รายงานการวิจัย

เรื่อง

มาตรการทางกฎหมายอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์

Criminal Law Measures to Protect Computer Data

โดย

ผู้ช่วยศาสตราจารย์ สมศักดิ์ เธียรจรูญกุล

การวิจัยครั้งนี้ได้รับทุนอุดหนุนการวิจัยจากกองทุนรัตนโกสินทร์สมโภช 200 ปี

ประจำปี 2559

มหาวิทยาลัยสุโขทัยธรรมาธิราช

ชื่อเรื่อง มาตรการทางกฎหมายอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์
ชื่อผู้วิจัย ผู้ช่วยศาสตราจารย์สมศักดิ์ เธียรจรูญกุล
ปีที่แล้วเสร็จ 2561

บทคัดย่อ

การศึกษาวิจัยมาตรการทางกฎหมายอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์ฉบับนี้เป็นการวิจัยเอกสาร โดยมีวัตถุประสงค์ในการศึกษาวิจัยดังต่อไปนี้ 1. ศึกษาลักษณะและประเภทของข้อมูลคอมพิวเตอร์ ในฐานะวัตถุแห่งการกระทำกับลักษณะแห่งการกระทำโจรกรรมข้อมูลคอมพิวเตอร์ 2. วิเคราะห์บทบัญญัติและอุปสรรคในการบังคับใช้กฎหมายทางอาญาเกี่ยวกับการคุ้มครองข้อมูลคอมพิวเตอร์จากการกระทำโจรกรรมข้อมูลคอมพิวเตอร์ 3. เพื่อเสนอแนะการปรับปรุงกฎหมายที่เกี่ยวข้องกับมาตรการทางอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์ โดยวิธีการศึกษาวิจัยนี้เป็นการวิจัยเอกสาร รวบรวมบทบัญญัติความผิดเกี่ยวกับลักษณะแห่งการกระทำโจรกรรมข้อมูลคอมพิวเตอร์ คำพิพากษาศาลฎีกา ตำราและบทความที่เกี่ยวข้องของไทยและต่างประเทศ เมื่อรวบรวมเสร็จจะทำการวิเคราะห์บทบัญญัติของกฎหมายทางอาญาที่เกี่ยวข้องว่ามีข้อบกพร่องอย่างไร ทั้งในทางทฤษฎีและการปรับใช้ในทางคดี เพื่อจัดทำข้อเสนอแนะแก้ไขเพิ่มเติมกฎหมาย หรือเสนอแนะฐานความผิดใหม่เพื่อจัดวางมาตรการทางกฎหมายอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์

จากการศึกษาวิจัยมีข้อค้นพบตามวัตถุประสงค์ ดังนี้ 1. ลักษณะและประเภทของข้อมูลคอมพิวเตอร์มีดังนี้ ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย ส่วนการโจรกรรมข้อมูล หมายถึง ลักษณะแห่งการกระทำสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ซึ่งอาจทำโดยการเจาะระบบ (hack) โดยมิชอบ หรือเข้าถึงข้อมูลคอมพิวเตอร์โดยชอบ แต่สำเนาไปโดยมิชอบ หรืออาจเป็นการได้ไปด้วยวิธีสามัญ เช่น เห็นหน้าจอมอนิเตอร์คอมพิวเตอร์ หรือสมาร์ทโฟน และจดจำไป เป็นต้น 2. อุปสรรคคือไม่มีกฎหมายอาญาคุ้มครองข้อมูลคอมพิวเตอร์ในฐานะวัตถุแห่งการกระทำจากปัญหาการโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ 3. ข้อเสนอแนะต้องแก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยกำหนดให้มีฐานความผิดสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นไปโดยมิชอบ และความผิดฐานได้รับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ โดยรู้ว่าข้อมูลคอมพิวเตอร์ได้มาจากการกระทำความผิดฐานสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

คำสำคัญ : ข้อมูลคอมพิวเตอร์ สำเนาข้อมูลคอมพิวเตอร์ กฎหมายอาญา ความผิดเกี่ยวกับคอมพิวเตอร์

Title : Criminal Law Measures to Protect Computer Data
Researcher : Assistant Professor Somsak Tienjaroonkul
Year : 2018

Abstract

This documentary research study has 3 objectives : (1) To study characteristics and types of the computer data as the material of action, and the manner by which the data is hacked; (2) to analyze legal provisions and obstacles in the enforcement of criminal law related to the protection of computer data from hacking, and (3) to recommend amendment of the criminal law measures to protect the computer data. In this study is documentary research, legal provisions into the nature of the computer hacking offence, the Supreme Court judgement, texts and related articles of Thai and foreign sources were compiled. The related criminal law provisions were analyzed both in theory and application to the case, to identify loopholes in the law. Recommendation was made for amendment of the law measures or for development of a new offence in the criminal law measures to protect the computer data

The findings of this study are : (1) characteristics and types of computer data means data, statements, or sets of instructions contained in a computer system, the output of which may be processed by a computer system including electronic data, according to the Law of Electronic Transactions, whereas “computer hacking” means to illegally copy data from other computers by unauthorized access, or to legally access but illegally copy the data, or simply by e.g. viewing the computer or smartphone on-screen information for illegal intent; (2) Obstacles; there is no criminal law to protect the computer data from either hacking or data copying, and (3) recommend amendment; the Computer Crime Act B.E. 2550 must be amended by designating offence related to illegal copying of other people’s computer data as well as offence related to illegal importing of aforementioned the third party’s computer data.

Keywords: Computer Data, Computer Data Copying, Criminal Law, Computer Crime Act

กิตติกรรมประกาศ

ผู้วิจัยขอขอบคุณมหาวิทยาลัยสุโขทัยธรรมาธิราช กองทุนรัตนโกสินทร์สมโภช 200 ปี ผู้ให้ทุนสนับสนุนการวิจัยฉบับนี้ คณะกรรมการทุกชุดผู้ช่วยกลั่นกรองงานวิจัย รองศาสตราจารย์ชนินาฏ ลีดส์ ที่ปรึกษางานวิจัย และผู้สนับสนุนทุกท่าน

สมศักดิ์ เธียรจรูญกุล
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

บทที่ 1
บทนำ

1. ความสำคัญของปัญหาการวิจัย

งานวิจัยเรื่อง “มาตรการทางกฎหมายอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์” มีความเกี่ยวพัน กับงานวิจัยเรื่องเดิมที่สรุปรายงานการวิจัยเสร็จสิ้นแล้ว คือ เรื่อง “ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ตามประมวลกฎหมายอาญา” เนื่องจากบัตรอิเล็กทรอนิกส์บางประเภท หรือบางกรณีเก็บหรือรักษาไว้ในรูปข้อมูลคอมพิวเตอร์ หรือบัตรอิเล็กทรอนิกส์และมีที่ใช้เกี่ยวพันกับระบบคอมพิวเตอร์ บทบัญญัติของกฎหมายทั้งสองกรณี คือ บัตรอิเล็กทรอนิกส์ กับข้อมูลคอมพิวเตอร์ จึงมีความเกี่ยวพันกัน

อีกทั้งสังคมวัฒนธรรมปัจจุบันเทคโนโลยีเปลี่ยนไปจากอดีตมาก คอมพิวเตอร์เข้ามามีบทบาทสำคัญแทบทุกด้านทุกสาขาทั้งภาครัฐและเอกชน และ**ข้อมูลขององค์กรหรือข้อมูลส่วนบุคคลทั้งของภาครัฐ และเอกชนจำนวนมากมีลักษณะการใช้งานหรือถูกจัดเก็บในรูปของข้อมูลคอมพิวเตอร์ อันเป็นข้อมูลที่มีความสำคัญ โดยอาจเป็นข้อมูลทางบัญชี ข้อมูลทางการเงิน ข้อมูลสายการบิน ข้อมูลความลับ ทางราชการ หรือข้อมูลทางธุรกิจ หรือบัตรอิเล็กทรอนิกส์ รวมทั้งสิ่งบ่งชี้เฉพาะบุคคล** (identification) **ลายนิ้วมือ ลายมือ ลายเท้า บัตรประจำตัวประชาชน รหัสโทรศัพท์** (pinphone) **ประวัติการทำฟัน จอประสาทตา** (retina) **ที่จัดเก็บในรูปข้อมูลคอมพิวเตอร์**

เมื่อข้อมูลคอมพิวเตอร์ถูกโจรกรรมด้วยการสำเนาไป หรือวิธีการอื่น ย่อมก่อความเสียหายให้เจ้าของข้อมูลคอมพิวเตอร์ และบางกรณีความเสียหายอาจถึงขั้นประเมินค่ามิได้ เช่น ข้อมูลลูกค้าของสถาบันการเงิน หรือข้อมูลความลับของทางราชการ เป็นต้น

กรณีข้อมูลคอมพิวเตอร์ได้เคยเกิดการกระทำที่มีการคัดลอกหรือสำเนาข้อมูลคอมพิวเตอร์จนถึงขั้นเป็นคดีอาญานำเสนอคดีขึ้นสู่ศาล ทั้งยังมีประเด็นข้อกฎหมายพิพาทโต้แย้งไปถึงศาลฎีกา และคดีถึงที่สุด ด้วยการยกฟ้องจำเลย

คำพิพากษาฎีกาที่ 5161/2547 จำเลยเป็นพนักงานแผนกต่างประเทศของโจทก์ร่วมมีหน้าที่เตรียมเอกสารคำขอใบอนุญาตติดต่อหน่วยราชการ ติดต่อประสานงานกับลูกค้าต่างประเทศ ในวันเวลา และสถานที่เกิดเหตุตามฟ้อง จำเลยนำเอกสารจำนวนประมาณ 400 แผ่น ตามเอกสารหมาย จ.3 จากสำนักงานโจทก์ร่วมไปไว้ที่บ้านจำเลยเพื่อทำงานให้แก่โจทก์ร่วม กับนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลในการดำเนินธุรกิจต่างๆ ของโจทก์ร่วมจากแผ่นบันทึกข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ของ

โจทก์ร่วมจำนวนรวม 41 แผ่น มีปัญหาวินิจฉัยตามฎีกาของโจทก์ร่วมว่า การกระทำของจำเลยเป็นความผิดตามฟ้องหรือไม่

สำหรับความผิดฐานเอาไปเสียซึ่งเอกสารในประการที่น่าจะเกิดความเสียหายแก่โจทก์ร่วมหรือผู้อื่นนั้น โจทก์ร่วมฎีกาว่า โจทก์ร่วมมีระเบียบห้ามนำเอกสารออกนอกที่ทำการ แม้จะไม่ถือเป็นข้อห้ามเด็ดขาดตามระเบียบนั้น แต่มิได้หมายความว่า เมื่อพนักงานนำงานออกจากที่ทำการของโจทก์ร่วมไปทำต่อที่บ้านแล้วพนักงานไม่จำต้องนำเอกสารที่เหลือหรือมิได้ใช้งานแล้วมาคืนโจทก์ร่วม การที่จำเลยทำงานเสร็จแล้วกลับไม่นำเอกสารที่เกี่ยวข้องมาคืนเพื่อส่งคืนลูกค้าเป็นการทำให้โจทก์ร่วมเสียหายแล้ว เพราะเอกสารส่วนหนึ่งเป็นความลับของลูกค้า เห็นว่าตามคำเบิกความของนาง จ. พนักงานโจทก์ร่วม ตำแหน่งหัวหน้าฝ่ายต่างประเทศได้ความว่า เอกสารหมาย จ.3 ซึ่งลูกค้าส่งมาให้โจทก์ร่วมนั้น ส่วนใหญ่จะเป็นข้อมูลเกี่ยวกับหนังสือรับรองของบริษัท บัญชีรายชื่อผู้ถือหุ้น งบบัญชีกำไร-ขาดทุน และสำเนาหนังสือเดินทาง เอกสารดังกล่าวจึงล้วนเป็นเอกสารที่บุคคลสามารถไปขอตรวจสอบและขอคัดสำเนาได้จากกรมทะเบียนการค้ากระทรวงพาณิชย์ จึงไม่ถือเป็นความลับของบริษัทลูกค้าโจทก์ร่วมอันต้องปกปิด

ดังนั้น การที่จำเลยใช้เอกสารดังกล่าวปฏิบัติในหน้าที่ให้แก่โจทก์ร่วมเสร็จ แล้วไม่นำกลับคืนแก่โจทก์ร่วม จึงไม่น่าจะเป็นเหตุให้โจทก์ร่วมหรือลูกค้าของโจทก์ร่วมต้องเสียหาย การกระทำของจำเลย จึงไม่เป็นความผิดฐานเอาไปเสียซึ่งเอกสาร โดยประการที่น่าจะเกิดความเสียหายแก่โจทก์ร่วมหรือผู้อื่น ศาลล่างทั้งสองวินิจฉัยปัญหานี้ชอบแล้ว ศาลฎีกาเห็นพ้องด้วยฎีกาของโจทก์ร่วมข้อนี้ฟังไม่ขึ้น

ปัญหาวินิจฉัยตามฎีกาของโจทก์ร่วม การที่จำเลยนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลจากแผ่นบันทึกข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ของโจทก์ร่วม เป็นความผิดฐานลักทรัพย์หรือไม่ โจทก์ร่วมฎีกาว่าข้อมูลในเครื่องคอมพิวเตอร์ของโจทก์ร่วมมีรูปร่างเป็นตัวอักษร ภาพ แผนผังและตราสาร จึงเป็นทรัพย์ตาม ป.พ.พ. มาตรา 137 การที่จำเลยเอาข้อมูลของโจทก์ร่วมดังกล่าวไป จึงเป็นความผิดฐานลักทรัพย์ เห็นว่า ข้อมูล ตามพจนานุกรมให้ ความหมายว่า “ข้อเท็จจริง หรือสิ่งที่ถือหรือยอมรับว่าเป็นข้อเท็จจริง สำหรับใช้เป็นหลักอนุมานหาความจริงหรือการคำนวณ” ส่วนข้อเท็จจริง หมายความว่า “ข้อความแห่งเหตุการณ์ที่เป็นมาหรือที่เป็นอยู่ตามจริง ข้อความหรือเหตุการณ์ที่จะต้องวินิจฉัยว่าเท็จ หรือจริง” ดังนั้นข้อมูลจึงไม่นับเป็นวัตถุมีรูปร่าง สำหรับตัวอักษร ภาพ แผนผังและตราสาร เป็นเพียง สัญญลักษณ์ที่ถ่ายทอดความหมายของข้อมูลออกจากแผ่นบันทึกข้อมูลโดยอาศัยเครื่องคอมพิวเตอร์ มิใช่รูปร่างของข้อมูล เมื่อ ป.พ.พ. มาตรา 137 บัญญัติว่า ทรัพย์ หมายความว่า วัตถุมีรูปร่าง ข้อมูลในแผ่นบันทึกข้อมูลจึงไม่ถือเป็นทรัพย์ การที่จำเลยนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลจากแผ่นบันทึกข้อมูลของโจทก์ร่วม จึงไม่เป็นความผิดฐานลักทรัพย์ตามฟ้อง ศาลล่างทั้งสองพิพากษายกฟ้อง ศาลฎีกา เห็นพ้องด้วย ฎีกาของโจทก์ร่วมทุกข้อฟังไม่ขึ้น

ดังนั้น จากคำพิพากษาฎีกาข้างต้น การโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นไปโดย มิชอบ จึงไม่มีกฎหมายที่กำหนดให้เป็นความผิดและโทษ เพื่อคุ้มครองข้อมูลคอมพิวเตอร์

ต่อมามี **คำพิพากษาฎีกาที่ 4311/2557** วินิจฉัยว่า เครื่องคอมพิวเตอร์ก็คือวัตถุอื่นใดประเภทหนึ่ง ตามนิยามของประมวลกฎหมายอาญา มาตรา 1 (7) ดังนั้น หากมีการทำให้ปรากฏความหมายด้วยตัว อักษรโดยวิธีพิมพ์ลงในเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์นั้นก็เป็นเอกสาร

จากคำพิพากษาฎีกาทั้ง 2 ฉบับ ไม่ทำให้ช่องว่างแห่งกฎหมายอาญาที่ไม่สามารถคุ้มครองข้อมูลคอมพิวเตอร์ ได้รับการแก้ไขปัญหาจากกรณีการโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ลงได้ ไม่ว่าลักษณะแห่งการกระทำโจรกรรมหรือ สำเนาข้อมูลคอมพิวเตอร์จะกระทำโดยรูปแบบเจาะระบบหรือที่เรียกกันว่าแฮ็ก (hack) หรือรูปแบบโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไป โดยเข้าถึงระบบคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ หรือรูปแบบโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยวิธีสามัญก็ตาม ซึ่งตามคำพิพากษาฎีกาที่ 5161/2547 ก็ได้วินิจฉัยไว้ว่าการกระทำ “เอาไป” ตามประมวลกฎหมายอาญา มาตรา 334 ฐานลักทรัพย์ ต้องมีการพรากทรัพย์ไป แต่การโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยไม่มีสิทธิ ไม่ได้มีการพรากข้อมูลคอมพิวเตอร์ไป หากข้อมูลคอมพิวเตอร์ก็ยังคงอยู่กับผู้ทรงสิทธิดังเดิม เพียงมีการคัดลอกข้อมูลคอมพิวเตอร์ หรือจดจำไปเท่านั้น ดังที่ศาลฎีกาได้วินิจฉัยไว้ตามคำพิพากษาฎีกาที่ 5161/2547 “ข้อมูลคอมพิวเตอร์” ไม่ได้อยู่ในความหมายของคำว่า “ทรัพย์” ซึ่งผู้เขียนเห็นพ้องด้วยกับศาลฎีกา กล่าวคือ ข้อมูลคอมพิวเตอร์ไม่ใช่วัตถุที่มีรูปร่างอันอาจมีรูปร่างโดยตัวของมันเองหรือโดยอาศัย สิ่งอื่นเป็นรูปร่าง[1] อีกทั้งลักษณะแห่งการกระทำเป็นเพียง**การแบ่ง : Share** ข้อมูลคอมพิวเตอร์ **มิใช่เอาไป ในลักษณะที่พรากการครอบครองข้อมูลคอมพิวเตอร์ไปเสียทีเดียว** ข้อมูลคอมพิวเตอร์ก็ยังคงอยู่กับฮาร์ดดีสก์หรือแผ่นบันทึกข้อมูลของเจ้าของข้อมูลคอมพิวเตอร์ เมื่อข้อมูลคอมพิวเตอร์มิได้อยู่ในความหมายของคำว่าทรัพย์ การกระทำของจำเลยจึงไม่เป็นความผิดฐานลักทรัพย์

เมื่อการโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยไม่มีสิทธิ **มิใช่เอาไปในลักษณะที่พรากการครอบครองข้อมูลคอมพิวเตอร์ไปเสียทีเดียว** กรณีจึงไม่อาจเป็นความผิดฐานเอาไปเสียซึ่งเอกสารตามประมวลกฎหมายอาญา มาตรา 188 เช่นเดียวกัน

การศึกษาวิจัยมาตรการทางกฎหมายอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์จึงมีความสำคัญ เพื่อให้ได้ทราบถึงข้อบกพร่องหรือปัญหา รวมทั้งเพื่อให้ได้แนวทาง และข้อเสนอแนะในการปรับปรุงแก้ไขกฎหมายกับค้นหาและจัดวางมาตรการทางกฎหมายอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์ เพื่อผลในการป้องกันและปราบปรามอาชญากรรมที่มีลักษณะแห่งการกระทำโจรกรรมข้อมูลคอมพิวเตอร์ให้มีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

---

[1] จิตติ ติงศภัทิย์, *กฎหมายอาญา ภาค 2 ตอน 2 และภาค 3* , พิมพ์ครั้งที่ 3 กรุงเทพมหานคร : เนติบัณฑิตยสภา 2532, หน้า 2473 - 2477

2. วัตถุประสงค์ในการวิจัย

2.1 ศึกษาลักษณะและประเภทของข้อมูลคอมพิวเตอร์ ในฐานะวัตถุแห่งการกระทำ กับลักษณะแห่งการกระทำโจรกรรมข้อมูลคอมพิวเตอร์

2.2 วิเคราะห์บทบัญญัติและอุปสรรคในการบังคับใช้กฎหมายทางอาญา เกี่ยวกับการคุ้มครองข้อมูลคอมพิวเตอร์จากการกระทำโจรกรรมข้อมูลคอมพิวเตอร์

2.3 เพื่อเสนอแนะการปรับปรุงกฎหมายที่เกี่ยวข้องกับมาตรการทางอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์

3. นิยามศัพท์

“กฎหมายทางอาญา” หมายถึง ประมวลกฎหมายอาญาและความผิดทางอาญาตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ความหมายเฉพาะงานวิจัยนี้)

“โจรกรรมข้อมูล” หมายถึง ลักษณะแห่งการกระทำสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ซึ่งอาจทำโดยการเจาะระบบ (hack) โดยมิชอบ หรือเข้าถึงข้อมูลคอมพิวเตอร์โดยชอบ แต่สำเนาไปโดยมิชอบ หรืออาจเป็นการได้ไปด้วยวิธีสามัญ เช่น เห็นหน้าจอมอนิเตอร์คอมพิวเตอร์หรือสมาร์ทโฟน และจดจำไป เป็นต้น (ความหมายเฉพาะงานวิจัยนี้)

4. ขอบเขตในการศึกษาวิจัย

ข้อมูลคอมพิวเตอร์มีบทบัญญัติของกฎหมายที่เกี่ยวข้องหลายฉบับหลายสาขากฎหมาย การศึกษาวิจัยนี้จะมุ่งศึกษาเฉพาะความผิดทางอาญาเกี่ยวกับลักษณะแห่งการกระทำโจรกรรมข้อมูลคอมพิวเตอร์ในฐานะที่เป็นวัตถุแห่งการกระทำ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550[2] เท่านั้น ส่วนบทบัญญัติของกฎหมายที่เกี่ยวข้องอื่น ๆ บางส่วนอาจกล่าวถึง และนำมาวิเคราะห์ประกอบการวิจัย

---

[2] แก้ไขเพิ่มเติมล่าสุดโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 *ราชกิจจานุเบกษา*, เล่ม 134 ตอนที่ 10 ก, 24 มกราคม 2560

5. ระเบียบวิธีการวิจัย

วิธีการศึกษาวิจัยนี้เป็นการวิจัยเชิงคุณภาพจากเอกสาร โดยจะรวบรวมบทบัญญัติความผิดเกี่ยวกับลักษณะแห่งการกระทำโจรกรรมข้อมูลคอมพิวเตอร์ คำพิพากษาศาลฎีกา ตำราและบทความที่เกี่ยวข้องของไทยและต่างประเทศ เมื่อรวบรวมเสร็จจะทำการวิเคราะห์บทบัญญัติของกฎหมายอาญาที่เกี่ยวข้องว่ามีข้อบกพร่องอย่างไร ทั้งในทางทฤษฎีและการปรับใช้ในทางคดี เพื่อจัดทำข้อเสนอแนะแก้ไขเพิ่มเติมกฎหมาย หรือเสนอแนะฐานความผิดใหม่เพื่อจัดวางมาตรการทางกฎหมายอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์

การรวบรวมข้อมูลจากห้องสมุดตามสถาบันต่างๆ ดังนี้ เนติบัณฑิตยสภาฯ สำนักงานส่งเสริมงานตุลาการ มหาวิทยาลัยธรรมศาสตร์ ท่าพระจันทร์ มหาวิทยาลัยธรรมศาสตร์ ศูนย์รังสิต กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สถาบันวิจัยเพื่อการพัฒนาประเทศไทย (ทีดีอาร์ไอ) คณะนิติศาสตร์กับหอสมุดกลาง จุฬาลงกรณ์มหาวิทยาลัย และสถาบันบัณฑิตพัฒนบริหารศาสตร์

การรวบรวมข้อมูลจากเอกสารหนังสือ เช่น คำอธิบายกฎหมายว่าด้วยคอมพิวเตอร์ การใช้การตีความกฎหมาย ศาสตราจารย์จิตติ ติงศภัทิย์ คำอธิบายกฎหมายอาญา ศาสตราจารย์ ดร. เกียรติขจร วัจนะสวัสดิ์ คำอธิบายกฎหมายอาญา ศาสตราจารย์จิตติ ติงศภัทิย์ เล่ม 1 2 และเล่ม 3 อาชญากรรมทางเศรษฐกิจ HACK Step by Step เจาะระบบ ถอดรหัส เป็นต้น

6. ประโยชน์ที่ได้รับ

6.1 ได้ทราบถึงลักษณะและประเภทของข้อมูลคอมพิวเตอร์กับลักษณะแห่งการกระทำโจรกรรมข้อมูลคอมพิวเตอร์

6.2 ได้ทราบถึงข้อบกพร่องหรือปัญหาของบทบัญญัติกฎหมายทางอาญาเกี่ยวกับการคุ้มครองข้อมูลคอมพิวเตอร์จากการกระทำโจรกรรมข้อมูลคอมพิวเตอร์

6.3 ได้ข้อเสนอแนะปรับปรุงแก้ไขบทบัญญัติของกฎหมายทางอาญา เกี่ยวกับการคุ้มครองข้อมูลคอมพิวเตอร์จากการกระทำโจรกรรมข้อมูลคอมพิวเตอร์

6.4 ได้ข้อค้นพบเพื่อประโยชน์สำหรับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ในการพัฒนาปรับปรุงกฎหมายเกี่ยวกับคอมพิวเตอร์

6.5 ได้ข้อค้นพบเพื่อนำไปใช้สำหรับการเรียนการสอนของสาขาวิชานิติศาสตร์ และสำหรับปรับปรุงเอกสารการสอนชุดวิชากฎหมายอาญา 2 ของมหาวิทยาลัยสุโขทัยธรรมาธิราช

บทที่ 2
ลักษณะแห่งการกระทำและกฎหมายอาญาของประเทศไทยเกี่ยวกับข้อมูลคอมพิวเตอร์

เนื้อหาบทที่ 2 จะแบ่งออกเป็น 2 ส่วน คือลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์ กับกฎหมายอาญาของประเทศไทยเกี่ยวกับข้อมูลคอมพิวเตอร์ โดยที่งานวิจัยเป็นงานวิจัยทางกฎหมาย เนื้อหาส่วนของลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์ จึงไม่ได้ลงลึกถึงเทคนิคหรือวิธีการของการกระทำ หากเพียงให้เห็นว่ามีลักษณะแห่งการกระทำเพื่อให้ได้ข้อมูล คอมพิวเตอร์ไปในรูปแบบใดบ้าง และเป็นลักษณะแห่งการกระทำเพื่อให้ได้ข้อมูลคอมพิวเตอร์ไปที่มีอยู่จริงเท่านั้น ส่วนกฎหมายอาญาของประเทศไทยเกี่ยวกับข้อมูลคอมพิวเตอร์ จะเน้นวิเคราะห์ที่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เป็นด้านหลัก กับประมวลกฎหมายอาญา ซึ่งเป็นกฎหมายหลักหนึ่งในสี่ฉบับ หรือที่เรียกว่ากฎหมายสี่มุมเมือง บทที่ 2 จึงแบ่งหัวข้อออกเป็น 2 หัวข้อดังนี้

1. ลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์
2. กฎหมายอาญาของประเทศไทยเกี่ยวกับข้อมูลคอมพิวเตอร์

1. ลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์

ลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์ เพื่อให้ได้ไปซึ่งข้อมูลคอมพิวเตอร์มีหลากหลายรูปแบบ ซึ่งมีลักษณะแห่งการกระทำที่แตกต่างกัน โดยมีตั้งแต่การเจาะระบบ หรือที่เรียกกันว่าแฮ็ก (hack) ที่ต้องใช้ความรู้หรือวิธีการทางเทคโนโลยีระดับสูง หรือลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์ที่ผู้กระทำเข้าถึงตัวเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ จนถึงโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยวิธีสามัญธรรมดา

เกี่ยวกับลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์เป็นเพียงกล่าวถึงให้เห็นว่ามีลักษณะแห่งการกระทำเพื่อให้ได้ข้อมูลคอมพิวเตอร์ไปในรูปแบบใดบ้าง และเป็นลักษณะแห่งการกระทำเพื่อให้ได้ข้อมูลคอมพิวเตอร์ไปที่มีอยู่จริง ไม่ได้มุ่งเน้นในเชิงลึกถึงเทคโนโลยีหรือความเชี่ยวชาญในการเจาะระบบ หรือการแฮ็ก (hack) ที่ผู้กระทำต้องเชี่ยวชาญการใช้โปรแกรมหรือมีความรู้เกี่ยวกับระบบคอมพิวเตอร์ระดับสูง ด้วยเหตุที่งานวิจัยเป็นงานวิจัยทางกฎหมาย

รูปแบบลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์ ณ ที่นี้ จะแบ่งลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์ออกเป็น 3 รูปแบบ ดังนี้

1.1 เจาะระบบ หรือที่เรียกกันว่าแฮ็ก (hack)

1.2 โจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยเข้าถึงระบบคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์

1.3 โจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยวิธีสามัญ

1.1 เจาะระบบ หรือที่เรียกกันว่าแฮ็ก (hack)

การเจาะระบบหรือการแฮ็ก (hacking) ความหมายจากพจนานุกรมออนไลน์ให้ความหมายอยู่ 2 ความหมาย คือ[3]

1.1.1 To write or refine computer programs skillfully

1.1.2. To use one's skill in computer programming to gain illegal or unauthorized access to a file or network: hacked into the company's intranet.

คำศัพท์เดิม หมายถึง การเจาะเข้าใช้ระบบอย่างไม่ได้รับอนุญาต คือ คำว่า "แคร็คกิ้ง (cracking)" ในขณะที่แฮ็กกิ้ง (hacking) หมายถึง ผู้ที่ใช้คอมพิวเตอร์และซอฟต์แวร์อย่างชำนาญ แต่ที่ผ่านมาสังคมได้ใช้คำว่า "แฮ็กกิ้ง" ในความหมายของการกระทำในทางลบ หรือหมายถึง คนที่ขโมยข้อมูลหรือโจมตีระบบอื่นๆ แฮคเกอร์ จึงหมายถึง คนที่พยายามเจาะเข้าระบบคอมพิวเตอร์หรือเครือข่ายอื่น และแฮ็กเกอร์ (hacker) หรือนักเจาะระบบข้อมูลใช้หมายถึงผู้เชี่ยวชาญในสาขาคอมพิวเตอร์ บางครั้งยังใช้หมายถึงผู้เชี่ยวชาญในสาขาอื่นนอกจากคอมพิวเตอร์ด้วย โดยเฉพาะผู้ที่มีความรู้ในรายละเอียดหรือผู้ที่มีความเฉลียวในการแก้ปัญหาจากข้อจำกัด ความหมายที่ใช้ในบริบทของคอมพิวเตอร์นั้นได้เปลี่ยนแปลงไปจากความหมายดั้งเดิม

ในปัจจุบัน "แฮ็กเกอร์" นั้นใช้ใน 2 ความหมายหลักในทางที่ดีและไม่ค่อยดีนัก ความหมายซึ่งเป็นที่นิยม และพบได้บ่อยในสื่อนั้นมักจะไม่ดี โดยจะหมายถึงอาชญากรคอมพิวเตอร์ ส่วนในทางที่ดีนั้น "แฮ็กเกอร์" ยังใช้ในลักษณะของคำติดปาก หมายถึง ความเป็นพวกพ้อง หรือสมาชิกของกลุ่มคอมพิวเตอร์

นอกเหนือจากนี้ คำว่า "แฮ็กเกอร์" ยังใช้หมายถึงกลุ่มของผู้ใช้คอมพิวเตอร์โดยเฉพาะโปรแกรมที่มีความสามารถในระดับผู้เชี่ยวชาญ

---

[3] เว็บไซต์เวิลด์เพรสดอทคอม, *https://neay999.wordpress.com/บทที่-7-การเจาะระบบและวิ/* สืบค้นเมื่อวันที่ 8 พฤษภาคม 2560

รูปแบบของการโจมตี สิ่งที่ทำให้เกิดการโจมตีเนื่องจากการที่ผู้โจมตีมีแรงจูงใจดังนั้น สิ่งแรกที่นักเจาะระบบจะทำคือการตัดสินใจในจุดมุ่งหมายของเขา ขั้นตอนนี้เป็นกระบวนการคิดที่มีสติ

แต่บางครั้งเขาก็รู้เพียงแต่ว่าเขาต้องการที่จะโจมตีเป้าหมายที่ไม่มีเหตุผลที่ชัดเจน รูปแบบของการโจมตีนั้น ก็เปลี่ยนแปลงไปตามธรรมชาติของคอมพิวเตอร์และเครือข่ายที่มีวิวัฒนาการอย่างต่อเนื่อง

ในช่วงปี 1980 นั้นเป้าหมายส่วนใหญ่จะเป็นคอมพิวเตอร์แต่ละเครื่อง แต่ในช่วงปี 1990 นั้นเป้าหมายหลักก็กลายมาเป็นระบบเครือข่าย ปัจจุบันเป้าหมายหลักคือ ระบบเครือข่ายที่เป็นโครงสร้างของอินเทอร์เน็ตทั่วโลก

โดยทั่วไปนักโจมตีนั้นมีความรู้ความชำนาญสูงและการโจมตีนั้นจะเปลี่ยนจากการค้นหาบักหรือช่องโหว่ของซอฟต์แวร์หรือแอพพลิเคชั่นเฉพาะ ไปเป็นการโจมตีช่องโหว่ของ ซอฟต์แวร์หรือฮาร์ดแวร์ที่เป็นโครงสร้างของระบบ

จะเห็นได้ว่าแฮกเกอร์ในปัจจุบันสามารถเจาะระบบเราโดยผ่านทะลุ Firewall ได้อย่างง่ายดาย เพราะเรามีความจำเป็นต้องเปิดให้บริการ Web Server ในทุกองค์กร ดังนั้นการตรวจสอบเรื่องของ Web Application Source Code และ Web Server Configuration จึงเป็นทางออกสำหรับการแก้ไขปัญหาทางด้านความปลอดภัยของระบบให้รอดพ้นจากเหล่าไวรัสและแฮกเกอร์ซึ่งนับวันจะเพิ่มจำนวนและเพิ่มความสามารถขึ้นเป็นทวีคูณ[4]

1.2 โจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยเข้าถึงระบบคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์

ลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์มีรูปแบบที่มีการเข้าถึงระบบคอมพิวเตอร์หรืออุปกรณ์การเก็บข้อมูลคอมพิวเตอร์ ต่างกับลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์ในรูปแบบเจาะระบบ หรือที่เรียกกันว่าแฮ็ก ซึ่งมีรูปแบบที่ผู้กระทำมีความสามารถเข้าถึง หรือเอาข้อมูลคอมพิวเตอร์ไปทั้งที่อยู่ห่างโดยระยะทางกับตัวเครื่องคอมพิวเตอร์หรืออุปกรณ์การเก็บข้อมูลคอมพิวเตอร์

รูปแบบการกระทำด้วยการเข้าถึงระบบคอมพิวเตอร์หรืออุปกรณ์การเก็บข้อมูลคอมพิวเตอร์อาจ เข้าถึงได้ 2 รูปแบบ คือ เข้าถึงโดยมีสิทธิ กับเข้าถึงโดยไม่มีสิทธิ

รูปแบบแรก เข้าถึงโดยมีสิทธิ การเข้าถึงโดยมีสิทธิ หมายถึง ผู้กระทำเอาข้อมูลคอมพิวเตอร์ไปนั้น มีรหัสผ่าน หรือได้รับอนุญาตให้เข้าถึงข้อมูลคอมพิวเตอร์ได้ แต่ไม่มีสิทธิสำเนาข้อมูลคอมพิวเตอร์ไป ซึ่งอาจเป็นกรณีมีสิทธิเข้าถึงข้อมูลคอมพิวเตอร์ เพื่อใช้ประโยชน์ภายใน

[4] น.ต.จตุชัย แพงจันทร์, *Master in Security*, ไอดีซีอินโฟดิสทริบิวเตอร์เซ็นเตอร์ จก. 2550

องค์กร แต่ไม่มีสิทธินำหรือสำเนาข้อมูลคอมพิวเตอร์ไปใช้สำหรับประโยชน์ส่วนตัวหรือประโยชน์ขององค์กรอื่น

รูปแบบที่สอง เข้าถึงโดยไม่มีสิทธิ การเข้าถึงโดยไม่มีสิทธิ หมายถึง ผู้กระทำเอาข้อมูลคอมพิวเตอร์ไปนั้น ไม่มีรหัสผ่าน หรือไม่ได้รับอนุญาตให้เข้าถึงข้อมูลคอมพิวเตอร์ได้ แต่ผู้กระทำอาจมีอุปกรณ์อิเล็กทรอนิกส์บางชนิดที่สามารถดักจับหรือดูดข้อมูลคอมพิวเตอร์ เช่น เครื่องสกิมเมอร์ (skimmer เครื่องดูดหรือกวาดข้อมูล) ซึ่งเป็นการเข้าถึงและโจรกรรมข้อมูลคอมพิวเตอร์ไปโดยไม่มีสิทธิเข้าถึงข้อมูลคอมพิวเตอร์ ซึ่งต่างจากอย่างรูปแบบแรก

เครื่องสกิมเมอร์ (skimmer เครื่องดูดหรือกวาดข้อมูล) เป็นอุปกรณ์ที่ผู้กระทำเพื่อให้ได้ข้อมูลคอมพิวเตอร์ไปโดยไม่มีสิทธิ มักใช้กับการสำเนาหรือโจรกรรมข้อมูลคอมพิวเตอร์ที่เกี่ยวกับบัตรเครดิต หรือบัตร เอ.ที.เอ็ม เป็นต้น

1.3 โจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยวิธีสามัญ

ลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์รูปแบบนี้ หมายถึง ผู้กระทำไม่ได้มีความเชี่ยวชาญระบบคอมพิวเตอร์อย่างการเจาะระบบ หรือที่เรียกกันว่าแฮ็ก หรือไม่มีการกระทำในรูปแบบที่เข้าถึงระบบคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ หรือไม่มีอุปกรณ์อิล็กทรอนิกส์อย่างเครื่องสกิมเมอร์ (skimmer เครื่องดูดหรือกวาดข้อมูล)

หากแต่ผู้กระทำมีลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์อย่างการกระทำสามัญธรรมดา ที่กล่าวว่าสามัญธรรมดา เช่น การจดจำ ซึ่งอาจจดจำด้วยการเห็นจากหน้าจอคอมพิวเตอร์ที่ผู้อื่นกำลังใช้งานตัวเครื่องหรือระบบคอมพิวเตอร์ หรืออาจจดจำจากที่ผู้ทรงสิทธิในการเข้าถึงตัวเครื่องหรือระบบคอมพิวเตอร์ หรืออุปกรณ์การเก็บข้อมูลคอมพิวเตอร์ที่จดใส่กระดาษไว้เป็นต้น

กรณีการโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยวิธีสามัญ เป็นการโจรกรรมหรือได้ไปที่ไม่ใช่อาชญากรรมทางเทคโนโลยี (hitech crime) ต่อเมื่อผู้ได้ไปซึ่งข้อมูลเหล่านั้นนำไปพิมพ์และนำเข้าระบบคอมพิวเตอร์ก็จะเป็นข้อมูลคอมพิวเตอร์ที่ตนเองไม่ใช่ผู้ทรงสิทธิ แต่เจ้าของหรือผู้ทรงสิทธิที่ตนไปโจรกรรมมาจึงเป็นผู้มีสิทธิโดยชอบด้วยกฎหมาย

2. กฎหมายอาญาของประเทศไทยเกี่ยวกับข้อมูลคอมพิวเตอร์

ตามขอบเขตของการศึกษาวิจัยฉบับนี้จะมุ่งศึกษาค้นคว้าความผิดอาญาตามประมวลกฎหมายอาญา กับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นด้านหลัก ซึ่งจะแบ่งออกเป็น 2 หัวข้อ ดังต่อไปนี้

2.1 ประมวลกฎหมายอาญา

2.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550[5]

2.1 ประมวลกฎหมายอาญา

บทบัญญัติที่กำหนดความผิดอาญาอันเกี่ยวข้องกับการสำเนาหรือโจรกรรมข้อมูลคอมพิวเตอร์ที่สำคัญซึ่งจะนำมาใช้ในการวิเคราะห์แบ่งออกเป็น 3 หัวข้อ ดังต่อไปนี้

2.1.1 ความผิดฐานลักทรัพย์

2.1.2 ความผิดเกี่ยวกับเอกสาร

2.1.3 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์

2.1.1 ความผิดฐานลักทรัพย์

ตามประมวลกฎหมายอาญา มาตรา 334 บัญญัติว่า *"ผู้ใดเอาทรัพย์ของผู้อื่นหรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วยไปโดยทุจริต ผู้นั้นกระทำความผิดฐานลักทรัพย์ ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินหกหมื่นบาท"*

องค์ประกอบของความผิดฐานลักทรัพย์ มีดังต่อไปนี้

องค์ประกอบภายนอก

1. ผู้ใด
2. เอาไป
3. ทรัพย์ของผู้อื่น หรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วย

องค์ประกอบภายใน

1. เจตนา
2. โดยทุจริต

ความผิดฐานลักทรัพย์ถูกนำมาบังคับใช้เพื่อปรับบทความผิดแก่ลักษณะแห่งการกระทำที่เกี่ยวกับอาชญากรรมทางเทคโนโลยีหลายครั้ง ซึ่งบางคดีศาลก็ปรับบทครอบคลุมการกระทำของจำเลยเป็นความผิดฐานลักทรัพย์ แต่ในระยะหลังบางคดีก็ไม่อาจปรับบทให้ครอบคลุมการกระทำของจำเลยเป็นความผิดฐานลักทรัพย์ได้ แม้ใช้นิติวิธีทางกฎหมาย คือ หลักการตีความกฎหมายก็ตาม เหตุเพราะความผิดฐานลักทรัพย์ตามบทบัญญัติมาตรา 334 ข้างต้นมีถ้อยคำที่ก่อให้เกิดปัญหาการตีความกฎหมายเพื่อปรับบังคับใช้กับข้อเท็จจริงที่เกิดขึ้น กล่าวคือ องค์ประกอบของความผิดที่ว่าด้วย **"ทรัพย์"** กับ **"เอาไป"**

---

[5] แก้ไขเพิ่มเติมล่าสุดโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

คำว่า **“ทรัพย์”** ตามมาตรา 334 ศาสตราจารย์ จิตติ ติงศภัทิย์ อธิบายไว้ว่า[6] ความหมายของคำว่าทรัพย์ในความผิดฐานลักทรัพย์ตามมาตรา 334 ของประมวลกฎหมายอาญานั้น หากเป็นวัตถุมีรูปร่างและมีเจ้าของย่อมเป็นทรัพย์ในความหมายของมาตรานี้ วัตถุมีรูปร่างอาจมีรูปร่างโดยตัวของมันเองหรือโดยอาศัยสิ่งอื่นเป็นรูปร่างก็ได้ เช่น น้ำในขวด น้ำมันในแกลลอน อากาศหรือแก๊สที่บรรจุกระป๋องหรือบรรจุในถังหรือไหลไปตามท่อส่งแก๊ส เป็นต้น

คำว่า **“เอาไป”** หมายความถึง การพาทรัพย์เคลื่อนที่ไปจากการครอบครองของผู้อื่น ซึ่งต้องมีการกระทำเป็นสองลักษณะ คือ “แย่งการครอบครอง” กับ “พาเคลื่อนที่ไป”

ลักษณะแห่งการกระทำที่จะเป็นการแย่งการครอบครองนั้น ทรัพย์ที่ลักจะต้องมีผู้ครอบครองอยู่ และผู้กระทำเข้าครอบครองทรัพย์นั้นโดยการเข้าแย่งการครอบครอง กล่าวคือ ผู้กระทำเข้าถือเอาการครอบครองโดยที่ผู้ครอบครองเดิมไม่ยินยอมหรือไม่อนุญาต เมื่อผู้กระทำแย่งการครอบครองแล้ว เช่นนี้ ลักษณะแห่งการกระทำของผู้กระทำจึงถึงขั้นที่กฎหมายอาญาถือว่าเป็นความผิด คือ ลงมือลักทรัพย์แล้ว ส่วนการลักทรัพย์จะถึงขั้นที่กฎหมายกำหนดเป็นความผิดสำเร็จหรือยังอยู่ในขั้นพยายาม จะต้องพิจารณาที่การพาทรัพย์เคลื่อนที่ไปจากจุดเดิมที่ทรัพย์ตั้งอยู่[7]

ดังนั้น ความผิดฐานลักทรัพย์ตามมาตรา 334 ทรัพย์ที่จะถูกลักต้องมีรูปร่างและต้องถือเอาได้ ในลักษณะที่สามารถถูกแย่งการครอบครองและถูกพาเคลื่อนที่ไปได้ ในทางกลับกันหากสิ่งที่จะถูกลัก ไม่ใช่สิ่งที่มีรูปร่างและไม่อาจถือเอาได้ ย่อมไม่เป็นสิ่งที่สามารถถูกแย่งการครอบครองและไม่สามารถถูกพาเคลื่อนที่ไปได้ จึงมิใช่สิ่งซึ่งอยู่ในความหมายของคำว่าทรัพย์ที่จะถูกลักได้

2.1.2 ความผิดเกี่ยวกับเอกสาร

ความผิดเกี่ยวกับเอกสารมีส่วนเกี่ยวข้องกับการกระทำโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ ด้วยเหตุจากมีคำพิพากษาฎีกาสองฉบับเข้ามาเกี่ยวข้อง คือ คำพิพากษาฎีกาที่ 5161/2547 กับคำพิพากษา ฎีกาที่ 4311/2557 ซึ่งวินิจฉัยแตกต่างกัน กล่าวคือ คำพิพากษาฎีกาที่ 5161/2547 ข้อมูลคอมพิวเตอร์ไม่ใช่เอกสาร แต่คำพิพากษาฎีกาที่ 4311/2557 คือประมาณ 10 ปีถัดมา วินิจฉัยว่าเครื่องคอมพิวเตอร์ คือ วัตถุอื่นใดตามความหมายของประมวลกฎหมายอาญา มาตรา 1 (7) เช่นนี้ ข้อมูลคอมพิวเตอร์ จึงอยู่ในความหมายของเอกสารไปด้วย

---

[6] จิตติ ติงศภัทิย์, *กฎหมายอาญา ภาค 2 ตอน 2 และภาค 3*, พิมพ์ครั้งที่ 3 กรุงเทพมหานคร:เนติบัณฑิตยสภา 2532, หน้า 2473-2477

[7] จิตติ ติงศภัทิย์, *กฎหมายอาญา ภาค 2 ตอน 2 และภาค 3*, หน้า 2495

บทบัญญัติของประมวลกฎหมายอาญาที่เกี่ยวข้องและจะนำมาวิเคราะห์กับงานวิจัยฉบับนี้ที่สำคัญมี 3 มาตรา คือ มาตรา 1 (7) มาตรา 188 และมาตรา 264 โดยที่มาตราสำคัญอยู่ที่มาตรา 1 (7) นิยามของคำว่า “เอกสาร”

มาตรา 1 (7) บัญญัติว่า *"เอกสาร" หมายความว่า กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ ปรากฏ ความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่นจะเป็นโดย วิธีพิมพ์ ถ่ายภาพหรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น*

จากบทบัญญัตินิยามของคำว่า **“เอกสาร”** เมื่อมีคำพิพากษาฎีกาที่ 4311/2557 เครื่องคอมพิวเตอร์ คือ วัตถุอื่นใดตามความหมายของประมวลกฎหมายอาญา มาตรา 1 (7) เช่นนี้ ข้อมูลคอมพิวเตอร์ จึงอยู่ในความหมายของเอกสารไปด้วย หากมีการโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปก็ต้องวิเคราะห์กับประมวลกฎหมายอาญา มาตรา 188 ความผิดฐาน “ทำให้เสียหาย ทำลาย เอาไปเสีย หรือทำให้ไร้ประโยชน์ซึ่งเอกสาร” หรือหากมีการเปลี่ยนแปลงแก้ไขข้อมูลคอมพิวเตอร์โดยไม่มีอำนาจก็ต้องวิเคราะห์ด้วยประมวลกฎหมายอาญา มาตรา 264 ความผิดฐาน “ปลอมเอกสาร”

