับนี้มีความหมายครอบคลุมกว่ากฎหมายไทย คือ รวมเอกสารใดๆ ที่มีความหมายเหมือนกับบัตรประจำตัวประชาชน หนังสือเดินทาง เอกสารคนเข้าเมือง และใบอนุญาตขับขี่ เป็นต้น จึงเห็นได้ว่ากฎหมายของประเทศสหรัฐอเมริกา และประเทศสหราชอาณาจักรมีการบัญญัติที่ครอบคลุมประเภทของเอกสารมากกว่าในกฎหมายไทย

ในกฎหมายพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) ของประเทศสหรัฐอเมริกา มี

การกำหนดฐานความผิดที่เป็นแรงจูงใจให้บุคคลนั้นกระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล กล่าวคือ มีการบัญญัติโทษหนักขึ้นหากการกระทำความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลนั้น ทำขึ้นเพื่อให้ความสะดวกในการกระทำความผิดเกี่ยวกับการค้ายาเสพติด หรือเป็นการกระทำที่เชื่อมโยงกับการกระทำความผิดอาญาอื่นที่ใช้ความรุนแรง หรือเป็นการให้ความสะดวกแก่การก่อการร้ายระหว่างประเทศ ดังนี้ผู้เขียนเห็นว่าเป็นการบัญญัติกฎหมายที่มีความเหมาะสมเนื่องจาก การให้ความสะดวกแก่การกระทำความผิดฐานอื่นล้วนมีความร้ายแรง หากเกิดความผิดนั้นๆ ขึ้นก็จะสร้างความเสียหายเป็นอย่างมาก ทั้งต่อประเทศที่ความผิดนั้นเกิดขึ้น และประเทศอื่นๆ ในสังคมโลกด้วย จึงควรบัญญัติไว้เป็นความผิดต่างหากเพื่อกำหนดบทลงโทษที่หนักขึ้นได้

ผู้เสียหายในความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล เนื่องจากกฎหมายไทยยังไม่มีการบัญญัติความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นความผิดเฉพาะ การนำกฎหมายที่เกี่ยวข้องอื่นมาปรับใช้ ในบางกรณีจึงไม่สามารถให้ความคุ้มครองแก่บุคคลผู้ถูกโจรกรรมข้อมูลได้ กล่าวคือบุคคลผู้ถูกโจรกรรมข้อมูลไม่ใช่ผู้เสียหายในความผิดนั้น ไม่สามารถร้องทุกข์ หรือฟ้องร้องเพื่อดำเนินคดีได้ เช่น ในประมวลกฎหมายอาญา ลักษณะความผิดเกี่ยวกับการปลอมและการแปลง กฎหมายล้วนมุ่งคุ้มครองตัวเอกสาร มิได้มุ่งคุ้มครองข้อมูลซึ่งแสดงเอกลักษณ์บุคคลที่ถูกนำไปใช้ หรือคุ้มครองผู้ที่ถูกนำข้อมูลไปใช้แต่อย่างใด ผู้เขียนจึงมีความเห็นว่าประเทศไทยควรมีการบัญญัติกฎหมายขึ้นเฉพาะเพื่อให้ความคุ้มครองแก่ข้อมูลซึ่งแสดงเอกลักษณ์บุคคล เพื่อกำหนดให้ผู้ที่ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นผู้เสียหายที่แท้จริง ที่สามารถร้องทุกข์ หรือดำเนินการฟ้องร้องคดีได้ เนื่องจากในความเป็นจริงผู้ถูกโจรกรรมข้อมูลย่อมได้รับความเสียหาย เหมือนในพระราชบัญญัติยับยั้งและสันนิษฐานการลักข้อมูลส่วนบุคคล ค.ศ.1998 (The Identity Theft and Assumption Deterrence Act of 1998) ของประเทศสหรัฐอเมริกา และประมวลกฎหมายอาญาของประเทศแคนนาดา

การกำหนดโทษ ในความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ทุกประเทศกำหนดโทษอยู่สองประเภทเหมือนกัน คือโทษปรับ และโทษจำคุก แต่ในประเทศสหรัฐอเมริกา มีการแบ่งแยกระวางโทษตามความร้ายแรงของความผิด คือ กระทำความผิดฐานโจรกรรมข้อมูลซึ่ง

แสดงเอกลักษณ์บุคคล เพื่อความสะดวกในการกระทำความผิดเกี่ยวกับการค้ายาเสพติด การก่อการร้ายระหว่างประเทศ หรือเป็นการกระทำที่เชื่อมโยงกับการกระทำความผิดอาญาที่ใช้ความรุนแรง หรือได้มีการกระทำความผิดเช่นนี้มาก่อน และคดีถึงที่สุดแล้ว ผู้เขียนมีความเห็นว่ามีความเหมาะสมเป็นอย่างยิ่ง เนื่องจากถ้าการกระทำความผิดใดสร้างความเสียหาย กระทบต่อคนจำนวนมากก็สมควรได้รับโทษหนักกว่าการกระทำความผิดที่สร้างความเสียหายที่น้อยกว่าในประเทศสหรัฐอเมริกา และประเทศแคนาดามีมาตรการเยียวยาผู้เสียหาย ในเรื่องค่าเสียหาย และการแก้ไขประวัติเครดิตที่เสียหายอันเนื่องมาจากการถูกโจรกรรมข้อมูลด้วย ดังนี้ประเทศไทยควรควรนำกฎหมายของต่างประเทศมาเป็นแนวทางในการบัญญัติกฎหมายเรื่องการกำหนดโทษ และมาตรการเยียวยาผู้เสียหาย