บทบัญญัติประมวลกฎหมายอาญา มาตรา 188 กับมาตรา 264 มีดังนี้

ตามประมวลกฎหมายอาญา มาตรา 188 บัญญัติว่า *“ผู้ใดทำให้เสียหาย ทำลาย ซ่อนเร้น เอาไปเสีย หรือ ทำให้สูญหายหรือไร้ประโยชน์ ซึ่งพินัยกรรมหรือเอกสารใดของผู้อื่นในประการที่น่าจะเกิดความ เสียหายแก่ผู้อื่นหรือประชาชนต้องระวาง โทษจำคุกไม่เกินห้าปีและปรับไม่เกินหนึ่งแสนบาท”*

องค์ประกอบของความผิดฐานเอาไปเสียซึ่งเอกสาร มีดังต่อไปนี้

องค์ประกอบภายนอก

1. ผู้ใด
2. ทำให้เสียหาย ทำลาย ซ่อนเร้น เอาไปเสีย หรือ ทำให้สูญหายหรือไร้ประโยชน์
3. ซึ่งพินัยกรรมหรือเอกสารใดของผู้อื่น

พฤติการณ์ประกอบการกระทำ

1. ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

องค์ประกอบภายใน

1. เจตนา

ตามประมวลกฎหมายอาญา มาตรา 264 บัญญัติว่า

“ผู้ใดทำเอกสารปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด เติมหรือตัดทอนข้อความ หรือแก้ไข ด้วยประการใดๆ ในเอกสารที่แท้จริงหรือประทับตราปลอม หรือลงลายมือชื่อปลอมในเอกสาร โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ถ้าได้กระทำเพื่อให้

ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารที่แท้จริง ผู้นั้นกระทำความผิดฐานปลอมเอกสารต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดกรอกข้อความลงในแผ่นกระดาษหรือวัตถุอื่นใด ซึ่งมีลายมือชื่อของผู้อื่นโดยไม่ได้รับ ความยินยอม หรือโดยฝ่าฝืนคำสั่งของผู้อื่นนั้น ถ้าได้กระทำเพื่อนำเอาเอกสารนั้นไปใช้ในกิจการที่ อาจเกิดเสียหายแก่ผู้หนึ่งผู้ใดหรือประชาชน ให้ถือว่าผู้นั้นปลอมเอกสาร ต้องระวางโทษเช่นเดียวกัน"

องค์ประกอบของความผิดฐานปลอมเอกสารวรรคแรก มีดังต่อไปนี้

องค์ประกอบภายนอก

1. ผู้ใด
2. "ผู้ใดทำปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด เติมหรือตัดทอนข้อความหรือแก้ไขด้วยประการใดๆ ในเอกสารที่แท้จริง หรือประทับตราปลอม หรือลงลายมือชื่อปลอม
3. เอกสาร

พฤติการณ์ประกอบการกระทำ

1. ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

องค์ประกอบภายใน

1. เจตนา
2. ถ้าได้กระทำเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารที่แท้จริง

จากคำพิพากษาฎีกาที่ 4311/2557 ซึ่งวินิจฉัยว่าเครื่องคอมพิวเตอร์ คือ วัตถุอื่นใดตามความหมายของประมวลกฎหมายอาญา มาตรา 1 (7) กรณีเช่นนี้ ข้อมูลคอมพิวเตอร์จึงอยู่ในความหมายของเอกสาร เมื่อมีการแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์โดยไม่มีอำนาจซึ่งข้อมูลคอมพิวเตอร์เป็นเอกสารตามคำวินิจฉัยของศาลฎีกา จึงมีความผิดฐานปลอมเอกสารตามประมวลกฎหมายอาญา มาตรา 264

เมื่อข้อมูลคอมพิวเตอร์เป็นเอกสารตามคำวินิจฉัยของศาลฎีกา การกระทำให้ข้อมูลคอมพิวเตอร์เสียหาย ทำลาย ทำให้ไร้ประโยชน์ จึงสามารถผิดมาตรา 188 ตามประมวลกฎหมายอาญาได้[8]

---

[8] เกียรติขจร วัจนะสวัสดิ์, *คำบรรยายเนติบัณฑิตกฎหมายอาญา มาตรา 59-106* , เล่ม 4 หน้า 290 วันที่ 17 มิถุนายน 2559 *https://web.facebook.com/permalink.php?story_fbid=156796628063950&id=136630040080609&hc_location=ufi* สืบค้นเมื่อวันที่ 28 พฤศจิกายน 2560

ข้อสังเกต

ประการแรก ตามมาตรา 188 มีองค์ประกอบความผิดอันเป็นลักษณะการกระทำหนึ่ง คือ “เอาไปเสีย” ซึ่งมีลักษณะแห่งการกระทำไม่ต่างจากการ “เอาไป” ของความผิดฐานลักทรัพย์ กล่าวคือ ต้องมีการกระทำเป็นสองลักษณะ คือ “แย่งการครอบครอง” กับ “พาเคลื่อนที่ไป” ดังที่ได้วิเคราะห์อย่างละเอียดแล้ว ตามหัวข้อก่อนหน้า คือ 2.1.1 ความผิดฐานลักทรัพย์

ดังนั้น ข้อมูลคอมพิวเตอร์ที่ถูกสำเนาหรือโจรกรรมไป จึงไม่สามารถเป็นความผิดฐาน “เอาไปเสียซึ่งเอกสาร” ตามมาตรา 188 แห่งประมวลกฎหมายอาญาได้

ประการที่สอง ตามคำพิพากษาฎีกาที่ 4311/2557 ซึ่งวินิจฉัยไว้ว่าเครื่องคอมพิวเตอร์ คือ วัตถุอื่นใดตามความหมายของประมวลกฎหมายอาญา มาตรา 1 (7) กรณีเช่นนี้ข้อมูลคอมพิวเตอร์ จึงอยู่ในความหมายของเอกสาร ผู้วิจัยไม่เห็นพ้องด้วย เพราะเหตุว่า จากความหมายของบทนิยามคำว่าเอกสาร ตามประมวลกฎหมายอาญา มาตรา 1 (7) ที่บัญญัติว่า *"เอกสาร" หมายความว่า กระดาษหรือวัตถุอื่นใดซึ่งได้ ทำให้ ปรากฏ ความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผน แบบอย่างอื่นจะเป็นโดย วิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็น หลักฐานแห่งความหมายนั้น*

เอกสารต้องเป็นการที่บุคคลทำขึ้นเพื่อสื่อความหมาย ซึ่งผู้อื่นต้องสามารถประจักษ์แก่สายตา และสามารถเข้าใจความหมายของตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น หากไม่สามารถเข้าใจความหมายได้ ย่อมไม่ใช่เอกสารตามบทนิยามแห่งมาตรา 1 (7) ของประมวลกฎหมายอาญา

กรณีข้อมูลคอมพิวเตอร์มิได้ประจักษ์แก่สายตาในลักษณะที่สามารถสื่อความหมายได้ในตัวเอง โดยสภาพของข้อมูลคอมพิวเตอร์ที่อยู่บนฮาร์ดดิสก์ หรือแผ่นซีดี แผ่นดีวีดี หรือวัตถุอื่นใด เป็นสัญลักษณ์ภาษาที่บุคคลทั่วไปไม่สามารถประจักษ์แก่สายตา ไม่สามารถอ่านหรือเข้าใจความหมายของสัญลักษณ์ภาษาคอมพิวเตอร์ได้ ซึ่งหากจะสื่อความหมายต้องผ่านขั้นตอนกระบวนการแปลงข้อมูลคอมพิวเตอร์ด้วยเครื่องหรือซีพียูหรืออุปกรณ์ประมวลผลทางคอมพิวเตอร์อีกชั้นหนึ่ง ทำนองเดียวกับเครื่องจักรหรือนาฬิกาที่เดินไปด้วยกลไกของอุปกรณ์หรืออะหลั่ยต่างๆ ที่นำมาประกอบเป็นนาฬิกา ซึ่งไม่ใช่บุคคลทำให้สื่อความหมาย หากแต่เป็นเครื่องหรือซีพียูหรืออุปกรณ์ประมวลผลทางคอมพิวเตอร์ทำให้ปรากฏเป็นตัว อักษร ตัวเลข ผัง หรือแผน แบบอย่างอื่น และข้อมูลคอมพิวเตอร์ยังมิได้มีรูปลักษณ์ที่คงทนถาวรเพียงพอใช้เป็นพยานหลักฐานในรูปเอกสารได้

ดังนั้น ข้อมูลคอมพิวเตอร์จึงมิใช่เอกสารตามความหมายของมาตรา 1 (7) เช่นนี้ หากมีผู้ทำให้เสียหาย ทำลาย หรือทำให้สูญหาย หรือไร้ประโยชน์ แก่ข้อมูลคอมพิวเตอร์ก็ย่อมไม่ครบองค์ประกอบ ความผิดตามมาตรา 188 แห่งประมวลกฎหมายอาญาไปได้ อีกทั้งการ

กระทำที่ก่อให้เกิดความเสียหายแก่ข้อมูลคอมพิวเตอร์ เช่น การทำปลอม การทำแปลง การทำเท็จเกี่ยวกับเอกสาร จึงไม่อาจปรับบทความผิดเกี่ยวกับเอกสารแก่ผู้กระทำได้

2.1.3 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์

ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์มีส่วนเกี่ยวข้องกับข้อมูลคอมพิวเตอร์ในลักษณะที่หากบัตรอิเล็กทรอนิกส์อยู่ในรูปข้อมูลคอมพิวเตอร์ เมื่อถูกโจรกรรมหรือสำเนาไป ย่อมเกี่ยวพันโดยตรง แต่ฐานความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ มีบทบัญญัติระบุความผิดและโทษเกี่ยวกับการโจรกรรม หรือสำเนาข้อมูลคอมพิวเตอร์ไปหรือไม่ จักได้วิเคราะห์ในบทที่ 4

บทบัญญัติตามประมวลกฎหมายอาญาที่เกี่ยวกับบัตรอิเล็กทรอนิกส์มีอยู่ตามมาตรา 1 (14) มาตรา 8 และมาตรา 269/1 ถึงมาตรา 269/7 โดยประเด็นที่ต้องวิเคราะห์เป็นสำคัญเบื้องแรก คือ บัตรอิเล็กทรอนิกส์ที่มีอยู่ 4 ประเภท คือ บัตรอิเล็กทรอนิกส์ในรูปเอกสาร กับในรูปวัตถุอื่นใด ตามมาตรา 1 (14) (ก) บัตรอิเล็กทรอนิกส์ที่ไม่ได้ออกให้ผู้ทรงสิทธิในรูปเอกสาร หรือไม่ได้ออกให้ผู้ทรงสิทธิในรูปวัตถุอื่นใด ตามมาตรา 1 (14) (ข) และบัตรอิเล็กทรอนิกส์ที่อยู่ในรูปสิ่งอื่นใด ตามมาตรา 1 (14) (ค) ซึ่งบัตรอิเล็กทรอนิกส์ที่มีอยู่ 4 ประเภทนี้อยู่ในความหมายของข้อมูลคอมพิวเตอร์หรือไม่ หากบัตรอิเล็กทรอนิกส์ประเภทนั้น ๆ เป็นข้อมูลคอมพิวเตอร์ บทบัญญัติที่ระบุฐานความผิดตามมาตรา 269/1 ถึงมาตรา 269/7 ก็จะถูกนำมาวิเคราะห์ด้วย หากบัตรอิเล็กทรอนิกส์ประเภทนั้น ๆ ไม่เป็นข้อมูลคอมพิวเตอร์ บทบัญญัติ มาตรา 269/1 ถึงมาตรา 269/7 ก็จะไม่เกี่ยวข้องกับการโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์

ทั้งบทบัญญัติฐานลักทรัพย์ บทบัญญัติความผิดเกี่ยวกับเอกสาร และบทบัญญัติความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ จักได้วิเคราะห์ควบคู่กับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และกฎหมายอาญาต่างประเทศเกี่ยวกับการคุ้มครองข้อมูลคอมพิวเตอร์ ในบทที่ 4 วิเคราะห์ปัญหากฎหมายอาญาเกี่ยวกับการคุ้มครองข้อมูลคอมพิวเตอร์ต่อไป

2.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีส่วนเกี่ยวพันกับบัตรอิเล็กทรอนิกส์เช่นเดียวกัน เพราะเหตุว่า กฎหมายฉบับนี้บัญญัติบทนิยาม ฐานความผิดทางอาญา ซึ่งมีลักษณะคาบเกี่ยวกับบทนิยามความหมายและฐานความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ โดยที่ลักษณะแห่งการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์บางฐานความผิดต้องด้วยความผิดทางอาญาตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกรรมเดียวผิดกฎหมายหลายบท และบางกรณีลักษณะแห่งการกระทำเป็นช่องว่างแห่งกฎหมายของความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ แต่ก็สามารถปรับบทความผิดและลงโทษตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.2550 ฉบับนี้ได้ รวมทั้งบัตรอิเล็กทรอนิกส์บางประเภทก็มีที่ใช้กับระบบคอมพิวเตอร์ เช่น ชื่อผู้ใช้จดหมายอิเล็กทรอนิกส์ (usernamr) รหัสผ่านจดหมายอิเล็กทรอนิกส์ (password) ชื่อผู้ใช้และรหัสผ่านเข้าใช้อินเทอร์เน็ตทั้งระบบส่งสัญญาณผ่านสื่อที่เป็นสาย และระบบไวเลส (wireless) รหัสผ่านเข้าใช้และลงโปรแกรมคอมพิวเตอร์หรือเกมคอมพิวเตอร์ (serial number)[9] เป็นต้น ชื่อผู้ใช้และรหัสผ่านหรือรหัสลงโปรแกรมเหล่านี้อยู่ในความหมายของบัตรอิเล็กทรอนิกส์ ตามประมวลกฎหมายอาญา มาตรา 1 (14) (ข)

ส่วนลายมือชื่ออิเล็กทรอนิกส์[10] อยู่ในความหมายของบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา มาตรา 1 (14) (ค)

กฎหมายทั้งสามฉบับ คือ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ประมวลกฎหมายอาญาว่าด้วยความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ตามประมวลกฎหมายอาญา และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีความเชื่อมโยงระหว่างกัน โดยที่มีการตรากฎหมายหรือแก้ไขเพิ่มเติมกฎหมายใหม่ออกมาเรียงตามลำดับดังกล่าวข้างต้น จึงจำเป็นต้องวิเคราะห์ถึงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับบางประการเฉพาะส่วนที่เกี่ยวข้องกับประมวลกฎหมายอาญาว่าด้วยความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ เช่น บทนิยาม และฐานความผิดทางอาญาบางฐาน โดยไม่รวมถึงบทบัญญัติที่เกี่ยวกับความเป็นพยานหลักฐานและไม่รวมถึงที่เกี่ยวกับวิธีพิจารณาความ ซึ่งอยู่นอกเหนือวัตถุประสงค์และขอบเขตการศึกษาวิจัย

---

[9] มหาวิทยาลัยสุโขทัยธรรมาธิราช, *เอกสารการสอนชุดวิชากฎหมายอาญา 2 : ภาคความผิด* หน่วยที่ 1-5, หน้า 5-133

[10] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

สาระสำคัญของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่เกี่ยวข้องกับความผิดเกี่ยวกับข้อมูลคอมพิวเตอร์ที่จะวิเคราะห์ถึงจะแบ่งออกเป็น 3 หัวข้อ ดังนี้

2.2.1 หลักการและเหตุผล

2.2.2 บทนิยาม

2.2.3 ฐานความผิดทางอาญา

2.2.1 หลักการและเหตุผล

หลักการและเหตุผลของการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งปรากฏอยู่ท้ายพระราชบัญญัติ มีดังต่อไปนี้[11]

> ***"เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใดๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้"***

ข้อความของหลักการและเหตุผลตามพระราชบัญญัติฉบับนี้ กล่าวให้เห็นถึงความสำคัญของระบบคอมพิวเตอร์ที่มีส่วนต่อการดำเนินวิถีชีวิตประจำวัน การกระทำที่ก่อให้เกิดความเสียหายต่างๆ จึงต้องกำหนดเป็นความผิดและมีโทษทางอาญา เพราะเหตุว่าฐานความผิดต่างๆ ที่มีอยู่ตามประมวลกฎหมายอาญาไม่อาจครอบคลุมลักษณะแห่งการกระทำที่ก่อให้เกิดความเสียหายผ่านระบบคอมพิวเตอร์ได้ และระบบคอมพิวเตอร์บางกรณีการจะเข้าถึงได้อาจต้องมีชื่อผู้ใช้และ

---

[11] *ราชกิจจานุเบกษา เล่ม 128 ตอน 27 ก* วันที่ 18 มิถุนายน 2550

รหัสผ่านเข้าใช้ ซึ่งชื่อผู้ใช้และรหัสผ่านเข้าใช้ก็คือบัตรอิเล็กทรอนิกส์ตามที่กล่าวไว้แล้ว อีกทั้งระบบคอมพิวเตอร์ยังมีการเชื่อมโยงกับอุปกรณ์อิเล็กทรอนิกส์ต่างๆ อีกด้วย ซึ่งเป็นระบบคอมพิวเตอร์และอุปกรณ์ที่มีไว้บริการประชาชน โดยที่การเข้าถึงจะต้องมีรหัสผ่าน เช่น เครื่องฝาก-ถอนเงินสดอัตโนมัติ และรหัสบัตร เอ.ที.เอ็ม เป็นต้น

2.2.2 บทนิยาม

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดความหมายของถ้อยคำเป็นบทนิยามไว้ในมาตรา 3 โดยมีบทนิยามที่เกี่ยวข้องกับความผิดเกี่ยวกับข้อมูลคอมพิวเตอร์ ดังนี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

บทบัญญัติกำหนดความหมายของคำว่า **“ระบบคอมพิวเตอร์”** ดังกล่าว มีความหมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์และระบบปฏิบัติการหรือโปรแกรมต่างๆ ซึ่งรู้จักกันทั่วไปในชื่อที่เรียกว่า ฮาร์ดแวร์และซอฟต์แวร์ ที่พัฒนาขึ้นเพื่อประมวลผลข้อมูลแบบดิจิตัล (digital data) ซึ่งประกอบไปด้วยตัวเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (peripheral) ต่างๆ สำหรับการป้อนข้อมูล (input) หรือแสดงผลข้อมูล (output) และบันทึกหรือเก็บข้อมูล (store and record)

ระบบคอมพิวเตอร์จึงอาจเป็นตัวเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงเพียงเครื่องเดียว หรืออาจเป็นตัวเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงหลายเครื่อง อันมีลักษณะเป็นชุดเชื่อมต่อกัน โดยอาจเชื่อมต่อผ่านระบบเครือข่ายภายในที่เรียกว่าระบบแลน (LAN: Local Area Network) หรืออาจเป็นระบบอินทราเน็ต (intranet) หรือเชื่อมต่อผ่านระบบเครือข่ายภายนอกที่เรียกว่าระบบอินเทอร์เน็ต (internet) ก็ได้ และอาจเป็นการเชื่อมต่อกันผ่านสัญญาณที่ส่งไปกับสื่อที่เป็นสายหรือผ่านสัญญาณแบบไวเลส (wireless) ก็ได้ และทั้งต้องมีลักษณะการทำงานโดยอัตโนมัติตามโปรแกรมหรือซอฟต์แวร์ที่กำหนดไว้

เมื่อบทนิยามกำหนดความหมายของระบบคอมพิวเตอร์ไว้ว่าให้หมายความถึง **“ต้องมีลักษณะการทำงานโดยอัตโนมัติตามโปรแกรมหรือซอฟต์แวร์ที่กำหนดไว้”** ด้วย ดังนั้น ลำพังเครื่องคอมพิวเตอร์ที่ยังมิได้ลงโปรแกรมหรือซอฟต์แวร์ให้สามารถทำงานหรือประมวลผลข้อมูล

โดยอัตโนมัติแล้ว เช่น โน้ตบุ้คที่ซื้อมายังไม่ถือว่าเป็น “ระบบคอมพิวเตอร์” จนกว่าจะได้มีการทำงานผ่านระบบเครือข่ายหรือโดยซอฟต์แวร์[12]

ข้อสังเกต ความหมายของระบบคอมพิวเตอร์ที่ระบุไว้ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ข้างต้นย่อมหมายความรวมถึงเครื่องฝาก-ถอนเงินสดอัตโนมัติด้วย เนื่องจากเครื่องฝาก-ถอนเงินสดอัตโนมัติก็เป็นอุปกรณ์หรือชุดอุปกรณ์หรืออุปกรณ์ต่อพ่วง และตัวเครื่องคอมพิวเตอร์ที่เชื่อมต่อกัน โดยเชื่อมต่อผ่านระบบเครือข่ายที่มีระบบปฏิบัติการหรือโปรแกรม หรือซอฟต์แวร์ที่กำหนดให้ทำงานหรือประมวลผลข้อมูลโดยอัตโนมัติอยู่ด้วย ดังนั้น การกระทำใดๆ ที่ก่อความเสียหายแก่ผู้อื่นผ่านเครื่องฝาก-ถอนเงินสดอัตโนมัติ หากครบองค์ประกอบของความผิดฐานใดๆ ที่พระราชบัญญัติฉบับนี้กำหนดไว้ ก็จะเป็นความผิดและมีโทษทางอาญา

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

คำว่า **“ข้อมูลคอมพิวเตอร์”** ตามบทนิยามข้างต้น หมายถึง ข้อมูลหรือชุดคำสั่งทุกอย่างที่อยู่ในระบบคอมพิวเตอร์ รวมทั้งสิ่งอื่นใดซึ่งมีความหมายกว้างขวางอย่างมาก ขอเพียงอยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้

นอกจากนี้ ข้อมูลคอมพิวเตอร์ยังให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย ซึ่ง “ข้อมูลอิเล็กทรอนิกส์” อาจมิได้สร้างขึ้นด้วยระบบคอมพิวเตอร์ก็ได้ เช่น การสร้างขึ้นด้วยโทรเลข โทรพิมพ์ โทรสาร หรือโทรศัพท์เคลื่อนที่ (สมาร์ทโฟนบางรุ่นอาจเป็นระบบคอมพิวเตอร์) เพื่อให้ครอบคลุมถึงข้อมูลประเภทอื่นๆ ที่สร้างขึ้นด้วยวิธีการทางอิเล็กทรอนิกส์อื่นๆ ที่ไม่ใช่เทคโนโลยีคอมพิวเตอร์

อนึ่ง ฐานความผิดตามพระราชบัญญัติฉบับนี้หลายฐานจะเชื่อมโยง “ข้อมูลคอมพิวเตอร์” กับ “ระบบคอมพิวเตอร์” เข้าด้วยกันเป็นองค์ประกอบของความผิด ดังนั้น กรณีของโทรเลข โทรพิมพ์ หรือโทรสาร หากจะเป็นความผิดลักษณะแห่งการกระทำต้องเชื่อมโยงกับระบบคอมพิวเตอร์ เช่น การดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์โดยมิชอบ ตามมาตรา 8 กล่าวคือ ต้องเป็นกรณีที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ แต่หากเป็นการดักรับโทรเลข โทรพิมพ์ หรือโทรสารที่

---

[12] พรเพชร วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550* หน้า 4 เว็บไซต์มหาวิทยาลัยเชียงใหม่ *http://www.med.cmu.ac.th/home/file/cc_act_exp.pdf* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

ไม่ได้ส่งในระบบคอมพิวเตอร์ เช่นนี้ ย่อมไม่เป็นความผิดตามมาตรา 8 ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นต้น[13]

ข้อสังเกต

บัตรอิเล็กทรอนิกส์บางประเภทที่มิได้อยู่ในรูปเอกสารหรือวัตถุอื่นใดที่เก็บบันทึกไว้ในระบบคอมพิวเตอร์ ตามประมวลกฎหมายอาญา มาตรา 1 (14) (ข) และ (ค) หากอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ บัตรอิเล็กทรอนิกส์นั้นก็อยู่ในความหมายของข้อมูลคอมพิวเตอร์ตามบทนิยามนี้เช่นกัน อาทิ รหัส เอ.ที.เอ็ม ที่บันทึกไว้ในระบบปฏิบัติการของเครือข่ายเครื่องฝาก-ถอนเงินสดอัตโนมัติ หรือลายนิ้วมือ ลายมือ ลายเท้า ลายเส้นเลือดบนจอประสาทตา (retina)[14] ลายมือชื่ออิเล็กทรอนิกส์ที่บันทึกไว้ในระบบคอมพิวเตอร์และอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ เป็นต้น

2.2.3 ฐานความผิดทางอาญา

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดฐานความผิดบางฐานที่มีความเชื่อมโยงกับความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ โดยลักษณะแห่งการกระทำหนึ่งอาจเป็นความผิดทั้งประมวลกฎหมายอาญาความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ และเป็นความผิดตามพระราชบัญญัตินี้ด้วย กล่าวคือ เป็นกรรมเดียวผิดกฎหมายหลายบท แต่บางลักษณะแห่งการกระทำไม่เข้าองค์ประกอบความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ แต่สามารถปรับใช้บทบัญญัติความผิดตามพระราชบัญญัติฉบับนี้ได้ จึงกล่าวได้ว่า ช่องว่างแห่งกฎหมายของความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญานั้นสามารถใช้บทกฎหมายหรือฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ช่วยได้บ้างแต่ก็ไม่ทั้งหมด

ฐานความผิดตามพระราชบัญญัติฉบับนี้ที่มีส่วนเกี่ยวข้องกับข้อมูลคอมพิวเตอร์และเชื่อมโยงกับความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ซึ่งจะได้วิเคราะห์เรียงมาตราดังต่อไปนี้

1) ความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ มาตรา 5 บัญญัติว่า *“ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง โดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือนหรือปรับไม่เกิน หนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ”*

---

[13] พรเพชร วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*, หน้า 4-5

[14] มหาวิทยาลัยสุโขทัยธรรมาธิราช, *เอกสารการสอนชุดวิชากฎหมายอาญา 2 : ภาคความผิด* หน่วยที่ 1-5, หน้า 5-134

องค์ประกอบของความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบมีดังต่อไปนี้

องค์ประกอบภายนอก

1. ผู้ใด
2. เข้าถึงโดยมิชอบ
3. ซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

องค์ประกอบภายใน

เจตนา

ความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบนี้กล่าวได้ว่ามีที่มาจากบทบัญญัติของกฎหมายต่างประเทศที่เรียกว่าความผิดฐานเข้าถึง (Access) เช่น กฎหมายของประเทศสหรัฐอเมริกา Section 1030 Title 18 of the United States Code[15] เป็นต้น

ความผิดฐาน **“เข้าถึง”** เป็นความผิดที่ถือว่าเป็นความผิดพื้นฐานหรือบททั่วไปของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และยังเป็นความผิดที่อาจเป็นจุดเริ่มต้นในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฐานอื่นต่อไป เช่น การเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ตามมาตรา 7 หรือการดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ตามมาตรา 8 หรือการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติม ข้อมูลคอมพิวเตอร์โดยมิชอบ ตามมาตรา 9 เป็นต้น

การเข้าถึงนี้บางกรณีอาจเป็นการเข้าถึงตัวเครื่องคอมพิวเตอร์โดยตรง กล่าวคือ เครื่องคอมพิวเตอร์นั้นมีการตั้งค่ากำหนดรหัสผ่าน[16] เพื่อป้องกันมิให้บุคคลอื่นเข้าใช้เครื่องคอมพิวเตอร์ ผู้กระทำความผิดอาจดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและเข้าถึงหรือเข้าใช้เครื่องคอมพิวเตอร์นั้นๆ โดยนั่งอยู่หน้าตัวเครื่องคอมพิวเตอร์นั้นเอง หรือบางกรณีอาจเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์ โดยที่ผู้กระทำความผิดไม่ต้องเข้าถึงตัวเครื่องคอมพิวเตอร์ แต่ใช้วิธีเข้าถึงผ่านระบบอินเทอร์เน็ตเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการก็ได้

การเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์นี้อาจเป็นลักษณะเข้าถึงทั้งหมดหรือแต่บางส่วนก็ได้ เช่นนี้ อาจเข้าถึงฮาร์ดแวร์หรืออุปกรณ์ต่อพ่วงส่วนประกอบต่างๆ

---

[15] National Criminal Justice Information and Statistics Service, Law Enforcement Assistance Administration, U.S. Department of Justice, *COMPUTER CRIME:Criminal Justice Resource Manual* Washington D.C.:U.S. Government Printing Office 1979 P.145

[16] รหัสผ่านนี้ คือ บัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา มาตรา 1 (14) (ข)

ของคอมพิวเตอร์ ฮาร์ดดิสก์สำรอง หรือหน่วยความจำต่าง ๆ ที่ต่อพ่วงกับตัวเครื่องคอมพิวเตอร์ ซึ่งบันทึกข้อมูลเก็บไว้ในระบบเพื่อใช้ สำหรับการส่งหรือโอนถึงบุคคลใดบุคคลหนึ่ง หรืออาจเข้าถึงระบบคอมพิวเตอร์เพื่อเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ เช่น หมายเลขไอพี (IP address) ก็เข้าข่ายองค์ประกอบของความผิดนี้เช่นกัน

ส่วนช่องทางที่จะเข้าถึงนั้นอาจด้วยวิธีการต่าง ๆ ไม่ว่าจะเข้าถึงโดยผ่านทางเครือข่ายภายนอก หรืออาจเรียกว่าเครือข่ายสาธารณะ กล่าวคือ อินเทอร์เน็ต อันเป็นการเชื่อมโยงระหว่างเครือข่ายหลาย ๆ เครือข่ายเข้าด้วยกัน หรืออาจเข้าถึงโดยช่องทางผ่านระบบเครือข่ายเดียวกันหรือเครือข่ายภายในที่เรียกว่า ระบบแลน (LAN : local area network) อันเป็นเครือขายที่เชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้ๆ เข้าด้วยกัน และรวมถึงลักษณะการเข้าถึงโดยผ่านช่องทางการติดต่อสื่อสารแบบไร้สายหรือที่เรียกว่า ไวเลส (wireless) อีกด้วย

องค์ประกอบความของผิด “เข้าถึง” ต้องเป็นการเข้าถึง **“โดยมิชอบ”** หมายความว่า จะต้องเป็นการเข้าถึงโดยปราศจากสิทธิโดยชอบธรรม (without right) หรือปราศจากอำนาจตามกฎหมายที่จะเข้าถึง หรือไม่ได้รับความยินยอมหรือไม่ได้รับอนุญาตจากผู้ทรงสิทธิที่จะยินยอมหรืออนุญาต ในทางกลับกัน หากบุคคลที่เข้าถึงนั้นเป็นบุคคลที่มีสิทธิ ไม่ว่าด้วยถือสิทธิตามกฎหมาย หรือได้รับความยินยอมหรือได้รับอนุญาตจากเจ้าของระบบหรือผู้ทรงสิทธิ เช่น การเข้าถึงเพื่อดูแลระบบของผู้ดูแลเว็บไซต์ (webmaster) เป็นต้น

อนึ่ง หากบุคคลผู้ได้รับอนุญาตให้ทำการเข้าถึงนั้นได้กระทำการเข้าถึงระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์เกินกว่าที่ตนได้รับความยินยอมหรือได้รับอนุญาต เช่นนี้ ลักษณะแห่งการกระทำของบุคคลดังกล่าวก็เป็นการเข้าถึงโดยมิชอบ ตามความหมายนี้เช่นเดียวกัน[17]

องค์ประกอบของความผิดประการต่อมา คือ ระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน มาตรการการเข้าถึงโดยเฉพาะ หมายความว่า ระบบคอมพิวเตอร์นั้นๆ มีการกำหนดค่ารหัสผ่านไว้ ซึ่งอาจเป็นค่ารหัสการเข้าใช้ตัวเครื่องคอมพิวเตอร์ หรือค่ารหัสการเข้าใช้จดหมายอิเล็กทรอนิกส์ (e-mail) ทั้งชื่อผู้ใช้ (username) และรหัสผ่าน (password) หรือชื่อผู้ใช้ และรหัสผ่านเข้าใช้อินเทอร์เน็ตทั้งระบบส่งสัญญาณผ่านสื่อที่เป็นสายและระบบไวเลส (wireless) หรือ รหัสผ่านเข้าใช้เกมคอมพิวเตอร์ออนไลน์ หรือรหัสบัตร เอ.ที.เอ็ม สำหรับฝาก-ถอนเงินสดอัตโนมัติ ค่ารหัสผ่านเหล่านี้มีไว้สำหรับผู้ทรงสิทธิเท่านั้น มิใช่มีไว้เพื่อคนทั่วไปหรือเพื่อสาธารณะประโยชน์ บุคคลผู้เข้าถึงระบบคอมพิวเตอร์ที่มีการตั้ง

---

[17] พรเพชร วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*, หน้า 9

ค่ารหัสผ่านเหล่านี้ก็คือเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนนั่นเอง

ข้อสังเกต

บุคคลผู้เข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนนั้น หากวิเคราะห์ถึงคำพิพากษาฎีกาทั้ง 6 ฉบับ คือ คำพิพากษาฎีกาที่ 613/2540 คำพิพากษาฎีกาที่ 9/2543 คำพิพากษาฎีกาที่ 310/2546 คำพิพากษาฎีกาที่ 4165/2549 คำพิพากษาฎีกาที่ 2512/2550 คำพิพากษาฎีกาที่ 464/2551 ซึ่งข้อเท็จจริงไม่ว่าจะเป็นการลักบัตร เอ.ที.เอ็ม และได้รหัส เอ.ที.เอ็ม ไปใช้เบิกถอนเงินจากเครื่องฝาก-ถอนเงินสดอัตโนมัติ หรือกรณีพนักงานของสถาบันการเงิน ปลอมและใช้เอกสารปลอมของลูกค้าไปทำบัตร เอ.ที.เอ็ม จะได้บัตรและรหัส เอ.ที.เอ็ม ไปใช้เบิกถอนเงินจากเครื่องฝาก-ถอนเงินสดอัตโนมัติก็ตาม นอกจากเป็นความผิดตามมาตรา 269/5 ประกอบมาตรา 269/7 ในเรื่องความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์แล้ว ยังเป็นการเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน จึงครบองค์ประกอบของความผิดตามมาตรานี้ด้วย

2) ความผิดฐานการเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะโดยมิชอบ มาตรา 6 บัญญัติว่า *“ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ”*

องค์ประกอบของความผิดฐานการเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะโดยมิชอบ มีดังต่อไปนี้

องค์ประกอบภายนอก

1. ผู้ใด
2. ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ
3. ถ้านำไปเปิดเผยโดยมิชอบ
4. โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

องค์ประกอบภายใน

เจตนา

ความผิดฐานนี้มีวัตถุประสงค์คุ้มครองมิให้บุคคลที่ล่วงรู้นำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไปเปิดเผย

การที่ได้ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์นี้จะเป็นการล่วงรู้มาโดยชอบ คือ มีสิทธิรู้ หรืออาจล่วงรู้มาโดยมิชอบ คือ ไม่มีสิทธิรู้ก็ได้ แต่เมื่อรู้แล้วนำไปเปิดเผยแก่ผู้อื่น จะเป็นการเปิดเผยต่อบุคคลคนเดียวหรือหลายคนก็อยู่ในความหมายนี้[18] และการเปิดเผยนี้จะเป็นการเปิดเผยแบบให้เปล่าไม่มีค่าตอบแทน หรือจะเป็นการเปิดเผยแบบมีค่าตอบแทน หรือจำหน่าย หรือขายก็ได้

ประการสำคัญอยู่ที่ต้องเป็นการเปิดเผยโดยมิชอบ หมายความว่า เป็นการเปิดเผยโดยปราศจากสิทธิโดยชอบธรรม (without right) หรือปราศจากอำนาจตามกฎหมายที่จะเปิดเผย หรือไม่ได้รับความยินยอมหรือไม่ได้รับอนุญาตจากผู้ทรงสิทธิที่จะยินยอมหรืออนุญาต

ข้อสังเกต

ฐานความผิดนี้สามารถนำไปใช้ปรับบทสำหรับลักษณะแห่งการกระทำที่มีความเชื่อมโยงถึงความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ได้ในบางกรณี โดยเฉพาะในส่วนที่ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ยังมีช่องโหว่อยู่ เช่น การล่วงรู้ค่ารหัสการเข้าใช้จดหมายอิเล็กทรอนิกส์ (e-mail) ทั้งชื่อผู้ใช้ (username) และรหัสผ่าน (password) ซึ่งคือข้อมูลคอมพิวเตอร์ชนิดหนึ่ง แล้วนำไปขายหรือจำหน่าย เช่นนี้ เป็นช่องว่างของความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ กล่าวคือ การขายชื่อผู้ใช้ (username) และรหัสผ่าน (password) สำหรับเข้าใช้จดหมายอิเล็กทรอนิกส์ (e-mail) ของผู้อื่น ไม่มีประมวลกฎหมายอาญามาตราใดบัญญัติเป็นความผิด ดังนั้น มาตรา 6 แห่งพระราชบัญญัติฉบับนี้จึงสามารถปรับใช้เพื่ออุดช่องว่างนี้ได้

อย่างไรก็ตาม มาตรานี้ก็ไม่อาจอุดช่องว่างแห่งกฎหมายอาญาว่าด้วยความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ได้ทั้งหมด เช่น การล่วงรู้หมายเลขรหัสบนบัตรเติมเงินโทรศัพท์เคลื่อนที่ที่มีบาร์โค้ดของผู้อื่นแล้วนำไปจำหน่าย เช่นนี้ ย่อมไม่มีความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ เพราะประมวลกฎหมายอาญาไม่ได้บัญญัติให้หมายเลขรหัสบนบัตรเติมเงินโทรศัพท์เคลื่อนที่ดังกล่าวเป็นบัตรอิเล็กทรอนิกส์ ดังนั้น จึงไม่สามารถปรับบทความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ได้ ส่วนจะปรับใช้มาตรา 6 แห่งพระราชบัญญัติฉบับนี้ก็ไม่สามารถทำได้ เนื่องจากหมายเลขบนบัตรเติมเงินโทรศัพท์เคลื่อนที่ มิใช่มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ เพียงเป็นหมายเลขรหัสที่จะเข้าถึงมูลค่าการใช้บริการโทรศัพท์เคลื่อนที่ ซึ่งเป็นคนละกรณีกัน กรณีนี้จึงเป็นช่องว่างแห่งกฎหมายของความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ และยังคงเป็นปัญหาที่จำเป็นต้องได้รับการแก้ไข และ**หมายเลขรหัสบนบัตรเติมเงินโทรศัพท์เคลื่อนที่ที่มีบาร์โค้ดส่วนที่บันทึกไว้ในระบบคอมพิวเตอร์เป็นข้อมูลคอมพิวเตอร์** ซึ่งไม่มีกฎหมายทางอาญาบัญญัติคุ้มครองในฐานะวัตถุแห่งการกระทำเช่นเดียวกัน

---

[18] พรเพชร วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*, หน้า 10

2) ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะโดยมิชอบ มาตรา 7 บัญญัติว่า *"ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ"*

องค์ประกอบของความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ โดยมิชอบ มีดังต่อไปนี้

องค์ประกอบภายนอก

1. ผู้ใด
2. เข้าถึงโดยมิชอบ
3. ข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

องค์ประกอบภายใน

เจตนา

ความผิดฐานนี้มีองค์ประกอบคล้ายกับความผิดตามมาตรา 5 ต่างกันที่มาตรา 5 เป็นการเข้าถึงระบบคอมพิวเตอร์ แต่มาตรา 7 นี้เป็นการเข้าถึง "ข้อมูลคอมพิวเตอร์" ซึ่งสามารถพิจารณาความหมายได้จากบทนิยามมาตรา 3 ที่กล่าวไว้ข้างต้น ความผิดมาตรานี้เพียงเข้าถึงแม้ยังมิได้เอาข้อมูลคอมพิวเตอร์ของใครไป ก็เป็นความผิดแล้ว เช่น เข้าไปดูหรืออ่านจดหมายอิเล็กทรอนิกส์ของผู้อื่น เป็นต้น หรือหากเข้าถึงและเอาข้อมูลคอมพิวเตอร์ไปด้วยก็ย่อมเป็นความผิดฐานนี้เช่นกัน

ข้อสังเกต

มาตรานี้สามารถปรับใช้และมีส่วนช่วยในเรื่องช่องว่างแห่งกฎหมายที่เกิดกับความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ได้บ้างบางประการ เช่น การที่เก็บบัตรอิเล็กทรอนิกส์ที่มิได้อยู่ในรูปเอกสารหรือวัตถุอื่นใด[19] ไว้ เป็นไฟล์ข้อมูลในเครื่องคอมพิวเตอร์ แล้วถูกลักเอาไปเมื่อมีการออนไลน์ กรณีนี้ไม่อาจปรับบทด้วยความผิดฐานลักทรัพย์ เพราะเมื่อบัตรอิเล็กทรอนิกส์ถูกเก็บไว้เป็นไฟล์ข้อมูลในเครื่องคอมพิวเตอร์ ข้อมูลในเครื่องคอมพิวเตอร์ย่อมไม่ใช่ทรัพย์ที่จะถูกลักไปได้[20] และไม่อาจปรับบทความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ได้ เพราะไม่มีบทบัญญัติใดของประมวลกฎหมายอาญากำหนดให้เป็นความผิดและมีโทษทางอาญา แต่กรณีนี้สามารถปรับใช้ มาตรา 7 แห่ง

---

[19] หมายถึงบัตรอิเล็กทรอนิกส์ตามมาตรา 1 (14) (ข) และ (ค) ตามประมวลกฎหมายอาญา

[20] คำพิพากษาฎีกาที่ 5161/2547 วินิจฉัยชี้ขาดว่า "ข้อมูลในเครื่องคอมพิวเตอร์ไม่ใช่ทรัพย์ตามความหมายของมาตรา 334"

พระราชบัญญัติฉบับนี้ ฐานเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะโดยมิชอบได้ หากข้อมูลเหล่านั้นได้วางมาตรการป้องกันการเข้าถึงโดยเฉพาะไว้ กล่าวคือ มีการกำหนดค่ารหัสการเข้าถึงข้อมูล เช่น กำหนดรหัสผ่าน (password) ไว้ และยังมีความผิดฐานเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะโดยมิชอบ ตามมาตรา 5 อีกด้วย

อีกตัวอย่าง หากเก็บข้อมูลบัตรอิเล็กทรอนิกส์ไว้ในจดหมายอิเล็กทรอนิกส์ เช่น ชื่อผู้ใช้ (username) กับรหัสผ่าน (password) สำหรับการบริหารจัดการเว็บไซด์ เป็นต้น แล้วถูกเอาไปโดยวิธีการทางเทคโนโลยีคอมพิวเตอร์ เช่นนี้ ก็ไม่ผิดฐานลักทรัพย์ และไม่มีความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ แต่มีความผิดฐานเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะโดยมิชอบ ตามมาตรา 5 และมีความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะโดยมิชอบ ตามมาตรา 7 ด้วย

แต่กระนั้น ฐานความผิดเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะโดยมิชอบก็ไม่อาจอุดช่องว่างได้ทั้งหมด หากการเอาบัตรอิเล็กทรอนิกส์ที่มิได้อยู่ในรูปเอกสารหรือวัตถุอื่นใดของผู้อื่นไป โดยวิธีหรือช่องทางอื่นที่ไม่ใช่ใช้ช่องทางเทคโนโลยีคอมพิวเตอร์ เช่น วิธีพื้นๆ ด้วยการแอบจดจำหรือจดรายละเอียดเกี่ยวกับหมายเลขบัตรเครดิตและข้อมูลบนบัตรเครดิตไป กรณีนี้ก็ไม่เป็นความผิดฐานลักทรัพย์ เพราะข้อมูลเหล่านี้มิใช่ทรัพย์ และไม่เป็นความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ เพราะข้อมูลบนบัตรเครดิตมิใช่บัตรอิเล็กทรอนิกส์[21] และไม่สามารถปรับบทความผิดว่าด้วยการกระทำเกี่ยวกับคอมพิวเตอร์ได้ กรณีนี้เป็นปัญหาที่สำคัญเกิดเป็นคดีความที่ความผิดทางอาญาตามกฎหมายทุกฉบับไม่ครอบคลุมถึง จึงจำเป็นต้องได้รับการแก้ไขเพิ่มเติมกฎหมายเพื่ออุดช่องว่างแห่งกฎหมายนี้

3) ความผิดฐานดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ มาตรา 8 บัญญัติว่า *“ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”*

องค์ประกอบของความผิดฐานดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ มีดังต่อไปนี้

---

[21] เกียรติขจร วัจนะสวัสดิ์, *กฎหมายอาญา ภาคความผิด* เล่ม 2, พิมพ์ครั้งที่ 5 กรุงเทพมหานคร: หจก.จิรรัชการพิมพ์ 2551, หน้า 222

องค์ประกอบภายนอก

1. ผู้ใด

2 กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้

3. ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์

4. ข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

องค์ประกอบภายใน

เจตนา

มาตรา 8 มีวัตถุประสงค์เพื่อคุ้มครองสิทธิความเป็นส่วนตัวของบุคคลในการติดต่อสื่อสาร (The right of privacy of data communication) ผ่านช่องทางเทคโนโลยีคอมพิวเตอร์ ในทำนองเดียวกันกับการให้ความคุ้มครองสิทธิความเป็นส่วนตัวในการติดต่อสื่อสารรูปแบบอื่นๆ เช่น ห้ามดักฟังหรือแอบบันทึกการสนทนาทางโทรศัพท์ เป็นต้น[22]

องค์ประกอบที่ว่าด้วยกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้นี้ หมายความว่า เป็นการดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยวิธีการทางเทคนิค (technical means) ซึ่งผู้ดักรับนั้นอาจมีวัตถุประสงค์ เพื่อต้องการตรวจสอบ (monitoring) หรือแสวงหาข้อมูล หรือความเคลื่อนไหวของบุคคล หรือติดตามเนื้อหาสาระของข่าวสาร (surveillance) ที่สื่อสารถึงกันระหว่างบุคคล[23] โดยที่ผู้ดักรับไว้อาจทำการแอบบันทึกข้อมูล หรือแอบจดจำ หรือกระทำอย่างหนึ่งอย่างใดให้รับไว้ได้ซึ่งข้อมูลคอมพิวเตอร์ที่มีผู้ส่งผ่านถึงกันในระบบคอมพิวเตอร์

การดักรับไว้จะกระทำด้วยวิธีการอย่างไรก็ได้ที่เป็นการทำด้วยวิธีการทางอิเล็กทรอนิกส์ คือ ไม่จำกัดเพียงต้องเป็นวิธีการทางคอมพิวเตอร์เท่านั้น เช่น การทำให้ได้มาซึ่งเนื้อหาของข้อมูลโดยทางอื่นที่มิใช่วิธีการทางคอมพิวเตอร์ ด้วยการแอบบันทึกข้อมูลสื่อสารถึงกันโดยนำอุปกรณ์อิเล็กทรอนิกส์ไปเกี่ยวกับสายโทรศัพท์ หรือช่องสัญญาณตามตู้ชุมสายโทรศัพท์ก็ได้ เป็นต้น

ส่วนช่องทางหรือวิธีการดักรับไว้โดยผ่านเทคโนโลยีคอมพิวเตอร์อาจเป็นการลักลอบดักฟัง (listen) โดยใช้โปรแกรมหรือซอฟต์แวร์ต่างๆ อาจเป็นกลุ่มซอฟต์แวร์ที่เรียกว่า โทรจัน หรือกลุ่มซอฟต์แวร์อื่นๆ ทำการดักฟังการสนทนาของบุคคลที่กำลังสื่อสารกันผ่านโปรแกรมสื่อสารในระบบคอมพิวเตอร์ ซึ่งมีอยู่มากมายหลายโปรแกรม อาทิ เอ็มเอสเอ็น (msn) สไคพ์ (skyp) แมสเซนเจอร์ (messenger) ไลน์ (line) เป็นต้น

---

[22] พรเพชร วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*, หน้า 13

[23] พรเพชร วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*, หน้า 11

การดักรับนี้อาจทำการดักรับการสนทนา หรือการสื่อสาร หรือข้อมูลคอมพิวเตอร์อื่นๆ ที่มิใช่การดักฟังการสนทนาก็ได้ เช่น ดักรับข้อมูล หรือข้อความ หรือบทความงานวิจัยหรือรูปภาพ หรือโปรแกรมซอฟต์แวร์ที่ส่งผ่านทางจดหมายอิเล็กทรอนิกส์ หรือดักรับข้อมูลที่ส่งผ่านโปรแกรมสื่อสารต่าง ๆ ในระบบคอมพิวเตอร์ ซึ่งบุคคลอาจจำกัดผู้ที่มีสิทธิเข้ารับข้อมูลภายในกลุ่มของตนโดยโปรแกรมที่กำลังเป็นที่นิยมกัน ไม่ว่าจะเป็น instagram, facebook เป็นต้น หรืออาจลักลอบดักรับไว้ด้วยการใช้รหัสผ่าน (password) สำหรับเข้าใช้จดหมายอิเล็กทรอนิกส์ ซึ่งอาจได้รหัสผ่านมาด้วยวิธีใดๆ ก็ตาม[24] ทั้งนี้ การดักรับผ่านช่องทางเทคโนโลยีคอมพิวเตอร์ หมายรวมทั้งกรณีที่เป็นการส่งผ่านข้อมูลคอมพิวเตอร์ไปตามสื่อที่เป็นสายและกรณีที่เป็นการส่งผ่านข้อมูลคอมพิวเตอร์ไปตามสื่อไร้สายอื่นๆ เช่น ไวเลส (wireless) หรือบลูทูธ (bluetooth) ด้วย

การกระทำเพื่อดักรับไว้ด้วยวิธีการทางอิเล็กทรอนิกส์ตามมาตรานี้ ผู้กระทำได้กระทำไป “โดยมิชอบ” ซึ่งหมายถึงการไม่มีอำนาจกระทำได้ตามกฎหมาย หรือไม่ได้รับความยินยอม หรือไม่ได้รับการอนุญาตโดยผู้ทรงสิทธิ ในทางกลับกัน ถ้าผู้กระทำมีอำนาจที่จะกระทำได้ ไม่ว่าโดยกฎหมายหรือโดยความยินยอม หรือโดยการอนุญาตจากผู้ทรงสิทธิ ผู้กระทำย่อมไม่มีความผิด

องค์ประกอบประการต่อมา คือ ข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ หมายความว่า ข้อมูลคอมพิวเตอร์นั้นต้องอยู่ **“ระหว่างการส่ง”** เช่นนี้ หากเป็นข้อมูลที่เก็บไว้ในหน่วยความจำหรือฮาร์ดดิสก์หรือแผ่นซีดี แผ่นดีวีดี แล้วถูกลักลอบบันทึกไปย่อมไม่อยู่ในความหมายของมาตรานี้ แต่หากข้อมูลคอมพิวเตอร์ที่ถูกเก็บบันทึกไว้เหล่านี้ มีการนำมาใช้ส่งถึงกันผ่านระบบคอมพิวเตอร์แล้วถูกดักรับไปก็จะอยู่ในความหมายขององค์ประกอบนี้

ส่วนองค์ประกอบที่ว่าด้วยข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ หมายความว่า ข้อมูลคอมพิวเตอร์ที่มีการส่งผ่านในระบบคอมพิวเตอร์และถูกดักรับไว้นี้ เป็นข้อมูลส่วนตัวหรือข้อมูลเฉพาะตนหรือเฉพาะกลุ่มที่สื่อสารถึงกัน ไม่ได้ต้องการเผยแพร่ให้สาธารณะนำไปใช้ประโยชน์หรือรับทราบ นอกจากนี้ ต้องพิจารณาถึงวิธีการส่งหรือช่องทางการส่งด้วยว่า มีการปกปิดหรือมีมาตรการป้องกันหรือมีการส่งถึงกันในรูปแบบเฉพาะบุคคลหรือไม่ด้วย เช่น การส่งข้อมูลทางการค้าผ่านจดหมายอิเล็กทรอนิกส์ แล้วถูกแฮ็ก (hack) ไป หรืออาจถูกลักลอบใช้รหัสผ่านเข้าไปรับข้อมูลในจดหมายอิเล็กทรอนิกส์ก็ได้ เป็นต้น ลักษณะการส่งเช่นนี้ ถือว่าไม่ได้ต้องการให้ข้อมูลการค้าเหล่านั้นเป็นไปเพื่อประโยชน์สาธารณะ

แต่หากข้อมูลทางการค้าที่ไม่ได้ต้องการให้เป็นไปเพื่อประโยชน์สาธารณะใช้วิธีการส่งที่ไม่มีมาตรการป้องกันหรือไม่ได้ส่งถึงกันในรูปแบบเฉพาะบุคคล เช่น ไปพิมพ์ข้อมูลทาง

---

[24] การใช้รหัสผ่าน (password) สำหรับเข้าใช้จดหมายอิเล็กทรอนิกส์ มีความผิดตามมาตรา 269/5 แห่งประมวลกฎหมายอาญา ฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ

การค้าไว้ที่กระดานสนทนาของบริษัท หรือฝากเก็บข้อมูลไว้ที่บางเว็บไซต์ ซึ่งบุคคลทั่วไปเข้าดูได้โดยมิได้มีมาตรการป้องกัน แล้วมีบุคคลนอกบริษัทมาเห็นเข้าจึงรับข้อมูลทางการค้าไป เช่นนี้ ผู้ที่รับเอาข้อมูลทางการค้าไปก็ไม่มีความผิดตามมาตรานี้[25]

ข้อสังเกต

มาตรานี้มีความเกี่ยวพันกับการกระทำที่ก่อความเสียหายแก่บัตรอิเล็กทรอนิกส์โดยมีนัยสำคัญ ซึ่งความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ไม่ครอบคลุมถึง เพราะเหตุว่าข้อมูลบนบัตรเครดิตมิได้อยู่ในความหมายของบัตรอิเล็กทรอนิกส์ ด้วยการปรับใช้มาตรานี้เพื่อเอาผิดกับผู้ที่ลักลอบดักรับข้อมูลบนบัตรเครดิต

ลักษณะแห่งการกระทำดักรับข้อมูลบนบัตรเครดิตที่กระทำผ่านระบบคอมพิวเตอร์ อาจกระทำโดยส่งโทรจันเข้าสู่ตัวเครื่องคอมพิวเตอร์ของผู้ถือบัตรเครดิต เมื่อผู้ถือบัตรเครดิตทำธุรกรรมซื้อขายสินค้าผ่านระบบคอมพิวเตอร์ และชำระราคาค่าสินค้าด้วยบัตรเครดิต โดยจะต้องกรอกข้อมูล วันเดือนปีเกิด หมายเลขบัตรเครดิต วันเดือนปีหมดอายุของบัตรเครดิต และหมายเลข CVV หลังบัตรเครดิต แม้ภายหลังจะมีระบบป้องกันอีกชั้นด้วยการที่ผู้ถือบัตรเครดิตต้องทำการเข้ารหัส activate อีกชั้นหนึ่งก็ตาม โทรจันจะลักลอบเก็บข้อมูลเหล่านี้ไป กรณีนี้ ไม่เป็นลักทรัพย์ เพราะข้อมูลบนบัตรเครดิตไม่ใช่ทรัพย์ที่จะลักกันได้ ส่วนความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์หากผู้กระทำมิได้ดักรับข้อมูลสำหรับนำไปปลอมบัตรเครดิต กรณีนี้ มาตรา 269/2 ของประมวลกฎหมายอาญาจะไม่ครอบคลุมถึง และแม้จะนำข้อมูลบนบัตรเครดิตไปใช้ซื้อสินค้าหรือบริการ ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ก็ไม่ครอบคลุม เพราะเหตุว่าข้อมูลบนบัตรเครดิตมิได้อยู่ในความหมายของบัตรอิเล็กทรอนิกส์ แต่มาตรา 8 แห่งพระราชบัญญัตินี้สามารถปรับบทเอาผิดฐานดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบได้

การดักรับข้อมูลบนบัตรเครดิตอาจกระทำผ่านระบบคอมพิวเตอร์หรืออาจด้วยวิธีการอื่นทางอิเล็กทรอนิกส์ที่ไม่ใช่เทคโนโลยีคอมพิวเตอร์ และอาจไม่ต้องกระทำผ่านระบบคอมพิวเตอร์หรือวิธีการอื่นทางอิเล็กทรอนิกส์ก็ได้

วิธีการดักรับข้อมูลบนบัตรเครดิตอาจกระทำด้วยวิธีการอื่นทางอิเล็กทรอนิกส์ที่ไม่ใช่เทคโนโลยีคอมพิวเตอร์ก็ได้ เช่น การเจาะข้อมูลบัตรเครดิตโดยแอบลักลอบเข้าสู่ระบบโทรศัพท์ด้วยการนำสายโทรศัพท์ไปแอบเกี่ยวไว้ตามตู้ชุมสาย หรือโดยการใช้เครื่องมือก๊อปปี้ข้อมูลบัตรเครดิต

---

[25] พรเพชร วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*, หน้า 12

ที่เรียกว่า สกิมเมอร์ (skimmer hand held)[26] เครื่องมือชิ้นนี้มีความทันสมัยมาก ขนาดเล็กกะทัดรัด ใช้ง่าย ซึ่งเครื่องมือนี้จะก๊อบปี้ข้อมูลแถบแม่เหล็กของบัตรเครดิตจริง เพื่อนำมาทำบัตรเครดิตปลอม จากเดิมเครื่องนี้มีขนาดเท่าคอมพิวเตอร์มือถือหรือปาล์ม ต่อมาย่อลงเหลือแค่ประมาณซองบุหรี่ มาในวันนี้เหลือขนาดเล็กกว่าเพจเจอร์เครื่องจิ๋ว โดยผู้กระทำดักรับข้อมูลเหล่านี้จะใช้งานหรือร่วมมือกับแคชเชียร์ พนักงานเสิร์ฟ พนักงานร้าน พนักงานปั๊มน้ำมัน เมื่อลูกค้าชำระเงินค่าสินค้าหรือบริการด้วยบัตรเครดิตก็จะแอบใช้เครื่องสกิมเมอร์ (skimmer hand held) ก๊อปปี้ข้อมูลบัตรเครดิตที่รูดนี้เพียงไม่กี่วินาทีเท่านั้น[27] ซึ่งเจ้าหน้าที่ตำรวจจับกุมผู้กระทำความผิดบางคน ได้ โดยผู้กระทำบางคนเป็นชาวต่างชาติและเป็นต้นทางของการกระทำครั้งนี้

การกระทำลักษณะของการเกี่ยวสายนี้มิใช่การกระทำผ่านช่องทางด้วยการใช้ตัวเครื่องคอมพิวเตอร์เป็นเครื่องมือโดยตรง แต่กระทำด้วยวิธีการทางอิเล็กทรอนิกส์ดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ที่อยู่ระหว่างการส่งโดยมิชอบ เช่นนี้ ย่อมเป็นความผิดตามมาตรา 8 ของพระราชบัญญัตินี้ และมีความผิดตาม มาตรา 269/2 ของประมวลกฎหมายอาญาด้วย หากเป็นการกระทำเพื่อให้ได้ข้อมูลสำหรับปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ แต่หากมิใช่การกระทำเพื่อให้ได้ข้อมูลบัตรเครดิตสำหรับปลอมหรือแปลงบัตรเครดิต หรือบัตรอิเล็กทรอนิกส์จะเป็นความผิดตามมาตรา 269/2 หรือไม่ กล่าวคือ อาจทำเพื่อให้ได้ข้อมูลไปใช้โดยตรงเลย[28]

แต่การใช้เครื่องสกิมเมอร์แม้จะเป็นวิธีการทางอิเล็กทรอนิกส์ก็ตาม ก็มิใช่อยู่ระหว่างการส่งผ่านข้อมูลคอมพิวเตอร์ จึงไม่อาจปรับบทความผิดตามมาตรา 8 นี้ แต่ก็มีความผิดตามมาตรา 269/2 ของประมวลกฎหมายอาญา ฐานมีหรือทำเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลงหรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ เช่นเดียวกัน หากทำเพื่อให้ได้ข้อมูลไปใช้โดยตรง มิได้นำไปสำหรับปลอมบัตรเครดิตจะไม่มีความผิดตามมาตรา 269/2

ดังนี้ เมื่อปรับใช้กับความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ปัญหาจึงมีอยู่ว่าหากเป็นการกระทำให้ได้ข้อมูลบนบัตรเครดิตด้วยวิธีการอื่นที่มิใช่วิธีการอิเล็กทรอนิกส์ ด้วยการแอบจดข้อมูล วันเดือนปีเกิด หมายเลขบัตรเครดิต วันเดือนปีหมดอายุของบัตรเครดิต และหมายเลข CVV

---

[26] การรูดบัตรเครดิตเพื่อชำระค่าสินค้าหรือบริการจะมีการส่งผ่านข้อมูลไปในระบบคอมพิวเตอร์ เพราะเครื่องรูดบัตรเมื่อต่อเข้ากับสายโทรศัพท์แล้วจะเชื่อมโยงเข้ากับระบบคอมพิวเตอร์ด้วย แต่การก๊อปปี้ด้วยสกิมเมอร์มิได้ใช้ระหว่างการรูดบัตรอันอยู่ในระหว่างการส่งผ่านข้อมูลคอมพิวเตอร์

[27] วันชัย พูลเพิ่มพันธ์, ผู้สื่อข่าว หนังสือพิมพ์ข่าวสด จ.นครปฐม เว็บไซต์เอเอสดีแอลประเทศไทย *http://www.adslthailand.com/forum/viewtopic.php?t=59314* สืบค้นเมื่อวันที่วันที่ 11 มกราคม 2554, อ้างใน สมศักดิ์ เธียรจรูญกุล, รายงานการวิจัยเรื่อง *ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา*, ทุนอุดหนุนการวิจัยจากกองทุนรัตนโกสินทร์สมโภช 200 ปี มหาวิทยาลัยสุโขทัยธรรมาธิราช, ปี 2559

[28] ผู้สนใจประเด็นนี้โปรดดู สมศักดิ์ เธียรจรูญกุล, รายงานการวิจัยเรื่อง *ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา*, ทุนอุดหนุนการวิจัยจากกองทุนรัตนโกสินทร์สมโภช 200 ปี มหาวิทยาลัยสุโขทัยธรรมาธิราช, ปี 2559

หลังบัตรเครดิตไป ย่อมไม่อาจปรับบทมาตรา 8 แห่งพระราชบัญญัตินี้ได้ และความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ก็ไม่ครอบคลุมถึงด้วย นอกจากนี้ แม้จะกระทำด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้ได้ข้อมูลบัตรเครดิต หากมิได้กระทำในระหว่างส่งในระบบคอมพิวเตอร์ก็ไม่อาจปรับบทความผิดมาตรา 8 นี้ และถ้าการคัดลอกข้อมูลมิใช่สำหรับการปลอมบัตรเครดิต แต่นำข้อมูลบนบัตรเครดิตไปใช้โดยตรงก็มีปัญหาว่ามาตรา 269/2 จะไม่ครอบคลุมถึง

อนึ่ง ข้อมูลบนบัตรอิเล็กทรอนิกส์ที่ไม่อยู่ในความหมายของบัตรอิเล็กทรอนิกส์ดังกล่าวข้างต้น หากถูกเก็บอยู่ในรูปข้อมูลคอมพิวเตอร์ในระบบคอมพิวเตอร์ เมื่อถูกเจาะระบบ หรือแฮ็ก (hack) และโจรกรรมหรือสำเนาข้อมูลบนบัตรอิเล็กทรอนิกส์ที่อยู่ในรูปคอมพิวเตอร์ไป ซึ่งเป็นความผิดตามมาตรา 5 และมาตรา 7 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่ก็เป็นความผิดที่มีเจตนารมณ์เอาผิดแก่ลักษณะแห่งการกระทำ (access) ไม่ใช่ความผิดที่มีเจตนารมณ์ที่กฎหมายมุ่งคุ้มครองข้อมูลคอมพิวเตอร์ในฐานะวัตถุแห่งการกระทำ **ซึ่งหากมีผู้ได้รับข้อมูลคอมพิวเตอร์ต่อๆ ไปเป็นทอดๆ ผู้ได้รับข้อมูลต่อๆ กันเหล่านั้น ไม่มีกฎหมายอาญากำหนดให้มีความผิดและโทษ**

4) ความผิดฐานทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ มาตรา 9 บัญญัติว่า *“ผู้ใดทำให้เสียหาย ทำลาย แก้ไขเปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”*

องค์ประกอบของความผิดฐานทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลงเพิ่มเติมข้อมูลคอมพิว-เตอร์โดยมิชอบ มีดังต่อไปนี้

องค์ประกอบภายนอก

1. ผู้ใด
2. ทำให้เสียหาย ทำลาย แก้ไขเปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนโดยมิชอบ
3. ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่น

องค์ประกอบภายใน

เจตนา

วัตถุประสงค์ของบทบัญญัติมาตรา 9 นี้ มุ่งจะคุ้มครองความถูกต้องของข้อมูล (integrity) ความถูกต้องแท้จริง (authentication) เสถียรภาพของข้อมูลคอมพิวเตอร์ หรือความพร้อมในการใช้งานโปรแกรมและข้อมูลคอมพิวเตอร์ หรือการใช้ข้อมูลคอมพิวเตอร์ที่มีการบันทึกเก็บไว้ในระบบคอมพิวเตอร์ได้ มาตรานี้จึงเป็นการบัญญัติขึ้นเพื่อให้ข้อมูลคอมพิวเตอร์ซึ่ง

รวมทั้งโปรแกรมคอมพิวเตอร์ได้รับความคุ้มครองลักษณะเดียวกันกับวัตถุสิ่งของที่สามารถจับต้องได้ (corporeal object)[29]

มาตรานี้กล่าวได้ว่ามีส่วนขององค์ประกอบบางประการคล้ายคลึงประมวลกฎหมายอาญาว่าด้วยความผิดฐานทำให้เสียทรัพย์กับความผิดเกี่ยวกับการทำปลอม กล่าวคือ ทำให้เสียหาย ทำลาย มีลักษณะแห่งการกระทำทำนองเดียวกับการทำให้เสียทรัพย์ ต่างกันตรงที่วัตถุแห่งการกระทำเป็นทรัพย์ของผู้อื่น กับข้อมูลคอมพิวเตอร์ของผู้อื่น และแก้ไขเปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนมีลักษณะแห่งการกระทำทำนองเดียวกับการแก้ไขเปลี่ยนแปลง เพิ่มเติมในความผิดเกี่ยวกับการปลอมเอกสาร ซึ่งรวมทั้งทำนองเดียวกันกับปลอมบัตรอิเล็กทรอนิกส์ตามมาตรา 269/1 ดังนี้ มาตรา 9 แห่งพระราชบัญญัตินี้จึงสามารถปรับบทบังคับใช้กับความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ได้ในบางลักษณะบางกรณี

ข้อสังเกต

ความผิดตามมาตรา 9 สามารถปรับบังคับใช้กับการกระทำความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ได้ หากบัตรอิเล็กทรอนิกส์นั้นมีลักษณะอยู่ในความหมายของข้อมูลคอมพิวเตอร์ เช่น การที่เจ้าของเว็บไซต์ให้บริการกระดานสนทนาเก็บรักษาชื่อผู้ใช้ (username) และรหัสผ่าน (password) ไว้เป็นไฟล์ข้อมูลของระบบคอมพิวเตอร์ ผู้กระทำได้เข้าไปเปลี่ยนแปลงแก้ไข ชื่อผู้ใช้ (username) และรหัสผ่าน (password) โดยมิชอบ กล่าวคือ กระทำไปโดยไม่มีสิทธิตามกฎหมาย หรือไม่ได้รับความยินยอม หรือไม่ได้รับอนุญาตจากผู้ทรงสิทธิ เช่นนี้ ถือเป็นความผิดตามมาตรา 9 ของพระราชบัญญัตินี้ และยังมีความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/1 อีกด้วย

ทั้งนี้ การแก้ไขเปลี่ยนแปลงรหัสเบิกถอนเงินสดที่เครื่องฝาก-ถอนเงินสดอัตโนมัติก็เป็นการแก้ไข เปลี่ยนแปลงข้อมูลคอมพิวเตอร์ อันเป็นความผิดตามมาตรา 9 ด้วยเช่นกัน เพราะข้อมูลรหัสที่เก็บไว้ในเครื่องฝาก-ถอนเงินสดอัตโนมัติเชื่อมต่อกับระบบคอมพิวเตอร์และเป็นข้อมูลคอมพิวเตอร์ และยังมีความผิดฐานปลอมบัตรอิเล็กทรอนิกส์เป็นกรรมเดียวผิดกฎหมายหลายบท ตามมาตรา 90

5) ความผิดฐานจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด มาตรา 13 บัญญัติว่า *“ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือ มาตรา 11 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ”*

---

[29] พรเพชร วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*, หน้า 13-14

องค์ประกอบของความผิดฐานจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด มีดังต่อไปนี้

องค์ประกอบภายนอก

1. ผู้ใด
2. จำหน่ายหรือเผยแพร่
3. ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือ มาตรา 11

องค์ประกอบภายใน

เจตนา

วัตถุประสงค์ของมาตรานี้มุ่งที่จะคุ้มครองชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะมิให้มีการนำไปจำหน่าย หรือเผยแพร่เพื่อกระทำความผิดฐานอื่นๆ ตามที่ระบุต่อไป ซึ่งหมายถึงชุดคำสั่งเหล่านั้นมิได้มีไว้สำหรับสาธารณะประโยชน์

การจำหน่าย หมายถึงการส่งต่อไปยังผู้อื่นโดยอาจมีค่าตอบแทนหรือไม่ก็ได้[30] เช่น ขาย แลกเปลี่ยน ส่วนเผยแพร่ เป็นคำที่กว้างกว่าน่าจะรวมถึงการโฆษณา จ่าย แจก[31] และการจำหน่ายหรือเผยแพร่ชุดคำสั่งนี้ ไม่จำกัดจำนวนบุคคล อาจเพียงจำหน่ายหรือเผยแพร่ต่อบุคคลคนเดียว หรืออาจจำหน่ายหรือเผยแพร่ต่อบุคคลหลายคนก็ได้ และไม่จำกัดวิธีการหรือช่องทาง อาจจำหน่ายหรือเผยแพร่ผ่านช่องทางเทคโนโลยีคอมพิวเตอร์หรือทางหนึ่งทางใดที่ไม่ได้ใช้เทคโนโลยีคอมพิวเตอร์ก็ได้

ชุดคำสั่งเหล่านี้จัดทำขึ้นโดยเฉพาะเท่านั้น มิได้เผยแพร่เป็นการทั่วไป และชุดคำสั่งอยู่ในความหมายเป็นส่วนหนึ่งของคำว่าข้อมูลคอมพิวเตอร์หากอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ ชุดคำสั่งตามมาตรานี้อาจอยู่ในรูปเป็นแบบแผ่นดิสก์ หรือแผ่นซีดี หรือหน่วยความจำอื่นๆ หรืออาจเป็นไฟล์ดิจิทัลในลักษณะข้อมูลคอมพิวเตอร์ก็ได้

ข้อสังเกต

บัตรอิเล็กทรอนิกส์บางประเภทก็อยู่ในความหมายของชุดคำสั่งในลักษณะของข้อมูลคอมพิวเตอร์ซึ่งอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ เช่น รหัส activate บัตรเครดิต รหัสบัตร เอ.ที.เอ็ม รหัสผ่านเข้าบริหารจัดการเว็บไซด์หรือเว็บบอร์ด รหัสผ่าน (password) เข้าเล่นเกมคอมพิวเตอร์ออนไลน์ รหัสผ่านเพื่อลงโปรแกรม (serial number) เป็นต้น

---

[30] จิตติ ติงศภัทิย์, *กฎหมายอาญา ภาค 2 ตอน 2 และภาค 3*, หน้า 559

[31] พรเพชร วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*, หน้า 19

การจำหน่ายหรือเผยแพร่บัตรอิเล็กทรอนิกส์ที่แท้จริงเหล่านี้ ประมวลกฎหมายอาญาว่าด้วยความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์มิได้บัญญัติให้เป็นความผิด ซึ่งเป็นกรณีที่สำคัญประการหนึ่ง ซึ่งมาตรา 13 แห่งพระราชบัญญัตินี้สามารถปรับใช้กับลักษณะแห่งการกระทำเช่นนี้ได้

ปัญหาที่สำคัญ คือ หากแต่มีข้อมูลบนบัตรอิเล็กทรอนิกส์บางประเภทที่ไม่อยู่ในความหมายของชุดคำสั่งตามมาตรานี้ เช่น ข้อมูลบนบัตรเครดิต เป็นต้น ดังนี้ หากมีการจำหน่ายหรือเผยแพร่ข้อมูลบนบัตรเครดิตซึ่งคือบัตรอิเล็กทรอนิกส์ที่แท้จริง โดยที่ข้อมูลบนบัตรเครดิตมิใช่อยู่ในความหมายของชุดคำสั่งของมาตรานี้ ย่อมไม่เป็นความผิดอาญาตามมาตราใดและตามกฎหมายใดเลย ซึ่งข้อมูลบนบัตรเครดิตนี้มีการจำหน่าย หรือซื้อขายกันบนโลกออนไลน์มากมาย

อนึ่ง ยังมีข้อมูลคอมพิวเตอร์อีกหลากหลายชนิดที่ไม่ใช่ชุดคำสั่งหรือข้อมูลบนบัตรอิเล็กทรอนิกส์ เช่น ข้อมูลทางการค้า ข้อมูลทางบัญชีของสถาบันทางการเงิน ข้อมูลส่วนบุคคล ข้อมูลความลับทางราชการ เป็นต้น หากถูกโจรกรรมหรือสำเนาไปจำหน่ายจ่ายแจกก็ไม่มีกฎหมายอาญาใดมีเจตนารมณ์คุ้มครองข้อมูลคอมพิวเตอร์เหล่านี้ในฐานะวัตถุแห่งการกระทำ

จะเห็นได้ว่า แม้มีการแก้ไขเพิ่มพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 โดยฉบับแก้ไขเพิ่มเติม พ.ศ.2560 แล้ว ก็ยังไม่มีบทบัญญัติใดครอบคลุมสภาพปัญหาหรือแก้ไขปัญหาทางกฎหมายและให้ความคุ้มครองข้อมูลคอมพิวเตอร์ในฐานะวัตถุแห่งการกระทำโดยตรงดังกล่าวมาแล้วนี้ได้

จากลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์ และกฎหมายอาญาของประเทศไทยเกี่ยวกับข้อมูลคอมพิวเตอร์ของบทที่ 2 จะได้วิเคราะห์ถึงบทบัญญัติของกฎหมายเกี่ยวกับข้อมูลคอมพิวเตอร์ของต่างประเทศในบทที่ 3 ซึ่งจะนำไปสู่การวิเคราะห์มาตรการทางกฎหมายอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์ต่อไป

บทที่ 3
กฎหมายอาญาต่างประเทศเกี่ยวกับการคุ้มครองข้อมูลคอมพิวเตอร์

บทนี้จะกล่าวถึงเนื้อหากฎหมายเกี่ยวกับคอมพิวเตอร์ของต่างประเทศได้แก่ กฎหมายของประเทศอังกฤษ และกฎหมายของประเทศสหรัฐอเมริกา ซึ่งผู้วิจัยจะแยกออกเป็น 2 หัวข้อ ดังนี้

1. กฎหมายประเทศอังกฤษ
2. กฎหมายประเทศสหรัฐอเมริกา

1. กฎหมายประเทศอังกฤษ

กฎหมายเกี่ยวกับข้อมูลคอมพิวเตอร์ของประเทศอังกฤษซึ่งจะค้นคว้าวิจัยภายใต้ขอบเขตการศึกษาวิจัยของงานวิจัยเล่มนี้ที่จะกล่าวถึง ดังนี้

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

1.2 พระราชบัญญัติเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981)

1.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990)[32]

ความก้าวหน้าทางเทคโนโลยีด้านคอมพิวเตอร์สร้างความสะดวกสบายแก่การดำเนินวิถีชีวิตของมนุษย์เป็นอย่างมาก ไม่ว่าจะเป็นด้านการศึกษา สังคม เศรษฐกิจ การบริหารจัดการทั้งภาครัฐ และภาคเอกชน รวมทั้งการดำเนินงานของกระบวนการยุติธรรม

แต่ในขณะเดียวกันเทคโนโลยีคอมพิวเตอร์ก็กลายเป็นเครื่องมือในการกระทำความผิด โดยถูกอาชญากรนำไปใช้เป็นเครื่องมือในการกระทำความผิด เป็นผลให้อาชญากรรมมีความซับซ้อน ยากแก่การปราบปราม ติดตามจับกุมมาดำเนินคดี ส่วนอีกด้านหนึ่งก็เป็นปัญหาก่อผลกระทบในเชิงกฎหมาย กล่าวคือ ก่อให้เกิดประเด็นปัญหาข้อกฎหมายแทบทุกสาขาในทางกฎหมาย

---

[32] *Computer misuse act 1990*, เว็บไซต์หอจดหมายเหตุแห่งชาติ ประเทศอังกฤษ *http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=1353366* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

กฎหมายอาญาก็เช่นเดียวกันมีประเด็นข้อกฎหมายเกิดขึ้น ตั้งแต่ปัญหาการไม่มีบทบัญญัติของกฎหมายที่จะปรับใช้แก่กรณี ปัญหาด้านนิติวิธีการตีความกฎหมาย (Interpretation of law) ปัญหาในทางคดีที่องค์กรผู้บังคับใช้กฎหมายต้องควานหากฎหมายที่มีอยู่มาปรับใช้กับเหตุการณ์ที่เกิดขึ้น ซึ่งบางคดีมีความสุ่มเสี่ยงอย่างมากที่จะก้าวล่วงข้อห้ามหรือหลักกฎหมายสำคัญ เช่น **"ไม่มีกฎหมาย ย่อมไม่มีความผิดและไม่มีโทษ"** (nullum crimen, nulla poena sine lege)[33] หรือ ข้อห้ามใช้หลักกฎหมายใกล้เคียงอย่างยิ่งปรับแก่การกระทำที่ถูกกล่าวหาว่าเป็นความผิดอาญา[34]

ตัวอย่างกรณีที่น่าสนใจและน่าคิดอย่างมากว่า เป็นการวินิจฉัยชี้ขาดคดีที่สุ่มเสี่ยงต่อข้อห้ามของหลักกฎหมายที่สำคัญข้างต้นหรือไม่ กล่าวคือ เป็นคดีที่เกิดขึ้นและพิพากษาในขณะที่ยังไม่มีการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ซึ่งมีคดีที่จะศึกษา 2 คดี ดังนี้

คดีแรก ในดคี Cox v. Riley (1986) 54 จำเลยลบโปรแกรมคอมพิวเตอร์จาก print circuit card ซึ่งใช้สำหรับควบคุมระบบคอมพิวเตอร์ของเลื่อนยนต์ตัดไม้ของนายจ้าง ทำให้เครื่องมือนั้นไม่สามารถใช้งานได้ จำเลยถูกดำเนินคดีฟ้องร้อง ในข้อหาทำให้เสียทรัพย์ ตามพระราชบัญญัติความรับผิดทางอาญาเกี่ยวกับการทำให้เสียทรัพย์ ค.ศ. 1971 (The Criminal Damage Act 1971) ซึ่งมี สาระสำคัญว่า "ผู้ที่จะมีความผิดทางอาญา ถ้ากระทำการเป็นการทำลาย ให้เสียหาย หรือไร้ประโยชน์ในทรัพย์ของผู้อื่น โดยปราศจากข้ออ้างหรือข้อแก้ตัวตามกฎหมาย อาจกระทำโดยเจตนาหรือประมาท" จำเลยให้การต่อสู้ในประเด็นที่ว่า "โปรแกรมคอมพิวเตอร์ไม่ใช่ทรัพย์สิน อันเป็นวัตถุที่มีรูปร่างหรือจับต้องได้ในความหมายของพระราชบัญญัติความรับผิดทางอาญาเกี่ยวกับการทำให้เสียทรัพย์ ค.ศ. 1971 (The Criminal Damage Act 1971) ซึ่งใช้คำว่า "property" คดีนี้ศาลยุติธรรมหรือสภาขุนนางของประเทศอังกฤษ วินิจฉัยชี้ขาดว่า จำเลยมีความผิดตามข้อหาที่ถูกฟ้องฐานทำให้เสียทรัพย์ โดยให้เหตุผลว่า "เมื่อโปรแกรมคอมพิวเตอร์เสียหายไป ย่อมทำให้เลื่อยยนต์ที่ควบคุมด้วยระบบคอมพิวเตอร์ถูกทำให้เสียหายหรือไร้ประโยชน์แล้ว"[35]

---

[33] ธานินทร์ กรัยวิเชียร และวิชา มหาคุณ, *การตีความกฎหมาย* พิมพ์ครั้งที่ 2 กรุงเทพมหานคร:โรงพิมพ์ชวนพิมพ์ 2521, หน้า 28

[34] หยุด แสงอุทัย, *กฎหมายอาญา ภาค 1* กรุงเทพมหานคร:มหาวิทยาลัยธรรมศาสตร์ 2523, หน้า 54-55 อ้างใน มหาวิทยาลัยสุโขทัยธรรมาธิราช, *เอกสารการสอนชุดวิชากฎหมายอาญา 1: ภาคบทบัญญัติทั่วไป*, หน้า 108

[35] Yaman Akdeniz, Faculty of Law University of Leeds, *Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!* , เว็บไซต์คณะนิติศาสตร์ มหาวิทยาลัยลีดส์ *http://www.bailii.org/cgi-bin/format.cgi?doc=/uk/other/journals/WebJCLI/1996/issue3/akdeniz3.html&query=(Yaman)+AND+(Akdeniz)* สืบค้นเมื่อวันที่วันที่ 10 สิงหาคม พ.ศ. 2561

ข้อสังเกต คดีนี้จำเลยทำให้โปรแกรมคอมพิวเตอร์เสียหาย ซึ่งเป็นวัตถุแห่งการกระทำคนละประเภทหรือคนละชนิดกับเลื่อยยนต์ที่ควบคุมด้วยระบบคอมพิวเตอร์ นั่นย่อมหมายความว่า เจตนาประสงค์ต่อผลของจำเลยแม้มุ่งหมายไปที่โปรแกรมคอมพิวเตอร์ แต่การลบโปรแกรมคอมพิวเตอร์นั้น จำเลยย่อมมุ่งหมายประสงค์ให้เลื่อยยนต์ที่ควบคุมด้วยระบบคอมพิวเตอร์ทำงานตามปกติไม่ได้ ดังนั้น จึงวิเคราะห์ได้ว่า การที่จำเลยลบโปรแกรมคอมพิวเตอร์ เท่ากับจำเลยประสงค์ต่อผลให้เลื่อยยนต์ที่ควบคุมด้วยระบบคอมพิวเตอร์เสียหายนั่นเอง ซึ่งเป็นผลที่จำเลยมุ่งหมายให้เกิดขึ้นเช่นนั้นแก่เลื่อยยนต์ที่ควบคุมด้วยระบบคอมพิวเตอร์

คดีที่สอง ในคดี Whiteley (1991) จำเลยในคดีนี้ ถูกดำเนินคดีฟ้องร้องในข้อหาทำให้เสียทรัพย์ ตามพระราชบัญญัติความรับผิดทางอาญาเกี่ยวกับการทำให้เสียทรัพย์ ค.ศ. 1971 (The Criminal Damage Act 1971) เช่น เกี่ยวกับคดีข้างต้น โดยข้อเท็จจริงในคดี จำเลยได้กระทำการ hacking เข้าไปในระบบคอมพิวเตอร์เครือข่ายมหาวิทยาลัยหลายแห่ง โดยผ่านทางเครือข่ายทางการศึกษา (Joint Academic Network : Janet) แล้วแก้ไขเปลี่ยนแปลง ลบ เพิ่ม ตลอดจนเข้าควบคุม ระบบการบริหารจัดการระบบผู้ใช้ (user) ซึ่งเป็นอำนาจของผู้ควบคุมระบบ (web master) การกระทำของจำเลยดังกล่าว ก่อให้ระบบคอมพิวเตอร์เครือข่ายมหาวิทยาลัยเกิดความล้มเหลว ไม่สามารถดำเนินงานได้อย่างปกติ ศาลยุติธรรมหรือสภาขุนนางของประเทศอังกฤษ วินิจฉัยชี้ขาดว่าจำเลยมีความผิดตามข้อหาที่ถูกฟ้องฐานทำให้เสียทรัพย์ โดย Lord Lane CJ ได้ให้เหตุผลไว้ว่า “อนุภาคของแม่เหล็ก (magnetic particles) ที่อยู่บนแผ่นดีสก์หรือจานบันทึกโลหะ (metal disc) ถือเป็นส่วนหนึ่งของแผ่นดีสก์หรือจานบันทึกโลหะ (metal disc) นั้น หากสามารถพิสูจน์ได้ว่าจำเลยเป็นผู้กระทำการเปลี่ยนแปลง ลบ เพิ่มอนุภาคที่อยู่บนแผ่นดีสก์หรือจานบันทึกโลหะ (metal disc) อันทำให้เกิดความเสียหายต่อคุณค่าหรือการใช้ประโยน์ของแผ่นดีสก์หรือจานบันทึกโลหะ (metal disc) ย่อมเป็นความผิดในข้อหาทำให้เสียทรัพย์ ตามมาตรา 1 ของพระราชบัญญัติ ความรับผิดทางอาญาเกี่ยวกับการทำให้เสียทรัพย์ ค.ศ. 1971 (The Criminal Damage Act 1971)”[36]

ข้อสังเกต

สำหรับคดี Whiteley การที่จำเลยได้กระทำการ hacking เข้าไปในระบบคอมพิวเตอร์เครือข่ายมหาวิทยาลัย แล้วแก้ไขเปลี่ยนแปลง ลบ เพิ่ม ตลอดจนเข้าควบคุมระบบการบริหารจัดการระบบผู้ใช้ (user) ซึ่งเป็นอำนาจของผู้ควบคุมระบบ (web master) การกระทำ เช่นนี้

---

[36] Yaman Akdeniz, Faculty of Law University of Leeds, *Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!* , เว็บไซต์คณะนิติศาสตร์ มหาวิทยาลัยลีดส์ *http://www.bailii.org/cgi-bin / format.cgi?doc=/uk/other/journals/WebJCLI/1996/issue3/akdeniz3.html&query=(Yaman)+AND+(Akdeniz)* สืบค้นเมื่อวันที่วันที่ 10 สิงหาคม พ.ศ. 2561

เป็นการกระทำต่อ **“ข้อมูลคอมพิวเตอร์”**[37] ซึ่งมิใช่วัตถุมีรูปร่างในความหมายของคำว่าทรัพย์ การที่ศาลยุติธรรมหรือสภาขุนนางของประเทศอังกฤษวินิจฉัยไปถึง “อนุภาคของแม่เหล็ก (magnetic particles) ที่อยู่บนแผ่นดีสก์หรือจานบันทึกโลหะ (metal disc) ถือเป็นส่วนหนึ่งของแผ่นดีสก์หรือจานบันทึกโลหะ (metal disc) นั้น” ผู้วิจัยเห็นว่าไกลเกินไปกว่าความหมายของคำว่า ทรัพย์ ซึ่งต้องเป็นวัตถุมีรูปร่าง อาจถึงขนาดสุ่มเสี่ยงต่อการเทียบเคียงบทกฎหมายที่ใกล้เคียงอย่างยิ่งแก่การกระทำที่ถูกกล่าวหาว่าเป็นความผิดทางอาญา อันเป็นข้อห้ามตามหลักกฎหมายอาญา

ตัวอย่างคดีสำคัญที่ศาลยุติธรรมหรือสภาขุนนางของประเทศอังกฤษต้องตัดสินชี้ขาดยกฟ้องจำเลย เนื่องจากไม่อาจปรับบทบัญญัติของกฎหมายลงโทษตามกฎหมายที่มีอยู่เดิมได้ จนเป็นที่มาของการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) คดีดังกล่าวมีข้อเท็จจริงใจความสำคัญดังนี้

ในคดี R v. Gold (1988) จำเลยถูกดำเนินคดีฟ้องร้องในข้อหาปลอมแปลงเอกสารตามพระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) มาตรา 1 โดยมีข้อเท็จจริงในคดีว่า จำเลยได้รับรู้รหัสผ่าน (password) สำหรับใช้ในการเข้าถึงระบบคอมพิวเตอร์ของบริษัทโทรคมนาคม ซึ่งรหัสผ่านบริษัทโทรคมนาคมออกให้แก่วิศวกรของตน เพื่อใช้ในการบริหารจัดการดูแลรักษาระบบคอมพิวเตอร์ของบริษัท โดยที่รหัสผ่านนี้ สามารถเข้าถึงระบบคอมพิวเตอร์ของบริษัททุกส่วน รวมทั้งสามารถใช้บริการการสื่อสารโทรคมนาคมได้โดยไม่ต้องชำระค่าบริการ คดีนี้ศาลยุติธรรมหรือสภาขุนนางของประเทศอังกฤษวินิจฉัยชี้ขาดว่า “ความผิดฐานปลอมแปลงเอกสารจะต้องมีการทำให้เกิด หรือแสดงให้เห็นของที่ปลอมขึ้น เช่น ลายมือชื่อปลอม แต่จากข้อเท็จจริงของคดี รหัสผ่านที่จำเลยใช้นั้นเป็นของแท้จริง เพียงจำเลยใช้รหัสผ่านโดยปราศจากอำนาจเท่านั้น ศาลยุติธรรมหรือสภาขุนนางของประเทศอังกฤษ จึงตัดสินชี้ขาดคดีนี้ โดยยกฟ้องโจทก์และปล่อยจำเลยไป”[38]

ผลจากคดีของนาย Gold นี้ ก่อให้เกิดปัญหาในทางกฎหมายที่องค์กรผู้บังคับใช้กฎหมายไม่อาจแสวงหาบทบัญญัติของกฎหมายใดมาปรับใช้แก่การกระทำเช่นนี้ แม้แต่ Theft Act 1968/1978/1996 ก็ไม่อาจปรับแก่กรณีได้เช่นกัน เพราะการหลอกลวงนั้นจะต้องเป็นการหลอกลวงผู้อื่น หากแต่เครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์มิใช่ผู้อื่น คณะกรรมาธิการด้านกฎหมาย ของอังกฤษและสก๊อตแลนด์ (the Scottish and English Law Commissions) เห็นว่า **“ไม่มีกฎหมาย**

---

[37] คำพิพากษาฎีกาที่ 5161/2547 วินิจฉัยว่า “ข้อมูลคอมพิวเตอร์” ไม่ใช่ทรัพย์ในความหมายของมาตรา 334 แห่งประมวลกฎหมายอาญา

[38] Describe the origins and function of the Computer Misuse Act 1990, Evaluate the extent to which it is intended to serve as a deterrent to 'hacking', เว็บไซต์อาจารย์นิติศาสตร์ดอทเน็ต *http://www.lawteacher.net/criminal-law/acts/computer-misuse-act-1990.php* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

ที่ตราโดยรัฐสภาซึ่งสามารถครอบคลุมการกระทำความผิดต่อหรือผ่านระบบคอมพิวเตอร์ และการกระทำลักษณะเดียวกันกับนาย Gold ที่กระทำการลักลอบใช้บริการการสื่อสารโทรคมนาคมผ่านระบบเครือข่ายคอมพิวเตอร์ สมควรเป็นการกระทำที่เป็นความผิดตามกฎหมาย" ความจำเป็นที่เกิดช่องว่างทางกฎหมายอาญาจากคดีนาย Gold นี้เป็นแรงผลักดันที่สำคัญก่อให้เกิดการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ขึ้นเพื่อบังคับใช้แก่การกระทำที่กระทำต่อระบบคอมพิวเตอร์ หรือกระทำความผิดอื่นๆ โดยผ่านหรือใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ[39]

อนึ่ง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990(Computer Misuse Act 1990) ได้รับการแก้ไขเพิ่มเติมล่าสุดโดยพระราชบัญญัติว่าด้วยอาชญากรรมร้ายแรง 2015 (The Serious Crime Act 2015) โดยเพิ่มมาตรา 3ZA มีเนื้อหาเกี่ยวกับเขตอำนาจศาลประเทศอังกฤษ กับเหตุฉกรรจ์ ซึ่งเนื้อหาของบทบัญญัติไม่เกี่ยวข้องโดยตรงกับขอบเขตการศึกษาวิจัย จึงไม่ได้นำมาใช้กับการวิเคราะห์[40]

คดีแรกที่ได้รับการพิจารณาและพิพากษาลงโทษตามกฎหมายที่ตราขึ้นบังคับใช้ใหม่ในขณะนั้น คือ คดี R v. Ross Pearlstone [1991] ซึ่งจำเลยเข้าถึงระบบคอมพิวเตอร์เพื่อให้ได้ข้อมูลเกี่ยวกับโทรศัพท์ของ Mercury telephone และได้ใช้โทรศัพท์ภายใต้ชื่อบัญชีของนายจ้างเก่าฟรีไปสองรอบระยะเวลาบัญชี จำเลยถูกศาลยุติธรรมของประเทศอังกฤษ (ศาลแขวง : Magistrates Court) แห่งเมือง Bow Street พิพากษาลงโทษตามมาตรา 1 และมาตรา 2 ของพระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ฉบับนี้ โดยปรับเป็นเงิน 900 ปอนด์[41]

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ฉบับนี้ มีบทบัญญัติที่สำคัญซึ่งจะกล่าวถึงโดยแบ่งออกเป็น 4 หัวข้อดังนี้

1.1.1 ความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจ

---

[39] เว็บไซต์อาจารย์นิติศาสตร์ดอทเน็ต *http://www.lawteacher.net/criminal-law/acts/computer-misuse-act-1990.php* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

[40] เว็บไซต์สำนักงานอัยการประเทศอังกฤษ *https://www.cps.gov.uk/legal-guidance/computer-misuse-act-1990* สืบค้นเมื่อวันที่ 1 มิถุนายน 2561

[41] เว็บไซต์หน่วยงานพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ ประเทศอังกฤษ *http://www.computerevidence.co.uk/Cases/CMA.htm* และเว็ปไซต์มหาวิทยาลัยบริสตอล *http://www.cs.bris.ac.uk/Teaching/Resources/COMSM2005/Lecture14.pdf* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

1.1.2 ความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจเพื่อจะกระทำหรืออำนวยความสะดวกในการกระทำความผิดอื่น

1.1.3 ความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์

1.1.4 ความผิดเกี่ยวกับการทำ จัดหาหรือรับไว้ซึ่งสิ่งใดๆ เพื่อใช้ในการกระทำความผิดตามมาตรา 1 หรือมาตรา 3

1.1.1 ความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ได้วางข้อกำหนดการกระทำที่ถือว่าเป็นความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจหรือปราศจากข้ออ้าง หรือข้อแก้ตัวตามกฎหมายไว้ในมาตรา 1 โดยมีใจความสำคัญดังต่อไปนี้

อนุมาตรา (1) บุคคลจะมีความผิด เมื่อ..

(a) ผู้กระทำได้กระทำการให้คอมพิวเตอร์ปฏิบัติการหรือดำเนินการแสดงผลโดยเจตนาที่จะผ่านมาตรการป้องกันการเข้าถึงโปรแกรมคอมพิวเตอร์ใดๆ หรือข้อมูลที่เก็บรักษาไว้ในคอมพิวเตอร์ใดๆ

(b) ผู้กระทำผ่านมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ โดยปราศจากอำนาจ

(c) ผู้กระทำรู้อยู่ในขณะที่กระทำการให้คอมพิวเตอร์ปฏิบัติการหรือแสดงผลเป็นการกระทำโดยปราศจากอำนาจ

อนุมาตรา (2) เจตนาของผู้กระทำความผิดตามมาตรานี้ ไม่จำต้องมุ่งประสงค์ต่อ..