จากการวิเคราะห์เห็นได้ว่ากฎหมายไทยที่มีอยู่ในปัจจุบันไม่สามารถนำมาบังคับใช้กับการกระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลได้ในทุกกรณี เนื่องจากไม่มีการบัญญัติฐานความผิดไว้โดยเฉพาะ ทำให้เกิดช่องว่างทางกฎหมาย ซึ่งปัญหาการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นปัญหาที่นับวันจะทวีจำนวนเพิ่มขึ้น และการกระทำความผิดก่อให้เกิดผลกระทบในหลายด้าน ทั้งด้านบุคคลผู้ถูกโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล แล้วยังกระทบต่อความมั่นคงของระบบเศรษฐกิจ ความเชื่อมั่นของประชาชนต่อองค์กร หรือสถาบันทางการเงินที่ต้องเข้ามามีส่วนเกี่ยวข้องกับการกระทำความผิด อีกทั้งการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลยังเป็นฐานความผิดที่เอื้อต่อการกระทำความผิดอาญาที่ร้ายแรงอื่นๆ ตามมาด้วย เช่น การก่อการร้าย การค้ายาเสพติด ฯลฯ ดังนี้เห็นควรนำแนวทางการบัญญัติกฎหมายในฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของประเทศสหรัฐอเมริกา ประเทศแคนาดา และประเทศสหราชอาณาจักรมาเป็นแนวทางในการกำหนดกฎหมายเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของประเทศไทย

5.2 **ข้อเสนอแนะ**

เมื่อศึกษาและวิเคราะห์ถึงปัญหาเกี่ยวกับการบังคับใช้กฎหมายไทยที่เกี่ยวข้องกับความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล จะเห็นว่ากฎหมายไทยยังมีความไม่ครอบคลุม ไม่สามารถนำกฎหมายที่มีอยู่มาปรับใช้กับการกระทำความผิดได้ในทุกกรณี จึงสมควรให้มีการกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นฐานความผิดขึ้นโดยเฉพาะ ซึ่งจากการศึกษาเปรียบเทียบกับกฎหมายของประเทศสหรัฐอเมริกา และประเทศแคนาดา ที่มีการบัญญัติฐานความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้เป็นการเฉพาะ และประเทศสหราชอาณาจักร ที่ไม่มีการบัญญัติฐานความผิดไว้เฉพาะเหมือนกับประเทศไทย แต่มีกฎหมายที่มีความเกี่ยวข้องกับความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลหลายฉบับ เห็นว่ากฎหมายของต่างประเทศนั้นบัญญัติได้ครอบคลุมความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล ผู้เขียนจึงเห็นสมควรนำการบัญญัติกฎหมายของต่างประเทศมาเป็นแนวทางในการกำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของประเทศไทย การแก้ไขปัญหาการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลจะต้องมีความชัดเจน ครอบคลุมถึงข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในทุกลักษณะ และการบัญญัติฐานความผิดองค์ประกอบความผิดต้องมีความชัดเจน ผู้เขียนจึงมีความเห็นว่าเพื่อการบัญญัติกฎหมายเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลให้มีประสิทธิภาพ และครอบคลุมทุกลักษณะของการกระทำความผิด ผู้เขียนขอเสนอให้มีการแก้ไข ปรับปรุงบทบัญญัติแห่งกฎหมายไทย ดังนี้

1. กำหนดให้มีการบัญญัติความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเป็นการเฉพาะ เพื่อให้สามารถนำบทกฎหมายมาบังคับใช้กับการกระทำความผิดได้โดยตรง และมีความเหมาะสมกับรูปแบบของความผิดที่เกิดขึ้น เนื่องจากในปัจจุบันประเทศไทยกำลังมีการพิจารณาร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ซึ่งเป็นร่างกฎหมายที่มีหลักการสำคัญในการให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลไว้แล้ว จึงเห็นควรบัญญัติความผิดฐานโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลไว้ในร่างพระราชบัญญัตินี้

2. การกำหนดคำนิยามของข้อมูลซึ่งแสดงเอกลักษณ์บุคคลให้มีความครอบคลุมในทุกประเภทของข้อมูลซึ่งแสดงเอกลักษณ์บุคคล เห็นควรให้มีการแก้ไข เพิ่มเติมคำนิยามของข้อมูลส่วนบุคคล ในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

เนื่องจากในร่างพระราชบัญญัติฉบับนี้มีการให้คำนิยามของคำว่า “ข้อมูลส่วนบุคคล” ไว้แล้วว่าหมายความถึง ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรมบรรดาที่มีชื่อของบุคคลนั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย แต่ผู้เขียนเห็นว่ายังไม่ครอบคลุมถึงข้อมูลทางอิเล็กทรอนิกส์ ดังเช่นในกฎหมายของประเทศสหรัฐอเมริกา และประเทศแคนาดาที่ได้บัญญัติคุ้มครองข้อมูลทางอิเล็กทรอนิกส์ไว้ด้วย จึงเห็นควรบัญญัติเพิ่มเติม บทบัญญัติให้เป็น ดังนี้

“ข้อมูลส่วนบุคคล หมายความถึง ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคลไม่ว่าจะอยู่ในรูปของเอกสาร หรือข้อมูลทางอิเล็กทรอนิกส์ เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรมบรรดาที่มีชื่อของบุคคลนั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย”

3. การแก้ไข เพิ่มเติมฐานความผิดเกี่ยวกับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ในมาตรา 58 ให้ครอบคลุมถึงการกระทำความผิดหลักๆ ดังนี้

(ก) **การได้มาซึ่งข้อมูลหรือเอกสารแสดงเอกลักษณ์บุคคลของผู้อื่นโดยมิชอบด้วยกฎหมาย และการได้มาซึ่งข้อมูลหรือเอกสารแสดงเอกลักษณ์บุคคลของผู้อื่นโดยชอบด้วยกฎหมาย แต่มีเจตนาจะนำข้อมูลที่ได้มาไปใช้แสวงหาประโยชน์โดยทุจริต**