(a) ข้อมูลหรือโปรแกรมคอมพิวเตอร์ใดโดยเฉพาะ

(b) ข้อมูลหรือโปรแกรมคอมพิวเตอร์ประเภทใดโดยเฉพาะ หรือ

(c) ข้อมูลหรือโปรแกรมคอมพิวเตอร์ที่เก็บไว้ในเครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่งโดยเฉพาะ

อนุมาตรา (3) ผู้กระทำความผิดตามมาตรานี้ ต้องระวางโทษ..

(a) ระวางโทษในอังกฤษและเวลส์ จำคุกไม่เกิน 12 เดือน หรือปรับสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ

(b) ระวางโทษในสก๊อตแลนด์ จำคุกไม่เกิน 6 เดือน หรือปรับสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ

(c) กรณีเป็นความผิดที่ร้ายแรง ระวางโทษจำคุกไม่เกิน 2 ปี หรือปรับสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ

บทบัญญัติตามมาตรา 1 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) วางองค์ประกอบของความผิดให้การเข้าถึง (access) ข้อมูลหรือโปรแกรมคอมพิวเตอร์ โดยต้องมีการกระทำอย่างใดๆ ให้ระบบปฏิบัติการของคอมพิวเตอร์ทำงาน และไม่ว่าการเข้าถึงจะประสบความสำเร็จหรือไม่ก็เป็นความผิดแล้ว หากเปรียบเทียบกับความผิดฐานบุกรุก กรณีการเข้าถึงเพียงการเคาะประตูบ้านก็ถือว่าเป็นการลงมือ กระทำความผิดแล้ว แม้อาจเข้าถึงไม่สำเร็จ ไม่สามารถผ่านมาตรการป้องกันของระบบคอมพิวเตอร์ ไปได้ก็ตาม

การเข้าถึงไม่จำกัดว่าผู้กระทำมีความมุ่งหมายเข้าถึงข้อมูลหรือโปรแกรมคอมพิวเตอร์ใดโดยเฉพาะเจาะจงหรือไม่ก็ล้วนเป็นความผิด เสมือนหนึ่งบุกรุกเข้าไปในบ้านผู้อื่น โดยที่มิได้มีเป้าประสงค์สิ่งใดหรือทรัพย์ใดในบ้าน เพียงล่วงล้ำเข้าไปในบ้านโดยปราศจากอำนาจตามกฎหมายหรือ ความยินยอมจากผู้ที่มีสิทธิให้ความยินยอมก็เป็นความผิดฐานบุกรุกแล้ว

อนึ่ง การเข้าถึงนี้ต้องมีการผ่านมาตรการป้องกันการเข้าถึงด้วย เช่น การผ่านเข้าไปโดยการแฮ็ก (hack) รหัสผู้ใช้ (password) หรือฝ่าโปรแกรมป้องกันระบบ (firewall) เข้าไปในระบบคอมพิวเตอร์ เป็นต้น ดังนั้น จึงไม่รวมถึงกรณีที่ผู้มีสิทธิเข้าถึงระบบคอมพิวเตอร์เปิดหน้าจอมอนิเตอร์ทิ้งไว้ แล้วมีผู้เดินผ่านมาเห็นหรืออ่านที่หน้าจอมอนิเตอร์

อย่างไรก็ตาม ความผิดตามมาตรานี้จะต้องเป็นการเข้าถึงโดยปราศจากอำนาจและผู้กระทำต้องรู้ในขณะกระทำการเข้าถึงระบบคอมพิวเตอร์ด้วยว่าตนกำลังเข้าถึงโดยปราศจากอำนาจ ประเด็นนี้เป็นปัญหาสำคัญและยากต่อการพิสูจน์ถึงองค์ประกอบภายในประการนี้ หากจำเลยเป็นบุคคลากรขององค์กรแห่งนั้นๆ ทั้งการมีอำนาจเข้าถึงหรือไม่ หรือการมีอำนาจเข้าถึงแค่ไหนเพียงไร หรือการได้รับอนุญาตหรือความยินยอมหรือไม่ ใครเป็นผู้มีสิทธิให้การอนุญาตหรือความยินยอม ปัญหานี้เป็นเหตุแห่งการยกฟ้องคดีโดยศาลยุติธรรมของประเทศอังกฤษหลายต่อหลายคดี อาทิ

ในคดี DPP v. Bignell [1998] จำเลยเป็นเจ้าหน้าที่ตำรวจของสำนักงานตำรวจแห่งชาติ ถูกดำเนินคดีฟ้องร้องข้อหาเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจตามมาตรา 1 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) โดยข้อเท็จจริงในคดีนี้ จำเลยซึ่งเป็นเจ้าหน้าที่ตำรวจของสำนักงานตำรวจแห่งชาติใช้คอมพิวเตอร์ขององค์กรเข้าถึงข้อมูลและระบบคอมพิวเตอร์ขององค์กร เพื่อให้ได้ข้อมูลสำหรับการใช้งานเพื่อประโยชน์ส่วนตัว อย่างไรก็ตาม องค์กรผู้บังคับใช้กฎหมายไม่สามารถดำเนินคดีต่อการกระทำของเขา เพราะเหตุว่าการกระทำนั้นไม่ได้อยู่ในความหมายของพระราชบัญญัติว่าด้วย

การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) มาตรา 1 ฐานเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ความผิดฐานนี้มีเจตนารมณ์เพื่อใช้กับแฮ็กเกอร์ (hacker) จากภายนอก ดังนั้น ศาลยุติธรรมของประเทศอังกฤษจึงพิพากษายกฟ้องจำเลย[42]

ข้อสังเกต

คดีนี้ จำเลยเป็นผู้มีสิทธิใช้รหัสผ่าน (password) เข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ขององค์กรได้ ซึ่งรหัสผ่านคือบัตรอิเล็กทรอนิกส์ตามมาตรา 1 (14) (ข) ตามประมวลกฎหมายอาญาของไทย แม้จำเลยจะใช้รหัสผ่านเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ขององค์กรเพื่อประโยชน์ส่วนตัว ก็เป็นเพียงการใช้ที่ผิดวัตถุประสงค์เท่านั้น หาได้ไม่มีสิทธิใช้หรือใช้โดยปราศจากอำนาจไม่ เช่นนี้ หากเปรียบกับฐานความผิดมาตรา 269/5 ตามประมวลกฎหมายอาญาของไทย ฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบแล้ว นี่เป็นกรณีที่น่าคิดว่าไม่สามารถปรับบทลงโทษแก่จำเลยได้ เพราะจำเลยเป็นผู้ที่มีสิทธิหรือมีอำนาจใช้บัตรอิเล็กทรอนิกส์นั้น

อนึ่ง นอกจากข้อกฎหมายประเด็นการเข้าถึงโดยปราศจากอำนาจโดยรู้อยู่ หรือการได้รับอนุญาตหรือได้รับความยินยอมโดยถูกต้องหรือไม่ ซึ่งได้กล่าวถึงในคดี DPP v Bignell [1998] ข้างต้นแล้ว ข้อต่อสู้อีกประการที่ทำให้ศาลยุติธรรมของประเทศอังกฤษพิพากษายกฟ้องจำเลย คือ การที่จำเลยกล่าวอ้างว่า จำเลยเสพติดการแฮ็ก (addicted to hacking) ลักษณะอาการ เสพติดการแฮ็กดังกล่าว เสมือนหนึ่งอาการป่วยทางจิต ซึ่งจำเลยใช้เป็นข้อต่อสู้คดีจนหลุดพ้นจาก ความรับผิดทางอาญา ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) หากจะกล่าวไป ข้อต่อสู้ดังกล่าวมิใช่ประเด็นข้อกฎหมายอันเกิดจาก บทบัญญัติของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) โดยตรง แต่เป็นข้อต่อสู้ที่มีอยู่ตามปกติของกฎหมายอาญา ซึ่งอาจเปรียบได้กับมาตรา 65 ตามประมวลกฎหมายอาญาของไทย คือ การอ้างว่าเป็นผู้กระทำความผิดจิตบกพร่อง โรคจิตหรือจิตฟั่นเฟือน และได้กระทำในขณะที่ไม่รู้ผิดชอบ

ในคดี R v. Paul Bedworth จำเลยในคดีนี้ถูกฟ้องร้องตามมาตรา 1 และมาตรา 3 ของ Computer Misuse Act 1990 ต่อศาล Crown Court ซึ่งมีเขตอำนาจศาลเหนือคดีที่มีอัตราโทษสูงกว่าศาลแขวง (Magistrates Court) และคดีนี้การกระทำของจำเลยเข้าขั้นความผิดร้ายแรง ทั้งพัวพันกับจำเลยในคดีอื่นอีก เช่น R v Strickland, R v Woods, R v Richard Goulden และอีกหลายคน ซึ่งพวกเขาเรียกตัวเองว่าแก๊งค์แปดคนเล็ก ๆ สีเขียว (groove machine

---

[42] เว็บไซต์อาจารย์นิติศาสตร์ดอทเน็ต *http://www.lawteacher.net/criminal-law/acts/computer-misuse-act-1990.php* และเว็บไซต์หน่วยงานพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ ประเทศอังกฤษ *http://www.computerevidence.co.uk/Cases/CMA.htm* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

: 8LGM) โดยก่อความเสียหายเป็นวงเงินที่ค่อนข้างสูง โดยข้อเท็จจริงมีอยู่ว่า พวกจำเลยแฮ็กเข้าไปในเว็บไซต์ชื่อดังขององค์กรขนาดใหญ่หลายแห่ง เช่น Janet, BT, Financial Times, ITN's Oracle network เครือข่ายของนาซ่า เว็บไซต์คณะกรรมาธิการยุโรป โดยความเสียหายที่ถูกกล่าวหาว่าเกิดจากการกระทำของจำเลยเป็นเงิน 120,000 ปอนด์ ไฮไลท์ของปัญหาในคดีนี้ คือ การพิสูจน์ “เจตนา” ตามกฎหมายอาญาว่าจำเลยเป็นผู้กระทำความผิด ซึ่งจำเลยต่อสู้คดีอ้างการเสพติดการแฮ็กเป็นอาการป่วยที่ทำให้การกระทำของจำเลยขาดเจตนา กล่าวคือ จำเลยไม่อาจควบคุมตนเอง หรือกระทำไปโดยไม่รู้ผิดชอบในขณะกระทำ ประเด็นของคดี จึงมีว่าการที่เสพติดการแฮ็ก และนาย Paul Bedworth กล่าวอ้างว่าเขาไม่สามารถที่จะมีความตั้งใจหรือเจตนาในการกระทำความผิดใด ๆ ตามกฎหมาย ซึ่งได้รับการตรวจพิสูจน์โดยผู้เชี่ยวชาญด้านจิตเวชเป็นพยานที่ยืนยันเป็นหลักฐานว่า จำเลยเสพติดการแฮ็ก นาย Bedworth ถูกศาลยุติธรรมของประเทศอังกฤษ (Crown Court) แห่งเมือง Southwark พิพากษาชี้ขาดให้พ้นผิด[43]

ส่วนตัวอย่างคดีของการฝ่าฝืนข้อห้ามตามมาตรา 1 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ฐานเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์โดยปราศจากอำนาจ อาทิ

คดีแรก ในคดี Ellis v. DPP [2001] จำเลยถูกฟ้องร้องดำเนินคดีในฐานความผิดเข้าถึงข้อมูล หรือระบบคอมพิวเตอร์โดยปราศจากอำนาจ ตามมาตรา 1 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ข้อเท็จจริงของคดีนี้ จำเลยเคยเป็นศิษย์เก่าของมหาวิทยาลัย ซึ่งมีสิทธิเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ของมหาวิทยาลัย ภายหลังจำเลยสำเร็จการศึกษาไปแล้ว จำเลยไม่มีสิทธิเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ของมหาวิทยาลัย แต่จำเลยยังคงกระทำเช่นนั้นอย่างต่อเนื่อง จำเลยฝ่ามาตรการป้องกันการเข้าถึงข้อมูล หรือระบบคอมพิวเตอร์เครือข่ายของมหาวิทยาลัย โดยมิได้มีความมุ่งหมายเฉพาะเจาะจงต่อข้อมูล หรือโปรแกรมคอมพิวเตอร์ใด ศาลยุติธรรมของประเทศอังกฤษ (ศาลแขวง :

---

[43] เว็บไซต์อาจารย์นิติศาสตร์ดอทเน็ต *http://www.lawteacher.net/criminal-law/acts/computer-misuse-act-1990.php* และเว็บไซต์หน่วยงานพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ ประเทศอังกฤษ *http://www.computerevidence.co.uk/Cases/CMA.htm* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561 และ Yaman Akdeniz, Faculty of Law University of Leeds, *Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!* , เว็บไซต์คณะนิติศาสตร์ มหาวิทยาลัยลีดส์ *http://www.bailii.org/cgi-bin/format.cgi?doc=/uk/other/journals/WebJCLI/1996/issue3/akdeniz3.html&query=(Yaman)+AND+(Akdeniz)* สืบค้นเมื่อวันที่วันที่ 10 สิงหาคม พ.ศ. 2561

Magistrates Court) วินิจฉัยชี้ขาดให้จำเลยมีความผิดตามมาตรา 1 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990)[44]

คดีที่สอง R v. Susan Holmes [15/02/2008] คดีนี้ จำเลยถูกจับกุมโดยสก๊อตแลนด์ยาร์ดในเดือนตุลาคม 2007 และต่อมาถูกดำเนินคดีฟ้องร้องในข้อหาเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ โดยปราศจากอำนาจ ตามมาตรา 1 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) โดยข้อเท็จจริงของคดีนี้มีอยู่ว่า จำเลยเป็นอดีตลูกจ้างของหน่วยงาน Nannies Inc ซึ่งเป็นผู้มีอำนาจเข้าถึงจดหมายอิเล็กทรอนิกส์ของอดีตนายจ้าง ภายหลังจำเลยออกจากหน่วยงาน Nannies Inc ไปอยู่กับหน่วยงานอื่นที่เป็นคู่แข่ง แต่จำเลยยังคงใช้ รหัสผ่าน (password) เข้าถึงบัญชีจดหมายอิเล็กทรอนิกส์ (AOL) ของนายจ้างเก่าโดยที่ปราศจากอำนาจไปแล้ว Nannies Inc นายจ้างเก่าเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ (AOL) แล้วเห็นความผิดปกติ ซึ่งเกิดขึ้นระหว่างเดือนมกราคมถึงมีนาคม 2007 จึงทำการสอบถามไปยัง AOL เพื่อให้ช่วยตรวจสอบสืบค้น ปรากฏว่า AOL พบการเชื่อมต่อและเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ (AOL) จากหลายที่อยู่ (IP addresses) และ AOL สืบไปถึงที่อยู่ (IP addresses) ซึ่งเชื่อมโยงถึงจำเลย หมายความว่า แม้จำเลยออกจากหน่วยงาน Nannies Inc ไปอยู่กับหน่วยงานคู่แข่งแล้ว แต่ยังคงใช้รหัสผ่านเข้าอ่านจดหมายอิเล็กทรอนิกส์ของนายจ้างเก่าอยู่ เช่นนี้ ศาลยุติธรรมของประเทศอังกฤษ (ศาลแขวง : Magistrates Court) จึงพิพากษาว่า จำเลยมีความผิดฐานเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์โดยปราศจากอำนาจ ตามมาตรา 1 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990)[45]

ข้อสังเกต

สำหรับสองคดีข้างต้น มีข้อสังเกตอยู่ 2 ประการ ดังนี้

ประการแรก ทั้งสองคดีต่างกันตรงที่คดีแรกจำเลย Ellis ไม่มีความมุ่งหมายเฉพาะเจาะจงต่อข้อมูลหรือโปรแกรมคอมพิวเตอร์ แต่คดีหลัง Susan Holmes มีความมุ่งหมายเฉพาะเจาะจงที่จะเข้าถึงข้อมูลคอมพิวเตอร์ คือ ข้อมูลในจดหมายอิเล็กทรอนิกส์ แต่ทั้งสองคดีก็มีความผิดตามมาตรา 1 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) เช่นเดียวกัน

---

[44] เว็บไซต์หนังสืออิเล็กทรอนิกส์ *http://books.google.co.th/books?id=-VtTiR8niBEC&pg=PR16&lpg=PR16&dq=Ellis+v+DPP+%5B2001%5D&source=bl&ots=6zt68mcNJk&sig=LvD2CsrelerffCv1Yfw0-u5yXRE&hl=th&ei=FK89TcGgLYbluAPH-p3fCg&sa=X&oi=book_result&ct=result&resnum=5&ved=0CDQQ6AEwBA#v=onepage&q=Ellis%20v%20DPP%20%5B2001%5D&f=false* , หน้า 442 สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

[45] John Leyden เว็บไซต์เดอะรีจิสเตอร์ *http://www.theregister.co.uk/2008/02/18/nanny_agency_hack_conviction/* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

ประการที่สอง ทั้งสองคดีหากเปรียบเทียบกับประมวลกฎหมายอาญาของไทยว่าด้วยความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์แล้ว ทั้งสองกรณีมีความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/5 เช่นเดียวกัน กล่าวคือ กรณี Susan Holmes แม้ครั้งหนึ่งเคยมีสิทธิ หรือมีอำนาจที่จะใช้ แต่เมื่อสิทธิหรืออำนาจที่จะใช้หมดไปแล้ว ย่อมเป็นการใช้โดยมิชอบด้วยกฎหมาย ส่วนกรณี Ellis รหัสผ่าน (password) นั้นตนเคยเป็นผู้ถือสิทธิ แต่เมื่อ Ellis สำเร็จการศึกษาไปแล้ว สถานภาพของการเป็นผู้ถือสิทธิก็หมดไป ย่อมหมายความว่า Ellis ไม่ใช่ผู้ถือสิทธิในรหัสผ่านนั้นอีกต่อไป รหัสผ่านนั้นเป็นสมบัติของทางมหาวิทยาลัย เมื่อ Ellis ยังคงหาช่องทางเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ของมหาวิทยาลัย ย่อมเป็นการกระทำโดยมิชอบด้วยกฎหมาย

1.1.2 ความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจเพื่อจะกระทำหรืออำนวยความสะดวกในการกระทำความผิดอื่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ได้วางข้อกำหนดการกระทำที่ถือว่าเป็นความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจเพื่อจะกระทำหรืออำนวยความสะดวกในการกระทำความผิดอื่นไว้ในมาตรา 2 โดยมีใจความสำคัญ ดังต่อไปนี้

อนุมาตรา (1) ผู้ที่จะมีความผิดตามมาตรานี้ หากว่ากระทำความผิดตามมาตรา 1 โดยเจตนา

(a) กระทำในสิ่งที่มาตรานี้บังคับใช้ หรือ

(b) เพื่อให้ความสะดวกในการกระทำความผิดอย่างอื่น (ความผิดอย่างอื่นนั้นไม่ว่าจะกระทำด้วยตนเองหรือโดยบุคคลอื่น) และความผิดที่เขาตั้งใจจะกระทำการหรืออำนวยความสะดวก ให้ถือว่าเป็นความผิดที่บัญญัติไว้ในมาตรานี้

อนุมาตรา (2) มาตรานี้ใช้กับการตัดสินชี้ขาด..

(a) สำหรับความผิดที่ระบุไว้ในกฎหมาย หรือ

(b) สำหรับผู้กระทำความผิดที่มีอายุตั้งแต่ 21 ปีขึ้นเป็น (18 ปี สำหรับในประเทศอังกฤษและเวลส์)[46]

อนุมาตรา (3) เพื่อวัตถุประสงค์ของมาตรานี้ ไม่ว่าความผิดที่จะกระทำนั้นรวมทั้งจะได้กระทำลงในขณะที่มีการเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจ หรือจะได้กระทำในเวลาอื่น ๆ ต่อไปก็ตาม

อนุมาตรา (4) ผู้กระทำอาจมีความผิดตามมาตรานี้ แม้ปรากฏข้อเท็จจริงว่าการกระทำความผิดที่จะกระทำนั้นเป็นกรณีที่เป็นไปไม่ได้

---

[46] เว็บไซต์หอจดหมายเหตุแห่งชาติประเทศอังกฤษ *http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=1353366* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

อนุมาตรา (5) ผู้กระทำความผิดตามมาตรานี้ ต้องระวางโทษ

(a) ในอังกฤษและเวลส์ ต้องระวางโทษจำคุกไม่เกิน 12 เดือน หรือปรับไม่เกินสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ

(b) ในสก๊อตแลนด์ ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ

(c) กรณีเป็นความผิดร้ายแรง ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับเป็นเงิน หรือทั้งจำทั้งปรับ

กล่าวโดยสรุป ความผิดตามมาตรานี้ ได้วางองค์ประกอบของความผิดที่อาจกล่าวได้ว่า ต่อเนื่องจากความผิดตามมาตรา 1 ซึ่งบัญญัติถึงการ “เข้าถึง” ข้อมูลหรือระบบคอมพิวเตอร์โดยปราศจากอำนาจ แต่มาตรา 2 นี้ ผู้กระทำความผิดมีลักษณะแห่งการกระทำที่มีวัตถุประสงค์เป็นอันตรายมากกว่า กล่าวคือ ผู้กระทำไม่เพียงเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์โดยปราศจากอำนาจเท่านั้น หากต้องการที่จะกระทำความผิดอย่างอื่นหรืออำนวยความสะดวกในการที่จะกระทำความผิดอย่างอื่นด้วย ซึ่งอาจกระทำความผิดไปในขณะหรือต่อเนื่องกันไปกับการเข้าถึงหรืออาจปูทางไว้สำหรับจะกระทำความผิดในโอกาสต่อไป

ในคดี R v. Malcolm Farquharson (09/12/1993) จำเลยทั้งสองถูกฟ้องร้องดำเนินคดีต่อศาลยุติธรรม (ศาลแขวง : Magistrates Court) เมือง Croydon ตามมาตรา 1 คือ ข้อหาเข้าถึงข้อมูล หรือระบบคอมพิวเตอร์โดยปราศจากอำนาจ และมาตรา 2 คือ เข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจ เพื่อจะกระทำหรืออำนวยความสะดวกในการกระทำความผิดอื่นแห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) โดยข้อเท็จจริงมีอยู่ว่า จำเลยสมรู้ร่วมคิดกับนาย Pearce ซึ่งถูกดำเนินคดีฟ้องร้องในอีกคดีหนึ่ง (R v. Pearce) แฮ็ก (hacking) เข้าไปในระบบคอมพิวเตอร์เพื่อเข้าถึงข้อมูลเกี่ยวกับโทรศัพท์เคลื่อนที่ โดยมีวัตถุประสงค์เพื่อให้ได้ข้อมูลเกี่ยวกับโทรศัพท์เคลื่อนที่นั้นไปปรับจูน (cloning) โทรศัพท์เคลื่อนที่ การกระทำของจำเลยทั้งสาม (คดีนี้สองคนและอีกคดีหนึ่งคน) เป็นการกระทำที่ผิดตามมาตรา 1 ฐานเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์โดยปราศจากอำนาจ และการที่จำเลยมีเป้าหมายเพื่อให้ได้ข้อมูลเกี่ยวกับโทรศัพท์เคลื่อนที่ไปเพื่อปรับจูน เป็นการกระทำที่ผิดตามมาตรา 2 คือ เข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจเพื่อจะกระทำหรืออำนวยความสะดวกในการกระทำความผิดอื่น ศาลยุติธรรม (ศาลแขวง : Magistrates Court) เมือง Croydon พิพากษาลงโทษจำคุกจำเลยทั้งสองในคดีนี้ คนละ 6 เดือน[47]

---

[47] เว็บไซต์หน่วยงานพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ ประเทศอังกฤษ *http://www.computer evidence.co.uk/Cases/CMA.htm* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

ข้อสังเกต

คดีนี้ เมื่อวิเคราะห์ข้อเท็จจริงตามกฎหมายไทย ผู้วิจัยมีข้อสังเกตอยู่ 2 ประการ ดังนี้

ประการแรก จะพบว่าเป็นการกระทำที่เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เช่นเดียวกัน ตามมาตรา 5 ฐานเข้าถึงระบบคอมพิวเตอร์ โดยมิชอบ และมาตรา 7 ฐานเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ โดยมิชอบ หากแต่มาตรา 7 นี้ไม่ต้องการองค์ประกอบที่ว่าด้วย **“เพื่อจะกระทำหรืออำนวยความสะดวกในการกระทำความผิดอื่น”** อันต่างจากมาตรา 2 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990)

ประการที่สอง นอกจากนี้ เมื่อวิเคราะห์ประมวลกฎหมายอาญาว่าด้วยความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ข้อเท็จจริงในคดีนี้จะต้องด้วยมาตรา 269/2 ฐานทำ หรือมีเครื่องมือ หรือวัตถุสำหรับปลอมหรือแปลง หรือเพื่อใช้ หรือให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ กล่าวคือ โทรศัพท์เคลื่อนที่ และซิมการ์ดอยู่ในความหมายของบัตรอิเล็กทรอนิกส์ในรูปวัตถุอื่นใด ตามมาตรา 1 (14) (ก) แห่งประมวลกฎหมายอาญา เช่นนี้ การนำข้อมูลเกี่ยวกับโทรศัพท์เคลื่อนที่ไปปรับจูนก็คือการปลอมบัตรอิเล็กทรอนิกส์ ดังนั้น อุปกรณ์หรือเครื่องคอมพิวเตอร์ที่จำเลยทั้งสองในคดี R v. Malcolm Farquharson ใช้ในการกระทำความผิด ก็คือ เครื่องมือหรือวัตถุสำหรับกระทำการปลอมบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/2 นั่นเอง

1.1.3 ความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ได้วางข้อกำหนดการกระทำที่ถือว่าเป็นความผิดเกี่ยวกับการกระทำความผิดฐานเข้าถึงโดยปราศจากอำนาจทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ ไว้ในมาตรา 3 โดยมีใจความ สำคัญ ดังต่อไปนี้[48]

อนุมาตรา (1) บุคคลจะมีความผิด เมื่อ..

(a) เขากระทำการเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจ

(b) ผู้กระทำรู้อยู่ในขณะที่กระทำว่าตนกระทำไปโดยปราศจากอำนาจ และ

(c) องค์ประกอบ (ในอนุมาตรา 1 นี้) ใช้บังคับกับอนุมาตรา 2 หรืออนุมาตรา 3

อนุมาตรา (2) อนุมาตรานี้ใช้บังคับ ถ้าบุคคลเจตนากระทำความผิด

---

[48] มาตรา 3 ได้รับการแก้ไขเพิ่มเติม และมีผลบังคับใช้เมื่อวันที่ 10 มกราคม 2007, Police and Justice Act 2006 เว็บไซต์หอจดหมายเหตุแห่งชาติประเทศอังกฤษ *http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=1353366* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

(a) ทำให้เกิดความเสียหายต่อระบบปฏิบัติการของคอมพิวเตอร์

(b) กีดกันหรือขัดขวางการเข้าถึงข้อมูลหรือโปรแกรมของระบบคอมพิวเตอร์

(c) ทำให้เกิดความเสียหายต่อโปรแกรมหรือความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ หรือ

(d) เพื่อให้การกระทำต่างๆ ที่กล่าวถึงตาม (a) ถึง (c) ข้างต้นบรรลุผล

อนุมาตรา (3) อนุมาตรานี้บังคับใช้ ถ้าบุคคลกระทำโดยประมาทเป็นเหตุให้เกิดลักษณะต่างๆ ที่กล่าวถึงตาม (a) ถึง (c) ของอนุมาตรา (2) ข้างต้น

อนุมาตรา (4) เจตนาที่กล่าวถึงในอนุมาตรา (2) ข้างต้น หรือความประมาทที่กล่าวถึงในอนุมาตรา (3) ข้างต้น ไม่จำต้องเกี่ยวกับ..

(a) คอมพิวเตอร์เตอร์เครื่องใดโดยเฉพาะเจาะจง

(b) ข้อมูลหรือโปรแกรมใดโดยเฉพาะเจาะจง หรือ

(c) ข้อมูลหรือโปรแกรมประเภทใดโดยเฉพาะเจาะจง

อนุมาตรา (5) ภายใต้บทมาตรานี้

(a) การกล่าวอ้างถึงการกระทำความผิดให้รวมถึงผู้มีส่วนร่วมในการกระทำความผิดด้วย

(b) การกระทำให้หมายความรวมถึงการกระทำที่เกี่ยวเนื่องด้วย

(c) การกล่าวถึงความเสียหาย การกีดกันหรือขัดขวางให้รวมถึงการให้เกิดผลแม้เพียงชั่วคราว

อนุมาตรา (6) ผู้กระทำความผิดตามมาตรานี้ ต้องระวางโทษ..

(a) ในอังกฤษและเวลส์ ต้องระวางโทษจำคุกไม่เกิน 12 เดือน หรือปรับไม่เกินสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ

(b) ในสก๊อตแลนด์ ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ

(c) กรณีเป็นความผิดร้ายแรง ต้องระวางโทษจำคุกไม่เกินสิบปี หรือปรับเป็นเงิน หรือทั้งจำทั้งปรับ

ความผิดตามมาตรา 3 ฐานความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ข้างต้นนี้ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) วางองค์ประกอบของความผิดหมายความรวมถึง การเข้าถึงโดยปราศจากอำนาจทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือขัดขวาง หรือกีดกันการเข้าถึงข้อมูลคอมพิวเตอร์ หรือทำให้เกิดความเสียหายต่อโปรแกรมคอมพิวเตอร์ หรือความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ ไม่ว่าจะกระทำโดยเจตนาหรือประมาท โดย

จะมีความมุ่งหมายต่อคอมพิวเตอร์เครื่องหนึ่งเครื่องใดหรือโปแกรมหรือข้อมูลคอมพิวเตอร์โดยเฉพาะเจาะจงหรือไม่ก็ตาม ล้วนถูกกำหนดให้เป็นความผิดตามมาตรานี้ ทั้งนี้ ยังหมายความรวมถึงผู้มีส่วนร่วมกระทำความผิด ไม่ว่าจะตัวการ ผู้ใช้ ผู้สนับสนุน และการกระทำที่เกี่ยวเนื่อง ซึ่งอาจทำความเสียหายให้ ไม่ว่าจะชั่วคราวหรือถาวร

ลักษณะแห่งการกระทำที่ต้องด้วยมาตรานี้ ซึ่งก่อความเสียหายอาจกระทำด้วยการแฮ็กเข้าไปลบหรือเปลี่ยนแปลงแก้ไขโปรแกรมหรือข้อมูลคอมพิวเตอร์ ย้ายและคัดลอกแทนที่ด้วยโปรแกรม หรือข้อมูลคอมพิวเตอร์อื่น หรือการเข้าถึงแล้วทำลายฐานข้อมูลของธุรกิจคู่แข่ง หรือเข้าไปคัดลอกเอาข้อมูลทางการเงิน การบัญชี หมายเลขบัญชีของสถาบันการเงิน ข้อมูลเกี่ยวกับบัตรเครดิต ข้อมูลผู้ใช้ (username) และรหัสผ่าน (password) ต่างๆ หรืออาจทำความเสียหายด้วยการปล่อยไวรัส หนอนไวรัส โทรจัน หรือการยิงนุก หรือการเข้ายึดอำนาจการบริหารจัดการเว็บไซด์ ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ได้บัญญัติกำหนดการตีความ (interpretation) ถ้อยคำต่างๆ ของกฎหมายฉบับนี้ไว้

วัตถุประสงค์ของมาตรา 3 ส่วนหนึ่งเป็นการบัญญัติขึ้นเพื่อแก้ไขปัญหาของคำว่าทรัพย์สิน (property) ตามกฎหมาย The Criminal Damage Act 1971 และ Theft Act 1968/1978/1996 รวมถึงคำว่าเอกสาร ตามกฎหมาย Forgery and Counterfeiting Act 1981 ซึ่งทั้งคำว่าทรัพย์สินและ คำว่าเอกสารมิได้มีความหมายครอบคลุมบรรดาข้อมูลและโปรแกรมคอมพิวเตอร์เหล่านี้ เพราะ เหตุว่า ข้อมูลและโปรแกรมคอมพิวเตอร์ไม่ใช่วัตถุมีรูปร่างที่จะถูกลักเอาในลักษณะที่เป็นการตัด การครอบครองหรือตัดกรรมสิทธิ์ไปได้อย่างทรัพย์ และทั้งไม่ใช่เอกสารที่สามารถประจักษ์แก่สายตาอย่างคงทนถาวรที่จะใช้อ้างอิงเป็นพยานหลักฐานอย่างเอกสารได้ โดยเฉพาะ Forgery and Counterfeiting Act 1981 ได้บัญญัติกำหนดนิยามความหมายของคำว่าเอกสารไว้แล้ว ตามมาตรา 5 (5) ซึ่งได้กล่าวถึงข้างต้นแล้ว

คดีตัวอย่างสำหรับมาตรา 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) จะได้กล่าวถึง 2 คดี ดังนี้

คดีแรก ตัวอย่างคดีที่สำคัญสำหรับความผิดที่กระทำลงภายใต้บทบัญญัติมาตรา 3 นี้ ก็คือ การกระทำของกลุ่มที่เรียกตนเองว่า “แก๊งค์แปดคนเล็กๆ สีเขียว” (groove machine : 8LGM) ซึ่งแม้นาย Paul Bedworth หนึ่งในสมาชิกของกลุ่มจะหลุดพ้นความรับผิดไปได้ในคดีของเขา โดยอ้างการเสพติดการแฮ็กว่าเป็นอาการป่วยทางจิต จนศาลยุติธรรมของประเทศอังกฤษ (Crown Court) แห่งเมือง Southwark พิพากษาชี้ขาดยกฟ้อง แต่ข้ออ้างที่ทำให้นาย Paul Bedworth พ้นผิดนี้ เป็นเหตุส่วนตัวนาย Paul Bedworth คนเดียว มิใช่เหตุในลักษณะคดีอันจะส่งผลต่อบรรดาผู้ร่วมกระทำความผิดได้ บรรดาผู้ร่วมกระทำความผิดอื่นๆ ใน “แก๊งค์แปดคนเล็กๆ

สีเขียว” (groove machine : 8 LGM) ถูกฟ้องร้องดำเนินคดีจนถูกพิพากษาตัดสินให้มีความผิดตามมาตรา 3 ดังคดีสำคัญซึ่งจะกล่าวต่อไปนี้

ในคดี R v. Strickland, R v. Woods [21 พฤษภาคม 1993][49] คดีนี้ จำเลยถูกฟ้องร้องดำเนินคดีต่อศาลยุติธรรมของประเทศอังกฤษ (Crown Court) แห่งเมือง Southwark ในข้อหาความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจ ตามมาตรา 1 และข้อหาความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ ตามมาตรา 3 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990)

โดยข้อเท็จจริงในคดีนี้มีความเป็นมาว่า จำเลยสมรู้ร่วมคิดกับพวกทั้งหมดแปดคน เช่น นาย Karl Strickland นาย Neil Woods นาย Paul Bedworth เป็นต้น ทั้งแปดคนรู้จักกันบนกระดานสนทนาต่าง ๆ และติดต่อกันผ่านทางอินเทอร์เน็ตแลกเปลี่ยนข้อมูล รหัสผ่าน และช่องทางการแฮ็ก โดยติดต่อกันภายใต้ชื่อสมมติในโลกเสมือนจริง โดยที่ไม่ได้รู้จักกันมาก่อน และไม่มีใครรู้จักตัวจริง ชื่อจริงของกันและกัน ทั้งแปดคนสมรู้ร่วมคิดกันแฮ็คเว็บไซต์องค์กรขนาดใหญ่ของหลายประเทศ ทั้งในอังกฤษ ยุโรป และอเมริกา ไม่ว่าจะเป็นองค์กรภาครัฐหรือองค์กรภาคเอกชน หรือเว็บไซต์ของสถาบันการศึกษา หรือเว็บไซต์ขององค์การระหว่างประเทศ เช่น เครือข่ายของมหาวิทยาลัย (Janet) BT สื่อมวลชน (Financial Times) ITN's Oracle network เครือข่ายขององค์การอวกาศนาซ่า เว็บไซต์คณะกรรมาธิการยุโรป บริษัทผู้ให้บริการการสื่อสารโทรศัพท์เคลื่อนที่บริติช เทเลคอม โปลีเทคนิคของใจกลางกรุงลอนดอน และเมื่อกลุ่มของจำเลยกระทำการแฮ็กเครือข่ายระบบคอมพิวเตอร์แต่ละครั้งก็จะทิ้งชื่อกลุ่ม “แก๊งค์แปดคนเล็กๆ สีเขียว” (groove machine : 8 LGM) ของตนไว้ การกระทำของกลุ่มคนทั้งแปดสร้างความเสียหายปั่นป่วนให้กับข้อมูลและระบบคอมพิวเตอร์กระจายไปในหลายประเทศ

ต่อมา ในวันที่ 26 มิถุนายน 1991 เจ้าหน้าที่ตำรวจจับกุมชายสามคนในเวลาประมาณเที่ยงคืน คือ นาย Karl Strickland นาย Neil Woods และนาย Paul Bedworth ภายในบ้านของแต่ละคน ขณะกำลังแฮ็กข้อมูลและระบบคอมพิวเตอร์ ภายหลังเมื่อถูกจับ จำเลยทั้งสามจึงรู้จักกัน ภายใต้การแนะนำของเจ้าหน้าที่ตำรวจ และถูกตั้งข้อหากระทำความผิดตามมาตรา 3 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ทั้งสามได้แฮ็กเข้าไปลักลอบใช้บริการโทรศัพท์เคลื่อนที่ของ บริติช เทเลคอม สองในสาม

---

[49] Yaman Akdeniz, Faculty of Law University of Leeds, *Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!* เว็บไซต์คณะนิติศาสตร์ มหาวิทยาลัยลีดส์ *http://www.bailii.org/cgi-bin/format.cgi?doc=/uk/other/journals/WebJCLI/1996/issue3/akdeniz3.html&query=(Yaman)+AND+(Akdeniz)* สืบค้นเมื่อวันที่วันที่ 10 สิงหาคม พ.ศ. 2561

คน คือ นาย Karl Strickland และนาย Neil Woods ถูกตัดสินให้มีความผิด อีกทั้งนาย Neil Woods ยังยอมรับอีกว่าเป็นผู้แฮ็กระบบคอมพิวเตอร์ของโปลีเทคนิคของใจกลางกรุงลอนดอน เป็นเหตุให้เกิดความเสียหายเป็นเงิน 15,000 ปอนด์ ส่วนนาย Karl Strickland เป็นผู้แฮ็กเข้าถึงระบบคอมพิวเตอร์ของ ITN's Oracle network และเครือข่ายขององค์การอวกาศนาซ่า

ศาลยุติธรรมของประเทศอังกฤษ (Crown Court) แห่งเมือง Southwark ตัดสินให้ทั้งสองมีความผิดตามมาตรา 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ให้จำคุกคนละหกเดือน

คดีที่สอง ในคดี R v. Richard Goulden [10 มิถุนายน 1992] สำหรับกรณีของนาย Richard Goulden ซึ่งแฮ็กระบบคอมพิวเตอร์ของบริษัทการพิมพ์ โดยกระทำต่อโปรแกรม apple workstation โดยเข้าไปแก้ไขข้อมูลด้วยการติดตั้งโปรแกรมรักษาความปลอดภัยให้การเข้าถึงระบบคอมพิวเตอร์ต้องใช้รหัสผ่าน ซึ่งแต่เดิมการเข้าถึงระบบคอมพิวเตอร์ของบริษัทแห่งนี้ไม่ต้องใช้รหัสผ่าน ทำให้มีเพียงนาย Richard Goulden คนเดียวเท่านั้นที่รู้รหัสผ่านสำหรับการเข้าถึงระบบคอมพิวเตอร์ของบริษัท ซึ่งนาย Richard Goulden กระทำไปเนื่องจากมีส่วนได้เสียและเพื่อปกป้องผลประโยชน์ของตน แต่ทางบริษัทกล่าวอ้างว่าได้รับความเสียหายจากการกระทำของนาย Richard Goulden เป็นเงิน 2,275 ปอนด์ และความเสียหายที่เกิดจากการที่บริษัทแห่งนี้ไม่สามารถดำเนินงานการพิมพ์ด้วยระบบคอมพิวเตอร์ เมื่อคำนวนจำนวนวันของการทำงานมีค่าเสียหายเป็นเงิน 36,000 ปอนด์ และทั้งค่าจ้างผู้เชี่ยวชาญมาแก้ไขการติดตั้งโปรแกรมรักษาความปลอดภัยที่นาย Richard Goulden ทำไว้อีก 1,000 ปอนด์ ศาลยุติธรรมของประเทศอังกฤษ (Crown Court) แห่งเมือง Southwark ตัดสินชี้ขาดให้รอการลงโทษและคุมประพฤติมีกำหนด 2 ปี และปรับ 1,650 ปอนด์[50]

ข้อสังเกต

สำหรับสองคดีตัวอย่างดังกล่าว เมื่อวิเคราะห์กับบทบัญญัติของกฎหมายไทยมีข้อสังเกตแยกออกเป็นสองประการ ดังนี้

ประการแรก ในคดี “แก๊งค์แปดคนเล็กๆ สีเขียว” (groove machine : 8 LGM) การแฮ็กเข้าไปตามเว็บไซต์ชื่อดังต่างๆ ย่อมมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 5 ฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ มาตรา 9 ฐานทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ และมาตรา 10 ฐานกระทำโดยมิชอบ เพื่อให้ระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจน ไม่

---

[50] Yaman Akdeniz, Faculty of Law University of Leeds, *Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!* เว็บไซต์คณะนิติศาสตร์ มหาวิทยาลัยลีดส์ *http://www.bailii.org/cgi-bin/format.cgi?doc=/uk/other/journals/WebJCLI/1996/issue3/akdeniz3.html&query=(Yaman)+AND+(Akdeniz)* สืบค้นเมื่อวันที่วันที่ 10 สิงหาคม พ.ศ. 2561

สามารถทำงานได้ตามปกติ โดยเฉพาะในส่วนที่มีการแฮ็กเข้าไปลักลอบใช้บริการโทรศัพท์ เคลื่อนที่ของบริติช เทเลคอม สามารถปรับบทได้กับความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ตามประมวลกฎหมายอาญา มาตรา 269/5 ฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ เพราะเหตุว่า หมายเลยโทรศัพท์เคลื่อนที่ก็คือบัตรอิเล็กทรอสิกส์ตามมาตรา 1 (14) (ข) คือเป็นบัตรอิเล็กทรอนิกส์ที่ไม่มีการออกเอกสารหรือวัตถุอื่นใดให้ เมื่อบุคคลทั้งสามคือ นาย Karl Strickland นาย Neil Woods และนาย Paul Bedworth แฮ็กเข้าไปในระบบคอมพิวเตอร์ ใช้หมายเลขโทรศัพท์เคลื่อนที่ของผู้อื่น โดยไม่มีกฎหมายรองรับสิทธิของตน กรณีเช่นนี้ หากเป็นข้อเท็จจริงที่เกิดขึ้นในประเทศไทย ผู้กระทำย่อมต้องด้วยมาตรา 269/5 ฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ส่วนข้อแก้ตัวของนาย Paul Bedworth ที่ว่าเสพติดการแฮ็ก อันเป็นอาการป่วยทางจิตที่ส่งผลถึงความรับผิดทางอาญา ประเด็นนี้ต้องพิเคราะห์ตามมาตรา 65 ของประมวลกฎหมายอาญา เป็นอีกกรณีหนึ่งแยกต่างหาก

อนึ่ง สำหรับการแฮ็กข้อมูลเกี่ยวกับโทรศัพท์เคลื่อนที่มราเป็นข้อมูลคอมพิวเตอร์ ซึ่งมีบัตรอิเล็กทรอนิกส์ตามกฎหมายไทยดังกล่าว แต่หากผู้กระทำความผิดไม่ได้นำไปใช้ปรับจูนโทรศัพท์หรือใช้ในการสื่อสาร ก็ไม่มีความผิดตามมาตรา 269/5 และเมื่อนำข้อมูลคอมพิวเตอร์เหล่านี้จำหน่ายก็ไม่มีกฎหมายอาญาบัญญัติเป็นความผิด อีกทั้งไม่มีความผิดฐานลักทรัพย์ เพราะข้อมูลคอมพิวเตอร์ไม่ใช่ทรัพย์ตามกฎหมายไทย

ประการที่สอง ในคดี R v. Richard Goulden การกระทำเช่นนี้มิได้ฝ่ามาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ จึงไม่ต้องด้วยมาตรา 5 และมาตรา 7 ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หากแต่เป็นเรื่องของมาตรา 9 ฐานทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ และมาตรา 10 ฐานกระทำโดยมิชอบ เพื่อให้ระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานได้ตามปกติ ข้อเท็จจริงกรณีนี้น่าคิดว่า การที่ระบบคอมพิวเตอร์ของบริษัทการพิมพ์ไม่ได้ติดตั้งระบบรักษาความปลอดภัยและไม่มีรหัสผ่าน (password) และเมื่อนาย Richard Goulden แฮ็กเข้าไปติดตั้งระบบป้องกันและรหัสผ่าน (Password) เช่นนี้ จะถือได้หรือไม่ว่าเป็นการปลอมบัตรอิเล็กทรอนิกส์ เนื่องจากหากเป็นการปลอมเอกสาร 264 ของประมวลกฎหมายอาญาก็ไม่จำต้องมีเอกสารที่แท้จริงอยู่แต่เดิม ครั้นเมื่อวิเคราะห์ถึงการปลอมบัตรอิเล็กทรอนิกส์ตามมาตรา 269/1 จะได้ข้อสรุปคือไม่สามารถเป็นความผิด เช่นเดียวกับมาตรา 264 เนื่องจากไม่ใช่กระทำเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นบัตรอิเล็กทรอนิกส์หรือเอกสารที่แท้จริง

1.1.4 ความผิดเกี่ยวกับการทำ จัดหาหรือรับไว้ซึ่งสิ่งใดๆ เพื่อใช้ในการกระทำความผิด ตามมาตรา 1 หรือมาตรา 3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ได้วางข้อกำหนดเป็นฐานความผิดใหม่ขึ้น โดยระบุให้การ กระทำที่ถือว่าเป็นความผิดเกี่ยวกับการทำ จัดหาหรือรับไว้หรือจัดซื้อ ซึ่งวัตถุสิ่งของ

ใดๆ เพื่อใช้ในการ กระทำความผิดตามมาตรา 1 หรือมาตรา 3 ไว้ในมาตรา 3 A โดยมีใจความสำคัญดังต่อไปนี้[51]

อนุมาตรา (1) บุคคลมีความผิด ถ้าเขาทำ ปรับใช้วัตถุ หรือจัดหาให้หรือเสนอจัดหาให้ซึ่งวัตถุหรือสิ่งใดๆ โดยเจตนาที่จะใช้ในการกระทำความผิด หรือให้ความช่วยเหลือ (สนับสนุน) ในการกระทำความผิด ภายใต้มาตรา 1 หรือมาตรา 3

อนุมาตรา (2) บุคคลมีความผิด ถ้าเขากระทำการที่น่าเชื่อได้ว่าให้ความช่วยเหลือ (สนับสนุนผู้สนับสนุนอีกชั้นหนึ่ง) ในการจัดหาหรือเสนอจัดหาวัตถุหรือสิ่งใดๆ เพื่อใช้ในการกระทำความผิด หรือให้ความช่วยเหลือในการกระทำความผิด ภายใต้มาตรา 1 หรือมาตรา 3

อนุมาตรา (3) บุคคลมีความผิด ถ้าเขาได้รับวัตถุหรือสิ่งใดๆ เพื่อใช้ในการกระทำความผิด หรือให้ความช่วยเหลือในการกระทำความผิด ภายใต้มาตรา 1 หรือมาตรา 3

อนุมาตรา (4) ภายใต้มาตรานี้ วัตถุสิ่งของใดๆ หมายรวมถึงโปรแกรมหรือข้อมูลคอมพิวเตอร์ที่จัดขึ้นในรูปแบบอิเล็กทรอนิกส์

อนุมาตรา (5) ผู้กระทำความผิดตามมาตรานี้ต้องระวางโทษ..