ความผิดฐานการได้มาซึ่งข้อมูลหรือเอกสารแสดงเอกลักษณ์บุคคลนี้สามารถแบ่งได้เป็น 2 กรณี คือ การได้มาโดยมิชอบด้วยกฎหมาย ซึ่งย่อมเป็นความผิดอยู่แล้ว แต่ทั้งนี้ให้รวมถึงกรณีการได้ข้อมูลมาโดยชอบด้วยกฎหมายแต่มีเจตนาที่จะนำข้อมูลไปใช้แสวงหาประโยชน์โดยทุจริตด้วย เนื่องจากบางกรณีข้อมูลซึ่งแสดงเอกลักษณ์บุคคลอาจปรากฏอยู่ในที่สาธารณะได้อาจเพราะความตั้งใจหรือมิได้ตั้งใจของผู้เป็นเจ้าของข้อมูลก็ตาม ข้อมูลนั้นย่อมต้องได้รับการคุ้มครองเช่นกัน เพราะบุคคลอื่นไม่มีสิทธิที่จะนำข้อมูลของผู้อื่นไปใช้โดยมิได้รับความยินยอมไม่ว่าในทางใดๆ

(ข) การจัดทำขึ้นซึ่งเอกสารแสดงเอกลักษณ์บุคคลปลอม

ความผิดฐานการจัดทำขึ้นซึ่งเอกสารแสดงเอกลักษณ์บุคคลปลอมนี้อาจเกิดเป็นการกระทำกรรมเดียวผิดกฎหมายหลายบทได้ เนื่องมาจากในปัจจุบันกฎหมายไทยในประมวลกฎหมายอาญามีการบัญญัติฐานความผิดการปลอมเอกสาร ปลอมเอกสารสิทธิ ปลอมเอกสารราชการ ปลอมหนังสือเดินทาง และปลอมบัตรอิเล็กทรอนิกส์ ฯลฯ แต่กฎหมายปัจจุบันยังเป็นการบัญญัติกฎหมายถึงเอกสารบางประเภทเท่านั้น ทำให้ยังไม่ครอบคลุมเอกสารแสดงเอกลักษณ์บุคคลทุกประเภท จึงเห็นควรบัญญัติไว้กว้างๆ เพื่อให้ครอบคลุมเอกสารทุกประเภทอย่างเช่นในกฎหมายของประเทศสหรัฐอเมริกา และประเทศแคนาดา

(ค) การมีไว้ในความครอบครองซึ่งข้อมูลหรือเอกสารซึ่งแสดงเอกลักษณ์บุคคลเพื่อนำไปแสวงหาประโยชน์โดยมิชอบเพื่อตนเอง หรือผู้อื่น

ความผิดฐานการมีไว้ในครอบครองซึ่งข้อมูลหรือเอกสารซึ่งแสดงเอกลักษณ์บุคคลนี้สามารถแบ่งการครอบครองเอกสารออกได้เป็น 2 ประเภท คือการครอบครองเอกสารจริง และการครอบครองเอกสารปลอม กรณีผู้ได้มาซึ่งข้อมูลหรือเอกสารแสดงเอกลักษณ์บุคคลของผู้อื่นโดยชอบ การมีไว้ในครอบครองย่อมไม่เป็นความผิด แต่หากครอบครองไว้เพื่อนำไปใช้แสวงหาประโยชน์โดยมิชอบในอนาคต เห็นควรบัญญัติการครอบครองนั้นเป็นความผิด

(ง) การจำหน่าย หรือการโอนซึ่งข้อมูลหรือเอกสารซึ่งแสดงเอกลักษณ์บุคคลหรือเอกสารซึ่งแสดงเอกลักษณ์บุคคลปลอมของตนเองหรือผู้อื่น

ความผิดฐานการจำหน่าย หรือโอนซึ่งข้อมูลหรือเอกสารซึ่งแสดงเอกลักษณ์บุคคลหรือเอกสารซึ่งแสดงเอกลักษณ์บุคคลปลอมของตนเองหรือผู้อื่น การบัญญัติเช่นนี้จะทำให้มีความครอบคลุมการกระทำความผิดมากขึ้น กล่าวคือรวมถึงข้อมูลหรือเอกสารซึ่งแสดงเอกลักษณ์บุคคลทุกประเภท ยิ่งไปกว่านั้นยังรวมถึงการจำหน่ายหรือโอนข้อมูลซึ่งแสดงเอกลักษณ์บุคคลของตนเองด้วย ทั้งนี้ตามแนวทางกฎหมายของประเทศสหรัฐอเมริกาและประเทศสหราชอาณาจักร

(จ) ทำขึ้น โอน และครอบครองเครื่องมือทำเอกสารแสดงตัวบุคคลหรือเอกสารแสดงตัวบุคคลปลอม

ความผิดฐานการทำขึ้น โอน และครอบครองเครื่องมือทำเอกสารแสดงตัวบุคคลหรือเอกสารแสดงตัวบุคคลปลอม บัญญัติขึ้นเพื่อให้ครอบคลุมถึงกระบวนการในการจัดทำขึ้นซึ่งเอกสารแสดงตัวบุคคลปลอม เพื่อเป็นการกำจัดแหล่งผลิตเอกสารปลอม และยังบัญญัติให้ครอบคลุมถึงเครื่องมือที่ใช้จัดทำเอกสารแสดงตัวบุคคลทุกประเภทด้วย

3. การกำหนดโทษสำหรับการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลควรแบ่งแยกตามความร้ายแรงของความผิดที่เกิดขึ้น กล่าวคือกรณีที่กระทำการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลในกรณีต่อไปนี้ ให้มีระวางโทษหนักกว่ากรณีทั่วไป คือ การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคล

(ก) เพื่อความสะดวกในการกระทำความผิดเกี่ยวกับการค้ายาเสพติด

(ข) เพื่อการให้ความสะดวกแก่การก่อการร้ายระหว่างประเทศ

(ค) เพื่อไปกระทำความผิดอาญาที่ใช้ความรุนแรงอื่น หรือ

(ง) กระทำความผิดโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลซ้ำ ซึ่งคดีถึงที่สุดแล้ว

(จ) เพื่อกระทำให้ผู้อื่น หรือประชาชนได้รับความเสียหายอย่างร้ายแรง

ทั้งนี้เพราะการกระทำความผิดใดที่สร้างความเสียหาย หรือกระทบต่อคนจำนวนมาก การกระทำนั้นก็สมควรได้รับโทษหนักกว่าการกระทำความผิดที่สร้างความเสียหายที่น้อยกว่า ซึ่งเป็นไปตามหลักความได้สัดส่วน

4. การกำหนดมาตรการเพื่อเป็นการคุ้มครองผู้เสียหาย เห็นควรให้มีการแก้ไข เพิ่มเติมมาตรการในการระงับความเสียหายของผู้เป็นเจ้าของข้อมูลในทันที หรือในขณะดำเนินการฟ้องร้องคดี เพื่อให้เกิดความเสียหายแก่ผู้เป็นเจ้าของข้อมูลอย่างน้อยที่สุด

รายการอ้างอิง

ภาษาไทย

กาญจนา นาคสกุล. ความหมายของคำที่น่าสนใจ[ออนไลน์]. แหล่งที่มา: http://www.blog.prachyanun.com/view.php?article_id=1175.[20 พฤศจิกายน 2555]

กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง[ออนไลน์]. แหล่งที่มา: http://www.mfa.go.th/humanrights/images/stories/iccprt.pdf. [20 พฤศจิกายน 2555]

เกรียงไกร เจริญธนาวัฒน์. หลักกฎหมายว่าด้วยสิทธิเสรีภาพ. กรุงเทพมหานคร: วิญญูชน, 2547.

เกียรติขจร วัจนะสวัสดิ์. กฎหมายอาญา ภาคความผิด เล่ม2. พิมพ์ครั้งที่ 5. กรุงเทพมหานคร: จิรรัชการพิมพ์, 2550.

เกียรติขจร วัจนะสวัสดิ์. กฎหมายอาญา ภาคความผิด เล่ม3. กรุงเทพมหานคร: จิรรัชการพิมพ์, 2550.

เกียรติขจร วัจนะสวัสดิ์. คำอธิบายกฎหมายอาญา ภาค 1. พิมพ์ครั้งที่ 9. กรุงเทพมหานคร: จิรรัชการพิมพ์, 2549.

เกียรติขจร วัจนะสวัสดิ์. คำอธิบายหลักกฎหมายวิธีพิจารณาความอาญา ว่าด้วยการดำเนินคดีในขั้นตอนก่อนการพิจารณา. พิมพ์ครั้งที่ 7. กรุงเทพมหานคร: พลสยามพริ้นติ้ง, 2553.

คะนึง ฦาไชย. กฎหมายวิธีพิจารณาความอาญา เล่ม1. พิมพ์ครั้งที่ 9. กรุงเทพมหานคร: โรงพิมพ์เดือนตุลา, 2551.

ชูชีพ ปิณฑะสิริ. การละเมิดสิทธิส่วนตัว. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. 2525.

ฎีกาตัดสินเกี่ยวกับปัญหาข้อกฎหมาย[ออนไลน์]. แหล่งที่มา: www.law-community.com/newsdata/file_data/1304306256.doc.[18 พฤศจิกายน 2555]

ณัฐฐ์วัฒน์ สุทธิโยธิน. ทฤษฎีความรับผิดทางอาญา[ออนไลน์]. แหล่งที่มา: http://www.stou.ac.th/Schools/Slw/upload/41716_2.pdf.[18 พฤศจิกายน 2555]

ทวีเกียรติ มีนะกนิษฐ. คำอธิบายกฎหมายอาญา ภาคความผิดและลหุโทษ. พิมพ์ครั้งที่ 3. กรุงเทพมหานคร: วิญญูชน, 2549.

ทีมข่าวภูมิภาค. 2 สาวร้อง ปวีณา ถูกมิจฉาชีพใช้สำเนาบัตรตระเวนจ้อโกง[ออนไลน์]. แหล่งที่มา : http://www.thairath.co.th/content/region/306214.[8 เมษายน 2555]

นวลจันทร์ ทัศนชัยกุล. อาชญากรรม การป้องกัน: การควบคุม. พิมพ์ครั้งที่ 2. นนทบุรี: พรทิพย์การพิมพ์, 2548.

บรรเจิด สิงคะเนติ และคณะ. รายงานวิจัยฉบับสมบูรณ์ เรื่อง ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Right to Privacy). กรุงเทพมหานคร: สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ.

ปกรณ์ มณีปกรณ์. อาชญาวิทยาและทัณฑวิทยา. พิมพ์ครั้งที่ 2. กรุงเทพมหานคร: เอ็ม.ที.เพรส, 2553.

ผาสุก เจริญเกียรติ. Identity Theft อาชญากรรมใกล้ตัว. ดุลพาห 56, 1 (มกราคม-เมษายน 2552): 176.

มานิตย์ จุมปา. คำอธิบายกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์. กรุงเทพมหานคร: วิญญูชน, 2553.

ราชบัณฑิตยสถาน. พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. 2542. กรุงเทพมหานคร: นานมีบุ๊คพับลิเคชั่นส์, 2546.