(a) ในอังกฤษและเวลส์ ต้องระวางโทษจำคุกไม่เกิน 12 เดือน หรือปรับไม่เกินสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ

(b) ในสก๊อตแลนด์ ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินสูงสุดตามกฎหมาย หรือทั้งจำทั้งปรับ

(c) กรณีเป็นความผิดร้ายแรง ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับหรือทั้งจำทั้งปรับ

ความผิดฐานนี้เป็นการบัญญัติขึ้นใหม่และมีผลบังคับใช้เมื่อปี ค.ศ. 2007 อันเป็นการอุดช่องว่างของกฎหมายตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) โดยที่แต่เดิมกฎหมายฉบับดังกล่าวข้างต้นไม่มีความผิดฐานนี้ด้วย การกำหนดให้การกระทำโดยเจตนาสำหรับการทำ หรือจัดหา หรือรับไว้ หรือจำหน่ายซึ่งวัตถุหรือสิ่งใดๆ ที่ใช้ในการกระทำความผิดตามมาตรา 1 และมาตรา 3 รวมถึงการกระทำของผู้ให้ความช่วยเหลือหรือให้ความสนับสนุน ซึ่งอาจกล่าวได้ว่ารวมถึงบรรดาผู้ร่วมกระทำความผิดทั้งหลาย

---

[51] มาตรา 3 A ได้รับการแก้ไขเพิ่มเติม โดยบัญญัติเพิ่มฐานความผิดนี้ขึ้นใหม่และมีผลบังคับใช้เมื่อวันที่ 10 มกราคม 2007, Police and Justice Act 2006 เว็บไซต์หอจดหมายเหตุประเทศอังกฤษ *http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=1353366* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

วัตถุหรือสิ่งใดๆ อาจเป็นระบบคอมพิวเตอร์ที่เป็นฮาร์ดแวร์ ซอฟท์แวร์ รวมถึงเครื่องมือ หรืออุปกรณ์ต่อพ่วงต่างๆ (accessory) ทั้งในรูปแบบระบบหรือข้อมูลคอมพิวเตอร์ หรือในรูปแบบอิเล็กทรกนิกส์ สำหรับจำหน่าย หรือใช้หรือเพื่อใช้ในการกระทำความผิดด้วย

ข้อสังเกต

มาตรานี้หากจะเปรียบกับกฎหมายไทยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประมวลกฎหมายอาญาว่าด้วยความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ จะแยกข้อสังเกตออกเป็น 3 ประการ ดังนี้

ประการแรก พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทยไม่ได้บัญญัติฐานความผิดทำ ปรับใช้วัตถุ หรือจัดหาให้หรือเสนอจัดหาให้ซึ่งวัตถุหรือสิ่งใดๆ โดยเจตนาที่จะใช้ในการกระทำความผิด หรือให้ความช่วยเหลือไว้ ซึ่งน่าสนใจว่าเป็นช่องว่างแห่งกฎหมายที่สมควรจะมีการแก้ไขเพิ่มเติมให้มีฐานความผิดลักษณะเดียวกันกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ของประเทศอังกฤษ อย่างไรก็ตาม ประเด็นนี้อยู่นอกเหนือขอบเขตการศึกษาวิจัย จึงไม่ได้วิเคราะห์เพื่อหาข้อสรุปและข้อเสนอแนะสำหรับประเด็นนี้

ประการที่สอง เมื่อวิเคราะห์เปรียบเทียบกับประมวลกฎหมายอาญาว่าด้วยความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ อาจเปรียบได้กับมาตรา 269/2 บัญญัติว่า *“ผู้ใดทำเครื่องมือหรือวัตถุสำหรับปลอมหรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลง สิ่งใดๆ ซึ่งระบุไว้ในมาตรา 269/1 หรือมีเครื่องมือหรือวัตถุเช่นว่านั้น เพื่อใช้หรือให้ได้ข้อมูล ในการปลอมหรือแปลง ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงห้าปี และปรับตั้งแต่สองหมื่นบาท ถึงหนึ่งแสนบาท”* หากแต่ข้อแตกต่าง คือ

กรณีแรก พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ของประเทศอังกฤษ เป็นการบัญญัติถึงวัตถุหรือสิ่งใดๆ ที่ใช้หรือเพื่อใช้สำหรับกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แต่สำหรับมาตรา 269/2 ของประมวลกฎหมายอาญา ไม่จำกัดว่าจะเป็นเครื่องมือหรือวัตถุสำหรับกระทำความผิดเกี่ยวกับคอมพิวเตอร์เท่านั้น อาจเป็นเครื่องมือหรือวัตถุอื่นๆ แม้ไม่ใช่การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งอาจ เป็นเครื่องมือหรือวัตถุในรูปแบบอิเล็กทรอนิกส์ หรืออาจเป็นเครื่องมือหรืออุปกรณ์อื่นๆ เช่น สกิมเมอร์ (skimer) แท่นพิมพ์ บัตรพลาสติกขาว เป็นต้น

กรณีที่สอง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ของประเทศอังกฤษ ไม่ได้จำกัดว่าเป็นวัตถุหรือสิ่งใดๆ สำหรับการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ แต่เป็นวัตถุหรือสิ่งใดๆ ที่ใช้หรือเพื่อใช้กระทำความผิดตาม มาตรา 1 ฐานเข้าถึงโดยปราศจากอำนาจ และมาตรา 3 ฐานเข้าถึงโดยปราศจากอำนาจ

ทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ ส่วนมาตรา 269/2 ของประมวลกฎหมายอาญาเป็นเครื่องมือ หรือวัตถุสำหรับใช้หรือเพื่อใช้ในการปลอมหรือแปลง หรือเพื่อให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์

กรณีที่สาม ผู้วิจัยเห็นว่าเป็นประเด็นสำคัญที่เห็นอยู่แล้วว่า ประมวลกฎหมายอาญาว่าด้วยความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ไม่มีบทบัญญัติเกี่ยวกับการได้รับวัตถุหรือสิ่งใดๆ เพื่อใช้ในการกระทำความผิด หรือให้ความช่วยเหลือในการกระทำความผิด ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ของประเทศอังกฤษ ได้บัญญัติลักษณะแห่งการกระทำเช่นนี้ไว้ อย่างไรก็ตาม ลักษณะแห่งการกระทำว่าด้วยการได้รับเครื่องมือหรือวัตถุเพื่อใช้ในการปลอมหรือแปลง หรือเพื่อให้ได้ข้อมูลในการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ ซึ่งประเด็นนี้เป็นเรื่องของประมวลกฎหมายอาญาว่าด้วยความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์อยู่นอกเหนือขอบเขตการศึกษาวิจัย จึงไม่ได้วิเคราะห์เพื่อหาข้อสรุปและข้อเสนอแนะสำหรับประเด็นนี้ ซึ่งผู้สนใจสามารถหาอ่านได้จากงานวิจัยอีกเรื่องหนึ่งของผู้วิจัย[52]

ประการที่สาม คำว่าข้อมูลคอมพิวเตอร์ตามมาตรา 3A ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) มีความหมายถึงข้อมูลคอมพิวเตอร์ที่ใช้หรือเป็นเครื่องมือในการกระทำความผิดตามมาตรา 1 และมาตรา 3 ของพระราชบัญญัติฉบับเดียวกัน เช่น โปรแกรมคอมพิวเตอร์ที่ใช้ในการเจาะระบบหรือแฮ็ก เป็นต้น ซึ่งเป็นคนละความหมายกับข้อมูลคอมพิวเตอร์ที่พึงได้รับความคุ้มครองในฐานะวัตถุแห่งการกระทำที่ถูกเจาะระบบหรือแฮ็กเอาไป

1.2 พระราชบัญญัติเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981)[53]

บทบัญญัติของพระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) กล่าวถึงการกระทำความผิดที่เกี่ยวกับการปลอมแปลงเอกสาร เช่น เงินตรา แสตมป์ ใบหุ้น หนังสือเดินทาง เช็ค เช็คเดินทาง บัตรรับรองเช็ค บัตรเครดิต เป็นต้น กล่าวคือ เป็นบทบัญญัติที่ว่าด้วยความผิดที่เกี่ยวกับการปลอมแปลงเอกสาร ซึ่งบัญญัติในทำนอง เดียวกันกับประมวลกฎหมายอาญาของไทย ความผิดเกี่ยวกับเอกสาร มาตรา 264 ถึงมาตรา 268 เพียงมีข้อแตกต่างกันในบางประการ

---

[52] สมศักดิ์ เธียรจรูญกุล, รายงานการวิจัยเรื่อง *ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา* ทุนอุดหนุนการวิจัยจากกองทุนรัตนโกสินทร์สมโภช 200 ปี มหาวิทยาลัยสุโขทัยธรรมาธิราช, ปี 2559

[53] Forgery and Counterfeiting Act 1981 เว็บไซต์หอจดหมายเหตุแห่งชาติประเทศอังกฤษ *http://www.legislation.gov.uk/ukpga/1981/45* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

โดยที่ในช่วงระยะเวลาก่อนที่จะมีการแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (พ.ศ. 2547) ด้วยการเพิ่มฐานความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์กับฐานความผิดเกี่ยวกับหนังสือเดินทาง ประมวลกฎหมายอาญาว่าด้วยความผิดเกี่ยวกับเอกสาร มิได้ระบุถึงบัตรเครดิตและหนังสือเดินทางเป็นวัตถุแห่งการกระทำโดยเฉพาะเจาะจง การปรับใช้แก่กรณีบัตรทางการเงินต่างๆ ตามกฎหมายไทยจึงเป็นการปรับใช้มาตรา 264 ความผิดฐานปลอมเอกสารทั่วไปเป็นหลัก

แต่พระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) ได้ระบุบัตรทางการเงินบางประเภท เช่น บัตรเครดิต บัตรรับรองเช็ค รวมทั้งหนังสือเดินทาง เป็นวัตถุแห่งการกระทำในมาตรา 5 (5) ด้วย การบังคับใช้กฎหมายขององค์กรภาครัฐในประเทศอังกฤษ จึงสามารถดำเนินกระบวนการยุติธรรมต่อการกระทำความผิดเกี่ยวแก่บัตรทางการเงินตามที่ระบุไว้ได้โดยเฉพาะเจาะจง

ตามพระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) มีบทบัญญัติที่กำหนดลักษณะแห่งการกระทำความผิดที่จะกล่าวถึง 2 ลักษณะ ซึ่งสามารถปรับใช้แก่บัตรทางการเงินต่างๆ อันเป็นบัตรอิเล็กทรอนิกส์ประเภทหนึ่งตามประมวลกฎหมายอาญาของไทย โดยจะแบ่งออกเป็น 2 หัวข้อ ดังต่อไปนี้

1.2.1 การทำสิ่งปลอมแปลง หรือใช้สิ่งที่ปลอมแปลง

1.2.2 การครอบครองสิ่งที่ปลอมแปลง หรือทำหรือมีอุปกรณ์หรือวัตถุสำหรับการปลอมแปลง

1.2.1 การทำสิ่งปลอมแปลง หรือใช้สิ่งที่ปลอมแปลง พระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) วางบทบัญญัติโดยมีใจความสำคัญ ดังต่อไปนี้

บทบัญญัติมาตรา 1 กำหนดองค์ประกอบของความผิด โดยมีสาระสำคัญ ดังนี้ ผู้ใดปลอมแปลงเอกสาร เพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารที่แท้จริง และด้วยเหตุผลที่ให้ผู้หนึ่งผู้ใดยอมรับเอกสารเช่นว่านั้นจะเกิดความเสียหายขึ้นกับผู้ยอมรับเองหรือเกิดกับผู้อื่น

องค์ประกอบของความผิดฐานนี้ เอกสารหมายความรวมถึงบัตรทางการเงินต่างๆ เช่น บัตรเครดิต ใบบันทึกการขาย เป็นต้น ดังนั้น การปลอมบัตรเครดิตซึ่งอาจปลอมทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด หรือเพียงการได้บัตรเครดิตที่แท้จริงมาแล้วลงลายมือชื่อของตนเองลงไปเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าตนเป็นผู้ทรงสิทธิบัตรเครดิตใบนั้น หรือการได้บัตรเครดิตที่แท้จริงมาแล้ว

นำไปใช้จ่ายโดยลงลายมือชื่อผู้ถือบัตรบนใบบันทึกการขาย เหล่านี้ ย่อมอยู่ในความหมายของการปลอมแปลงเอกสารตามมาตรา 1 แห่ง Forgery and Counterfeiting Act 1981 แล้ว[54]

นอกจากนี้ การปลอมแปลงเอกสารอาจเกิดขึ้นในลักษณะที่ทำปลอมเป็นจำนวนมาก เช่น การปลอมใบบันทึกการขายจำนวนมาก เพื่อผลในการที่ร้านค้าที่รับซื้อใบบันทึกการขายปลอมจะนำไปเรียกเก็บเงินจากผู้ออกบัตร หรืออาจเป็นการปลอมบัตรเครดิตจำนวนมาก เพื่อนำไปขายให้แก่ผู้ต้องการบัตรเครดิตปลอมสำหรับนำไปใช้จ่าย[55]

การปลอมแปลงเอกสารเป็นฐานความผิดที่มุ่งปกป้องมิให้เกิดการกระทำที่ก่อให้เกิดเครื่องมือสำหรับกระทำความผิดอื่นต่อไป โดยผู้ที่ได้เอกสารปลอมแปลงไปจะนำไปใช้ในการก่ออาชญากรรม สำหรับกรณีนี้ พระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) ได้วางข้อกำหนดความผิดฐานใช้เอกสารปลอมไว้ตามมาตรา 3 โดยมีสาระสำคัญ ดังต่อไปนี้ ผู้ใดใช้เอกสารปลอมแปลง โดยรู้อยู่หรือควรจะรู้ได้ว่าเป็นของปลอมแปลง โดยเจตนาชักจูงใจให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารที่แท้จริง และด้วยเหตุผลที่ให้ผู้หนึ่งผู้ใดยอมรับเอกสารเช่นว่านั้นจะเกิดความเสียหายขึ้นกับผู้ยอมรับเองหรือเกิดกับผู้อื่น

บทบัญญัติทั้งสองมาตรา คือ มาตรา 1 กับมาตรา 3 ของ Forgery and Counterfeiting Act 1981 มิใช่บทกฎหมายที่บัญญัติสำหรับบัตรอิเล็กทรอนิกส์หรือบัตรเครดิตโดยตรง หากแต่ศาลยุติธรรมของประเทศอังกฤษตีความกฎหมายสองมาตรานี้ปรับใช้กับข้อเท็จจริงที่เกิดขึ้นกับบัตรเครดิต ดังคดีนี้

คดี R v. Abdulla จำเลยถูกดำเนินคดีนี้นอกเหนือจากคดีอื่นๆ อีก โดยมีข้อเท็จจริงว่า Barclaycard ออกบัตรเครดิตใบหนึ่งให้แก่ P. Abdulla ซึ่งเป็นภรรยาของจำเลย จำเลยลงลายมือชื่อหลังบัตรเครดิตที่แท้จริงใบนั้นว่า A. Abdulla ศาลยุติธรรมแห่งเมือง Croydon วินิจฉัยชี้ขาดว่า “บัตรเครดิตเป็นเอกสารภายใต้บทบัญญัติมาตรา 1 แห่ง Forgery and Counterfeiting Act 1981 และการแสดงข้อความอันเป็นเท็จก็คือ ลายมือชื่อของจำเลยที่จำเลยเจตนาลงลายมือชื่อว่า A. Abdulla เพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าจำเลยเป็นผู้ทรงสิทธิบัตรเครดิตใบนั้น แม้จำเลยจะอ้างว่า ได้รับความยินยอมจากภรรยาตนเองแล้วก็ตาม จำเลยก็ไม่พ้นจากความรับผิดตามมาตรา 1 แห่ง Forgery and Counterfeiting Act 1981 ไปได้ เพราะความยินยอมของภรรยาจำเลย

---

[54] Smith & Hogan *Criminal law* 6th ed., pp. 645-664

[55] Melhem, Ahmed Al *“The Legal Regime of Payment Cards:A comparative Study between American, British and Kuwaiti Laws, With Particular reference to Credit Cards.”* pp. 571

ไม่อาจยกเว้น ความรับผิดฐานปลอมแปลงเอกสารนี้ได้ เนื่องจาก ผู้ออกบัตร Barclaycard มิได้ยินยอมด้วย[56]

สำหรับโทษของความผิดตามมาตรา 1 และมาตรา 3 ของ Forgery and Counterfeiting Act 1981 ถูกระบุไว้ในมาตรา 6 (2) (3) มีโทษจำคุกไม่เกิน 10 ปี

ข้อสังเกต คำพิพากษาของศาลยุติธรรมอังกฤษฉบับนี้ กล่าวได้ว่า วางหลักไว้ไม่ต่างจากกฎหมายไทย คือ ในฐานความผิดเกี่ยวกับการปลอมเอกสาร ความยินยอมไม่อาจอ้างเป็นเหตุยกเว้นความรับผิดได้ เพราะเอกสารปลอมอาจสร้างความเสียหายให้ผู้หนึ่งผู้ใดหรือประชาชนก็ได้ มิใช่เพียงผู้ทรงสิทธิในเอกสารหรือเจ้าของเอกสารเท่านั้นที่จะเป็นผู้เสียหายได้

1.2.2 การครอบครองสิ่งที่ปลอมแปลง หรือทำหรือมีอุปกรณ์หรือวัตถุสำหรับการ ปลอมแปลง พระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) วางบทบัญญัติเกี่ยวกับการครอบครองสิ่งที่ปลอมแปลง หรือทำ หรือมีอุปกรณ์หรือวัตถุสำหรับการปลอมแปลง โดยมีใจความสำคัญ ดังต่อไปนี้

มาตรา 5 ของ พระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) กล่าวถึงการกระทำความผิดเกี่ยวกับเงิน แสตมป์ เช็ค บัตรทางการเงินต่างๆ หนังสือเดินทาง หนังสือรับรอง หรือประกาศนียบัตร โดยวางหลักองค์ประกอบของความผิดไว้ตามอนุมาตรา (1) ซึ่งมีใจความสำคัญ ดังต่อไปนี้

อนุมาตรา (1) เป็นการวางบทบัญญัติกำหนดองค์ประกอบของความผิดฐานครอบครองเอกสารปลอม กล่าวคือ กรณีเป็นความผิดสำหรับผู้ใดที่ครอบครองหรือควบคุม โดยที่รู้หรือควรจะรู้ว่าเอกสารนั้นเป็นของปลอม และโดยเจตนาที่ตนเองจะใช้หรือให้ผู้อื่นใช้เอกสารปลอมนั้นชักจูงใจให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารที่แท้จริง และด้วยเหตุผลที่ให้ผู้หนึ่งผู้ใดยอมรับเอกสารเช่นว่านั้นจะเกิดความเสียหายขึ้นกับผู้ยอมรับเองหรือเกิดกับผู้อื่น

องค์ประกอบของความผิดมาตรา 5 นี้ นอกจากอนุมาตรา (1) แล้ว ยังระบุฐานความผิดที่กล่าวถึงเอกสารปลอมเป็นวัตถุแห่งการกระทำอีกหนึ่งฐานความผิด คือ อนุมาตรา (2) ความผิดทั้งสองฐานจะต้องวิเคราะห์บทนิยามของคำว่า “เอกสาร” ตามมาตรา 5 (5) ซึ่งได้บัญญัติให้ความหมายไว้ตาม (a) ถึง (m) ระบุเอกสาร 12 ประเภทให้อยู่ในความหมายของคำว่าเอกสาร ตามมาตรา 5 นี้ เช่น เงินตรา แสตมป์ ใบหุ้น หนังสือเดินทาง เช็ค เช็คเดินทาง บัตรรับรองเช็ค บัตรเครดิต เป็นต้น

---

[56] Melhem, Ahmed Al *“The Legal Regime of Payment Cards:A comparative Study between American, British and Kuwaiti Laws, With Particular reference to Credit Cards.”* pp. 572

เมื่อบัตรเครดิตและหนังสือเดินทาง[57] อยู่ในความหมายของเอกสารตามมาตรา 5 ของ พระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) การปรับใช้แก่ผู้กระทำความผิดที่ครอบครองบัตรเครดิตปลอมและมีเจตนานำไปใช้หรือให้ผู้อื่นนำไปใช้ย่อมตรงตามเจตนารมณ์ของกฎหมาย และมาตรา 5 นี้จะมีความเฉพาะเจาะจงมากกว่า คือ ระบุเอกสารอะไรบ้างที่อยู่ในความหมาย หากเปรียบกับ Theft Act 1968 มาตรา 25 ที่กำหนดเป็นการทั่วไปถึงสิ่งที่ผิดกฎหมาย

กรณีมาตรา 5 ของพระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) อาจเปรียบได้กับมาตรา 269/4 วรรคแรก ตามประมวลกฎหมายอาญาของไทย หากแต่มาตรา 269/4 วรรคแรก มีความครอบคลุมกว้างกว่า คือ รวมบัตรอิเล็กทรอนิกส์ทุกประเภท ไม่เพียงบัตรเครดิตและหนังสือเดินทางอิเล็กทรอนิกส์เท่านั้น

ส่วนอนุมาตรา (2) ของมาตรา 5 แห่งพระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) มีสาระสำคัญกำหนดให้เพียงผู้ที่ครอบครองเอกสารปลอม โดยรู้หรือควรจะรู้ว่าเป็นเอกสารปลอม โดยปราศจากข้ออ้างหรือข้อแก้ตัวตามกฎหมายก็เป็นความผิดแล้ว

ข้อสังเกต หากวิเคราะห์เปรียบเทียบระหว่างอนุมาตรา (2) ของมาตรา 5 พระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) กับความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ตามประมวลกฎหมายอาญาของไทยแล้ว จะไม่มีฐานความผิดลักษณะนี้ คือ กรณีต้องเป็นการมีไว้เพื่อใช้ตามมาตรา 269/4 วรรคแรก แต่ถ้าเพียงมีไว้หรือครอบครองเท่านั้น ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญาของไทยยังไม่ถือเป็นความผิด และกรณีหากเป็นข้อมูลคอมพิวเตอร์ทั้งที่เป็นบัตรอิเล็กทรอนิกส์และไม่ใช่บัตรอิเล็กทรอนิกส์ ก็ไม่มีกฎหมายกำหนดให้เป็นความผิดฐานครอบครองข้อมูลคอมพิวเตอร์ แต่ประเด็นนี้อยู่นอกเหนือขอบเขตการศึกษาวิจัยเช่นเดียวกัน ซึ่งผู้สนใจสามารถนำไปศึกษาค้นคว้าได้เป็นอีกหัวข้อหนึ่ง

อนุมาตรา (3) ของมาตรา 5 แห่ง พระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) มีใจความสำคัญว่า ผู้ใดทำหรือมีเครื่องจักรหรือวัตถุ หรือกระดาษหรือสิ่งอื่นใดสำหรับปลอมแปลงภายใต้การควบคุมดูแล โดยรู้หรือโดยออกแบบมาเฉพาะเจาะจง หรือปรับใช้สำหรับการทำปลอมเอกสารภายใต้มาตรานี้ ด้วยเจตนาที่

---

[57] ปัจจุบันหลายประเทศทำหนังสือเดินทางเป็นหนังสือเดินทางอิเล็กทรอนิกส์ และบางประเทศก็มีบาร์โค้ด (bar code) อยู่ที่หนังสือเดิน ประเทศไทยก็เช่นเดียวกัน ซึ่งหมายความว่า หนังสือเดินทางที่ประเทศไทยออกให้แก่พลเมืองเป็นหนังสือเดินทางอิเล็กทรอนิกส์ อันอยู่ในความหมายของบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา มาตรา 1 (14) (ก)

ตนเองหรือผู้อื่นทำปลอมเอกสารภายใต้มาตรานี้ และโดยเจตนาที่ตนเองจะใช้ หรือให้ผู้อื่นใช้เอกสารปลอมนั้น ชักจูงใจให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารที่แท้จริง และด้วยเหตุผลที่ให้ผู้หนึ่งผู้ใดยอมรับเอกสารเช่นว่านั้นจะเกิดความเสียหายขึ้นกับผู้ยอมรับเองหรือเกิดกับผู้อื่น

ความผิดฐานนี้กำหนดวางองค์ประกอบสำหรับเอาผิดกับผู้ที่ทำหรือมีเครื่องมือสำหรับปลอมเอกสาร ซึ่งหมายรวมถึงสำหรับทำปลอมบัตรเครดิต หนังสือเดินทางอิเล็กทรอนิกส์ และบัตรทางการเงินต่างๆ ที่ระบุไว้ตามมาตรา 5 (5) ด้วย

ข้อสังเกต หากเปรียบเทียบกับประมวลกฎหมายอาญาของไทยว่าด้วยความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ จะมีความคล้ายคลึงกับมาตรา 269/2 ซึ่งบัญญัติว่า *"ผู้ใดทำเครื่องมือหรือวัตถุสำหรับปลอม หรือแปลง หรือสำหรับให้ได้ข้อมูลในการปลอมหรือแปลงสิ่งใดๆ ซึ่งระบุไว้ใน มาตรา 269/1 หรือมีเครื่องมือหรือวัตถุเช่นว่านั้น เพื่อใช้หรือให้ได้ข้อมูลในการปลอมหรือแปลง ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงห้าปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนบาท"* โดยในกรณีนี้ ผู้วิจัยมีข้อสังเกต 2 ประการ ดังนี้

ประการแรก กรณีเป็นเพียงมีข้อแตกต่างในเรื่ององค์ประกอบของความผิดว่าด้วยวัตถุแห่งการกระทำระหว่างเอกสารต่างๆ ที่บัญญัติไว้ตามมาตรา 5 (5) แห่งพระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) กับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญาของไทย

ประการที่สอง ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญาของไทยไปไกลกว่าหรือก้าวหน้ากว่าพระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) กล่าวคือ มาตรา 269/2 ตามประมวลกฎหมายอาญาของไทยระบุถึงการทำ หรือมีเครื่องมือหรือวัตถุ **"เพื่อให้ได้ข้อมูลสำหรับการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์"** ด้วย ไม่เพียงเฉพาะทำ หรือมีเครื่องมือ หรือวัตถุสำหรับปลอมหรือแปลงบัตรอิเล็กทรอนิกส์เท่านั้นโดยประการนี้มาตรา 269/2 ตามประมวลกฎหมายอาญาของไทย จึงมีส่วนสัมพันธ์เชื่อมโยงกับบทบัญญัติของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของไทย

อย่างไรก็ตาม หากไม่ใช่เพื่อได้ข้อมูลคอมพิวเตอร์ไปเพื่อปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ก็ไม่มีกฎหมายอาญาใดคุ้มครองข้อมูลคอมพิวเตอร์ในฐานะวัตถุแห่งการกระทำ

อนุมาตรา (4) บัญญัติวางองค์ประกอบของความผิดไว้มีใจความสำคัญกล่าวถึง ผู้ใดทำ หรือมีเครื่องจักรหรือวัตถุหรือกระดาษหรือสิ่งอื่นใดสำหรับปลอมแปลงภายใต้การควบคุมดูแล โดยปราศจากข้ออ้างหรือข้อแก้ตัวตามกฎหมายเป็นความผิด

บทบัญญัติของอนุมาตรา (4) ข้างต้นระบุให้เพียงการมีไว้หรือทำเครื่องจักร หรือวัตถุ หรือกระดาษหรือสิ่งอื่นใดสำหรับปลอมแปลงภายใต้การควบคุมดูแลโดยไม่มีข้ออ้างตามกฎหมายก็เป็นความผิดแล้ว

ข้อสังเกต หากเปรียบเทียบกับฐานความผิดตามมาตรา 269/2 ตามประมวลกฎหมายอาญาของไทยว่าด้วยความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ กรณีนี้ เช่นเดียวกันกับอนุมาตรา (2) ของ มาตรา 5 แห่ง พระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) คือ ประมวลกฎหมายอาญาของไทยว่าด้วยความผิดเกี่ยวกับบัตรอิเล็ก-ทรอนิกส์ไม่ได้บัญญัติให้เพียงการมีเครื่องมือหรือวัตถุสำหรับการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ แต่กฎหมายไทยต้องมีมูลเหตุจูงใจ **“เพื่อใช้หรือให้ได้ข้อมูลสำหรับการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์”** จึงมีความผิด[58]

บทบัญญัติที่กำหนดฐานความผิดตามมาตรา 5 อนุมาตรา (1) ถึงอนุมาตรา (4) มีระวางโทษที่แตกต่างกัน สำหรับโทษของความผิดตามอนุมาตรา (1) และอนุมาตรา (3) ของมาตรา 5 แห่ง พระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) ถูกระบุไว้ในมาตรา 6 (2) (3) มีโทษจำคุกไม่เกิน 10 ปี และระวางโทษของฐานความผิดตามอนุมาตรา (2) และอนุมาตรา (4) ของมาตรา 5 แห่งพระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) ถูกระบุไว้ในมาตรา 6 (4) คือ จำคุกไม่เกิน 2 ปี แต่เนื่องจากอัตราโทษไม่ใช่สาระสำคัญที่จะวิเคราะห์ในงานวิจัยนี้ สาระสำคัญอยู่ที่องค์ประกอบของกฎหมาย จึงไม่ได้กล่าวถึงรายละเอียดมากนัก

2. กฎหมายประเทศสหรัฐอเมริกา

บทบัญญัติของกฎหมายประเทศสหรัฐอเมริกาที่เกี่ยวข้องมีที่สำคัญ 2 ฉบับ ซึ่งจะนำมาวิเคราะห์ถึงการกระทำสำเนาหรือโจรกรรมข้อมูลคอมพิวเตอร์ โดยแบ่งออกเป็น 2 หัวข้อ ดังนี้

2.1 รัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986)

2.2 รัฐบัญญัติเกี่ยวกับการยับยั้งการโจรกรรมข้อมูลส่วนบุคคล ค.ศ. 1998 (Identity theft and Assumption Deterrence Act 1998)

---

[58] ผู้สนใจโปรดดู สมศักดิ์ เธียรจรูญกุล, รายงานการวิจัยเรื่อง *ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา* ทุนอุดหนุนการวิจัยจากกองทุนรัตนโกสินทร์สมโภช 200 ปี มหาวิทยาลัยสุโขทัยธรรมาธิราช, ปี 2559

2.1 รัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986)

รัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) ฉบับนี้อยู่ในประมวลกฎหมายสหรัฐเมริกา (United States Code : U.S.C.) บรรพที่ 18 (Title 18) หมวด 47 (Chapter 47) มาตรา 1030 การฉ้อโกงและการกระทำที่เกี่ยวข้องกับการเชื่อมต่อกับระบบคอมพิวเตอร์ (Fraud and related activity in connection with computers)[59]

กฎหมายฉบับนี้หลังจากการตราขึ้นบังคับใช้เมื่อ ค.ศ. 1986 แล้ว มีการแก้ไขเพิ่มเติมในปี ค.ศ. 1986, 1988, 1994, 1996, กับในปี ค.ศ. 2001 โดย USA Patriot Act 2002 เนื่องจากเหตุผลที่สำคัญประการหนึ่ง คือ เหตุการณ์ 911 ที่คนร้ายใช้หมายเลขประกันสังคม พาสปอร์ตหนังสือเดินทางอิเล็กทรอนิกส์ปลอม ซึ่งถือเป็นเครื่องมือสำหรับการเข้าถึง (access devices) ชนิดหนึ่ง รวมทั้งเครื่องมือสำหรับการเข้าถึง (access devices) อื่นๆ เป็นช่องทางในการก่อให้เกิดเหตุการณ์ร้ายแรงนั้นขึ้น และต่อมามีการแก้ไขเพิ่มเติมให้มีผลบังคับใช้ล่าสุดในปี ค.ศ. 2008 โดยรัฐบัญญัติเกี่ยวกับการบังคับใช้กฎหมายโจรกรรมข้อมูลส่วนบุคคลและการฟื้นฟู ค.ศ. 2007 (Identity Theft Enforcement and Restitution Act of 2007) ด้วยการแก้ไขเพิ่มเติมให้กฎหมายฉบับนี้ในอนุมาตรา (b) ของมาตรา 1030 ให้มีผลบังคับใช้ไม่เพียงแต่กับผู้กระทำความผิดหรือพยายามกระทำความผิดเท่านั้น แต่ให้ครอบคลุมถึงผู้สมรู้ร่วมคิดหรือผู้สมคบกระทำความผิดด้วย[60]

รัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) ฉบับนี้มีวัตถุประสงค์ปกป้องและกำหนดความผิดทางอาญาที่กระทำต่อหรือผ่านระบบคอมพิวเตอร์ โดยเฉพาะระบบคอมพิวเตอร์ที่เกี่ยวกับรัฐบาลสหรัฐอเมริกา หรือสถาบันการเงิน หรือธุรกิจ หรือองค์กรเอกชน ซึ่งอาชญากรรมนั้นเกี่ยวข้องกับรัฐบาลสหรัฐอเมริกา หรือกระทบการค้าระหว่างมลรัฐ หรือระหว่างประเทศ[61]

โดยที่การอาศัยกฎหมายเดิมๆ ที่มีอยู่ ไม่ว่าจะเป็น Theft หรือ Larceny ก็ไม่สามารถบังคับใช้กับอาชญากรรมที่กระทำต่อหรือกระทำผ่านเทคโนโลยีได้อย่างสมวัตถุประสงค์หรือเจตนารมณ์ของกฎหมาย โดยเฉพาะการกระทำความผิดต่อหรืออาศัยช่องทางผ่านเทคโนโลยีคอมพิวเตอร์ เนื่องจากข้อมูลต่างๆ ในระบบคอมพิวเตอร์ไม่ใช่วัตถุที่มีรูปร่าง ส่วนการกระทำที่เป็น

---

[59] *เว็บไซต์คณะนิติศาสตร์ มหาวิทยาลัยคอร์แนล https://www.law.cornell.edu/uscode/text/18/1030* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

[60] *Ibid.*

[61] *Ibid.*

การฉ้อโกงก็มิได้กระทำการหลอกผู้อื่นหรือตัวบุคคล แต่กระทำต่ออุปกรณ์หรือเครื่องจักรทางอิเล็กทรอนิกส์ หรือคอมพิวเตอร์ อีกทั้งการบังคับใช้รัฐบัญญัติเกี่ยวกับการฉ้อโกงโดยบัตรเครดิต ค.ศ. 1984 (The credit card fraud act 1984) ซึ่งกฎหมายฉบับนี้ก็มุ่งที่จะปกป้องเครื่องมือสำหรับการเข้าถึง (access devices) เป็นการเฉพาะเจาะจง แต่การกระทำฉ้อโกงทางคอมพิวเตอร์หรือการกระทำความผิดเกี่ยวกับคอมพิวเตอร์บางลักษณะมิได้กระทำต่อหรืออาศัยเครื่องมือสำหรับการเข้าถึง (access devices) การกระทำอาจด้วยการเขียนโปรแกรมไวรัสแล้วปล่อยออกไป หรือการเขียนโปรแกรมขึ้นเพื่อสร้างความเสียหายอย่างโปรแกรมการยิงนุก หรือ**การเจาะระบบด้วยวิธีการที่ไม่ต้องใช้หรืออาศัยเครื่องมือสำหรับการเข้าถึง (access devices)** ก็ได้ หากแต่การกระทำเหล่านี้สร้างความเสียหายต่อระบบคอมพิวเตอร์ หรือต่อข้อมูลคอมพิวเตอร์ หรือต่อข้อมูลทางการเงินการธนาคาร หรือต่อความมั่นคงแห่งรัฐ ซึ่งอาจมีผลกระทบต่อเครื่องมือสำหรับการเข้าถึง (access devices) ด้วยก็ได้ จึงมีความจำเป็นที่ต้องตรารัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) เพื่ออุดช่องว่างแห่งกฎหมายของกฎหมายเดิมๆ และเพื่อเสริมรัฐบัญญัติเกี่ยวกับการฉ้อโกงโดยบัตรเครดิต ค.ศ. 1984 (The credit card fraud act 1984) ให้สมบูรณ์ยิ่งขึ้น

โดยธุรกิจที่ได้รับผลจากการปกป้องคุ้มครองโดยกฎหมายฉบับนี้อย่างเด่นชัด คือ ธุรกิจสายการบินในประเทศสหรัฐอเมริกา ซึ่งจากรายงานของ ARC เพียงปี ค.ศ. 2008 สายการบินต่างๆ ได้รับความเสียหายจากการฉ้อโกงทางออนไลน์ถึง 1.4 พันล้านดอลล่าห์สหรัฐอเมริกา และปี ค.ศ. 2009 เฉพาะสายการบิน Airlines Tackle เพียงแห่งเดียวได้รับความเสียหายจากการฉ้อโกงทางออนไลน์ถึง 1.4 พันล้านดอลล่าห์สหรัฐอเมริกา โดยส่วนใหญ่ความเสียหายเกิดจากการซื้อขายตั๋วเครื่องบินทางอินเทอร์เน็ตด้วยข้อมูลบนบัตรเครดิต และเป็นเครือข่ายผู้กระทำความผิดจากตัวแทนที่ได้รับการแต่งตั้งจาก ARC[62] ซึ่งเหตุการณ์ทำนองนี้ก็เกิดขึ้นในประเทศไทยแล้ว หลายเหตุการณ์ และบางเหตุการณ์ก่อความเสียหายนับร้อยล้านบาท ดังปรากฏเป็นข่าวทางสื่อมวลชน

เกี่ยวกับรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) จะแบ่งออกเป็น 2 หัวข้อ ดังนี้

2.1.1 บทบัญญัติของกฎหมาย

2.1.2 คำพิพากษาของศาล

2.1.1 บทบัญญัติของกฎหมาย

[62] เว็บไซด์เวิลด์เพรสดอทคอม *http://nvflyer.wordpress.com/2010/12/05/the-computer-fraud-and-abuse-act-revenue-protection-weapon-for-airlines/* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

มาตรา 1030 แห่งรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) มีใจความสาระสำคัญดังนี้

อนุมาตรา (a) ผู้ใด..

อนุมาตราย่อย (1) มีการเข้าถึง (accessed) ระบบคอมพิวเตอร์โดยเจตนาโดยปราศจากอำนาจหรือเกินขอบอำนาจ และด้วยการกระทำเช่นว่านั้น ได้ไปซึ่งข้อมูลที่ได้ถูกระบุไว้โดยรัฐบาลสหรัฐอเมริกาโดยคำสั่งของฝ่ายบริหาร หรือบทบัญญัติของกฎหมายมุ่งจะคุ้มครองมิให้เปิดเผยข้อมูลโดยปราศจากอำนาจ ด้วยเหตุผลความมั่นคงของประเทศหรือความสัมพันธ์ระหว่างประเทศ หรือข้อมูลใดๆ ที่ถูกควบคุมตามความหมายที่ระบุไว้ในวรรค y ของมาตรา 11 แห่งรัฐบัญญัติพลังงานปรมาณู ค.ศ. 1954 (the Atomic Energy Act of 1954) ด้วยเหตุผลที่เชื่อได้ว่าข้อมูลดังกล่าวที่ได้รับไปนั้น เพื่อให้สามารถใช้ไปในทางเป็นอันตรายต่อประเทศสหรัฐอเมริกา หรือเพื่อประโยชน์ของชาติต่างประเทศโดยมีเจตนาอย่างใด ๆ ดำเนินการติดต่อสื่อสาร ส่งผ่าน ส่งมอบหรือสาเหตุที่จะสื่อสาร การส่งมอบหรือถ่ายโอนข้อมูลหรือความพยายามที่จะติดต่อสื่อสาร ส่งมอบ ส่งผ่านหรือ ทำให้มีการสื่อสาร การส่งมอบหรือถ่ายโอนข้อมูลเดียวกันนี้ เพื่อบุคคลหนึ่งบุคคลใดซึ่งไม่มีสิทธิที่จะรับหรือจงใจเก็บรักษาไว้และไม่ส่งไปยังเจ้าหน้าที่หรือพนักงานของสหรัฐอเมริกาซึ่งมีสิทธิได้รับข้อมูลนั้น

อนุมาตราย่อย (2) จงใจหรือเจตนาเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบอำนาจ และได้รับไปซึ่ง..

(A) ข้อมูลที่มีอยู่ในบันทึกทางการเงินของสถาบันการเงินหรือของบริษัทผู้ออกบัตรตามที่กำหนดไว้ในมาตรา 1602 (n) ของบรรพที่ 15 (Title 15) หรือที่มีอยู่ในแฟ้มของผู้บริโภคในการรายงานหน่วยงานคุ้มครองผู้บริโภค ซึ่งมีการกำหนดไว้ในรัฐบัญญัติการรายงานเครดิตที่เป็นธรรม (the Fair Credit Reporting Act, Title 15 USC section 1681 et seq.)

(B) ข้อมูลจากหน่วยงานใดหรือหน่วยงานของประเทศสหรัฐอเมริกา หรือ

(C) ข้อมูลจากคอมพิวเตอร์เครื่องใดๆ ที่ได้รับการคุ้มครอง

อนุมาตราย่อย (3) โดยเจตนาปราศจากอำนาจที่จะเข้าถึงระบบคอมพิวเตอร์ที่มิได้มีไว้เพื่อสาธารณะของกระทรวงหรือหน่วยงานของสหรัฐอเมริกา หรือเข้าถึงระบบคอมพิวเตอร์ของกระทรวงหรือหน่วยงานของสหรัฐอเมริกาที่มีไว้สำหรับใช้งานโดยรัฐบาลสหรัฐอเมริกาโดยเฉพาะเจาะจง หรือกรณีระบบคอมพิวเตอร์นั้นมิได้มีไว้สำหรับใช้งานโดยรัฐบาลสหรัฐอเมริกาโดยเฉพาะเจาะจง แต่มีไว้เพื่อใช้งานโดยหรือสำหรับรัฐบาลของสหรัฐอเมริกา และการกระทำดังกล่าวส่งผลกระทบต่อการใช้งานโดยหรือสำหรับรัฐบาลของประเทศสหรัฐอเมริกา

อนุมาตราย่อย (4) รู้อยู่แล้วและมีเจตนาที่จะฉ้อโกง เข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยปราศจากอำนาจหรือเกินขอบอำนาจ และด้วยวิธีการเช่นว่านั้นการ

กระทำดังกล่าวมีเจตนาฉ้อโกง และได้รับสิ่งใดๆ ที่มีมูลค่าไป เว้นแต่วัตถุประสงค์ของการฉ้อโกงและสิ่งที่ได้มานั้น เป็นเพียงเพื่อการใช้งานคอมพิวเตอร์และมูลค่าการใช้งานดังกล่าวไม่เกิน 5,000 ดอลล่าห์สหรัฐอเมริกาในช่วงระยะเวลา 1 ปี

อนุมาตรายย่อย (5)

(A) รู้อยู่แล้วถึงสาเหตุของการส่งผ่านโปรแกรม ข้อมูล รหัส หรือคำสั่ง และเป็นผลมาจากการกระทำดังกล่าว จงใจทำให้เกิดความเสียหายโดยปราศจากอำนาจต่อระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง

(B) เจตนาเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยปราศจากอำนาจ และเป็นผลมาจากการกระทำดังกล่าว โดยประมาทก่อให้เกิดความเสียหาย หรือ

(C) เจตนาเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยปราศจากอำนาจ และเป็นผลมาจากการกระทำดังกล่าวก่อให้เกิดความเสียหาย

อนุมาตรายย่อย (6) รู้อยู่แล้วและมีเจตนาที่จะฉ้อโกง ลักลอบค้า (ตามที่ระบุไว้ในมาตรา 1029)[63] รหัสผ่าน (password) หรือข้อมูลที่คล้ายคลึงกัน ซึ่งใช้สำหรับการเข้าถึงระบบคอมพิวเตอร์ โดยปราศจากอำนาจ ถ้า..

(A) การค้าดังกล่าวมีผลกระทบต่อการค้าระหว่างมลรัฐหรือระหว่างประเทศ หรือ

(B) ระบบคอมพิวเตอร์ดังกล่าวถูกใช้โดยหรือสำหรับรัฐบาลของประเทศสหรัฐอเมริกา

อนุมาตรายย่อย (7) มีเจตนาที่จะกรรโชกเงินหรือสิ่งอื่นๆ อันมีมูลค่าจากบุคคลหนึ่งบุคคลใด มีผลถึงในการค้าระหว่างมลรัฐหรือระหว่างประเทศ รวมถึงการสื่อสารใดๆ ทั้ง..

(A) เป็นภัยคุกคามต่อความเสียหายให้แก่คอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง

(B) เป็นภัยคุกคามต่อการรับข้อมูลข่าวสารจากระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยปราศจากอำนาจหรือเกินขอบอำนาจ อันจะทำให้เสียการรักษาความลับของข้อมูลที่ได้จากระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยปราศจากอำนาจหรือเกินขอบอำนาจ หรือ

---

[63] รัฐบัญญัติเกี่ยวกับการฉ้อโกงโดยบัตรเครดิต ค.ศ. 1984 (The credit card fraud act 1984) มาตรา 1029 (e) (5) บัญญัติว่า *the term "traffic" means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of* เว็บไซด์คณะนิติศาสตร์ มหาวิทยาลัยคอร์แนล *https://www.law.cornell.edu/uscode/text/18/1029* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

(C) ต้องการหรือเรียกร้องเงินหรือสิ่งอื่นๆ ที่มีมูลค่าที่เกี่ยวข้องกับการก่อความเสียหายให้กับระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง ความเสียหายที่เกิดจากสาเหตุเช่นว่านั้นเพื่ออำนวยความสะดวกในการกรรโชก

ต้องระวางโทษตามที่บัญญัติไว้ตามอนุมาตรา (c) แห่งมาตรานี้

อนุมาตรา (b) ผู้ใดสมคบหรือพยายามกระทำความผิดตามอนุมาตรา (a) ของมาตรานี้ ต้องระวางโทษตามที่บัญญัติไว้ตามอนุมาตรา (c) แห่งมาตรานี้

สำหรับระวางโทษตามอนุมาตรา (c) ระวางโทษสำหรับความผิดตามอนุมาตรา (a) หรือ (b) ของมาตรานี้ โดยสรุป คือ มีการแยกระวางโทษตามฐานความผิด ซึ่งมีทั้งจำคุก 1 ปี 5 ปี กับ 10 ปี สำหรับการกระทำความผิดครั้งแรก หากเป็นการกระทำความผิดซ้ำจะมีโทษจำคุกถึง 20 ปี และกฎหมายฉบับนี้ได้นำหลักเรื่องมูลค่าของความเสียหายที่เกิดจากการกระทำมาใช้กับโทษปรับด้วย กล่าวคือ มีการกำหนดจำนวนเงินที่จะปรับตามฐานความผิดอาจจะปรับ 5,000 หรือ 10,000 หรือ 100,000 ดอลล่าห์สหรัฐอเมริกา หรือปรับเป็นเงินสองเท่าของมูลค่าความเสียหายที่จำเลยได้ก่อให้เกิดขึ้น[64]

ข้อสังเกต รัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) เมื่อวิเคราะห์เปรียบเทียบกับรัฐบัญญัติเกี่ยวกับการฉ้อโกงโดยบัตรเครดิต ค.ศ. 1984 (The credit card fraud act 1984) และความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ตามประมวลกฎหมายอาญา ซึ่งบางประเภทเป็นข้อมูลคอมพิวเตอร์ เช่น ชื่อผู้ใช้ กับรหัสผ่าน เพื่อเข้าใช้อินเทอร์เน็ต จดหมายอิเล็กทรอนิกส์ รหัส เอ.ที.เอ็ม เป็นต้น โดยมีข้อสังเกต 3 ประการ ดังต่อไปนี้

ประการแรก กรณีการเข้าถึงระบบคอมพิวเตอร์ที่ใช้รหัสผ่าน (password) โดยปราศจากอำนาจจะมีความผิดต่อรัฐบัญญัติเกี่ยวกับการฉ้อโกงโดยบัตรเครดิต ค.ศ. 1984 (The credit card fraud act 1984) ด้วยเนื่องจากรหัสผ่านเป็นเครื่องมือสำหรับการเข้าถึง (access devices) ชนิดหนึ่ง เป็นกรรมเดียวผิดกฎหมายหลายบท ซึ่งมีลักษณะทำนองเดียวกับกฎหมายของประเทศ-ไทย คือ ระหว่างความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญากับพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ประการที่สอง กรณีรัฐบัญญัติเกี่ยวกับการฉ้อโกงโดยบัตรเครดิต ค.ศ. 1984 (The credit card fraud act 1984) กฎหมายฉบับนี้มีเครื่องมือสำหรับการเข้าถึง (access devices) เป็นวัตถุแห่งการกระทำที่ถือเป็นความมุ่งหมายหลักซึ่งต้องการคุ้มครอง โดยมุ่งที่ตัวเครื่องมือสำหรับ

---

[64] มาตรา 1030 (c) U.S.C. แห่งรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986)

การเข้าถึง (access devices) ในลักษณะที่เป็นคำนาม ทำนองเดียวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญาของประเทศไทย ส่วนรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) มุ่งที่การเข้าถึง (access) ในลักษณะที่เป็นกิริยาอาการ หรือในลักษณะของการกระทำ กล่าวคือ วัตถุประสงค์หรือเจตนารมณ์ของกฎหมายมุ่งคุ้มครองต่างกัน เช่นเดียวกันกับกฎหมายของประเทศไทยระหว่างความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญาที่มุ่งคุ้มครองตัวบัตรอิเล็กทรอนิกส์ กับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่มุ่งคุ้มครองการเข้าถึงเป็นหลัก

ประการที่สาม กรณีที่รัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) กำหนดให้การกระทำบางประการเชื่อมโยงให้เป็นความผิดเกี่ยวกับการฉ้อโกงและความผิดเกี่ยวกับการกรรโชก ซึ่งความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญากับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ได้บัญญัติให้มีความผิดในลักษณะนี้ ทำให้ต้องอาศัยนิติวิธีการตีความกฎหมายกับบรรดากฎหมายเดิมๆ ที่มีอยู่ โดยนำความผิดฐานฉ้อโกง ตามมาตรา 341 หรือมาตรา 342 ตามแต่กรณี หรือความผิดฐานลักทรัพย์ มาตรา 334 ตามประมวลกฎหมายอาญา มาบังคับใช้ ซึ่งเป็นประเด็นที่น่าคิดว่าจะครบองค์ประกอบของกฎหมายหรือไม่ เช่น กรณีการลักเอาบัตร เอ.ที.เอ็ม พร้อม รหัส เอ.ที.เอ็ม ของผู้อื่นไปใช้เบิกเงินสดจากเครื่องฝาก-ถอนเงินสดอัตโนมัติ เป็นต้น ซึ่งการจะกล่าวว่าเป็นความผิดฐานฉ้อโกง ตามมาตรา 341 หรือมาตรา 342 ผู้กระทำก็มิได้หลอกลวงผู้อื่น หากจะมีการหลอกลวงว่าเป็นผู้มีสิทธิใช้บัตร เอ.ที.เอ็ม และรหัส เอ.ที.เอ็ม ก็เป็นการหลอกลวงที่กระทำต่อเครื่องฝาก-ถอนเงินสดอัตโนมัติที่เป็นอุปกรณ์หรือเครื่องจักรอิเล็กทรอนิกส์ มิใช่ผู้อื่น ส่วนจะกล่าวว่าเป็นความผิดฐานลักทรัพย์ ตามมาตรา 334 ตามประมวลกฎหมายอาญา ผู้กระทำก็มิได้แย่งการครอบครองเงินที่ออกจากเครื่องฝาก-ถอนเงินสดอัตโนมัติ เพราะเหตุว่า เมื่อเครื่องฝาก-ถอนเงินสดอัตโนมัติได้รับข้อมูลรหัส เอ.ที.เอ็ม ที่ป้อนเข้ามาที่เครื่องฝาก-ถอนเงินสดอัตโนมัติ เครื่องฝาก-ถอนเงินสดอัตโนมัติรับข้อมูลแล้วว่าเป็นรหัสที่ถูกต้องจึงยอมปล่อยเงินออกมา หากกล่าวอีกนัยหนึ่ง เป็นการที่เครื่องฝาก-ถอนเงินสดอัตโนมัติยินยอมปล่อยเงินออกมา เพราะผู้กระทำได้ป้อนข้อมูลรหัส เอ.ที.เอ็ม ที่ถูกต้อง การกระทำของผู้กระทำจึงไม่ใช่แย่งการครอบครอง ดังนั้น ไม่อาจครบองค์ประกอบของความผิดฐานลักทรัพย์ ตามมาตรา 334 ของประมวลกฎหมายอาญา **สำหรับกรณีนี้ หากวิเคราะห์ตามมาตรา 1030 (a) (4) ของรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) ย่อมครบองค์ประกอบเป็นความผิดฐานฉ้อโกงทางคอมพิวเตอร์** ดังนั้น ความผิดเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์ของรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) จึงเป็นบทบัญญัติที่น่าสนใจพิจารณาอย่างยิ่ง ส่วนลักษณะแห่งการกระทำตามตัวอย่างนี้

จะมีความผิดตามกฎหมายใด ความผิดฐานใดตามกฎหมายของประเทศไทยที่มีอยู่หรือไม่ อย่างไรก็ตาม ประเด็นนี้ไม่อยู่ในขอบเขตการศึกษาวิจัยฉบับนี้ ผู้สนใจสามารถศึกษาได้เป็นอีกหนึ่งหัวข้อ

ประการที่สี่ กรณีที่มีช่องว่างแห่งกฎหมาย เช่นกรณีคดีที่เกิดขึ้นในประเทศอังกฤษ ในคดี DPP v Bignell [1998] จำเลยซึ่งเป็นเจ้าหน้าที่ตำรวจของสำนักงานตำรวจแห่งชาติใช้คอมพิวเตอร์ขององค์กร เข้าถึงข้อมูลและระบบคอมพิวเตอร์ขององค์กร เพื่อให้ได้ข้อมูลสำหรับการใช้งาน หรือเพื่อประโยชน์ส่วนตัว อย่างไรก็ตาม องค์กรผู้บังคับใช้กฎหมายไม่สามารถดำเนินคดีต่อการกระทำของเขา เพราะเหตุว่าการกระทำนั้นไม่ได้อยู่ในความหมายของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) มาตรา 1 ฐานเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ความผิดฐานนี้มีเจตนารมณ์เพื่อใช้กับแฮ็กเกอร์ (hacker) จากภายนอก ดังนั้น ศาลยุติธรรมของประเทศอังกฤษจึงพิพากษายกฟ้อง แต่กับรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) จะไม่เกิดปัญหาตามคดีของประเทศอังกฤษเช่นนี้ เนื่องจากบทบัญญัติของกฎหมายได้กำหนด ให้แม้เป็นผู้มีสิทธิใช้รหัสผ่าน (password) หากจำเลยใช้รหัสผ่านที่ได้รับเกินขอบอำนาจ จำเลยจะมีความผิด และหากเปรียบกับฐานความผิดมาตรา 269/5 ตามประมวลกฎหมายอาญาของไทย ฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบแล้ว นี่เป็นกรณีที่น่าคิดว่าสามารถ ปรับบทลงโทษแก่จำเลยได้หรือไม่ เพราะรหัสผ่าน คือบัตรอิเล็กทรอนิกส์ตามมาตรา 1 (14) (ข) ตามประมวลกฎหมายอาญา และจำเลยเป็นผู้ที่มีสิทธิหรือมีอำนาจใช้บัตรอิเล็กทรอนิกส์นั้น[65]

2.1.2 คำพิพากษาของศาล

สำหรับการบังคับใช้รัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) มีคดีที่น่าสนใจที่จะยกมากล่าวถึง 3 คดี ดังต่อไปนี้

คดีแรก ในคดี United States v. Czubinski (96-1317 No.) 1997[66] จำเลยถูกฟ้องร้องดำเนินคดีข้อหาฉ้อโกงทางคอมพิวเตอร์ตามมาตรา 1030 (a) (4) ของรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) โดยจำเลยโต้แย้งต่อสู้คดีว่า ข้อมูลที่จำเลยเข้าถึงไม่ได้มีมูลค่าหรือไม่ใช่ทรัพย์สินที่มีมูลค่าตามที่กฎหมายกำหนด ซึ่งตามมาตราข้างต้น สิ่งใดๆ ที่จำเลยได้รับไปต้องมีมูลค่าเกินกว่า 5,000 ดอลล่าห์สหรัฐอเมริกาในช่วงระยะเวลา 1 ปี

---

[65] ผู้สนใจโปรดดู สมศักดิ์ เธียรจรูญกุล, รายงานการวิจัยเรื่อง *ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา* ทุนอุดหนุนการวิจัยจากกองทุนรัตนโกสินทร์สมโภช 200 ปี มหาวิทยาลัยสุโขทัยธรรมาธิราช, ปี 2559

[66] เว็บไซต์ไฟน์ลอว์ดอทคอม *http://caselaw.findlaw.com/us-1st-circuit/1061981.html* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

ข้อเท็จจริงในคดีนี้มีอยู่ว่า จำเลยทำงานเป็นตัวแทนฝ่ายบริการด้านการภาษีของ Internal Revenue Service (IRS) ในการติดต่อสำนักงานบอสตันของผู้เสียภาษี ในการปฏิบัติหน้าที่อย่างเป็นทางการของจำเลย ส่วนใหญ่เกี่ยวข้องกับการตอบคำถามจากผู้เสียภาษี จำเลย Czubinski เข้าถึงข้อมูลจากที่หนึ่งของ IRS ของระบบคอมพิวเตอร์สืบค้นข้อมูลระบบ IDRS แบบบูรณาการซึ่งเป็นที่รู้จักกัน จำเลยทำงานอยู่ที่เวสต์เวอร์จิเนีย และสามารถใช้รหัสผ่านที่ถูกต้องติดต่อแทนรหัสการค้นหาบางอย่างและหมายเลขประกันสังคมผู้เสียภาษีอากร จำเลย Czubinski ก็สามารถดึงข้อมูลเหล่านี้ไปยังหน้าจอมอนิเตอร์ของเขาใน Boston ได้

ในปี 1992 จำเลย Czubinski ดำเนินการค้นหาข้อมูลด้วยการเข้าถึงโดยเกินไปจากขอบอำนาจที่ตนมี ทำให้ได้ไฟล์ข้อมูล IDRS ไปจำนวนมาก จำเลยรู้และไม่สนใจกฎ IRS ที่มีข้อห้ามการเข้าถึงไฟล์ข้อมูล IDRS จำเลยได้ข้อมูลเกี่ยวกับการเสียภาษีของบุคคลสำคัญสองคนที่เกี่ยวข้องกับการรณรงค์เลือกตั้งในเมืองบอสตัน คือ เดวิด ดุ๊ก (ประธานคณะกรรมการรณรงค์เลือกตั้งของพรรคการเมืองหนึ่งในเขตบอสตัน) กับ จิม เคลลี่ (Jim Kelly's : ซึ่งจิม เคลลี่พ่ายแพ้ต่อจำเลยในการเลือกตั้งตำแหน่งที่ปรึกษาของคณะกรรมการรณรงค์เลือกตั้งเขต 2) และยังได้ข้อมูลเกี่ยวกับการเสียภาษีของบุคคลในสังคมอีกจำนวนมาก

อย่างไรก็ตาม พยานหลักฐานของอัยการฝ่ายรัฐไม่สามารถพิสูจน์ได้มากกว่าการที่จำเลย เข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ จำเลยจะได้ข้อมูลเหล่านั้นไปใช้เพื่อให้ได้มูลค่าทางทรัพย์สินเกินกว่า 5,000 ดอลล่าห์สหรัฐอเมริกาในช่วงระยะเวลา 1 ปีอย่างไรหรือไม่ หรือจำเลยได้ใช้ไปในทางเป็นผลต่อคู่แข่งทางการเมือง หรือทุจริตฉ้อโกงทำให้ได้สิ่งใดๆ อันมีมูลค่า เกินกว่า 5,000 ดอลล่าห์สหรัฐอเมริกาในช่วงระยะเวลา 1 ปี อันเป็นข้อต่อสู้ของจำเลย

ศาลอุทธรณ์ (Court of Appeals) คณะที่ 9 (Ninth Circuit) ของประเทศสหรัฐอเมริกา วินิจฉัยว่า ความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินไปจากขอบอำนาจ[67] กับความผิดฐานฉ้อโกงทางคอมพิวเตอร์ตามมาตรา 1030 (a) (4) มีองค์ประกอบต่างกัน ต้องพิจารณาเจตนารมณ์ของกฎหมายที่ประสงค์จะลงโทษแยกออกจากกัน

การกระทำของจำเลยปรากฏข้อเท็จจริงว่า จำเลยเข้าถึงระบบคอมพิวเตอร์เกินไปจากขอบอำนาจ เนื่องจากจำเลยมีรหัสผ่านที่แท้จริง หาใช่รหัสผ่านปลอม เพียงจำเลยเข้าถึงเกินไปกว่าสิทธิที่ตนมีอยู่ แม้จำเลยจะกระทำการเข้าถึงเกินขอบอำนาจอันส่งผลระหว่างมลรัฐ หากแต่พยานหลักฐานของอัยการฝ่ายรัฐ ไม่สามารถพิสูจน์ได้ว่าจำเลยเปิดเผยข้อมูลต่อบุคคลที่สาม หรือ

---

[67] รัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) มาตรา 1030 (a) (2), ผู้วิจัย

กระทำโดยทุจริต ฉ้อโกง ทำให้ได้สิ่งใดๆ อันมีมูลค่าเกินกว่า 5,000 ดอลล่าห์สหรัฐอเมริกาในช่วงระยะเวลา 1 ปี ดังนั้น การกระทำของจำเลยจึงไม่ครบองค์ประกอบของมาตรา 1030 (a) (4)

ข้อสังเกต รหัสผ่านของจำเลยในคดีนี้ถือเป็นบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา ซึ่งน่าสนใจวิเคราะห์ว่า หากเป็นประมวลกฎหมายอาญาของประเทศไทย การกระทำของจำเลยที่ใช้รหัสผ่านที่แท้จริง แต่ใช้เกินขอบอำนาจจะต้องด้วยมาตรา 269/5 หรือไม่ ซึ่งกรณีนี้ผู้วิจัยเห็นว่าไม่มีความผิดตามมาตรานี้[68] นอกจากนี้ ข้อเท็จจริงในคดีผู้วิจัยเห็นว่าข้อเท็จจริงของคดีต้องด้วยมาตรา 1030 (a) (2) ของรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) แต่ฝ่ายโจทก์ไม่ได้ยื่นฟ้องจำเลยข้อหานี้ จึงไม่มีประเด็นข้อหานี้ให้ศาลวินิจฉัย

คดีที่สอง ในคดี United States v. Dimetriace Eva Lavon John (08-10459 No.) 2010[69] โดยมี นาย Smith, Owen and Haynes เป็นองค์คณะ ซึ่งจำเลยถูกดำเนินคดีฟ้องร้องหลายข้อหาตามรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) มาตรา 1030 (a) (2) (A) และ (C) กล่าวคือ เข้าถึงระบบคอมพิวเตอร์เกินขอบอำนาจและได้รับไปซึ่งข้อมูลจากสถาบันการเงินหรือจากคอมพิวเตอร์เครื่องใดๆ กับรัฐบัญญัติเกี่ยวกับการฉ้อโกงโดยบัตรเครดิต ค.ศ. 1984 (The credit card fraud act 1984) ตามมาตรา 1029 (a) (2) และ (5) กล่าวคือ รู้อยู่แล้วและเจตนาฉ้อโกงเกี่ยวกับเครื่องมือสำหรับการเข้าถึง (access devices)

ข้อเท็จจริงในคดีมีอยู่ว่า จำเลย (จอห์น) ทำงานในฐานะผู้จัดการฝ่ายบัญชีที่ซิตี้กรุ๊ปเป็นเวลาประมาณสามปี และอาศัยอำนาจตนในตำแหน่งดังกล่าวเข้าถึงระบบคอมพิวเตอร์ภายในของซิตี้กรุ๊ปและข้อมูลบัญชีของลูกค้าที่มีอยู่ในนั้น ในเดือนกันยายนปี 2005 จำเลยให้ข้อมูลบัญชีลูกค้าที่เปิดใช้งานแก่ Leland Riley ลูกพี่ลูกน้องของจำเลย กับพวกที่ร่วมกันกระทำความผิดจำเลยเข้าถึงและพิมพ์ข้อมูลเกี่ยวกับบัญชีลูกค้าของบริษัทไม่น้อยกว่า 76 บัญชีให้แก่ Riley ไป ก่อนที่จำเลยจะถูกจับกุมดำเนินคดี ข้อมูลอยู่ในรูปของทั้งภาพสแกนเช็คที่เขียนโดยผู้ถือบัญชี หรือพิมพ์หน้าจอคอมพิวเตอร์ที่มีข้อมูลรายละเอียดของบัญชี Riley โดย Cohorts ใช้ข้อมูลที่ได้จากจำเลยกระทำการฉ้อโกงจาก 4 บัญชี

คณะลูกขุนและผู้พิพากษาในศาลชั้นต้น (District Court) ชี้ขาดให้จำเลยมีความผิดฐานใช้เครื่องมือสำหรับการเข้าถึง (access devices) โดยเกินขอบอำนาจตามมาตรา 1029

---

[68] ผู้สนใจโปรดดู สมศักดิ์ เธียรจรูญกุล, รายงานการวิจัยเรื่อง *ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา* ทุนอุดหนุนการวิจัยจากกองทุนรัตนโกสินทร์สมโภช 200 ปี มหาวิทยาลัยสุโขทัยธรรมาธิราช, ปี 2559

[69] เว็บไซด์ไฟน์ลอว์ดอทคอม *http://caselaw.findlaw.com/us-5th-circuit/1507168.html* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

(a) (2) และ (5) แห่งรัฐบัญญัติเกี่ยวกับการฉ้อโกงโดยบัตรเครดิต ค.ศ. 1984 (The credit card fraud act 1984) และมีความผิดตามมาตรา 1030 (a) (2) (A) และ (C) แห่งรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986)

ศาลอุทธรณ์ (Court of Appeals) วินิจฉัยสถานะของจำเลยว่าเป็นผู้ที่กระทำการเข้าถึงระบบคอมพิวเตอร์เกินขอบอำนาจหรือไม่ โดยวิเคราะห์จากคำนิยามตามมาตรา 1030 (e) (6)[70] จำเลยเป็นพนักงานของซิตี้กรุ๊ปและ**มีข้อตกลงว่าจำเลยมีสิทธิเข้าถึงข้อมูลของกิจการมากน้อยแค่ไหน** บรรดาข้อมูลของลูกค้าที่จำเลยได้ไปนั้นอยู่ในส่วนที่จำเลยไม่มีสิทธิเข้าถึง จำเลยรู้อยู่แล้วยังเอาข้อมูลเหล่านั้นไป จำเลยจึงกระทำการเข้าถึงข้อมูลและระบบคอมพิวเตอร์เกินขอบอำนาจแล้ว[71]

เมื่อจำเลยเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ของซิตี้กรุ๊ปเกินขอบอำนาจและได้รับข้อมูลทางบัญชีของลูกค้าซิตี้กรุ๊ปไป ซึ่งซิตี้กรุ๊ปเป็นสถาบันการเงิน การกระทำของจำเลยจึงเป็นความผิดต้องด้วยมาตรา 1030 (a) (2) (A) แห่งรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986)

นอกจากนี้ จำเลยยังให้ข้อมูลทางบัญชีของซิตี้กรุ๊ปโดยมีเครื่องมือสำหรับการเข้าถึง (access devices) เป็นส่วนหนึ่งของข้อมูล อันเป็นผลให้เกิดการฉ้อโกงเรียกเก็บเงินจากลูกค้าของซิตี้กรุ๊ป และนำข้อมูลทางบัญชีไปใช้จ่ายชำระค่าสินค้า ซึ่งเพียงบัญชีเดียวในชื่อบัญชีของ Carolyn Baker เกิดความเสียหายถึง 78,750 ดอลล่าห์สหรัฐอเมริกา เมื่อประเมินจากทั้ง 76 บัญชีมูลค่าความเสียหายประมาณได้ถึง 1,451,865 ดอลล่าห์สหรัฐอเมริกา การกระทำของจำเลยจึงต้องด้วยมาตรา 1029 (a) (5) ของรัฐบัญญัติเกี่ยวกับการฉ้อโกงโดยบัตรเครดิต ค.ศ. 1984 (The credit card fraud act 1984)

ข้อสังเกต จากข้อเท็จจริงของคดีนี้ มีข้อสังเกต 2 ประการ ดังนี้

ประการแรก บรรดาข้อมูลทางบัญชีของคดีนี้ซึ่งอยู่ในความหมายของเครื่องมือสำหรับการเข้าถึง (access devices) นั้น หากปรับแก่บทบัญญัติของกฎหมายไทยว่าด้วยความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ถ้าเป็นตัวเลข รหัสต่างๆ ที่มิได้มีการออกเอกสารหรือวัตถุอื่นใดก็

---

[70] รัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) มาตรา 1030 (e) (6) *the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter; and*

[71] คำวินิจฉัยนี้ชี้ให้เห็นว่าบุคคลากรหรือพนักงานในองค์กรก็สามารถกระทำความผิดตามรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) ได้ อันต่างจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ของประเทศอังกฤษ ซึ่งปรากฏในคดี DPP v Bignell [1998]

จะเป็นบัตรอิเล็กทรอนิกส์ต้องด้วยมาตรา 1 (14) (ข) แต่ในส่วนข้อมูลคอมพิวเตอร์ต่างๆ ที่เป็นส่วนหนึ่งของบัตรเครดิต บัตร เอ.ที.เอ็ม บัตรเดบิต เหล่านี้จะไม่อยู่ในความหมายของบัตรอิเล็กทรอนิกส์ โดยเฉพาะกรณีมีการนำข้อมูลของบัตรเครดิต บัตร เอ.ที.เอ็ม บัตรเดบิต ไปใช้ชำระค่าสินค้าหรือบริการ หากการกระทำเกิดขึ้นในเขตอำนาจของกฎหมายไทยก็ไม่สามารถปรับบทความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญาได้

ประการที่สอง การกระทำของจำเลยที่เป็นความผิดตามมาตรา 1030 (a) (2) (A) แห่งรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) หากปรับตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของกฎหมายประเทศไทย ย่อมเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 5 ฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ และเป็นความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะโดยมิชอบตามมาตรา 7 เพราะข้อเท็จจริงของคดี **มีข้อตกลงว่าจำเลยมีสิทธิเข้าถึงข้อมูลของกิจการมากน้อยแค่ไหน** แต่อย่างไรก็ตาม ไม่มีกฎหมายคุ้มครองข้อมูลคอมพิวเตอร์ในฐานะวัตถุแห่งการกระทำ ผู้ได้รับข้อมูลคอมพิวเตอร์ที่ไม่อยู่ในความหมายของบัตรอิเล็กทรอนิกส์ต่อจากจำเลยก็ไม่มีความผิดทางอาญา

คดีที่สาม ในคดี United States v. Batti (09-2050 No.) 2011[72] จำเลยในคดีนี้ถูกฟ้องร้องดำเนินคดีต่อศาลชั้นต้น (District Court of Michigan) ข้อหาตามรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) มาตรา 1030 (a) (2) (C) และ มาตรา 1030 (c) (2) (B) (iii)[73] กล่าวคือ จงใจหรือเจตนาเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบอำนาจ และได้รับไปซึ่งข้อมูลจากคอมพิวเตอร์เครื่องใดๆ ที่ได้รับการคุ้มครอง และข้อมูลที่ได้รับไปนั้นมีมูลค่าเกินกว่า 5,000 ดอลล่าห์สหรัฐอเมริกา ซึ่งมีโทษปรับไม่เกิน 10,000 ดอลล่าห์สหรัฐอเมริกาหรือปรับไม่เกินสองเท่าของมูลค่าความเสียหาย หรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ

ข้อเท็จจริงในคดีมีอยู่ว่า จำเลยทำงานในแผนกไอที (IT) ของบริษัท Campbell-Ewald, an advertising company ในเมือง มิชิแกน (Michigan) ประมาณ 6 ปี ต่อมาจำเลยถูกไล่ออกเมื่อเดือนมีนาคม 2007 จากเหตุการณ์ที่จำเลยลักลอบเข้าถึงระบบคอมพิวเตอร์ของผู้บริหารระดับซีอีโอของบริษัท โดยปราศจากอำนาจ ทำให้ได้ไปซึ่งข้อมูลอันเป็นความลับของบริษัท จำเลยกระทำการคัดลอก และส่งข้อมูลข้ามบริษัท อาทิ ข้อมูลเกี่ยวกับค่าตอบแทนของผู้บริหาร งบการเงิน รายงานของประธานกรรมการ แผนกลยุทธ์ เป้าหมาย และวัตถุประสงค์ของบริษัท อันเป็นข้อมูลสำหรับผู้บริหารระดับสูงของบริษัทเท่านั้น รวมถึงข้อมูลความลับทางธุรกิจในจดหมายอิเล็กทรอนิกส์ที่ติดต่อระหว่าง บริษัท Campbell-Ewald, an advertising company กับ General Motors ซึ่งเป็นลูกค้ารายใหญ่ที่สุดของบริษัท

วันที่ 18 เมษายน 2007 ขณะที่ผู้เชี่ยวชาญกำลังตรวจสอบระบบ Server ของบริษัทและของ General Motors อยู่ ผู้เชี่ยวชาญได้พบความผิดปกติไม่น้อยกว่า 21 ครั้งที่มีการเข้าถึงระบบคอมพิวเตอร์ จึงแนะนำให้รองประธานและผู้จัดการทั่วไปของบริษัท Campbell-Ewald, an advertising company คือ นาย Joseph Naporano แจ้งความกับเจ้าหน้าที่เอฟบีไอ เจ้าหน้าที่เอฟบีไอจับกุมและสอบปากคำจำเลย พบว่าแม้ภายหลังที่จำเลยถูกให้ออกจากบริษัทไปแล้วก็ยังมีการ

---

[72] เว็บไซต์ไฟน์ลอว์ดอทคอม *http://caselaw.findlaw.com/us-6th-circuit/1552671.html* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

[73] มาตรา 1030 (c) *The punishment for an offense under subsection (a) or (b) of this section is.. (2) (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a) (2), if (iii) the value of the information obtained exceeds $5,000*; ภายหลังได้รับการแก้ไขเพิ่มเติมในปี ค.ศ. 1986 โดยแก้ไขเพิ่มเติมให้มีโทษปรับไม่เกิน 10,000 ดอลล่าห์สหรัฐอเมริกาหรือปรับไม่เกินสองเท่าของมูลค่าความเสียหาย ความดังนี้ “Subsec. (c) (2) (B). Pub.L. 99-474, *"under this title" for "of not more than the greater of $10,000 or twice the value obtained or loss created by the offense", "not more than" for "not than", and "; and" for the period at end of subpar. (B), respectively.”* เว็บไซต์พานิกดอทคอม *http://www.panix.com/~eck/computer-fraud-act.html* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

เข้าถึงระบบคอมพิวเตอร์ของบริษัท โดยที่แม้มีการเปลี่ยนรหัสผ่าน (password) แล้ว แต่ก็เปลี่ยนเพียงเล็กน้อย ซึ่งจำเลยสามารถเดาได้

จากการกระทำของจำเลยทำให้บริษัทเกิดความเสียหายนอกเหนือจากงานที่ทำโดยเอฟบีไอ ค่าใช้จ่ายที่เกิดจากบริษัทรักษาความปลอดภัยคอมพิวเตอร์ที่ดำเนินการตรวจสอบและ Naporano ได้รับคำแนะนำด้านกฎหมายเกี่ยวกับการละเมิดความปลอดภัยจากที่ปรึกษาภายนอก บริษัท Campbell - Ewald รวมค่าใช้จ่ายทั้งหมดของการตรวจสอบโดยบริษัทรักษาความปลอดภัย และคำแนะนำจากที่ปรึกษาเป็นจำนวนเงิน 47,565 ดอลล่าห์สหรัฐอเมริกา นอกจากนี้ พนักงานของ Campbell - Ewald ต้องให้ความช่วยเหลือด้านการตรวจสอบ รวมเวลาของพนักงาน Campbell - Ewald ทุกคนใช้เวลาไปประมาณ 747 ชั่วโมงเกี่ยวกับเหตุการณ์การละเมิดความปลอดภัยนี้เป็นเงิน 163,549 ดอลล่าห์สหรัฐอเมริกา และมูลค่าการตลาดกับต้นทุนการผลิตของชิ้นข้อมูลวิดิโอโฆษณา ของ General Motors เป็นเงิน 305,000 ดอลล่าห์สหรัฐอเมริกา

ศาลชั้นต้นและคณะลูกขุน (District Court of Michigan) เริ่มนั่งพิจารณาคดีวันที่ 28 ตุลาคม 2008 พบว่า มูลค่าการตลาดและต้นทุนการผลิตของชิ้นข้อมูลวิดิโอโฆษณาของ General Motors เป็นเงิน 305,000 ดอลล่าห์สหรัฐอเมริกาเป็นพยานหลักฐานที่ชัดเจน และประเมินค่าความเสียหายได้เป็นอย่างดีว่าเกินกว่า 5,000 ดอลล่าห์สหรัฐอเมริกาตามที่มาตรา 1030 (a) (2) (C) และ มาตรา 1030 (c) (2) (B) (iii) แห่งรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) กำหนดเป็นองค์ประกอบของความผิด คณะลูกขุนลงมติให้จำเลยมีความผิดและต้องชดใช้ค่าใช้จ่ายในการตรวจสอบระบบรักษาความปลอดภัยของข้อมูลและค่าใช้จ่ายด้านกฎหมายเป็นเงิน 47,565 ดอลล่าห์สหรัฐอเมริกาแก่บริษัท Campbell – Ewald ส่วนเวลาของพนักงาน Campbell - Ewald ทุกคนใช้เวลาไปรวมประมาณ 747 ชั่วโมงเกี่ยวกับเหตุการณ์การละเมิดความปลอดภัยนี้เป็นเงิน 163,549 ดอลล่าห์สหรัฐอเมริกาให้คิดเป็นค่าใช้จ่ายที่กำหนดอัตราโดยรัฐบาล (หมายความว่าให้ใช้อัตราค่าจ้างพนักงานที่เป็นอัตรากลางที่กำหนดโดยรัฐบาล)

จำเลยอุทธรณ์ โต้แย้งประเด็นค่าใช้จ่ายที่เกิดจากบริษัทรักษาความปลอดภัยคอมพิวเตอร์ที่ดำเนินการตรวจสอบ และค่าใช้จ่ายด้านกฎหมายเกี่ยวกับการละเมิดความปลอดภัยจากที่ปรึกษาภายนอกในจำนวนเงิน 47,565 ดอลล่าห์สหรัฐอเมริกา และมูลค่าความเสียหายที่กฎหมายกำหนดองค์ประกอบไว้ว่าต้องเกินกว่า 5,000 ดอลล่าห์สหรัฐอเมริกา โดยกล่าวว่าข้อมูลเหล่านั้นไม่สามารถประเมินมูลค่าเป็นเงินได้ และไม่ใช่ทรัพย์สินที่มีราคา

ศาลอุทธรณ์ (Court of Appeals) คณะที่ 6 โดยนาย MOORE, GIBBONS และ McKEAGUE ตัดสินชี้ขาดเมื่อวันที่ 14 มกราคม 2011 พิพากษายืนตามศาลล่าง

ข้อสังเกต คดีนี้อาจวิเคราะห์ข้อเท็จจริงออกเป็นสองช่วงเวลา คือ ก่อนที่จำเลยจะถูกให้ออกจากงานได้ใช้รหัสผ่านเข้าถึงข้อมูลและระบบคอมพิวเตอร์เกินขอบอำนาจ กับช่วงเวลาหลังจากที่จำเลยถูกให้ออกจากงานมีการเดารหัสผ่านจดหมายอิเล็กทรอนิกส์และใช้รหัสผ่านนั้นขโมยข้อมูลไป โดยจะได้ตั้งข้อสังเกตแบ่งออกเป็นสองช่วงเวลาเป็น 3 ประการ ดังนี้

ประการแรก ก่อนที่จำเลยจะถูกให้ออกจากงานได้ใช้รหัสผ่านเข้าถึงข้อมูลและระบบคอมพิวเตอร์เกินขอบอำนาจนั้น รหัสผ่านที่จำเลยใช้เป็นรหัสผ่านที่แท้จริง ซึ่งจำเลยมีสิทธิใช้แต่ใช้เกินขอบอำนาจ หาใช่รหัสผ่านปลอมไม่ หากเปรียบกับบทความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา รหัสผ่านเป็นบัตรอิเล็กทรกนิกส์ตามมาตรา 1 (14) (ข) แต่มีปัญหาว่าอาจปรับบทความผิดแก่จำเลยตามฐานความผิดใดได้หรือไม่ ทำนองเดียวกับคดีที่สองข้างต้น เพราะมาตราที่มีอยู่จะนำมาปรับบทดังมาตรา 269/5 ก็ต้องเป็นบัตรอิเล็กทรกนิกส์ของผู้อื่น แต่รหัสผ่านที่จำเลยใช้เป็นบัตรอิเล็กทรอนิกส์แม้เป็นของบริษัท แต่ที่จำเลยเป็นผู้มีสิทธิถือและใช้ ปัญหาจึงมีว่าความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบจะไม่ครอบคลุม ถึงการมีสิทธิใช้ แต่ใช้เกินขอบอำนาจ และไม่ครอบคลุมถึงความผิดฐานเข้าถึงระบบคอมพิวเตอร์ โดยมิชอบ ตามมาตรา 5 และความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะโดยมิชอบ ตามมาตรา 7 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เพราะข้อเท็จจริงคดีนี้**ไม่มีข้อตกลงว่าจำเลยมีสิทธิเข้าถึงข้อมูลมากน้อยเพียงใด** ต่างกับคดี United States v. Dimetriace Eva Lavon John (08-10459 No.) 2010 ซึ่ง**มีข้อตกลงว่าจำเลยมีสิทธิเข้าถึงข้อมูลของกิจการมากน้อยแค่ไหน**

ประการที่สอง ช่วงเวลาหลังจากที่จำเลยถูกให้ออกจากงานมีการเดารหัสผ่านจดหมายอิเล็กทรอนิกส์และใช้รหัสผ่านนั้นขโมยข้อมูลไป รหัสผ่าน (password) ที่จำเลยเดาได้และนำไปใช้นั้น แน่นอนว่ารหัสผ่านเป็นบัตรอิเล็กทรกนิกส์ตามมาตรา 1 (14) (ข) ตามประมวลกฎหมายอาญา และเป็นกรณีที่จำเลยใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ อันเป็นความผิดตามมาตรา 269/5 และมีความผิดฐานเข้าถึงระบบคอมพิวเตอร์ โดยมิชอบ ตามมาตรา 5 และความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะโดยมิชอบ ตามมาตรา 7 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ประการที่สาม บรรดาข้อมูลเหล่านี้ไม่อยู่ในความหมายของคำว่าทรัพย์ตามมาตรา 334 ของประมวลกฎหมายอาญา จึงไม่อาจมีความผิดฐานลักทรัพย์ และหากจะปรับด้วยมาตรา 8 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ข้อมูลคอมพิวเตอร์ของผู้อื่นนั้นต้องเป็นข้อมูลคอมพิวเตอร์ของผู้อื่นที่**อยู่ระหว่างการส่งในระบบคอมพิวเตอร์** เช่นนี้ **เมื่อข้อมูลคอมพิวเตอร์ของผู้อื่นไม่ได้อยู่ระหว่างการส่ง แต่เก็บไว้ในฮาร์ดดิสก์ หรือ การส่งจดหมายอิเล็กทรอนิกส์เสร็จสิ้นแล้วและข้อมูลเก็บอยู่ที่เซิฟเวอร์ server** ย่อมไม่อาจ

ปรับบทเป็นความผิดได้ อันต่างจากบทบัญญัติของกฎหมายประเทศสหรัฐอเมริกาที่มีการตรากฎหมายเฉพาะออกมารองรับ กรณีข้อเท็จจริงเช่นนี้ ดังจะได้กล่าวถึงในหัวข้อถัดไป

2.2 รัฐบัญญัติเกี่ยวกับการยับยั้งการโจรกรรมข้อมูลส่วนบุคคล ค.ศ. 1998 (Identity theft and Assumption Deterrence Act 1998)[74]

รัฐบัญญัติเกี่ยวกับการยับยั้งการโจรกรรมข้อมูลส่วนบุคคล ค.ศ. 1998 (Identity theft and Assumption Deterrence Act 1998) ฉบับนี้ได้รับการแก้ไขเพิ่มเติมล่าสุดและมีผลบังคับใช้เมื่อปี ค.ศ. 2008 โดยรัฐบัญญัติเกี่ยวกับการบังคับใช้กฎหมายโจรกรรมข้อมูลส่วนบุคคลและการฟื้นฟู ค.ศ. 2007 (Identity Theft Enforcement and Restitution Act of 2007) ซึ่งผ่านสภาซีเนต (Senate) เมื่อวันที่ 5 พฤศจิกายน 2007 โดยการสนับสนุนของ Senator Patrick Leahy Vermont[75]

กฎหมายฉบับนี้บัญญัติอยู่ในบรรพที่ 18 (Title 18) แห่งประมวลกฎหมายสหรัฐอเมริกา (U.S.C.) หมวดที่ 47 (Chapter 47) มาตรา 1028 Fraud and related activity in connection with identification documents, authentication features, and information และมาตรา 1028 A Aggravated identity theft

การโจรกรรมข้อมูลส่วนบุคคล หรือ identity theft เป็นอาชญากรรมที่เติบโตอย่างมีนัยสำคัญผันแปรตามที่มีการใช้งานเพิ่มขึ้นของอินเทอร์เน็ต ตามที่รัฐบัญญัติเกี่ยวกับการยับยั้งการโจรกรรมข้อมูลส่วนบุคคล ค.ศ. 1998 (Identity theft and Assumption Deterrence Act 1998) จุดประสงค์ของกฎหมายก็เพื่อให้รัฐบาลกลางบังคับใช้กฎหมายต่อการโจรกรรมข้อมูลส่วนบุคคลได้ดีขึ้น และสามารถดำเนินคดีอาชญากรรมทางอินเทอร์เน็ต cybercrimes อื่น ๆ รวมทั้งการฟื้นฟูหรือเยียวยาให้ผู้ที่ตกเป็นเหยื่อของอาชญากรรมดังกล่าว วัตถุประสงค์ของกฎหมายฉบับนี้เพื่อเสริม บรรพที่ 18 ของประมวลกฎหมายสหรัฐอเมริกา คือ มาตรา 1029 ตามรัฐบัญญัติเกี่ยวกับการฉ้อโกง โดยบัตรเครดิต ค.ศ. 1984 (The credit card fraud act 1984) และมาตรา 1030 ตามรัฐบัญญัติเกี่ยวกับ การฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) ให้การบังคับใช้สมเจตนารมณ์และบังคับใช้กับอาชญากรได้ดีขึ้น[76]

---

[74] เว็บไซต์ไฟน์ลอว์ดอทคอม *http://codes.lp.findlaw.com/uscode/18/I/47/1028* และเว็บไซต์คณะนิติศาสตร์ มหาวิทยาลัยคอร์แนล *https://www.law.cornell.edu/search/site/1028* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

[75] เว็บไซต์สภาคองเกรส *http://www.govtrack.us/congress/billtext.xpd?bill=s110-2168* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

[76] เว็บไซต์อิฮาวดอทคอม *http://www.ehow.com/about_6661635_identity-theft-restitution-act.html* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

โดยที่บทบัญญัติของกฎหมายทั้ง 3 ฉบับมุ่งที่จะกำหนดลักษณะที่จะคุ้มครองต่างกัน คือ รัฐบัญญัติเกี่ยวกับการฉ้อโกงโดยบัตรเครดิต ค.ศ. 1984 (The credit card fraud act 1984) ประสงค์คุ้มครองที่ตัวเครื่องมือสำหรับการเข้าถึง (access devices) อันเป็นวัตถุแห่งการกระทำ ส่วนรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) มุ่งประสงค์ที่จะคุ้มครองการเข้าถึง (access) อันเป็นลักษณะแห่งการกระทำ และข้อมูลคอมพิวเตอร์ในฐานะวัตถุแห่งการกระทำ แต่รัฐบัญญัติเกี่ยวกับการยับยั้งการโจรกรรมข้อมูลส่วนบุคคล ค.ศ. 1998 (Identity theft and Assumption Deterrence Act 1998) ประสงค์จะคุ้มครองข้อมูลส่วนบุคคลหรือข้อมูลบ่งชี้เฉพาะเจาะจงตัวบุคคล (identity) ซึ่งเป็นวัตถุแห่งการกระทำ

บทบัญญัติของรัฐบัญญัติเกี่ยวกับการยับยั้งการโจรกรรมข้อมูลส่วนบุคคล ค.ศ. 1998 (Identity theft and Assumption Deterrence Act 1998) มีอยู่ 2 มาตรา คือ มาตรา 1028 และมาตรา 1028 A ซึ่งมีสาระสำคัญ ดังต่อไปนี้

มาตรา 1028 การฉ้อโกงและการกระทำความผิดเกี่ยวกับเอกสารหรือข้อมูลส่วนบุคคล (Fraud and related activity in connection with identification documents, authentication features, and information)[77] มีใจความสำคัญ คือ

อนุมาตรา (a) ผู้ใดในกรณีเงื่อนไขที่ระบุไว้ตามอนุมาตรา (c) ของมาตรานี้

อนุมาตราย่อย (1) เจตนาและโดยมิชอบด้วยกฎหมาย ผลิตเอกสารแสดงตน หรือเครื่องหมายตรวจสอบ (รับรอง) ความถูกต้อง หรือเอกสารแสดงตนปลอม

อนุมาตราย่อย (2) เจตนาจำหน่ายจ่ายโอนเอกสารแสดงตน หรือเครื่องหมายตรวจสอบ (รับรอง) ความถูกต้อง หรือเอกสารแสดงตนปลอม โดยรู้อยู่ว่าเอกสารนั้นได้มาจากการลักหรือผลิตขึ้นโดยมิชอบด้วยกฎหมาย

อนุมาตราย่อย (3) เจตนาครอบครองและเจตนาจะใช้อย่างผิดกฎหมายหรือจำหน่ายจ่ายโอนโดยผิดกฎหมาย ซึ่งเอกสารแสดงตนของผู้อื่น (นอกเหนือไปจากที่ออกโดยชอบด้วยกฎหมายสำหรับการใช้ของผู้ครอบครอง) หรือเครื่องหมายตรวจสอบ (รับรอง) ความถูกต้อง หรือเอกสารแสดงตนปลอม ตั้งแต่ 5 ฉบับขึ้นไป

อนุมาตราย่อย (4) เจตนาครอบครองเอกสารแสดงตนของผู้อื่น (นอกเหนือไปจากที่ออกโดยชอบด้วยกฎหมายสำหรับการใช้งานของผู้ครอบครอง) หรือเครื่องหมายตรวจสอบ (รับรอง) ความถูกต้อง หรือเอกสารแสดงตนปลอม โดยมีเจตนาใช้เอกสารแสดงตนหรือเครื่องหมาย ตรวจสอบ (รับรอง) ความถูกต้องเช่นว่านั้นเพื่อการหลอกลวงประเทศสหรัฐอเมริกา

---

[77] เว็บไซต์ไฟน์ลอว์ดอทคอม *http://codes.lp.findlaw.com/uscode/18/I/47/1028* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

อนุมาตราย่อย (5) เจตนาผลิต จำหน่ายจ่ายโอน หรือครอบครองเครื่องมือทำเอกสาร หรือเครื่องหมายตรวจสอบ (รับรอง) ความถูกต้อง โดยเจตนาให้เครื่องมือทำเอกสารหรือเครื่องหมายตรวจสอบ (รับรอง) ความถูกต้องเช่นว่านั้น นำมาใช้ในการผลิตเอกสารแสดงตน หรือเครื่องหมายตรวจสอบ (รับรอง) ความถูกต้องปลอม หรือเครื่องมือทำเอกสารอื่นใดสำหรับใช้เพื่อการเช่นว่านั้น

อนุมาตราย่อย (6) เจตนาครอบครองเอกสารแสดงตนหรือเครื่องหมายรับรอง (ตรวจสอบ) ความถูกต้อง ซึ่งเป็นหรือปรากฏว่าเป็นเอกสารแสดงตนหรือเครื่องหมายตรวจสอบ (รับรอง) ความถูกต้อง (สำหรับประชาชน) ของประเทศสหรัฐอเมริกาที่ถูกลักหรือผลิตขึ้นโดยมิชอบด้วยกฎหมาย โดยรู้ว่าถูกลักหรือผลิตขึ้นโดยมิชอบด้วยกฎหมาย

อนุมาตราย่อย (7) เจตนาจำหน่ายจ่ายโอน ครอบครอง หรือใช้โดยมิชอบด้วยกฎหมาย ซึ่งสิ่งบ่งชี้เฉพาะเจาะจง (อัตลักษณ์ : means of identification) ของบุคคลอื่น โดยเจตนาที่จะกระทำหรือให้ความช่วยเหลือหรือยุยงหรือสมรู้ร่วมคิดกับการกระทำใดๆ ที่ผิดกฎหมายที่ถือเป็นการละเมิดกฎหมายของรัฐบาลกลาง หรือกระทำความผิดทางอาญาที่ร้ายแรงภายใต้การบังคับใช้กฎหมายใดๆ ของมลรัฐหรือของท้องถิ่น หรือ

อนุมาตราย่อย (8) เจตนาลักลอบค้าเครื่องหมายตรวจสอบ (รับรอง) ความถูกต้องไม่ว่าจะแท้จริงหรือปลอม เพื่อใช้กับเอกสารแสดงตนปลอม เครื่องมือทำเอกสาร หรือสิ่งบ่งชี้เฉพาะเจาะจง (อัตลักษณ์ : means of identification)

ต้องระวางโทษตามที่บัญญัติไว้ในอนุมาตรา (b) ของมาตรานี้

อนุมาตรา (b) ระวางโทษสำหรับความผิดตามอนุมาตรา (a) ของมาตรานี้ คือ ..

อนุมาตราย่อย (1) เว้นแต่ที่บัญญัติไว้ตามอนุมาตราย่อย (3) และ (4) ต้องระวางโทษปรับภายใต้บรรพนี้ หรือจำคุกไม่เกิน 15 ปี หรือทั้งจำทั้งปรับ ถ้าความผิดนั้น คือ..

(A) การผลิตหรือจำหน่ายจ่ายโอนเอกสารแสดงตน เครื่องหมายตรวจสอบ (รับรอง) ความถูกต้อง หรือเอกสารแสดงตนปลอม ซึ่งเป็นหรือปรากฏว่าเป็น..

(i) เอกสารแสดงตน เครื่องหมายตรวจสอบ (รับรอง) ความถูกต้องที่ออกโดยหรือภายใต้อำนาจของสหรัฐอเมริกา หรือ

(ii) สูติบัตร หรือใบอนุญาตขับขี่ หรือบัตรประจำตัวบุคคล

(B) การผลิตหรือจำหน่ายจ่ายโอนเอกสารแสดงตน เครื่องหมายตรวจสอบ (รับรอง) ความถูกต้อง หรือเอกสารแสดงตนปลอมตั้งแต่ 5 ชิ้นขึ้นไป

(C) ความผิดตามอนุมาตราย่อย (5) ของอนุมาตรา (a) หรือ

(D) ความผิดตามอนุมาตราย่อย (7) ของอนุมาตรา (a) เกี่ยวกับการโอนครอบครองหรือใช้ตั้งแต่ 1 ครั้งขึ้นไป ซึ่งสิ่งบ่งชี้เฉพาะเจาะจง (อัตลักษณ์ : means of identification) ถ้าผล

ของ การกระทำความผิดทำให้บุคคลนั้นได้รับมาซึ่งสิ่งใดๆ ที่มีมูลค่ารวมกันตั้งแต่ 1,000 ดอลล่าห์สหรัฐ อเมริกาขึ้นไปในช่วงระยะเวลา 1 ปี

อนุมาตรายย่อย (2) เว้นแต่ที่บัญญัติไว้ตามอนุมาตรายย่อย (3) และ (4) ต้องระวางโทษปรับภายใต้บรรพนี้ หรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ ถ้าความผิดนั้น คือ..