รู้ทันเทคนิคการขโมยข้อมูล[ออนไลน์]. แหล่งที่มา:http://foh9.blogspot.com/2012/04/blog-post_04.html.[20 พฤศจิกายน 2555]

แรงงานต่างด้าวสัญชาติลาวหลบหนีเข้าเมืองผิดกฎหมายและปลอมแปลงเอกสารทางราชการ [ออนไลน์]. แหล่งที่มา : http://atcloud.com/discussions/18474. [8 เมษายน 2555]

วรพจน์ วิศรุตพิชญ์. สิทธิและเสรีภาพตามรัฐธรรมนูญ. กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, 2538.

วิเชียร ดิเรกอุดมศักดิ์. วิ.อาญาพิสดาร เล่ม1. กรุงเทพมหานคร: แสงจันทร์การพิมพ์, 2554.

สมคิด เลิศไพฑูรย์ และคณะ. รายงานวิจัยฉบับสมบูรณ์ การคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในบัตรประจำตัวประชาชนแบบอเนกประสงค์. กรุงเทพมหานคร: สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์.

สราวุธ ปิติยาศักดิ์. กฎหมายเทคโนโลยีสารสนเทศ. กรุงเทพมหานคร: สำนักพิมพ์นิติธรรม, 2555.

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ. ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ... และร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ...กรุงเทพมหานคร: โรงพิมพ์เดือนตุลา, 2544.

สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. คำอธิบายความผิดเกี่ยวกับ การปลอมและการแปลง ตามประมวลกฎหมายอาญา. กรุงเทพมหานคร: วิญญูชน, 2555.

โสภา ชปีลมันน์. อาชญากรรม: ปัญหาที่ควรแก้ไขในสังคมปัจจุบัน. กรุงเทพมหานคร: โรงพิมพ์ไทยวัฒนาพานิช.

หยุด แสงอุทัย. กฎหมายอาญา ภาค 2-3. พิมพ์ครั้งที่ 7. กรุงเทพมหานคร: มหาวิทยาลัยธรรมศาสตร์,2538.

หยุด แสงอุทัย. ความรู้เบื้องต้นเกี่ยวกับกฎหมายทั่วไป. พิมพ์ครั้งที่ 16. กรุงเทพมหานคร: สำนักพิมพ์ประกายพรึก, 2548.

อภิรัตน์ เพ็ชรศิริ. ทฤษฎีอาญา. พิมพ์ครั้งที่ 2. กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน, 2552.

อัจจิมา กนกมณีโชติกุล. ความรับผิดทางแพ่งอันเกิดจากการล่วงละเมิดข้อมูลข่าวสารส่วนบุคคล. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 2553.

อดีตหนุ่มแบงก์แสบ สวมรอยบัตรลูกค้า รูดปรื๊ดนับสิบล้าน. หนังสือพิมพ์ไทยรัฐ[ออนไลน์]. แหล่งที่มา: http://www.thairath.co.th/today/view/180573. [21 มิถุนายน 2554]

Bob Hammond. เครดิตดีต้องรักษา มีปัญหาต้องแก้ไข. แปลโดย ภูริทัต ทองปรีชา. กรุงเทพมหานคร: วี.พริ้นท์ (1991) จำกัด, 2551.

ภาษาอังกฤษ

Chris Jay Hoofnagle. Identity Theft: Making The Known Unknowns Known. Harvard Journal of Law & Technology Vol.21. No.1 (Fall 2007): pp. 100-104.

California V. Greenwood [online]. Available from : http://en.wikipedia.org/wiki/California_v._Greenwood.[April 2013]

Jake Stroup, The 8 Types of Identity Theft [online]. Available from: http://idtheft.about.com/od/Basics/a/The-8-Types-Of-Identity-Theft.htm. [20 November 2012]

Jake Stroup, The Identity Theft and Assumption Deterrence Act of 1998 [online], Available from http://idtheft.about.com/od/glossary/a/ITADA.htm. [10 December 2012]

Jake Stroup. Insurance Identity Theft: The New Type of Identity Theft [online]. Available from: http://idtheft.about.com/od/identitytheft101/a/Insurance-Identity-Theft.htm. [20 November 2012]

Identity Theft Task Force. The President's Identity Theft Task Force Combating Identity Theft a Strategic Plan. (April 2007).

Identity Theft [online] Available from: http://en.wikipedia.org/wiki/Identity_theft. [20November 2012]

Identity Theft and Assumption Deterrence Act of 1998 [online] Available from http://www.ckfraud.org/title_18.html. [November 2012]

Identity Theft and Assumption Deterrence Act of 1998 [online], Available from: http://itlaw.wikia.com/wiki/Identity_Theft_and_Assumption_Deterrence_Act_of_1998. [10 December 2012]

Identity Theft in Canada [online], Available from: http://www.spamlaws.com/id-theft-can.html. [February 2013]

Martin T. Biegelman. Identity Theft Handbook Detection,Prevention,and Security. New Jersey: John Wiley & Sons, Inc, 2009.

Mohamed Chawki & Mohamed S. Abdel Wahab. Identity Theft in Cyberspace: Issues and Solutions. Lex Electronica Vol.11, 1 (Spring 2006): 2.

Pam Dixon. Medical Identity Theft: The Information Crime that Can Kill You. The World Privacy Forum (May 2006):p.2.

The Bureau of Justice Assistance. Preventing Identity Theft: a Guide for Consumers. Washington DC, 2005.

The Fair Credit Reporting Act [online]. Available from: http://www.ftc.gov/os/statutes/031224fcra.pdf. [2 February 2013]

Theft Act 1968 [online]. Available from:

http://www.legislation.gov.uk/ukpga/1968/60/contents. [2 February 2013]

ภาคผนวก

ภาคผนวก ก

Identity Theft and Assumption Deterrence Act of 1998
Title 18 United States Code - Section 1028
Fraud and Related Activity in Connection with Identification Documents and Information.