(A) ผลิตด้วยประการใดๆ จำหน่ายจ่ายโอน หรือใช้สิ่งบ่งชี้เฉพาะเจาะจง (อัตลักษณ์ : means of identification) เอกสารแสดงตน เครื่องหมายตรวจสอบ (รับรอง) ความถูกต้อง หรือเอกสารแสดงตนปลอม หรือ

(B) กรณีเป็นความผิดตามอนุมาตรายย่อย (3) หรือ (7) ของมาตรานี้

อนุมาตรายย่อย (3) ระวางโทษปรับภายใต้บรรพนี้ หรือจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ ถ้าความผิดนั้น เพื่อ..

(A) อำนวยความสะดวกสำหรับอาชญากรรมค้ายาเสพติด (ตามที่กำหนดใน มาตรา 929 (a) (2))

(B) ในการสมรู้ร่วมคิดกับอาชญากรรมที่ร้ายแรง (ตามที่กำหนดใน มาตรา 924 (c) (3)) หรือ

(C) เป็นการกระทำความผิดซ้ำตามมาตรานี้อีก

อนุมาตรายย่อย (4) ระวางโทษปรับภายใต้บรรพนี้ หรือจำคุกไม่เกิน 30 ปี หรือทั้งจำทั้งปรับ ถ้าการกระทำความผิดนั้นเพื่อที่จะอำนวยความสะดวก สำหรับการกระทำความผิดฐานก่อการร้ายในประเทศ (ตามที่กำหนดตามมาตรา 2331 (5) ภายใต้บรรพนี้) หรือการกระทำความผิดฐานก่อการร้ายระหว่างประเทศ (ตามที่กำหนดใน มาตรา 2331 (1) ของบรรพนี้)

อนุมาตรายย่อย (5) ในกรณีความผิดอื่นๆ ภายใต้อนุมาตรา (a) นอกจากที่ระบุไว้ ทรัพย์สินส่วนบุคคลใดๆ ที่ใช้หรือตั้งใจใช้ในการกระทำความผิดให้ริบตกเป็นของประเทศสหรัฐอเมริกา และ

อนุมาตรายย่อย (6) ในกรณีความผิดอื่นๆ ปรับภายใต้บรรพนี้ หรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ

การปรับตามบรรพนี้ หมายถึง บรรพที่ 18 ของ U.S.C. ซึ่งกฎหมายฉบับนี้ได้นำหลักเรื่องมูลค่าของความเสียหายที่เกิดจากการกระทำมาใช้กับโทษปรับด้วย กล่าวคือ มีการกำหนดจำนวนเงินที่จะปรับตามฐานความผิดอาจจะปรับ 5,000 หรือ 10,000 หรือ 100,000 ดอลล่าห์สหรัฐอเมริกา หรือปรับเป็นเงินสองเท่าของมูลค่าความเสียหายที่จำเลยได้ก่อให้เกิดขึ้น อันเป็นลักษณะหรือแนวทางเดียวกับมาตรา 1030 (c) แห่งรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986)

ฐานความผิดดังกล่าวในมาตรา 1028 (a) ข้างต้นจะบังคับใช้กับการกระทำที่ส่งผลหรือภายใต้เงื่อนไขที่บัญญัติไว้ตามอนุมาตรา (c) ดังนี้

อนุมาตรา (c) กรณีที่กล่าวถึงตามอนุมาตรา (a) ของมาตรานี้ คือ..

อนุมาตรายย่อย (1) เอกสารแสดงตน เครื่องหมายตรวจสอบ (รับรอง) ความถูกต้อง หรือเอกสารแสดงตนปลอม หรือเครื่องมือทำเอกสารที่ออกแบบมาหรือในลักษณะเดียวกัน สำหรับใช้ผลิตเอกสารแสดงตน เครื่องหมายตรวจสอบ (รับรอง) ความถูกต้อง หรือเอกสารแสดงตนปลอมนั้นเป็นหรือออกโดยหรือภายใต้อำนาจของสหรัฐอเมริกา

อนุมาตรายย่อย (2) การกระทำความผิดนั้นเป็นความผิดตามอนุมาตรา (a) (4) แห่งมาตรานี้ หรือ

อนุมาตรายย่อย (3) ในกรณีอย่างใดอย่างหนึ่งตามที่กำหนดนี้

(A) การผลิต การจำหน่ายจ่ายโอนการครอบครอง หรือใช้ที่ฝ่าฝืนกฎหมายตามมาตรานี้ที่ส่งผลกระทบต่อการค้าระหว่างมลรัฐหรือระหว่างประเทศ รวมทั้งการโอนเงินของเอกสารทางอิเล็กทรอนิกส์ หรือ

(B) สิ่งบ่งชี้เฉพาะเจาะจง (อัตลักษณ์ : means of identification) เอกสารแสดงตน เอกสารแสดงตนปลอม หรือเครื่องมือทำเอกสารเป็นการผลิต การจำหน่ายจ่ายโอนการครอบครอง หรือใช้ที่ฝ่าฝืนกฎหมายตามมาตรานี้ ในระหว่างการขนส่งทางไปรษณีย์

สำหรับบทบัญญัติที่กำหนดฐานความผิดตามมาตรา 1028 (a) ของรัฐบัญญัติเกี่ยวกับการยับยั้งการโจรกรรมข้อมูลส่วนบุคคล ค.ศ. 1998 (Identity theft and Assumption Deterrence Act 1998) มีข้อพึงพิจารณา คือ ได้มีการบัญญัติบทนิยามหรือความหมายไว้ตามอนุมาตรา (d) ซึ่งเป็นเนื้อหาสำคัญอันจะทำให้ทราบได้ว่า ที่กฎหมายฉบับนี้มุ่งประสงค์จะคุ้มครองข้อมูลส่วนบุคคลหรือข้อมูลบ่งชี้เฉพาะเจาะจงตัวบุคคล (Identity) อันเป็นวัตถุแห่งการกระทำนี้มีความหมายครอบคลุมข้อมูลหรือสิ่งบ่งชี้เฉพาะเจาะจงอะไรบ้าง อีกทั้งบทนิยามเหล่านี้ จะใช้กับมาตรา 1028 A ที่จะกล่าวถึงถัดไปด้วย โดยถ้อยคำสำคัญบางถ้อยคำที่จะกล่าวถึงในบางอนุมาตรามีดังต่อไปนี้

อนุมาตรา (d) ในมาตรานี้และมาตรา 1028 A

อนุมาตรายย่อย (1) คำว่า “เครื่องหมายตรวจสอบ (รับรอง) ความถูกต้อง” (authentication feature) หมายความว่า โฮโลแกรมใดๆ (hologram) ลายน้ำ ใบรับรอง สัญลักษณ์ รหัส ภาพ อนุกรม ของตัวเลขหรือตัวอักษร หรือคุณลักษณะอื่นๆ ไม่ว่าจะโดยเอกเทศหรือรวมทั้งที่ต้องใช้ร่วมกับ เครื่องหมายอื่น โดยผู้มีอำนาจออกให้ควบคู่กันบนเอกสารแสดงตน เครื่องมือทำเอกสาร หรือสิ่ง บ่งชี้เฉพาะเจาะจง (อัตลักษณ์ : means of identification) สำหรับตรวจสอบเอกสารปลอม แก้ไข เปลี่ยนแปลง หรือปลอมแปลงเป็นอย่างอื่น

อนุมาตรา ย่อย (2) คำว่า “เครื่องมือทำเอกสาร” หมายความว่า เครื่องมืออย่างใดๆ เครื่อง พิมพ์ แม่แบบ ไฟล์คอมพิวเตอร์ แผ่นดิสก์ อุปกรณ์อิเล็กทรอนิกส์ อุปกรณ์เครื่องคอมพิวเตอร์ ฮาร์ดแวร์หรือโปรแกรม (ซอฟต์แวร์) ที่ประกอบกันเป็นการเฉพาะเจาะจงหรือใช้เป็นหลัก สำหรับการทำเอกสารแสดงตน เอกสารแสดงตนปลอม หรือเครื่องมือทำเอกสารเช่นว่านั้น

อนุมาตรา ย่อย (3) คำว่า “เอกสารแสดงตน” หมายความว่า เอกสารที่ทำขึ้นหรือที่ออกโดยหรือภายใต้อำนาจของรัฐบาลสหรัฐอเมริกา มลรัฐ หน่วยงานทางปกครองของรัฐ รัฐบาลต่างประเทศ หน่วยงานทางปกครองของรัฐบาลต่างประเทศ องค์การระหว่างประเทศ หรือกึ่งองค์การระหว่างประเทศ ซึ่งเมื่อเสร็จสมบูรณ์ประกอบกับข้อมูลเฉพาะเจาะจงบุคคลเป็นรูปแบบ (เอกสารแสดงตน) ที่เจตนาหรือได้รับการยอมรับกันทั่วไปเพื่อวัตถุประสงค์ในการบ่งชี้เฉพาะตัวบุคคล

อนุมาตรา ย่อย (4) คำว่า “เอกสารแสดงตนปลอม” หมายความว่า รูปแบบเอกสารที่เจตนา หรือได้รับการยอมรับกันทั่วไปเพื่อวัตถุประสงค์ในการบ่งชี้เฉพาะตัวบุคคล ที่..

(A) ไม่ได้ออกโดยหรือภายใต้อำนาจของรัฐ หรือโดยกิจการนิติบุคคลที่ออกภายใต้อำนาจของรัฐ แต่ถูกเปลี่ยนแปลงต่อมาเพื่อวัตถุประสงค์ในการหลอกลวง และ

(B) ซึ่งปรากฏว่า (เอกสารแสดงตนนั้น) ต้องออกโดยหรือภายใต้อำนาจของรัฐบาลสหรัฐอเมริกา มลรัฐ หน่วยงานทางปกครองของรัฐ รัฐบาลต่างประเทศ หน่วยงานทางปกครองของรัฐบาลต่างประเทศ องค์การระหว่างประเทศ หรือกึ่งองค์การระหว่างประเทศ

อนุมาตรา ย่อย (5) คำว่า “เครื่องหมายตรวจสอบ (รับรอง) ความถูกต้องปลอม” หมายความว่า เครื่องหมายตรวจสอบ (รับรอง) ความถูกต้องอย่างใดๆ ที่..

(A) เป็นของแท้โดยกำเนิด แต่โดยไม่ได้รับอนุญาตจากผู้มีอำนาจออก มีการแก้ไขหรือเปลี่ยนแปลง เพื่อวัตถุประสงค์ในการหลอกลวง

(B) เป็นของแท้ แต่ได้รับการจ่ายแจกหรือมีไว้สำหรับจ่ายแจกโดยไม่ได้รับอนุญาตจาก ผู้มีอำนาจออกและไม่ได้รับมอบอำนาจโดยชอบด้วยกฎหมาย ที่จะทำเอกสารแสดงตน เครื่องมือทำเอกสาร หรือสิ่งบ่งชี้เฉพาะเจาะจง ซึ่งผู้มีอำนาจออกเจตนาใช้เครื่องหมายตรวจสอบ (รับรอง) ความถูกต้องติดอยู่หรือฝังตัวอยู่ (ในเอกสารต่างๆ ข้างต้น) หรือ

(C) จะปรากฏว่าเป็นของแท้ แต่ไม่ใช่ของแท้

อนุมาตรา ย่อย (7) คำว่า “สิ่งบ่งชี้เฉพาะเจาะจง” (อัตลักษณ์ : means of identification) หมายความว่า ชื่อหรือหมายเลขใดๆ ที่อาจจะใช้เพียงอย่างเดียวหรือใช้ร่วมกับข้อมูลอื่นๆ ในการ ระบุตัวบุคคลที่เฉพาะเจาะจง รวมถึง..

(A) ชื่อ หมายเลขประกันสังคม วันเดือนปีเกิดอย่างเป็นทางการ หมายเลขประจำตัวหรือใบอนุญาตขับขี่ที่ออกโดยรัฐหรือหน่วยงานภาครัฐ หมายเลขทะเบียนคนต่างด้าว หมายเลขหนังสือ เดินทาง หมายเลขประจำตัวของนายจ้างหรือผู้เสียภาษีอากร

(B) ข้อมูลเฉพาะทางชีวภาพ เช่น ลายนิ้วมือ เสียง ภาพจอประสาทตา (retina) หรือม่านตา (iris) หรืออื่นๆ ที่เป็นลักษณะทางกายภาพของร่างกายที่บ่งชี้เฉพาะบุคคล

(C) หมายเลขชุดอิเล็กทรอนิกส์ ที่อยู่ หรือรหัสผ่าน หรือ

(D) ข้อมูลบ่งชี้การสื่อสารโทรคมนาคม หรือเครื่องมือสำหรับการเข้าถึง (access device), (ตามที่บัญญัติไว้ในมาตรา 1029 (e))

อนุมาตราย่อย (8) คำว่า “บัตรประจำตัวบุคคล” หมายความว่า เอกสารแสดงตนที่ออกโดยรัฐหรือองค์กรปกครองส่วนท้องถิ่น เพื่อจุดประสงค์ในการบ่งชี้เฉพาะ

ในคดีระหว่าง สหรัฐอเมริกา โจทก์ Appellee -, V. Castellanos Ruben, จำเลยผู้อุทธรณ์[78] ความเป็นมาของคดี Ruben Castellanos สมคบคิดและกระทำความผิดร่วมกับอีกสองคนเพื่อผลิต และขายเอกสารแสดงตนปลอม ก่อนวันที่ 27 สิงหาคม 1997 เขาเช่าห้องจากที่เขาได้วางแผนที่จะผลิตหรือทำปลอมเอกสาร จากนั้นสองสัปดาห์ คือ ระหว่างวันที่ 27 สิงหาคม ถึงวันที่ 10 กันยายน 1997 ร่วมกับผู้ร่วมกระทำความผิดอื่นร้องขอให้ลูกค้าซื้อเอกสารแสดงตนปลอม โดยนาย Castellanos ทำปลอมบัตรคนต่างด้าวมีถิ่นที่อยู่และบัตรประกันสังคมอันเป็นบัตรประจำตัวปลอม โดยการพิมพ์ข้อมูลชีวประวัติลงบนบัตรเคลือบลามิเนต เขาได้รับ $ 50.00 ต่อเอกสารปลอมจากลูกค้า วันที่ 10 กันยายน 1997 เมื่อนาย Castellanos ถูกจับ เขาได้ถือกระเป๋ายี่ห้อ Duffle ขนาดใหญ่ โดยเจ้าหน้าที่ของรัฐบาลนับบัตรคนต่างด้าวมีถิ่นที่อยู่ปลอมได้ 192 ฉบับ บัตรประกันสังคมปลอม 24 ฉบับ พลาสติกลามิเนตกับ I - 551 โฮโลแกรม สำหรับบัตรคนต่างด้าวมีถิ่นที่อยู่ 16 ฉบับ และพลาสติกใสลามิเนตสำหรับบัตรประกันสังคม 31 ฉบับ

นาย Castellanos ถูกตั้งข้อหา 2 ข้อหา คือ สมคบกระทำความผิดเอกสารเกี่ยวกับการโอนสัญชาติเป็นพลเมืองหรือสถานะการมีถิ่นที่อยู่ตามกฎหมายโดยเจตนา (อันเป็นการละเมิด 18 USC § 371) และเจตนาครอบครองเอกสารโดยมีเจตนาที่จะผลิตเอกสารแสดงตนปลอม (อันเป็นการละเมิด 18 USC § 1028 (a) (5)) เขา (นาย Castellanos) สารภาพมีส่วนร่วมกระทำความผิด มีการพิจารณาคดีวันที่ 16 มิถุนายน 1998 ศาลและผู้เกี่ยวข้องเห็นพ้องกันว่า USSG § 2L2.1 (a) นำไปใช้กับความผิดแนวทางที่ให้ระดับความผิดฐานเกี่ยวกับเอกสารแสดงตนผิดกฎหมายเป็นระดับ 11 และหากความผิดที่เกี่ยวข้องมีเอกสาร 100 ฉบับหรือมากกว่า ความผิดจะเพิ่มขึ้นเป็นระดับ 9 หลังจากศาลแขวงได้การตรวจสอบพยานหลักฐานและได้ฟังการโต้แย้งของที่ปรึกษา ได้ความว่านาย Castellanos ถือในกระเป๋า Duffle ขณะเมื่อเขาถูกจับ ศาลนับเอกสารไม่ว่าจะปลอมสมบูรณ์หรือปลอมไม่สมบูรณ์ เป็นบัตรคนต่างด้าวมีถิ่นที่อยู่ปลอม 192 ฉบับ และบัตรประกันสังคมปลอม 24

---

[78] เว็บไซต์ไฟน์ลอว์ดอทคอม *http://caselaw.findlaw.com/us-7th-circuit/*1436041.*html* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

ฉบับ รวมทั้งหมดมีเอกสารปลอม 216 ฉบับ ซึ่งความผิดจะต้องเพิ่มเป็นระดับ 9 สำหรับเอกสารปลอมกว่า 100 ฉบับ และลดลง 3 ระดับสำหรับการสารภาพยอมรับผิด โทษตามกฎหมายของนาย Castellanos อยู่ระหว่างจำคุก 24-30 เดือน ศาลแขวงพิพากษาลงโทษจำคุก 24 เดือน

ประเด็นข้อโต้แย้งของคดี มาตรา 1028 “การฉ้อโกงและการกระทำความผิดเกี่ยวกับเอกสารปลอม” บทบัญญัติของ United States Code อธิบายถึงความผิดของการฉ้อโกงซึ่งเชื่อมโยงกับเอกสารแสดงตนปลอม บทบัญญัติของกฎหมายให้นิยามของคำว่า “เอกสารแสดงตน”[79] เอกสารที่ทำขึ้น หรือที่ออกโดย หรือภายใต้อำนาจของรัฐบาลสหรัฐอเมริกา มลรัฐ หน่วยงานทางปกครองของรัฐ รัฐบาลต่างประเทศ หน่วยงานทางปกครองของรัฐบาลต่างประเทศ องค์การ ระหว่างประเทศ หรือกึ่งองค์การระหว่างประเทศ ซึ่งเมื่อเสร็จสมบูรณ์ประกอบกับข้อมูลเฉพาะ เจาะจงบุคคลเป็นรูปแบบ (เอกสารแสดงตน) ที่เจตนาหรือได้รับการยอมรับกันทั่วไปเพื่อวัตถุ-ประสงค์ในการบ่งชี้เฉพาะตัวบุคคล

ประมวลกฎหมายสหรัฐอเมริกา บรรพ 18 U.S.C. , มาตรา 1028 (d) (1) ศาลแขวงวินิจฉัยว่า ทั้งหมด 216 ฉบับที่ถือโดยนาย Castellanos เป็น “เอกสารแสดงตน” ดังความหมายของบทนิยามตามกฎหมายข้างต้น ซึ่งต้องด้วยบทบัญญัติของ 2L2.1 อันเป็นแนวทางที่ใช้กับความผิดของการกระทำเกี่ยวกับเอกสารที่ผิดกฎหมาย เรา (ศาลแขวง) ดำเนินกระบวนพิจารณาตรวจสอบข้อเท็จจริงของคดีต่อไปจนกว่าจะได้ความว่าจำเลยเป็นผู้กระทำความผิดอย่างชัดเจน

ประเด็นแรก นาย Castellanos โต้แย้งประเด็นโดยมุ่งเน้นที่เนื้อหาของความหมายคำว่า “เอกสารแสดงตน” บรรดาวัตถุต่างๆ ที่เขาครอบครองขณะถูกจับกุมเป็นเพียงวัตถุที่ยังไม่สมบูรณ์เพียงพอที่จะเป็น “เอกสารแสดงตน” ในความหมายตามที่มีการกำหนดไว้ใน มาตรา 1028 (d) (1) เพราะบัตรไม่ได้มี “ความสมบูรณ์” ดังคำจำกัดความ วัตถุเหล่านั้นยังไม่ได้เป็นเอกสารแสดงตน เพราะเป็นเพียงแค่บัตรตั้งต้นสำหรับผลิตเท่านั้น ถึงแม้ว่านาย Castellanos ยอมรับว่าเขามีจุดประสงค์เพื่อใช้ในการผลิตเอกสารแสดงตนปลอม แต่ยังไม่ได้ประมวลผลข้อมูลสำหรับการผลิตเอกสารแสดงตนปลอม ดังนั้น จึงไม่สามารถนับรวมเพื่อให้การกระทำของเขาอยู่ภายใต้บทบัญญัติ 2L2.1 ที่ต้องได้รับโทษหนักขึ้น

ตามหลักการ เรา (ศาล) ไม่สามารถยอมรับนาย Castellanos เนื่องจากทราบว่านาย Castellanos มุ่งหมายในการกระทำความผิดละเมิดประมวลกฎหมายสหรัฐอเมริกา (USC) บรรพ 18 มาตรา 1028 โดยต้องการจำหน่ายเอกสารแสดงตนที่ผิดกฎหมาย ดังนั้น ไม่อาจวินิจฉัยได้ว่า การกระทำความผิดเกี่ยวกับการจำหน่ายเอกสารแสดงตนที่ผิดกฎหมายของเขาจะไม่ถูกลงโทษ นอกจากนี้เรา (ศาล) เชื่อว่าภาษาธรรมดาตามมาตรา 1028 (d) ไม่สนับสนุนการกระทำที่ให้รัฐบัญญัติ

---

[79] มาตรา 1028 (d) (3), (ผู้วิจัย)

มีผลบังคับใช้เฉพาะกับเอกสารแสดงตนที่สมบูรณ์แล้ว บทนิยามของกฎหมายดังกล่าว อธิบายถึง “เอกสารแสดงตน” เป็นเอกสารที่ทำโดยหน่วยงานของรัฐเพื่อวัตถุประสงค์ในการระบุ ตัวตนของบุคคลนั้น เมื่อระบุข้อมูลที่เฉพาะเจาะจงของแต่ละบุคคลเพิ่มลงในเอกสารซึ่งก็มีจุดมุ่งหมายและเป็นที่ยอมรับสำหรับการระบุได้เฉพาะเจาะจง ส่วน “เมื่อ” โดยสภาพของบัตรเป็น ลักษณะของเอกสารที่เห็นประจักษ์ว่าเป็นเอกสารแสดงตน “เมื่อใด” ดำเนินการเพียงปรับหรือ เปลี่ยนข้อมูลลงบนบัตรก็สามารถระบุเฉพาะเจาะจงตัวบุคคลได้

ใด ๆ ที่เป็นข้อสงสัยที่เกี่ยวกับความหมายของรัฐบัญญัติตามมาตรา 1028 เนื้อหาและเจตนารมณ์ของกฎหมายจากการประชุมของสภาคองเกรสก็คือเนื้อหาของการนิยาม “เอกสารแสดงตน” ให้มีความหมายอย่างกว้าง โดยครอบคลุมเอกสารทั้งที่สมบูรณ์และไม่สมบูรณ์อยู่ในความหมายของบทนิยาม

ความหมายของ “เอกสารแสดงตน” จึงมีวัตถุประสงค์รวมทั้งเอกสารแสดงตนที่ว่างเปล่า ซึ่งยังไม่เสร็จสมบูรณ์ แต่อยู่ในสภาพพร้อมระบุข้อมูลเกี่ยวกับตัวบุคคลด้วย

อ้างอิง H.R.Rep. หมายเลข 97-802 วันที่ 9 (1982) พิมพ์ซ้ำในปี 1982 USCCAN 3,519, 3,527[80]

นอกจากนี้ยังมีคดีซึ่งศาลที่มีการพิจารณาประเด็นอย่างเดียวกันไว้เกี่ยวกับคำนิยามของ “เอกสารแสดงตน” รวมถึงเอกสารที่ไม่สมบูรณ์ด้วย ดูคดี United States v. VIERA, 149 F.3d 7, 9 (1st Cir.1998) (per curiam); คดี United States v. Salazar, 70 F.3d 351, 352 (5th Cir.1995); คดี United States v. Martinez - Cano, 6 F.3d 1400, 1403 (9th Cir.1993) (ครอบคลุมเนื้อหาสำหรับการผลิตเอกสารปลอมบางส่วนที่สมบูรณ์และบัตรอื่น ๆ ซึ่งว่างเปล่า); คดี United States v. Pahlavani, 802 F .2 d 1505, 1506 (4th Cir.1986) (ประวัติความเป็นมาของกฎหมาย สรุปว่าการประชุมของคองเกรส มีวัตถุประสงค์ตามแบบฟอร์ม I - 94 กระทรวงยุติธรรมรายงานการประชุมเกี่ยวกับความหมายตามกฎหมายของ “เอกสารแสดงตน”) ดังนั้น เรา (ศาล) จึงสรุปได้ว่าสภาคองเกรสมีวัตถุประสงค์ให้รวมถึงเอกสารแสดงตนที่ไม่สมบูรณ์ให้อยู่ในความหมายตามกฎหมายของ “เอกสารแสดงตน” สำหรับเจตนารมณ์ของ มาตรา 1028 (d) (1) ดังนั้น เรา (ศาล) จึงเห็นด้วยกับการกำหนดขอบเขตเนื้อหาซึ่งเอกสารทั้งหมดของนาย Castellanos ไม่ว่าจะสมบูรณ์หรือไม่สมบูรณ์เคยใช้ในคดีก่อนหน้าสำหรับการจำหน่าย และสามารถนับเพื่อวัตถุประสงค์ในการเพิ่มระวางโทษในการพิพากษาภายใต้ มาตรา 2L2.1

ประเด็นที่สอง ในประเด็นนี้ นาย Castellanos อ้างโต้แย้งว่า หากเอกสารที่ว่างเปล่าที่เขาครอบครองอยู่ภายใต้ขอบเขตนิยามของมาตรา 1028 (d) เขามีจริงเพียง 26 ฉบับ ซึ่งนั่นก็

[80] หมายเลขและข้อมูลทางคดี ซึ่งคำพิพากษาฉบับนี้ อ้างอิงถึงคำพิพากษาคดีก่อนหน้า (ผู้วิจัย)

คือ 24 ฉบับบัตรคนต่างด้าวมีถิ่นที่อยู่ที่ว่างเปล่า มีแผ่น (sheet) 8 ฉบับที่มีรอยพิมพ์หรือรอยประทับ และ 2 ฉบับบัตรประกันสังคมปลอม มีแผ่น (sheet) 12 ฉบับที่มีข้อมูลของบัตรประกันสังคม นาย Castellanos อ้างถึงหมายเหตุข้อ 2 ของ มาตรา 2L2.1 ซึ่งกล่าวว่า เอกสารหรือวัตถุหลายส่วนที่จะดำเนินการเป็นส่วนหนึ่งของชุดเอกสารเพื่อใช้สำหรับผลิตชิ้นเดียว บทบัญญัติ USSG มาตรา 2L2.1 อ้างว่าสำเนาเอกสารหลายๆ ชิ้นของแต่ละบัตรเป็นส่วนหนึ่งของชุด จึงควรจะนับเป็นเอกสารชุดเดียวกันที่ใช้สำหรับบุคคลคนเดียว

ประเด็นเป็นเรื่องสำคัญที่จะต้องทราบว่าภายใต้ความหมายของเอกสารเป็น “ชุด” เมื่อ “เป็นการผลิต” ที่ผู้กระทำความผิดจะ “มีวัตถุประสงค์ใช้สำหรับคนเดียว” ดูคดี United States v. Torres, 81 F.3d 900, 904 (9th Cir.1996) (ข้อสังเกต แนวทางของมาตรา 2L2.1 “ยังคงกล่าวไว้ว่า เอกสารหลายส่วนของชุดเพื่อใช้สำหรับบุคคลคนเดียวควรถือว่าเป็นเอกสารเดียวกันหนึ่งชุด ”) ดู Salaza ; 70 F.3d ที่ 352 n. 2 (ข้อสังเกตในสุภาษิตกฎหมายถือว่าเป็นเอกสารชุดเดียวกัน) CF. (ในสัญญาสัมปทานมีข้อวินิจฉัยของจำเลยที่ “เอกสารเป็นชุด” ต้องมีเอกสารเสร็จหรือกลุ่มของเอกสารที่สมบูรณ์แล้วเป็นรายบุคคล); ดู Martinez - Cano, 6 F.3d at 1402 (พูดถึงคดีก่อนหน้าเกี่ยวกับหมายเหตุข้อ 2 ข้อสังเกตความแตกต่างระหว่างเอกสารเดี่ยวกับเอกสารเป็นชุด) เกี่ยวกับวัตถุประสงค์บัตรประกันสังคม 12 ฉบับหรือบัตรคนต่างด้าวมีถิ่นที่อยู่ 8 ฉบับ แม้ว่านาย Castellanos ไม่ได้พิสูจน์ข้อโต้แย้งว่าข้อมูลในเอกสารแผ่นเดียว อาจยืนยันว่าบุคคลเพียงคนเดียวอาจจะซื้อ และใช้สำหรับการระบุเฉพาะเจาะจงตัวบุคคลทั้งบัตรประกันสังคมและบัตรลงทะเบียนคนต่างด้าว ศาลแขวงอาจมีนับชุดประกันสังคม 24 ฉบับ และบัตรคนต่างด้าวมีถิ่นที่อยู่และเพิ่มเติมแยกบัตรคนต่างด้าวมีถิ่นที่อยู่จำนวน 172 ฉบับ ซึ่งยังคงมีปริมาณมากกว่า 100 ฉบับ ดังนั้น จึงยังคงส่งผลให้ระดับความผิดต้องเพิ่มขึ้น นอกจากนี้ยังมีหลักฐานว่าเอกสารในกระเป๋ายี่ห้อ Duffle ของนาย Castellanos ไม่จำเป็นต้องเป็นชุดของเอกสารไว้สำหรับบุคคลหนึ่งคนตามหมายเหตุข้อ 2 เรา (ศาล) จึงต้องสรุปในบันทึกนี้ที่ศาลแขวงคำนวณจำนวนเอกสารแสดงตนไว้ได้อย่างถูกต้องที่นาย Castellanos ครอบครองเพื่อวัตถุประสงค์ในการผลิตหรือทำปลอมสำหรับการพิจารณาพิพากษาระวางโทษ

ข้อสรุป สำหรับเหตุผลที่นำเสนอข้างต้นเราเก็บไว้ที่ศาลแขวงคำนวนอย่างถูกต้องว่าคำว่า “เอกสารแสดงตน” รวมถึงเอกสารที่ว่างเปล่าและการคำนวณอย่างถูกต้องว่าความผิดที่นาย Castellanos สมรู้ร่วมคิดกระทำการปลอมเอกสารแสดงตนที่ผิดกฎหมายมีจำนวนมากกว่า 100 ฉบับ อันอยู่ภายใต้บังคับของ USSG มาตรา 2L2.1 (b) ศาลแขวงวินิจฉัยไว้ชอบแล้ว พิพากษายืน

ส่วนบทบัญญัติตามมาตรา 1028 A การขโมยข้อมูลส่วนบุคคล (Aggravated identity theft)[81] มีสาระสำคัญ คือ

อนุมาตรา (a) การกระทำความผิด

อนุมาตราย่อย (1) กรณีทั่วไป ผู้ใดเกี่ยวข้องกับอาชญากรรมร้ายแรงตามอนุมาตรา (c) เจตนาโอน ครอบครองหรือใช้โดยปราศจากอำนาจตามกฎหมายซึ่งสิ่งบ่งชี้เฉพาะเจาะจง (อัตลักษณ์ : means of identification) ของผู้อื่น จะต้องได้รับโทษเพิ่มนอกเหนือจากโทษสำหรับอาชญากรรมร้ายแรงดังกล่าว โดยถูกพิพากษาให้จำคุกเพิ่ม 2 ปี

อนุมาตราย่อย (2) กรณีความผิดเกี่ยวกับการก่อการร้าย ผู้ใดเกี่ยวข้องกับอาชญากรรมร้ายแรงตามมาตรา 2332 b (g) (5) (B) เจตนาโอน ครอบครองหรือใช้โดยปราศจากอำนาจตามกฎหมาย ซึ่งสิ่งบ่งชี้เฉพาะเจาะจง (อัตลักษณ์ : means of identification) ของผู้อื่น หรือเอกสารแสดงตนปลอม[82] จะต้องได้รับโทษเพิ่มนอกเหนือจากโทษสำหรับอาชญากรรมร้ายแรงดังกล่าว โดยถูกพิพากษาให้จำคุกเพิ่ม 5 ปี

อนุมาตรา (c) บทนิยาม สำหรับวัตถุประสงค์ของมาตรานี้ คำว่า “อาชญากรรมร้ายแรงตาม อนุมาตราย่อย (c)” หมายความถึง ความผิดใดๆ ที่เป็นอาชญากรรมร้ายแรงในเรื่อง..

อนุมาตราย่อย (1) มาตรา 641 (เกี่ยวกับการขโมยเงิน ทรัพย์สินหรือค่าชดเชยสำหรับประโยชน์สาธารณะ) มาตรา 656 (ที่เกี่ยวข้องกับการขโมย การฉ้อฉลหรือการกระทำที่ไม่สุจริตโดยเจ้าหน้าที่หรือพนักงานธนาคาร) หรือมาตรา 664 (ส่วนที่เกี่ยวข้องกับการโจรกรรมโดยพนักงาน)

อนุมาตราย่อย (2) มาตรา 911 (เกี่ยวกับเอกสารแสดงความเป็นพลเมืองปลอม)

อนุมาตราย่อย (3) มาตรา 922 (a) (6) (เกี่ยวกับหลักฐานปลอมในการติดต่อซื้ออาวุธปืน)

อนุมาตราย่อย (4) การใดๆ ที่ระบุอยู่ในบรรพ (ที่เกี่ยวกับการฉ้อโกงและหลักฐานปลอม) นี้ นอกเหนือจากมาตรานี้หรือมาตรา 1028 (a) (7)

อนุมาตราย่อย (5) การใดๆ ที่ระบุอยู่ในบรรพที่ 63 (ที่เกี่ยวกับจดหมาย ธนาคารและฉ้อโกงทางโทรศัพท์)

อนุมาตราย่อย (6) การใดๆ ที่ระบุอยู่ในบรรพที่ 69 (ที่เกี่ยวกับสัญชาติและการเป็นพลเมือง)

---

[81] เว็บไซต์*คณะนิติศาสตร์ มหาวิทยาลัยคอร์แนล https://www.law.cornell.edu/search/site/1028* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

[82] อนุมาตรานี้ หมายถึง การกระทำความผิดเกี่ยวกับการก่อการร้ายโดยมีการโอนการครอบครองหรือใช้สิ่งบ่งชี้เฉพาะเจาะจง (อัตลักษณ์ : means of identification) ของผู้อื่นหรือเอกสารแสดงตนปลอม

อนุมาตรายย่อย (7) การใดๆ ที่ระบุอยู่ในบรรพที่ 75 (ที่เกี่ยวกับหนังสือเดินทางและวีซ่า)

อนุมาตรายย่อย (8) มาตรา 523 ของ Gramm - Leach - Bliley Act (15 U.S.C. 6823) (เกี่ยวกับการได้มาซึ่งข้อมูลของผู้บริโภคโดยการหลอกลวง)

อนุมาตรายย่อย (9) มาตรา 243 หรือมาตรา 266 ของรัฐบัญญัติคนเข้าเมืองและสัญชาติ (8 U.S.C. 1253 และ 1306) (ที่เกี่ยวกับการจงใจให้เกิดความล้มเหลวในการให้ออกจากประเทศสหรัฐอเมริกา ภายหลังจากที่คนต่างด้าวรอการส่งกลับ ด้วยการทำบัตรการลงทะเบียนคนต่างด้าวปลอม)

อนุมาตรายย่อย (10) การใดๆ ที่ระบุอยู่ในบรรพที่ 8 ของหมวดที่ II ของรัฐบัญญัติคนเข้าเมืองและสัญชาติ (8 USC 1321 et seq.) (การกระทำผิดเกี่ยวกับการตรวจคนเข้าเมืองต่างๆ) หรือ

อนุมาตรายย่อย (11) มาตรา 208 มาตรา 811 มาตรา 1107 (b) มาตรา 1128 B (a) หรือมาตรา 1632 ของรัฐบัญญัติประกันสังคม (42 U.S.C. 408, 1011, 1307 (b), 1320 a – 7 b (a) และ 1383 a) (เกี่ยวกับหลักฐานปลอมเกี่ยวกับรายการที่แสดงตามความในรัฐบัญญัติ)

จากการศึกษาวิจัยบทบัญญัติกฎหมายและคำพิพากษาของศาลทั้งประเทศอังกฤษและประเทศสหรัฐอเมริกาอันจะนำไปสู่การศึกษาวิจัยปัญหาทางกฎหมาย เพื่อค้นหามาตรการทางกฎหมายอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์ตามกฎหมายไทยต่อไป

บทที่ 4
วิเคราะห์ปัญหากฎหมายอาญาเกี่ยวกับการคุ้มครองข้อมูลคอมพิวเตอร์

การวิเคราะห์ปัญหากฎหมายอาญาเกี่ยวกับการคุ้มครองข้อมูลคอมพิวเตอร์ของบทที่ 4 จะแยกการวิเคราะห์ออกเป็น 3 หัวข้อ ดังต่อไปนี้

1. วิเคราะห์ข้อกฎหมายจากกรณีศึกษาทางคดีของประเทศไทย
2. วิเคราะห์พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
3. วิเคราะห์ความผิดฐานสำเนาข้อมูลคอมพิวเตอร์

1. วิเคราะห์ข้อกฎหมายจากกรณีศึกษาทางคดีของประเทศไทย

กรณีข้อมูลคอมพิวเตอร์ได้เคยเกิดการกระทำที่มีการคัดลอกหรือสำเนาข้อมูลคอมพิวเตอร์จนถึงขั้นเป็นคดีนำเสนอขึ้นสู่ศาล ทั้งยังมีประเด็นข้อกฎหมายพิพาทโต้แย้งไปถึงศาลฎีกา ซึ่งมีคำพิพากษาฎีกาที่ 5161/2547 กับคำพิพากษาฎีกาที่ 4311/2557 ดังนี้

1.1 คดีตามคำพิพากษาฎีกาที่ 5161/2547 ประเด็นเกี่ยวแก่การโจรกรรม หรือสำเนาข้อมูลคอมพิวเตอร์ ซึ่งคดีโต้แย้งกันจนขึ้นสู่ศาลฎีกา และคดีถึงที่สุดด้วยการยกฟ้องจำเลย[83]

คำพิพากษาฎีกาที่ 5161/2547 จำเลยเป็นพนักงานแผนกต่างประเทศของโจทก์ร่วม มีหน้าที่เตรียมเอกสารคำขอใบอนุญาตติดต่อหน่วยราชการ ติดต่อประสานงานกับลูกค้าต่างประเทศในวันเวลา และสถานที่เกิดเหตุตามฟ้อง จำเลยนำเอกสารจำนวนประมาณ 400 แผ่น ตามเอกสารหมาย จ.3 จากสำนักงานโจทก์ร่วมไปไว้ที่บ้านจำเลย เพื่อทำงานให้แก่โจทก์ร่วม กับนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลในการดำเนินธุรกิจต่างๆ ของโจทก์ร่วมจากแผ่นบันทึกข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ของโจทก์ร่วม จำนวนรวม 41 แผ่น มีปัญหาวินิจฉัยตามฎีกาของโจทก์ร่วมว่า การกระทำของจำเลยเป็นความผิดตามฟ้องหรือไม่ สำหรับความผิดฐานเอาไปเสียซึ่งเอกสารในประการที่น่าจะเกิดความเสียหายแก่โจทก์ร่วมหรือผู้อื่นนั้น โจทก์ร่วมฎีกาว่า โจทก์ร่วมมีระเบียบห้ามนำเอกสารออกนอกที่ทำการ แม้จะไม่ถือเป็นข้อห้ามเด็ดขาดตามระเบียบนั้น แต่มิได้หมายความว่า เมื่อพนักงานนำงานออกจากที่ทำการของโจทก์ร่วมไปทำต่อที่บ้านแล้ว พนักงานไม่จำต้องนำเอกสารที่เหลือหรือมิได้

---

[83] ข้อเท็จจริงของคดีนี้เกิดขึ้นก่อนที่จะมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ใช้งานแล้วมาคืนโจทก์ร่วม การที่จำเลยทำงานเสร็จแล้วกลับไม่นำเอกสารที่เกี่ยวข้องมาคืนเพื่อส่งคืนลูกค้า เป็นการทำให้โจทก์ร่วมเสียหายแล้ว เพราะเอกสารส่วนหนึ่งเป็นความลับของลูกค้า เห็นว่า ตามคำเบิกความของนาง จ. พนักงานโจทก์ร่วม ตำแหน่งหัวหน้าฝ่ายต่างประเทศได้ความว่า เอกสารหมาย จ.3 ซึ่งลูกค้าส่งมาให้โจทก์ร่วมนั้น ส่วนใหญ่จะเป็นข้อมูลเกี่ยวกับหนังสือรับรองของบริษัท บัญชีรายชื่อผู้ถือหุ้น งบบัญชีกำไร-ขาดทุน และสำเนาหนังสือเดินทาง เอกสารดังกล่าวจึงล้วนเป็นเอกสารที่บุคคลสามารถไปขอตรวจสอบและขอคัดสำเนาได้จากกรมทะเบียนการค้ากระทรวงพาณิชย์ จึงไม่ถือเป็นความลับของบริษัทลูกค้าโจทก์ร่วมอันต้องปกปิด ดังนั้น การที่จำเลยใช้เอกสารดังกล่าวปฏิบัติในหน้าที่ให้แก่โจทก์ร่วมเสร็จแล้วไม่นำกลับคืนแก่โจทก์ร่วม จึงไม่น่าจะเป็นเหตุให้โจทก์ร่วมหรือลูกค้าของโจทก์ร่วมต้องเสียหาย การกระทำของจำเลยจึงไม่เป็นความผิดฐานเอาไปเสียซึ่งเอกสารโดยประการที่น่าจะเกิดความเสียหายแก่โจทก์ร่วมหรือผู้อื่น ศาลล่างทั้งสองวินิจฉัยปัญหานี้ชอบแล้ว ศาลฎีกาเห็นพ้องด้วย ฎีกาของโจทก์ร่วมข้อนี้ฟังไม่ขึ้น

ปัญหาวินิจฉัยตามฎีกาของโจทก์ร่วม การที่จำเลยนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลจากแผ่นบันทึกข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ของโจทก์ร่วม เป็นความผิดฐานลักทรัพย์หรือไม่ โจทก์ร่วมฎีกาว่าข้อมูลในเครื่องคอมพิวเตอร์ของโจทก์ร่วมมีรูปร่างเป็นตัวอักษร ภาพ แผนผัง และตราสาร จึงเป็นทรัพย์ตาม ป.พ.พ. มาตรา 137 การที่จำเลยเอาข้อมูลของโจทก์ร่วมดังกล่าวไป จึงเป็นความผิดฐานลักทรัพย์ เห็นว่า ข้อมูล ตามพจนานุกรมให้ความหมายว่า "ข้อเท็จจริง หรือสิ่งที่ ถือหรือยอมรับว่าเป็นข้อเท็จจริง สำหรับใช้เป็นหลักอนุมานหาความจริงหรือการคำนวณ" ส่วนข้อเท็จจริง หมายความว่า "ข้อความแห่งเหตุการณ์ที่เป็นมาหรือที่เป็นอยู่ตามจริง ข้อความหรือเหตุการณ์ที่จะต้องวินิจฉัยว่าเท็จหรือจริง" ดังนั้น ข้อมูลจึงไม่นับเป็นวัตถุมีรูปร่าง สำหรับตัวอักษร ภาพ แผนผัง และตราสาร เป็นเพียงสัญญลักษณ์ที่ถ่ายทอดความหมายของข้อมูลออกจากแผ่นบันทึกข้อมูลโดยอาศัยเครื่องคอมพิวเตอร์ มิใช่รูปร่างของข้อมูล เมื่อ ป.พ.พ. มาตรา 137 บัญญัติว่า ทรัพย์ หมายความว่า วัตถุมีรูปร่าง ข้อมูลในแผ่นบันทึกข้อมูลจึงไม่ถือเป็นทรัพย์ การที่จำเลยนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลจากแผ่นบันทึกข้อมูลของโจทก์ร่วม จึงไม่เป็นความผิดฐานลักทรัพย์ตามฟ้อง ศาลล่างทั้งสองพิพากษายกฟ้อง ศาลฎีกาเห็นพ้องด้วย ฎีกาของโจทก์ร่วมทุกข้อฟังไม่ขึ้น

ข้อสังเกต

จากคำวินิจฉัยของคำพิพากษาศาลฎีกาข้างต้น ชี้ให้เห็นถึงปัญหาช่องว่างในทางกฎหมายอาญาที่สำคัญ ซึ่งไม่มีกฎหมายที่มีความผิดและโทษทางอาญาใดจะนำมาปรับบังคับใช้แก่การกระทำของจำเลย ที่นำแผ่นบันทึกข้อมูลเปล่าคัดลอกหรือสำเนาข้อมูลคอมพิวเตอร์ของผู้เสียหายไป อันเป็นการกระทำที่สร้างความเสียหายอย่างรุนแรงได้ นอกจากนี้ ยังส่งผลกระทบต่อประเด็นปัญหาข้อกฎหมายหลายประเด็นในหลายมาตราและกระทบต่อกฎหมายหลายฉบับ โดยผู้เขียนจะยกตัวอย่างผลกระทบต่อบทบัญญัติของประมวลกฎหมายอาญา ดังนี้

ผลแห่งการวินิจฉัยของศาลฎีกาที่ว่า “ข้อมูลคอมพิวเตอร์” ไม่ได้อยู่ในความหมายของคำว่า “ทรัพย์” ซึ่งผู้เขียนเห็นพ้องด้วยกับศาลฎีกา กล่าวคือ ข้อมูลคอมพิวเตอร์ไม่ใช่วัตถุที่มีรูปร่างอันอาจมีรูปร่างโดยตัวของมันเองหรือโดยอาศัยสิ่งอื่นเป็นรูปร่าง[84] อีกทั้งลักษณะแห่งการกระทำเป็นเพียง **การแบ่ง : Share** ข้อมูลคอมพิวเตอร์ **มิใช่เอาไปในลักษณะที่พรากการครอบครองข้อมูลคอมพิวเตอร์ ไปเสียทีเดียว** ข้อมูลคอมพิวเตอร์ก็ยังคงอยู่กับฮาร์ดดีสก์หรือแผ่นบันทึกข้อมูลของเจ้าของข้อมูลคอมพิวเตอร์ เมื่อข้อมูลคอมพิวเตอร์มิได้อยู่ในความหมายของคำว่าทรัพย์และการกระทำก็ไม่อยู่ในความหมายที่จะพรากไปได้ การกระทำของจำเลยจึงไม่เป็นความผิดฐานลักทรัพย์

อีกทั้ง ผลกระทบจากความที่ข้อมูลคอมพิวเตอร์มิใช่ทรัพย์ ตามความหมายของความผิดฐานลักทรัพย์แห่งประมวลกฎหมายอาญาแล้ว หากมีการกระทำใดๆ อื่นต่อข้อมูลคอมพิวเตอร์ก็อาจไม่มีความผิดทางอาญาไปด้วย เช่น ความผิดฐานทำให้เสียทรัพย์ ตามมาตรา 358 แห่งประมวลกฎหมายอาญา ผู้ที่ทำลาย ทำให้เสียหายฯ ต่อข้อมูลคอมพิวเตอร์ก็ย่อมไม่อาจเป็นความผิดฐานทำให้เสียทรัพย์ได้ หรือความผิดฐานรับของโจร หรือความผิดตามมาตรา 357 แห่งประมวลกฎหมายอาญา หากการที่มีผู้ลักลอบสำเนาข้อมูลคอมพิวเตอร์ไปอย่างข้อเท็จจริงตามคำพิพากษาศาลฎีกาดังกล่าวแล้วผู้ลักลอบสำเนาข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์นั้นให้แก่ผู้อื่น ผู้อื่นที่รับเอาสำเนาข้อมูลคอมพิวเตอร์ไปย่อมไม่มีความผิดฐานรับของโจรเช่นเดียว เนื่องจากเมื่อการกระทำสำเนาข้อมูลคอมพิวเตอร์ไม่เป็นความผิดฐานลักทรัพย์เสียแล้ว ผู้รับข้อมูลคอมพิวเตอร์ไปก็ไม่ใช่รับของร้ายอันได้จากการกระทำความผิดฐานลักทรัพย์ เป็นต้น