The Identity Theft and Assumption Deterrence Act of 1998 which became effective October 30, 1998, makes identity theft a Federal crime with penalties up to 15 years imprisonment and a maximum fine of $250,000. It establishes that the person whose identity was stolen is a *true* victim. Previously, only the credit grantors who suffered monetary losses were considered victims. This legislation enables the Secret Service, the Federal Bureau of Investigation, and other law enforcement agencies to combat this crime. It allows for the identity theft victim to seek restitution if there is a conviction. It also establishes the Federal Trade Commission as a central agency to act as a clearinghouse for complaints, (against credit reporting agencies and credit grantors) referrals, and resources for assistance for victims of identity theft. This statute may serve as a model for your state to enact similar legislation. It should also provide you leverage to influence law enforcement to investigate your case.

Title 18 USC 1028:

a. Whoever, in a circumstance described in subsection (c) of this section --
    1. knowingly and without lawful authority produces an identification document or a false identification document;
    2. knowingly transfers an identification document or a false identification document knowing that such document was stolen or produced without lawful authority;
    3. knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor) or false identification documents;

4. knowingly possesses an identification document (other than one issued lawfully for the use of the possessor) or a false identification document, with the intent such document be used to defraud the United States;
5. knowingly produces, transfers, or possesses a document-making implement with the intent such document-making implement will be used in the production of a false identification document or another document-making implement which will be so used;
6. knowingly possess an identification document that is or appears to be an identification document of the United States which is stolen or produced without lawful authority knowing that such document was stolen or produced without such authority shall be punished as provided in subsection (b) of this section; or
7. knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law or that constitutes a felony under any applicable State or local law;

b. The punishment for an offense under subsection (a) of this section is --
    1. except as provided in paragraph (3) and (4), a fine under this title or imprisonment for not more than 15 years, or both, if the offense is --
        A. the production or transfer of an identification document or false identification document that is or appears to be --
            a. an identification document issued by or under the authority of the United States; or
            b. a birth certificate, or a driver's license or personal identification card;
        B. the production or transfer of more than five identification documents or false identification documents;
        C. an offense under paragraph (5) of such subsection; or

D. an offense under paragraph (7) of such subsection that involves the transfer or use of 1 or more means of identification if, as a result of the offense, any individual committing the offense obtains anything of value aggregating $1,000 or more during any 1-year period;

2. except as provided in paragraphs (3) and (4), a fine under this title or imprisonment for not more than three years, or both, if the offense is --
   A. any other production, transfer, or use of means of identification, an identification document, or a false identification document; or
   B. an offense under paragraph (3) or (7) of such subsection;
3. a fine under this title or imprisonment for not more than 20 years, or both, if the offense is committed --
   A. to facilitate a drug trafficking crime (as defined in section 929(a)(2)) or this title;
   B. in connection with a crime of violence (as defined in section 924(c)(3)); or
   C. after a prior conviction under this section becomes final;
4. a fine under this title or imprisonment for not more than 25 years, or both, if the offense is committed to facilitate an act of international terrorism (as defined in section 2331(1) of this title);
5. in the case of any offense under subsection (a), forfeiture to the United States of any personal property used or intended to be used to commit the offense; and
6. a fine under this title or imprisonment for not more than one year, or both, in any other case.

c. The circumstance referred to in subsection (a) of this section is that --
   1. the identification document or false identification document is or appears to be issued by or under the authority of the United States or the

document-making implement is designed or suited for making such an identification document or false identification document;

2. the offense is an offense under subsection (a)(4) of this section; or
3. either --
    A. the production, transfer, possession, or use prohibited by this section is in or affects interstate or foreign commerce; or
    B. the means of identification, identification documents, false identification document, or document-making implement is transported in the mail in the course of the production, transfer, possession, or use prohibited by this section.
    C. In this section --
        1. the term "document-making implement" means any implement, impression, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an identification document, a false identification document, or another document-making
        2. the term "identification document" means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is a type intended to commonly accepted for the purpose of identification of individuals;
        3. the term "means of identification" means any name or number that may be used, alone or in conjunction with

any other information, to identify a specific individual, including any --

A. name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
B. unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
C. unique electronic identification number, address, or routing code; or
D. telecommunications identifying information or access device as defined in section 1029(e);

4. the term "personal identification card" means an identification document issued by a State local government solely for the purpose of identification;
5. the term "produce" includes alter, authenticate, or assemble; and
6. the term "State" includes any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States.

This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, or any activity authorized under chapter 224 of this title.

Attempt and Conspiracy – Any person who attempts or conspires to commit any offense of this section shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

Forfeiture Procedures – The forfeiture of property under this section, including any seizure and disposition of the property and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 (other than subsection (d) of that section) of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853).

Rule of Construction – For purpose of subsection (a)(7), a single identification document or false identification document that contains 1 or more means of identification shall be construed to be 1 means of identification.

ภาคผนวก ข

CANADIAN CRIMINAL CODE

IDENTITY THEFT AND IDENTITY FRAUD

Section 402.1 For the purposes of sections 402.2 and 403, “identity information” means any information — including biological or physiological information — of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including a fingerprint, voice print, retina image, iris image, DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, credit card number, debit card number, financial institution account number, passport number, Social Insurance Number, health insurance number, driver’s license number or password.

Section 402.2

(1) Everyone commits an offence who knowingly obtains or possesses another person’s identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.

(2) Everyone commits an offence who transmits, makes available, distributes, sells or offers for sale another person’s identity information, or has it in their possession for any of those purposes, knowing that or being reckless as to whether the information will be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.

(3) For the purposes of subsections (1) and (2), an indictable offence referred to in either of those subsections includes an offence under any of the following sections:

(a) section 57 (forgery of or uttering forged passport);

(b) section 58 (fraudulent use of certificate of citizenship);

(c) section 130 (personating peace officer);

(d) section 131 (perjury);

(e) section 342 (theft, forgery, etc., of credit card);

(f) section 362 (false pretence or false statement);

(g) section 366 (forgery);

(h) section 368 (use, trafficking or possession of forged document);

(i) section 380 (fraud); and

(j) section 403 (identity fraud).

(4) An accused who is charged with an offence under subsection (1) or (2) may be tried and punished by any court having jurisdiction to try that offence in the place where the offence is alleged to have been committed or in the place where the accused is found, is arrested or is in custody. However, no proceeding in respect of the offence shall be commenced in a province without the consent of the Attorney General of that province if the offence is alleged to have been committed outside that province.

(5) Everyone who commits an offence under subsection (1) or (2)

(a) is guilty of an indictable offence and liable to imprisonment for a term of not more than five years; or

(b) is guilty of an offence punishable on summary conviction.

Section 403.

(1) Everyone commits an offence who fraudulently personates another person, living or dead,

(a) with intent to gain advantage for themselves or another person;
(b) with intent to obtain any property or an interest in any property;
(c) with intent to cause disadvantage to the person being personated or another person; or
(d) with intent to avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice.

(2) For the purposes of subsection (1), personating a person includes pretending to be the person or using the person's identity information — whether by itself or in combination with identity information pertaining to any person — as if it pertains to the person using it.

(3) Everyone who commits an offence under subsection (1)

(*a*) is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years; or

(*b*) is guilty of an offence punishable on summary conviction.

ภาคผนวก ค

THE UNITED KINGDOM ACT

THE THEFT ACT OF 1968

Section 15

(1) A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it, shall on conviction on indictment be liable to imprisonment for a term not exceeding ten years.

(4) For purposes of this section 'deception' means any deception (whether deliberate or reckless) by words or conduct as to fact or as to law, including a deception as to the present intentions of the person using the deception or any other person.

Section 24A Dishonestly retaining a wrongful credit

(1) A person is guilty of an offence if

(a) A wrongful credit has been made to an account kept by him or in respect of which he has any right or interest;

(b) He knows or believes that the credit is wrongful; and

The dishonestly fails to take such steps as are reasonable in the circumstances to secure that the credit is cancelled.

THE DATA PROTECTION ACT OF 1998

Article 55 Unlawful obtaining etc. of personal data.

(1) A person must not knowingly or recklessly, without the consent of the data controller—

(a) obtain or disclose personal data or the information contained in personal data, or

(b) procure the disclosure to another person of the information contained in personal data.

(2) Subsection (1) does not apply to a person who shows—

(a) that the obtaining, disclosing or procuring—

(i) was necessary for the purpose of preventing or detecting crime, or

(ii) was required or authorised by or under any enactment, by any rule of law or by the order of a court,

(b) that he acted in the reasonable belief that he had in law the right to obtain or disclose the data or information or, as the case may be, to procure the disclosure of the information to the other person,

(c) that he acted in the reasonable belief that he would have had the consent of the data controller if the data controller had known of the obtaining, disclosing or procuring and the circumstances of it, or

(d) that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.

(3) A person who contravenes subsection (1) is guilty of an offence.

(4) A person who sells personal data is guilty of an offence if he has obtained the data in contravention of subsection (1).

(5) A person who offers to sell personal data is guilty of an offence if—

(a) he has obtained the data in contravention of subsection (1), or

(b) he subsequently obtains the data in contravention of that subsection.

THE IDENTITY CARD ACT OF 2006

Article 25 Possession of false identity documents etc.

(1) It is an offence for a person with the requisite intention to have in his possession or under his control—

(a) an identity document that is false and that he knows or believes to be false;

(b) an identity document that was improperly obtained and that he knows or believes to have been improperly obtained; or

(c) an identity document that relates to someone else.

(2)The requisite intention for the purposes of subsection (1) is—

(a) the intention of using the document for establishing registrable facts about himself; or

(b) the intention of allowing or inducing another to use it for establishing, ascertaining or verifying registrable facts about himself or about any other person (with the exception, in the case of a document within paragraph (c) of that subsection, of the individual to whom it relates).

(3) It is an offence for a person with the requisite intention to make, or to have in his possession or under his control—

(a) any apparatus which, to his knowledge, is or has been specially designed or adapted for the making of false identity documents; or

(b) any article or material which, to his knowledge, is or has been specially designed or adapted to be used in the making of false identity documents.

Article 26 Identity documents for the purposes of section 25(1) In section 25 “identity document” means any document that is, or purports to be—

(a) an ID card;

(b) a designated document;

(c) an immigration document;

(d) a United Kingdom passport (within the meaning of the Immigration Act 1971 (c. 77));

(e) a passport issued by or on behalf of the authorities of a country or territory outside the United Kingdom or by or on behalf of an international organisation;

(f) a document that can be used (in some or all circumstances) instead of a passport;

(g) a UK driving licence; or

(h) a driving licence issued by or on behalf of the authorities of a country or territory outside the United Kingdom.

Article 28 Providing false information

(1) A person is guilty of an offence if, in circumstances falling within subsection (2), he provides false information to any person —

(a) for the purpose of securing the making or modification of an entry in the Register;

(b) in confirming (with or without changes) the contents of an entry in the Register; or

(c) for the purpose of obtaining for himself or another the issue or modification of an ID card.

(2)Those circumstances are that, at the time of the provision of the information he—

(a) knows or believes the information to be false; or

(b) is reckless as to whether or not it is false.

ภาคผนวก ง

ท้ายพระราชบัญญัติบัตรประจำตัวประชาชน ค.ศ. 2006

(The Identity Card Act of 2006)

กฎหมายได้กำหนดข้อมูลที่สามารถจัดเก็บได้ไว้อย่างชัดเจน ซึ่งแบ่งข้อมูลออกเป็น 9 กลุ่ม ดังนี้

1.) ข้อมูลเกี่ยวกับตัวบุคคล

(ก) ชื่อตัว

(ข) ชื่ออื่นที่บุคคลมี หรือเป็นที่รู้จัก

(ค) วันเดือนปีเกิด

(ง) สถานที่เกิด

(จ) เพศ

(ฉ) สถานที่อยู่อาศัยหลักภายในประเทศสหราชอาณาจักร

(ช) สถานที่อยู่อาศัยแห่งอื่นทุกแห่งในประเทศสหราชอาณาจักรหรือในต่างประเทศ

2.) ข้อมูลที่ใช้ระบุตัวบุคคล

(ก) รูปภาพถ่าย

(ข) ลายมือชื่อ

(ค) ลายพิมพ์นิ้วมือ

(ง) ข้อมูลทางชีวภาพอื่นๆ เกี่ยวกับบุคคล

3.) ข้อมูลเกี่ยวกับสถานะ

(ก) สัญชาติ

(ข) สิทธิในการพำนักภายในประเทศสหราชอาณาจักร

(ค)ข้อกำหนดและเงื่อนไขเกี่ยวกับการได้รับอนุญาตให้เข้าประเทศสหราชอาณาจักร

4.) หมายเลขอ้างอิงที่เกี่ยวกับตัวบุคคล

(ก) หมายเลขประจำตัวประชาชน

(ข) หมายเลขประจำตัวอื่นที่รัฐบาลออกให้

(ค) หมายเลขประกันภัย

(ง) หมายเลขที่เกี่ยวกับเอกสารการเข้าเมือง

(จ) หมายเลขหนังสือเดินทางของประเทศสหราชอาณาจักร ตลอดจนหมายเลขเอกสารที่ใช้แทนหนังสือเดินทาง

(ฉ) หมายเลขประจำตัวใดที่ออกให้นอกประเทศสหราชอาณาจักร

(ช) หมายเลขที่เกี่ยวกับการติดต่อเข้าพำนักในประเทศ

(ซ) หมายเลขใบอนุญาตการทำงาน

(ญ) หมายเลขใบอนุญาตขับขี่

5.) บันทึกประวัติข้อมูล

(ก) ข้อมูลใดๆ ที่บันทึกในครั้งก่อนๆ

(ข) รายละเอียดของการเปลี่ยนแปลงข้อมูล

(ค) วันมรณะ

6.) ประวัติเกี่ยวกับการลงทะเบียน และบัตรประจำตัว

(ก) วันที่มีคำขอลงทะเบียน

(ข) วันที่มีคำขอให้เปลี่ยนแปลงทางทะเบียน

(ค) วันที่มีคำขอให้ยืนยันข้อมูลทางทะเบียน

(ง) เหตุผลของการไม่บันทึกข้อมูล

(จ) รายละเอียดเกี่ยวกับการออกบัตรประจำตัวทุกครั้ง รวมถึงรายละเอียดเกี่ยวกับบุคคลที่รับรองคำขอ การแจ้งบัตรหายหรือบัตรได้รับความเสียหาย ฯลฯ

(ฉ) รายละเอียดเกี่ยวกับข้อกำหนดของรัฐมนตรีที่ให้คืนบัตรประจำตัว

7.) ข้อมูลที่ใช้ในการตรวจสอบความถูกต้องสมบรูณ์

(ก)ข้อมูลที่ใช้ในการเปลี่ยนแปลงรายละเอียดทางทะเบียนในการออกบัตรประจำตัว

(ข) ข้อมูลที่ใช้ยืนยันทางทะเบียน

(ค) รายละเอียดเกี่ยวกับขั้นตอนในการแสดงตน หรือการตรวจสอบข้อมูล

(ง) รายละเอียดเกี่ยวกับขั้นตอนในการตรวจสอบความถูกต้อง ความสมบรูณ์ทางทะเบียน

(จ) รายละเอียดเกี่ยวกับการแจ้งต่างๆ ของบุคคล

8.) ข้อมูลที่ใช้ในการรักษาความปลอดภัยของข้อมูล

(ก) หมายเลขเอกลักษณ์ประจำตัวบุคคล

(ข) รหัสผ่าน หรือวิธีตั้งรหัสผ่านอื่น

(ค) คำถาม และคำตอบที่ใช้ยืนยันตัวบุคคล

9.) ประวัติการให้ข้อมูล

(ก) รายละเอียดเกี่ยวกับข้อมูลที่จัดให้แก่บุคคล

(ข) รายละเอียดเกี่ยวกับบุคคลที่ให้ข้อมูล

(ค) รายละเอียดเกี่ยวกับการให้ข้อมูล เมื่อมีการให้ข้อมูลในแต่ละครั้ง

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวฐาปณีย์ รติจารุภัทร เกิดเมื่อวันที่ 9 กรกฎาคม พ.ศ. 2530 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาปริญญาตรีนิติศาสตรบัณฑิต เกียรตินิยมอันดับสอง จากคณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อปีการศึกษา 2552 ได้รับประกาศนียบัตรว่าความของสำนักฝึกอบรมวิชาว่าความแห่งสภาทนายความ รุ่นที่ 33 เมื่อปีพ.ศ. 2552 สอบไล่ได้ความรู้ชั้นเนติบัณฑิต สมัยที่ 63 สำนักอบรมศึกษาแห่งเนติบัณฑิตยสภา ปีการศึกษา 2553 และเข้ารับการศึกษาต่อในหลักสูตรนิติศาสตรมหาบัณฑิต สาขากฎหมายอาญาและกระบวนการยุติธรรมทางอาญา ที่คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีพ.ศ. 2554