นอกจากนี้ ข้อมูลคอมพิวเตอร์ เมื่อวิเคราะห์ตามบทบัญญัติมาตรา 1 (7) ที่ให้นิยามความหมาย ของคำว่า “เอกสาร” โดยบัญญัติไว้ว่า *"เอกสาร" หมายความว่า กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่นจะเป็นโดยวิธีพิมพ์ถ่ายภาพหรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น*

จากความหมายของบทนิยามดังกล่าว ข้อมูลคอมพิวเตอร์ก็มิได้ประจักษ์แก่สายตาในลักษณะที่สามารถสื่อความหมายได้ในตัวเอง ซึ่งหากจะสื่อความหมายต้องผ่านขั้นตอนกระบวนการแปลงข้อมูลคอมพิวเตอร์ด้วยเครื่องและอุปกรณ์ประมวลผลทางคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ที่ปรากฏบนหน้าจอมอนิเตอร์ยังไม่ได้มีรูปลักษณ์ที่คงทนถาวรเพียงพอใช้เป็นพยานหลักฐานในรูปเอกสารได้[85] เมื่อปิดเครื่องคอมพิวเตอร์ข้อมูลบนจอมอนิเตอร์ก็หายไป ส่วนข้อมูลคอมพิวเตอร์ที่บน

---

[84] จิตติ ติงศภัทิย์, *กฎหมายอาญา ภาค 2 ตอน 2 และภาค 3* พิมพ์ครั้งที่ 3 กรุงเทพมหานคร:เนติบัณฑิตยสภา 2532, หน้า 2473-2477

[85] ข้อมูลคอมพิวเตอร์ไม่ใช่เอกสารหรือพยานเอกสาร แต่อยู่ในความหมายของพยานวัตถุ ตามคำพิพากษาฎีกาที่ 5161/2547 แต่เป็นเอกสารตามคำพิพากษาฎีกาที่ 4311/2557 (ผู้วิจัย)

ฮาร์ดดิสก์ก็ไม่อาจสื่อความหมายอย่างที่บุคคลทั่วไปสามารถอ่านหรือเข้าใจได้ ดังนั้น ข้อมูลคอมพิวเตอร์จึงไม่ใช่เอกสารตามความหมายของมาตรา 1 (7) เช่นนี้ หากมีผู้ทำให้เสียหาย ทำลาย ซ่อนเร้น เอาไปเสีย ทำให้สูญหาย หรือไร้ประโยชน์แก่ข้อมูลคอมพิวเตอร์ก็ย่อมไม่ครบองค์ประกอบของความผิดตาม มาตรา 188 แห่งประมวลกฎหมายอาญาไปได้ อีกทั้งการกระทำที่ก่อให้เกิดความเสียหายแก่ข้อมูลคอมพิวเตอร์ เช่น การทำปลอม การทำแปลง การทำเท็จ เกี่ยวกับเอกสาร จึงไม่อาจปรับบทความผิดเกี่ยวกับเอกสารแก่ผู้กระทำได้

1.2 คดีตามคำพิพากษาฎีกาที่ 4311/2557 ต่อมามีคดีเกี่ยวแก่ข้อมูลคอมพิวเตอร์ขึ้นสู่ศาลฎีกาอีกหนึ่งคดี ซึ่งศาลฎีกาวินิจฉัยว่า "ข้อมูลคอมพิวเตอร์เป็นเอกสาร"

คำพิพากษาฎีกาที่ 4311/2557 วินิจฉัยว่า การที่จำเลยที่ 1 ถึงที่ 3 ร่วมกันพิมพ์หนังสือแต่งตั้งตัวแทนจำหน่ายอุปกรณ์กันระเบิด แบรนด์ บาร์เทค พร้อมรายละเอียดลงในเครื่องคอมพิวเตอร์ ถือเป็นการใช้เครื่องคอมพิวเตอร์ซึ่งเป็นวัตถุอื่นใดทำให้ปรากฏความหมาย ซึ่งสามารถอ่านหรือสื่อความหมายได้ โดยบุคคลที่พิมพ์ตัวอักษรนั้น แล้วเก็บไว้ในเครื่องคอมพิวเตอร์ดังกล่าว เพื่อเป็นหลักฐาน ซึ่งจำเลยที่ 1 ถึงที่ 3 สามารถนำไปใช้ได้เมื่อต้องการจะใช้ จึงเป็นเอกสาร[86] ตามความหมายของบทบัญญัติดังกล่าวแล้ว

แต่อย่างไรก็ตาม ประมวลกฎหมายอาญา มาตรา 1 (9) ได้นิยามความหมายของคำว่า “เอกสารสิทธิ” หมายความว่า เอกสารที่เป็นหลักฐานแห่งการก่อ เปลี่ยนแปลง โอน สงวนหรือระงับซึ่งสิทธิ เมื่อหนังสือแต่งตั้งตัวแทนจำหน่ายอุปกรณ์กันระเบิดมีข้อความว่า ผู้เสียหายตกลงให้จำเลยที่ 1 เป็นตัวแทนในการจำหน่ายอุปกรณ์กันระเบิดดังกล่าว พร้อมระบุเงื่อนไขในการสั่งซื้อ ราคาขายและส่วนลด เงื่อนไข ในการชำระเงิน การส่งเสริมการขายและเงื่อนไขที่ทำให้ตัวแทนจำหน่ายสิ้นสุดลง หนังสือดังกล่าว จึง เป็นเพียงเอกสารที่ผู้เสียหายมอบอำนาจให้จำเลยที่ 1 มีอำนาจทำนิติกรรมแทนผู้เสียหายเท่านั้น ไม่เป็นเอกสารอันเป็นหลักฐานแห่งการก่อตั้งสิทธิ จึงไม่ใช่เอกสารสิทธิตามประมวลกฎหมายอาญา มาตรา 1 (9) จำเลยที่ 3 จึงไม่มีความผิดตามประมวลกฎหมายอาญา มาตรา 265 คงมีความผิดตามมาตรา 264 เท่านั้น

จากคำพิพากษาฎีกาฉบับนี้ นักกฎหมายผู้ใหญ่ ศาสตราจารย์ ดร.เกียรติขจร วัจนะสวัสดิ์ ได้ให้ความเห็นไว้ดังนี้[87]

---

[86] ประมวลกฎหมายอาญา มาตรา 1 (7) ได้นิยามความหมายของคำว่าเอกสาร หมายความว่า *กระดาษหรือวัตถุอื่นใด ซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผังหรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพหรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น*

[87] เกียรติขจร วัจนะสวัสดิ์, ศาสตราจารย์พิเศษ ดร. *คำบรรยายเนติบัณฑิต* เล่ม 4, หน้า 290 บรรยายวันที่ 17 มิถุนายน 2559

“ข้อสังเกต จากคำพิพากษาฎีกานี้คือ เครื่องคอมพิวเตอร์ที่มีข้อมูลปรากฏความหมาย ทำให้เครื่องนั้นเป็นเอกสารตามนิยามของมาตรา 1(7) ไม่ต่างไปจากกระดาษ ดังนั้น การทำลายข้อมูลในเครื่องคอมพิวเตอร์ของผู้อื่นก็เป็นความผิดตามมาตรา 188 และการปลอมข้อมูลในเครื่องคอมพิวเตอร์ก็เป็นความผิดฐานปลอมเอกสาร ตามบรรทัดฐานของฎีกานี้ ดังนั้น หากจำเลยพิมพ์ข้อความ และลงลายมือชื่อปลอมลงในกระดาษก็ทำให้กระดาษเป็นเอกสาร เมื่อพิมพ์ดังกล่าวลงในเครื่องคอมพิวเตอร์ ก็ทำให้เครื่องคอมพิวเตอร์นั้นเป็นเอกสารเช่นเดียวกัน”

ข้อสังเกต

ประการแรก จาก **คำพิพากษาฎีกาที่ 4311/2557** ซึ่งวินิฉัยไว้ว่า ข้อมูลคอมพิวเตอร์เป็นเอกสาร ตามประมวลกฎหมายอาญา มาตรา 1 (7) นั้น ด้วยความเคารพ เมื่อวิเคราะห์บทนิยามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 *“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย* กับลักษณะเฉพาะของข้อมูลคอมพิวเตอร์จะเป็นสัญลักษณ์ที่ปรากฏบนฮาร์ดดิสก์ หรืออุปกรณ์อื่น เช่น ทรัมไดร์ฟ แผ่นซีดี แผ่นดีวีดี เป็นต้น ซึ่งสัญลักษณ์เหล่านั้นไม่ประจักษ์แก่สายตา และไม่มีสภาพเป็นภาษา หรือตัวอักษร หรือสัญลักษณ์ที่คนทั่วไปสามารถเข้าใจ หรืออ่านได้ หรือสื่อความหมายได้ แต่อย่างใด

หากแต่ที่ปรากฏเป็นภาษาอันสื่อความหมายได้ เกิดจากการประมวลผลของอุปกรณ์อิเล็กทรอนิกส์ หรือเครื่องคอมพิวเตอร์แปลงสัญลักษณ์เหล่านั้นให้ปรากฏขึ้นบนจอมอนิเตอร์อีกชั้นหนึ่ง และเมื่อปิดเครื่องคอมพิวเตอร์ ข้อความที่สื่อความหมายได้ก็จะหายไป กลับไปเป็นสัญลักษณ์บนฮาร์ดดิสก์ ทรัมไดร์ฟ แผ่นซีดี แผ่นดีวีดี ซึ่งไม่ประจักษ์แก่สายตาและบุคคลทั่วไปไม่สามารถเข้าใจหรืออ่านได้ หรือสื่อความหมายได้

ด้วยบทนิยามของ “ข้อมูลคอมพิวเตอร์” และสภาพข้อเท็จจริงของ “ข้อมูลคอมพิวเตอร์” จึงไม่สามารถเป็นเอกสารตามความหมายของประมวลกฎหมายอาญา มาตรา 1 (7)

ดังนั้น การเปลี่ยนแปลง แก้ไข “ข้อมูลคอมพิวเตอร์” จึงไม่สามารถครบองค์ประกอบความผิดฐานปลอมเอกสาร ตามประมวลกฎหมายอาญา มาตรา 264 อีกทั้งไม่สามารถเป็นความผิดฐานทำให้เสียหายซึ่งเอกสาร ตามประมวลกฎหมายอาญา มาตรา 188 ได้เช่นเดียวกัน

ประการที่สอง แม้คำพิพากษาศาลฎีกาที่ 4311/2557 จะวินิจฉัยไว้ว่า ข้อมูลคอมพิวเตอร์เป็นเอกสารก็เพียงส่งผลให้การกระทำที่ทำให้ข้อมูลคอมพิวเตอร์เสียหาย หรือถูกแก้ไขเปลี่ยนแปลงในลักษณะการปลอม ตามประมวลกฎหมายอาญา มาตรา 188 กับมาตรา 264 ตามลำดับเท่านั้น

แต่ไม่ทำให้ช่องว่างแห่งกฎหมายอาญาที่ไม่สามารถคุ้มครองข้อมูลคอมพิวเตอร์ได้รับการแก้ไขปัญหาจากกรณีการโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ลงได้ ไม่ว่าลักษณะแห่งการกระทำโจรกรรม หรือสำเนาข้อมูลคอมพิวเตอร์จะกระทำโดยรูปแบบเจาะระบบ หรือที่เรียกกันว่าแฮ็ก (hack) หรือรูปแบบโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไป โดยเข้าถึงระบบคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ หรือรูปแบบโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยวิธีสามัญก็ตาม ซึ่งตามคำพิพากษาฎีกาที่ 5161/2547 ก็ได้วินิจฉัยไว้ว่าการกระทำ “เอาไป” ตามประมวลกฎหมายอาญา มาตรา 334 ฐานลักทรัพย์ ต้องมีการพรากทรัพย์ไป แต่การโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยไม่มีสิทธิ ไม่ได้มีการพรากข้อมูลคอมพิวเตอร์ไป แต่หากข้อมูลคอมพิวเตอร์ก็ยังคงอยู่กับผู้ทรงสิทธิดังเดิม เพียงมีการคัดลอกข้อมูลคอมพิวเตอร์ หรือจดจำไปเท่านั้น ดังที่ศาลฎีกาได้วินิจฉัยไว้ตาม คำพิพากษาฎีกาที่ 5161/2547 “ข้อมูลคอมพิวเตอร์” ไม่ได้อยู่ในความหมายของคำว่า “ทรัพย์” ซึ่งผู้เขียนเห็นพ้องด้วยกับศาลฎีกา กล่าวคือ ข้อมูลคอมพิวเตอร์ไม่ใช่วัตถุที่มีรูปร่างอันอาจมีรูปร่างโดยตัวข้อมูลคอมพิวเตอร์เองหรือโดยอาศัยสิ่งอื่นเป็นรูปร่าง[88] อีกทั้งลักษณะแห่งการกระทำเป็นเพียง **การแบ่ง : Share** ข้อมูลคอมพิวเตอร์ **มิใช่เอาไปในลักษณะที่พรากการครอบครองข้อมูลคอมพิวเตอร์ไปเสียทีเดียว** ข้อมูลคอมพิวเตอร์ก็ยังคงอยู่บนฮาร์ดดีสก์หรือแผ่นบันทึกข้อมูลของเจ้าของข้อมูลคอมพิวเตอร์ เมื่อข้อมูลคอมพิวเตอร์มิได้อยู่ในความหมายของคำว่าทรัพย์ และการกระทำก็ไม่ใช่การพรากทรัพย์ การกระทำของจำเลยจึงไม่เป็นความผิดฐานลักทรัพย์

เมื่อการโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยไม่มีสิทธิ **มิใช่เอาไปในลักษณะที่พรากการครอบครองข้อมูลคอมพิวเตอร์ไปเสียทีเดียว** กรณีจึงไม่อาจเป็นความผิดฐานเอาไปเสียซึ่งเอกสาร ตามประมวลกฎหมายอาญา มาตรา 188 เช่นเดียวกัน

---

[88] จิตติ ติงศภัทิย์, *กฎหมายอาญา ภาค 2 ตอน 2 และภาค 3* พิมพ์ครั้งที่ 3 กรุงเทพมหานคร:เนติบัณฑิตยสภาฯ 2532, หน้า 2473-2477

2. วิเคราะห์พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดความหมายของถ้อยคำต่างๆ เป็นบทนิยามไว้ในมาตรา 3 ความว่า

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย[89]

ส่วนฐานความผิดที่เกี่ยวข้องกับการลักลอบสำเนาข้อมูลคอมพิวเตอร์มีบัญญัติไว้สองมาตรา ดังนี้

มาตรา 5 บัญญัติว่า *"ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือนหรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ*

มาตรา 7 บัญญัติว่า *"ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ"*

ความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบนี้กล่าวได้ว่ามีที่มาจากบทบัญญัติของกฎหมายต่างประเทศที่เรียกว่าความผิดฐานเข้าถึง (access) เช่น กฎหมายของประเทศสหรัฐอเมริกา Section 1030 Title 18 of the United States Code[90] เป็นต้น

ความผิดฐาน**เข้าถึง**เป็นความผิดที่ถือว่าเป็นความผิดพื้นฐานหรือบททั่วไปของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และยังเป็นความผิดที่อาจเป็นจุดเริ่มต้นในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฐานอื่นต่อไป เช่น การเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ตามมาตรา

---

[89] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4 บัญญัติว่า..... *"ข้อมูลอิเล็กทรอนิกส์" หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร*

[90] National Criminal Justice Information and Statistics Service, Law Enforcement Assistance Administration, U.S. Department of Justice *COMPUTER CRIME:Criminal Justice Resource Manual* Washington D.C.:U.S. Government Printing Office 1979 P.145

7 หรือการดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ตามมาตรา 8 หรือการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ ตามมาตรา 9 เป็นต้น

การเข้าถึงนี้บางกรณีอาจเป็นการเข้าถึงตัวเครื่องคอมพิวเตอร์โดยตรง กล่าวคือ เครื่องคอมพิวเตอร์นั้นมีการตั้งค่ากำหนดรหัสผ่าน[91] เพื่อป้องกันมิให้บุคคลอื่นเข้าใช้เครื่องคอมพิวเตอร์ ผู้กระทำความผิดอาจดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและเข้าถึงหรือเข้าใช้เครื่องคอมพิวเตอร์นั้นๆ โดยนั่งอยู่หน้าตัวเครื่องคอมพิวเตอร์นั้นเอง หรือบางกรณีอาจเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์ โดยที่ผู้กระทำความผิดไม่ต้องเข้าถึงตัวเครื่องคอมพิวเตอร์ แต่ใช้วิธีเข้าถึงผ่านระบบอินเทอร์เน็ตเจาะหรือแฮ็กเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการก็ได้

การเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์นี้อาจเป็นลักษณะเข้าถึงทั้งหมดหรือแต่บางส่วนก็ได้ เช่นนี้ อาจเข้าถึงฮาร์ดแวร์หรืออุปกรณ์ต่อพ่วงส่วนประกอบต่างๆ ของคอมพิวเตอร์ ฮาร์ดดีสก์สำรองหรือหน่วยความจำต่างๆ ที่ต่อพ่วงกับตัวเครื่องคอมพิวเตอร์ ซึ่งบันทึกข้อมูลเก็บไว้ในระบบ เพื่อใช้สำหรับการส่งหรือโอนถึงบุคคลใดบุคคลหนึ่ง หรืออาจเข้าถึงระบบคอมพิวเตอร์เพื่อเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ เช่น หมายเลขไอพี (ip address) ก็เข้าข่ายองค์ประกอบของความผิดมาตรา 5 เช่นกัน

ส่วนช่องทางที่จะเข้าถึงนั้นอาจด้วยวิธีการต่างๆ ไม่ว่าจะเข้าถึงโดยผ่านทางเครือข่ายภายนอก หรืออาจเรียกว่าเครือข่ายสาธารณะ กล่าวคือ อินเทอร์เน็ตอันเป็นการเชื่อมโยงระหว่างเครือข่ายหลายๆ เครือข่ายเข้าด้วยกัน หรืออาจเข้าถึงโดยช่องทางผ่านระบบเครือข่ายเดียวกันหรือเครือข่ายภายในที่เรียกว่า ระบบแลน (LAN : local area network) อันเป็นเครือขายที่เชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้ๆ เข้าด้วยกัน และรวมถึงลักษณะการเข้าถึงโดยผ่านช่องทางการติดต่อสื่อสารแบบไร้สายหรือที่เรียกว่า ไวเลส (wireless) อีกด้วย

องค์ประกอบความของผิด “เข้าถึง” ต้องเป็นการเข้าถึง “โดยมิชอบ” หมายความว่าจะต้องเป็นการเข้าถึงโดยปราศจากสิทธิโดยชอบธรรม (without right) หรือปราศจากอำนาจตามกฎหมายที่จะเข้าถึง หรือไม่ได้รับความยินยอมหรือไม่ได้รับอนุญาตจากผู้ทรงสิทธิที่จะยินยอมหรืออนุญาต ในทางกลับกัน หากบุคคลที่เข้าถึงนั้นเป็นบุคคลที่มีสิทธิ ไม่ว่าด้วยถือสิทธิตามกฎหมายหรือได้รับความยินยอมหรือได้ รับอนุญาตจากเจ้าของระบบหรือผู้ทรงสิทธิ เช่น การเข้าถึงเพื่อดูแลระบบของผู้ดูแลเว็บไซต์ (webmaster) เป็นต้น ก็เป็นการเข้าถึงโดยชอบ

---

[91] รหัสผ่านนี้ คือ บัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา มาตรา 1 (14) (ข)

อนึ่ง หากบุคคลผู้ได้รับอนุญาตให้ทำการเข้าถึงนั้นได้กระทำการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์เกินกว่าที่ตนได้รับความยินยอมหรือได้รับอนุญาต เช่นนี้ ลักษณะแห่งการกระทำของบุคคลดังกล่าวก็เป็นการเข้าถึงโดยมิชอบตามความหมายนี้เช่นเดียวกัน[92]

องค์ประกอบของความผิดประการต่อมา คือ ระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึง โดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน มาตรการการเข้าถึงโดยเฉพาะ หมายความว่า ระบบคอมพิวเตอร์นั้นๆ มีการกำหนดค่ารหัสผ่านไว้ ซึ่งอาจเป็นค่ารหัสการเข้าใช้ตัวเครื่องคอมพิวเตอร์ หรือ ค่ารหัสการเข้าใช้จดหมายอิเล็กทรอนิกส์ (e-mail) ทั้งชื่อผู้ใช้ (username) และรหัสผ่าน (password) หรือชื่อผู้ใช้และรหัสผ่านเข้าใช้อินเทอร์เน็ตทั้งระบบส่งสัญญาณผ่านสื่อที่เป็นสายและระบบไวเลส (wireless) หรือรหัสผ่านเข้าใช้เกมคอมพิวเตอร์ออนไลน์ หรือรหัสบัตร เอ.ที.เอ็ม สำหรับฝาก-ถอนเงินสดอัตโนมัติที่ใช้กับตู้หรือเครื่องฝาก-ถอนเงินสดอัตโนมัติ ค่ารหัสผ่านเหล่านี้มีไว้สำหรับผู้ทรงสิทธิเท่านั้น มิใช่มีไว้เพื่อคนทั่วไปหรือเพื่อสาธารณะประโยชน์ บุคคลผู้เข้าถึงระบบคอมพิวเตอร์ที่มีการตั้งค่ารหัสผ่านเหล่านี้ก็คือเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนนั่นเอง

ส่วนความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ตามมาตรา 7 มีองค์ประกอบคล้ายกับความผิดตาม มาตรา 5 ต่างกันที่มาตรา 5 เป็นการเข้าถึงระบบคอมพิวเตอร์ แต่มาตรา 7 นี้เป็นการเข้าถึง **“ข้อมูลคอมพิวเตอร์”** ซึ่งสามารถพิจารณาความหมายของคำว่าข้อมูลคอมพิวเตอร์ได้จากบทนิยามมาตรา 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ประกอบมาตรา 4 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ที่กล่าวไว้ข้างต้น ความผิดตามมาตรา 7 นี้เพียงเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยมิชอบ แม้ยังไม่ได้เอาข้อมูลคอมพิวเตอร์ของใครไปก็เป็นความผิดแล้ว เช่น เข้าไปดูหรืออ่านจดหมายอิเล็กทรอนิกส์ของผู้อื่น เป็นต้น หรือหากเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยมิชอบ และเอาข้อมูลคอมพิวเตอร์ไปด้วยก็ย่อมเป็นความผิดฐานนี้เช่นกัน

ข้อสังเกต

1. ปัญหาช่องว่างแห่งกฎหมายอาญา กล่าวคือ ข้อเท็จจริงตามคำพิพากษาศาลฎีกาที่ 5161/2547 ในประเด็นที่จำเลยลักลอบสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นไปโดยเจ้าของข้อมูลคอมพิวเตอร์ไม่ยินยอมหรือไม่อนุญาต และศาลฎีกาต้องยกฟ้องโจทก์ เพราะเหตุที่ข้อเท็จจริงเกิดขึ้นก่อนที่จะมีการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้นบังคับใช้ จึงเป็นกรณีที่ไม่มีกฎหมายกำหนดให้การกระทำของจำเลยเป็นความผิดและมีโทษทาง

---

[92] พรเพชร วิชิตชลชัย, *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*, หน้า 9

อาญา โดยข้อเท็จจริงที่เกิดขึ้นมีลักษณะแห่งการกระทำ เจตนาของผู้กระทำ วัตถุแห่งการกระทำ และผลแห่งการกระทำของจำเลย แทบไม่ต่างจากกรณีข้อเท็จจริงที่เกิดขึ้นตามคดี R. v Gold (1988) ในประเทศอังกฤษเลย ซึ่งคดีดังกล่าว เป็นประเด็นกรณีศึกษาที่สำคัญประการหนึ่งอันส่งผลให้ประเทศอังกฤษต้องตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ขึ้นเพื่ออุดช่องว่างแห่งกฎหมายอาญาดังกล่าวแล้วข้างต้น

ข้อแตกต่างหากจะมีก็เป็นเพียงข้อแตกต่างของสองคดีที่มีอยู่เป็นเรื่องที่ไม่ส่งผลให้มีความแตกต่างต่อประเด็นข้อกฎหมาย อันก่อให้เกิดช่องว่างแห่งกฎหมายอาญา หากข้อแตกต่างเป็นเรื่องเกี่ยวกับข้อมูลคอมพิวเตอร์ที่เป็นข้อมูลการดำเนินธุรกิจต่างๆ ของผู้อื่น และข้อหาที่ถูกดำเนินคดีความผิดฐานลักทรัพย์ ในคดีคำพิพากษาฎีกาที่ 5161/2547 กับข้อมูลคอมพิวเตอร์ที่เป็นรหัสผ่าน (password) และข้อหาที่ถูกดำเนินคดีความผิดฐานปลอมแปลงเอกสารแห่งพระราชบัญญัติความผิดเกี่ยวกับการปลอมแปลง ค.ศ. 1981 (Forgery and Counterfeiting Act 1981) มาตรา 1 ตามคดี R. v Gold (1988) ที่เกิดในประเทศอังกฤษ ซึ่งคดีทั้งสองต่างก็ส่งผลให้เกิดปัญหาช่องว่างแห่งกฎหมายอาญา

2. วิเคราะห์ปรับบทกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จากบทบัญญัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่กล่าวมานี้ เมื่อวิเคราะห์ปรับบทกับข้อเท็จจริงตามคำพิพากษาฎีกาที่ 5161/2547 ก็ยังไม่อาจวินิจฉัยได้ว่าจำเลยในคดีนี้จะมีความผิดตามมาตรา 5 กับมาตรา 7 หรือไม่ เพราะข้อเท็จจริงไม่ปรากฏว่าระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่จำเลยลักลอบสำเนาไปนั้นมีมาตรการป้องกันการเข้าถึงหรือไม่ หากระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์นั้นไม่มีมาตรการป้องกันการเข้าถึง การกระทำลักลอบสำเนาข้อมูลคอมพิวเตอร์ของจำเลยก็ไม่ครบองค์ประกอบของกฎหมาย จำเลยย่อมไม่มีความผิด[93]

3. ประเด็นวัตถุแห่งการกระทำ เมื่อพิจารณาองค์ประกอบความผิดของบทบัญญัติ ตามมาตรา 5 กับมาตรา 7 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะเห็นได้ว่า บทบัญญัติของกฎหมายมุ่งไปที่ลักษณะแห่งการกระทำ คือ “การเข้าถึง” (access)

---

[93] อย่างไรก็ตาม ตามร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ..... มาตรา 15 ได้ปิดช่องว่างของฐานความผิดตามมาตรา 5 และมาตรา 7 นี้ โดยไม่ว่าจะเป็นการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงหรือไม่ก็เป็นความผิด ซึ่งมาตรา 15 ตามร่างฯ บัญญัติว่า *“ผู้ใดเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ*

ถ้าการกระทำความผิดตามวรรคหนึ่ง ได้กระทำต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ”

หาใช่บทบัญญัติที่มุ่งจะคุ้มครองวัตถุแห่งการกระทำที่เป็นข้อมูลคอมพิวเตอร์ ซึ่งปัจจุบันข้อมูลสำคัญต่างๆ จำนวนมากอยู่ในรูป หรือถูกเก็บรักษาไว้ในลักษณะของข้อมูลคอมพิวเตอร์ เช่น ชื่อผู้ใช้ (username) รหัสผ่าน (password) รหัสโทรศัพท์ (pincode) รหัสการจองตั๋วเครื่องบิน (booking number) ข้อมูลประวัติส่วนบุคคล ข้อมูลทางการค้าของเอกชน ข้อมูลของทางราชการ ข้อมูลจราจรคอมพิวเตอร์ ข้อมูลทางการเงินของบุคคลและของสถาบันทางการเงิน ข้อมูลเกี่ยวกับการติดต่อสื่อสารผ่านจดหมายอิเล็กทรอนิกส์ เป็นต้น ซึ่งข้อมูลคอมพิวเตอร์ต่างๆ เหล่านี้ล้วนไม่มีบทบัญญัติของกฎหมายที่มีความผิดและโทษทางอาญาใดกำหนดให้เป็นวัตถุแห่งการกระทำที่ได้รับความคุ้มครอง

3. วิเคราะห์ความผิดฐานสำเนาข้อมูลคอมพิวเตอร์

สำหรับบทบัญญัติของร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... มาตรา 16 ความผิดฐานสำเนาข้อมูลคอมพิวเตอร์ ผู้เขียนมีข้อความเห็นแยกเป็นสี่กรณี ดังต่อไปนี้

3.1 ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... มาตรา 16 กับบทบัญญัติของกฎหมายประเทศอังกฤษและประเทศสหรัฐอเมริกา

องค์ประกอบของความผิดตามร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... มาตรา 16[94] เมื่อวิเคราะห์เปรียบเทียบกับรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) มาตรา 1030 (a) ของประเทศสหรัฐอเมริกา กับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) มาตรา 2 และมาตรา 3 ของประเทศอังกฤษ ผู้เขียนมีข้อความเห็นดังต่อไปนี้

ประการแรก มาตรา 16 ตามร่างฯ ที่มีวัตถุประสงค์คุ้มครองตัวข้อมูลคอมพิวเตอร์มีความแตกต่างกับฐานความผิดตามมาตรา 2 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) กล่าวคือ มาตรา 2 มีลักษณะที่มุ่งคุ้มครองการบุกรุกเป็นด้านหลัก หากเปรียบกับฐานความผิดตามประมวลกฎหมายอาญาจะมีความมุ่งหมายลักษณะคล้ายคลึงกับความผิดฐานบุกรุก อันเป็นฐานความผิดทำนองเดียวกับมาตรา 15 ตามร่างฯ หรือตามมาตรา 5 และ มาตรา 7 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ฉบับปัจจุบัน

---

[94] เสนอโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ส่วนความผิดฐานทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ตามมาตรา 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) มีลักษณะที่คุ้มครองตัวข้อมูลคอมพิวเตอร์ในลักษณะการกระทำที่ก่อให้เกิดความเสียหาย หากเปรียบกับฐานความผิดตามประมวลกฎหมายอาญาก็ทำนองความผิดฐานทำให้เสียทรัพย์ อย่างไรก็ตาม **ศาลยุติธรรมของประเทศอังกฤษ "ตีความ" มาตรา 3 นี้ครอบคลุมไปถึงลักษณะแห่งการกระทำลักลอบสำเนาข้อมูลคอมพิวเตอร์ไปด้วย** ดังในคดี R v Strickland, R v Woods [21 พฤษภาคม 1993] ที่จำเลยแฮ็กเข้าไปลักลอบสำเนาข้อมูลคอมพิวเตอร์เกี่ยวกับโทรศัพท์เคลื่อนที่ไปให้มีความผิดตามมาตรา 3 ซึ่งความผิดฐานทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ในมาตรา 9 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550[95] รวมถึงมาตราอื่นๆ ครอบคลุมไปไม่ถึงการลักลอบสำเนาข้อมูลคอมพิวเตอร์ตามฐานความผิดใหม่ของร่างฯ มาตรา 16

ประการที่สอง รัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) มาตรา 1030 (a) โดยเฉพาะอนุมาตราย่อย 1 และ 2 กำหนดถึงองค์ประกอบของความผิดที่เป็นการเข้าถึงและได้รับไปซึ่งข้อมูลคอมพิวเตอร์ไม่ว่าจะเป็นข้อมูลคอมพิวเตอร์ที่เกี่ยวกับความมั่นคงแห่งรัฐ หรือข้อมูลของหน่วยงานใดของรัฐ หรือข้อมูลของสถาบันการเงิน หรือจะเป็นข้อมูลส่วนบุคคลของเอกชนก็ตาม ทั้งนี้เห็นได้ว่ากฎหมายมาตราดังกล่าวมีวัตถุประสงค์คุ้มครองที่ตัวข้อมูลคอมพิวเตอร์ และที่น่าสังเกตคือการได้รับไป ไม่ว่าจะเป็นการได้ไปหรือแฮ็กหรือลักลอบสำเนา โดยบุคคลภายในองค์กรเองหรือจากบุคคลภายนอกองค์กรก็ตาม อีกทั้งองค์ประกอบได้รับไปนี้มีความหมายรวมไปถึงบุคคลอื่นที่แม้ไม่ได้เป็นผู้แฮ็กหรือลักลอบสำเนา เพียงได้รับจากผู้แฮ็กหรือผู้ลักลอบสำเนาต่อๆ มา ก็ถือเป็นความผิดตามอนุมาตราย่อยทั้งสอง ลักษณะองค์ประกอบของความผิดหากพิจารณาไปถึงประมวลกฎหมายอาญาก็อาจเปรียบกับความผิดฐานรับของโจร ซึ่งอนุมาตราย่อยทั้งสอง ครอบคลุมถึงด้วย ดังกรณีศึกษาจากคำพิพากษาของศาลยุติธรรมสหรัฐอเมริกาในคดี United States v. Dimetriace Eva Lavon John (08-10459 No.) 2010 กับคดี United States v. Batti (09-2050 No.) 2011

เมื่อวิเคราะห์บทบัญญัติของมาตรา 16 ตามร่างฯ แล้ว จะพบว่าองค์ประกอบของความผิดกำหนดให้เป็นความผิดเฉพาะผู้กระทำการสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบเท่านั้น ฐานความผิดมิได้ครอบคลุมไปถึงบุคคลอื่นที่ได้รับข้อมูลคอมพิวเตอร์อันได้จากการกระทำผิด และเมื่อพิจารณาตลอดร่างฯ ทั้งฉบับ รวมไปถึงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ก็ไม่พบบทบัญญัติมาตราใดที่กำหนดให้ผู้รับข้อมูลคอมพิวเตอร์อันได้มาจาก

---

[95] มาตรา 9 *"ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ"*

การกระทำความผิดฐานสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ เป็นความผิด แม้กระทั่งประมวลกฎหมายอาญาก็ไม่อาจปรับบทมาตราใดแก่กรณีได้ ซึ่งหากเกิดข้อเท็จจริงดังกรณีศึกษาจากคำพิพากษาของศาลยุติธรรม ประเทศสหรัฐอเมริกาสองคดีข้างต้น ก็จะก่อให้เกิดปัญหาช่องว่างทางกฎหมายอาญาตามมาคือไม่มีกฎหมายที่มีความผิดและโทษทางอาญาจะปรับบทแก่กรณีได้

3.2 *วิเคราะห์ข้อห่วงใยที่เชื่อมโยงถึงกฎหมายลิขสิทธิ์*

บรรดาข้อห่วงใยที่สังคมออนไลน์แสดงข้อกังขาเกี่ยวกับฐานความผิด “การสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ” ที่มีการรวบรวมรายชื่อยื่นคัดค้านร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ต่อนายกรัฐมนตรี (พ.ศ.2554) โดยเนื้อหาของการคัดค้านต่อประเด็นการสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ มีเนื้อสาระดังนี้ ***“มีมาตราที่พูดถึงการสำเนาข้อมูลคอมพิวเตอร์ ระบุว่าการสำเนาข้อมูลคอมพิวเตอร์มีความผิด ในกฎหมายใช้คำว่าการสำเนาข้อมูลคอมพิวเตอร์โดยประการที่อาจจะก่อให้เกิดความเสียหาย ถือว่ามีความผิด แล้วมันแปลว่าอะไร ? ถ้าเราอ่านเราคงจะตีความว่าเป็นมาตราที่จะจัดการเรื่องลิขสิทธิ์ มีคนพูดๆ กันว่า ที่มาของมาตรานี้มาจากการผลักดันจากค่ายเพลงใหญ่ค่ายหนึ่ง”*** และ ***“ในต่างประเทศกฎหมายการป้องกันการสำเนาข้อมูลเข้มงวดแบบนี้ไหม ? กฎหมายลิขสิทธิ์ไม่ได้เขียนเข้มแบบนี้ แต่เต็มไปด้วยข้อยกเว้น เช่น หากนำไปใช้ในการสร้างสรรค์ก็ไม่มีความผิด หรือว่านำข้อมูลนี้ไปใช้กี่เปอร์เซ็นจากข้อมูลทั้งหมดก็ไม่มีความผิด แต่ว่ามาตราใน พ.ร.บ.คอมฯ นี้ มันตีขลุมมากๆ”*** [96]

ข้อกังขาข้างต้นเป็นความไม่สบายใจที่มีต่อฐานความผิดว่าด้วยการสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ตามมาตรา 16 แห่งร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ซึ่งสังคมออนไลน์มีความเห็นเสมือนหนึ่งไปในทางที่บทบัญญัติของมาตรานี้มีวัตถุประสงค์เอาผิดกับการกระทำอันเป็นการละเมิดลิขสิทธิ์ ในประเด็นนี้ผู้เขียนมีข้อความเห็นสองประการ ดังนี้

ประการแรก ข้อความเห็นว่าด้วยเจตนารมณ์ของกฎหมาย หากพิจารณาถึงวัตถุประสงค์หรือเจตนารมณ์ของกฎหมายของความผิดทั้งสอง คือ ความผิดเกี่ยวกับการกระทำอันเป็นการละเมิดลิขสิทธิ์กับความผิดเกี่ยวกับการสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ จะพบว่าเจตนารมณ์ของความผิดทั้งสองแตกต่างกัน

ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์ กฎหมายมีวัตถุประสงค์ต้องการคุ้มครองทรัพย์สินทางปัญญาในการที่บุคคลสร้างสรรค์ผลงาน ซึ่งในอีกด้านหนึ่งความผิดเกี่ยวกับการละเมิด

---

[96] เว็บไซต์หนังสือพิมพ์มติชน *http://www.matichon.co.th/mtc-flv-window.php?newsid=1303234913* สืบค้นเมื่อวันที่ 30 เมษายน 2554, อ้างใน สมศักดิ์ เธียรจรูญกุล, รายงานการวิจัยเรื่อง ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา, ทุนอุดหนุนการวิจัยจากกองทุนรัตนโกสินทร์สมโภช 200 ปี มหาวิทยาลัยสุโขทัยธรรมาธิราช, ปี 2559

ลิขสิทธิ์ต้องการส่งเสริมหรือสนับสนุนให้บุคคลสร้างสรรค์ผลงานจากความคิด สติปัญญา พัฒนาผลงาน

ส่วนความผิดเกี่ยวกับการสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ กฎหมายมีวัตถุประสงค์ หรือเจตนารมณ์ปกป้องคุ้มครองข้อมูลคอมพิวเตอร์ในลักษณะทำนองเดียวกับทรัพย์ในความผิดฐานลักทรัพย์ตามมาตรา 334 แห่งประมวลกฎหมายอาญา ซึ่งข้อมูลคอมพิวเตอร์ไม่อยู่ในความหมายของคำว่า ทรัพย์ เมื่อมีการลักลอบสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นไปโดยมิชอบ สร้างความเสียหายให้แก่เจ้าของข้อมูลคอมพิวเตอร์อย่างมากมาย แต่กฎหมายกลับไม่อาจเอาผิดและโทษทางอาญาได้ แม้แต่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ก็ไม่มีบทบัญญัติให้ความคุ้มครองข้อมูลคอมพิวเตอร์ในฐานะที่เป็นวัตถุแห่งการกระทำตามมาตรา 16 แห่งร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ได้ แต่ต้องพิจารณาองค์ประกอบความผิดเกี่ยวกับการกระทำในลักษณะการเข้าถึง (access) เท่านั้น ซึ่งจะครบองค์ประกอบของความผิดหรือไม่ยังต้องวิเคราะห์ข้อเท็จจริงเป็นกรณีๆ ไป อันต่างจากกฎหมายของประเทศสหรัฐอเมริกาดังกล่าวมาแล้วที่คุ้มครองตัวข้อมูลคอมพิวเตอร์โดยตรง เช่นนี้ ปัญหาประเด็นข้อกฎหมายก็จะเกิดขึ้นและมีอยู่ดังคำพิพากษาฎีกาที่ 5161/2547 และในคดี R. v Gold (1988) ที่เกิดในประเทศอังกฤษ ส่งผลให้เกิดเป็นช่องว่างทางกฎหมายอาญาช่องใหญ่มาก ซึ่งไม่มีกฎหมายที่มีความผิดและโทษทางอาญาคุ้มครองตัวข้อมูลคอมพิวเตอร์โดยตรง

ประการที่สอง กรณีกรรมเดียวผิดกฎหมายหลายบท สำหรับข้อห่วงใยของสังคมออนไลน์ที่มีต่อฐานความผิดว่าด้วยการสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต่อความผิดทางอาญาฐานละเมิดลิขสิทธิ์ ก็หาได้ไม่มีความเกี่ยวข้องหรือไม่มีความเชื่อมโยงระหว่างสองฐานความผิดแต่อย่างใดไม่ แม้ว่าสองฐานความผิดจะมีเจตนารมณ์แห่งกฎหมายที่แตกต่างกัน ในข้อเท็จจริงกลับพบว่า**ในบางกรณี**การกระทำหรือข้อเท็จจริงหนึ่งๆ สามารถเป็นความผิดครบองค์ประกอบของกฎหมายได้ทั้งสองฐานความผิด เช่น การสำเนาข้อมูลคอมพิวเตอร์ที่มีลิขสิทธิ์เพลง ลิขสิทธิ์ภาพยนต์ หรือข้อมูลคอมพิวเตอร์ที่มีลิขสิทธิ์อื่นๆ โดยเจ้าของไม่ยินยอมหรือไม่อนุญาต ย่อมเป็นความผิดทั้งฐานการสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบและฐานละเมิดลิขสิทธิ์ อันเป็นกรรมเดียวผิดต่อกฎหมายหลายบทตามมาตรา 90 ของประมวลกฎหมายอาญา

หากแต่ในอีกหลายกรณีการลักลอบสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบจะไม่เป็นความผิดฐานละเมิดลิขสิทธิ์ เช่น การลักลอบสำเนาข้อมูลคอมพิวเตอร์ที่เป็นชื่อผู้ใช้ (username) รหัสผ่าน (password) หรือข้อมูลบนบัตรเครดิตหรือบัตรเดบิต ข้อมูลจากบัตรประจำตัวประชาชนรุ่นใหม่ (smart card) ข้อมูลเกี่ยวกับบัตรเติมเงินโทรศัพท์เคลื่อนที่ และบัตรเงินสดต่างๆ ข้อมูลเกี่ยวกับบัญชีต่างๆ ของสถาบันการเงินหรือสายการบิน ข้อมูลทางการค้าของวิสาหกิจเอกชน ข้อมูลของทางราชการที่รวมถึงข้อมูลเกี่ยวกับความมั่นคงของรัฐ เป็นต้น ซึ่งข้อมูลคอมพิวเตอร์เหล่านี้

ไม่อยู่ภายใต้ความคุ้มครองของกฎหมายลิขสิทธิ์ เมื่อมีการลักลอบสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นไปโดยมิชอบ หากไม่มีฐานความผิดตามร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... มาตรา 16 ก็จะไม่มีกฎหมายที่กำหนดความผิดและมีโทษทางอาญาบังคับใช้แก่ผู้กระทำสำเนาหรือโจรกรรมข้อมูลคอมพิวเตอร์ ในแง่ที่กฎหมายมีเจตนารมณ์คุ้มครองตัวข้อมูลคอมพิวเตอร์โดยตรงได้เลย ซึ่งต้องไปพิจารณาความผิดเกี่ยวกับการเข้าถึง (access) ส่วนจะครบองค์ประกอบของความผิดเกี่ยวกับการเข้าถึง (access) หรือไม่ ต้องพิจารณาข้อเท็จจริงกันเป็นรายกรณีเช่นเดียวกัน

3.3 วิเคราะห์ข้อห่วงใยอื่นๆ

สังคมออนไลน์ยังตั้งข้อสังเกตต่อฐานความผิดการสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ คือ ***"การทำสำเนาคอมพิวเตอร์ อาจหมายถึงการคัดลอกไฟล์ การดาวน์โหลดไฟล์จากเว็บไซต์ต่างๆ มาตรานี้อาจมีไว้ใช้เอาผิดกรณีการละเมิดลิขสิทธิ์ภาพยนตร์หรือเพลง แต่แนวทางการเขียนเช่นนี้อาจกระทบไปถึงการแบ็กอัพข้อมูล การเข้าเว็บแล้วเบราว์เซอร์ดาวน์โหลดมาพักไว้ในเครื่องโดยอัตโนมัติ หรือที่เรียกว่า "แคช" (cache เป็นเทคนิคที่ช่วยให้เรียกดูข้อมูลได้รวดเร็วขึ้น โดยเก็บข้อมูลที่เคยเรียกดูแล้วไว้ในเครื่อง เพื่อให้การดูครั้งต่อไปไม่ต้องโหลดซ้ำ) ซึ่งผู้ใช้อาจมิได้มีเจตนาหรือกระทั่งรับรู้ว่ามีกระทำการดังกล่าว"***[97] และการตั้งข้อสังเกตต่อองค์ประกอบของกฎหมาย**โดยประการที่น่าจะเกิดความเสียหายต่อผู้อื่น**ตรงถ้อยคำว่า ***"น่าจะ"*** [98] ซึ่งข้อกังวลข้างต้นอาจแยกออกได้สามกรณี ดังนี้

กรณีแรก การแบ็กอัพข้อมูล ลักษณะของการแบ๊กอัพเป็นการสำเนาโปรแกรมหรือข้อมูลคอมพิวเตอร์ต่างๆ เช่นนี้ การแบ็กอัพข้อมูลย่อมอยู่ในความหมายขององค์ประกอบว่าด้วยการสำเนาข้อมูลคอมพิวเตอร์ หากแต่การจะมีความผิดและโทษตามมาตรา 16 ของร่างฯ ได้จะต้องครบองค์ประกอบของกฎหมาย ลำพังเพียงการแบ๊กอัพที่เป็นการทำสำเนาข้อมูลคอมพิวเตอร์ยังไม่อาจกล่าวได้ว่ามีความผิดฐานสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ซึ่งองค์ประกอบของฐานความผิดนี้สามารถแยกออกได้ ดังนี้ องค์ประกอบภายนอก 1.ผู้ใด 2.สำเนาโดยมิชอบ 3.ข้อมูลคอมพิวเตอร์ของผู้อื่น 4.โดยประการที่น่าจะเกิดความเสียหายต่อผู้อื่น ส่วนองค์ประกอบภายใน คือ เจตนา

---

[97] เว็บไซต์ประชาชาติธุรกิจดอทเน็ต *http://www.prachachat.net/news_detai...id=no&catid=06* สืบค้นเมื่อวันที่ 30 เมษายน 2554, อ้างใน สมศักดิ์ เธียรจรูญกุล, รายงานการวิจัยเรื่อง ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา, ทุนอุดหนุนการวิจัยจากกองทุนรัตนโกสินทร์สมโภช 200 ปี มหาวิทยาลัยสุโขทัยธรรมาธิราช, ปี 2559

[98] เว็บไซต์บ้านมหาดอทคอม *http://www.baanmaha.com/community/thread40335.html* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

เมื่อพิจารณาข้อเท็จจริงการแบ๊กอัพข้อมูลคอมพิวเตอร์กับองค์ประกอบของกฎหมายแล้ว หากข้อมูลคอมพิวเตอร์เป็นข้อมูลที่ชอบด้วยกฎหมาย เช่น โปรแกรมที่มีลิขสิทธิ์หรือข้อมูลอื่นๆ ที่ชอบด้วยกฎหมาย การแบ๊กอัพโดยมีวัตถุประสงค์เพียงต้องการสำรองหรือเก็บไว้หลายๆ แห่งเพื่อป้องกันความเสียหายต่อข้อมูลซึ่งอาจเกิดขึ้นได้ ก็จะเป็นการแบ๊กอัพหรือสำเนาข้อมูลคอมพิวเตอร์ที่ไม่อยู่ในความหมายของการสำเนาโดยมิชอบ หรือนัยกลับกันย่อมเป็นการสำเนาข้อมูลคอมพิวเตอร์โดยชอบด้วยกฎหมาย ผู้สำเนาหรือแบ๊กอัพก็ไม่มีความผิดฐานสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

กรณีที่สอง การเข้าเว็บแล้วเบราว์เซอร์ดาวน์โหลดมาพักไว้ในเครื่องโดยอัตโนมัติหรือที่เรียกว่า "แคช" (cache) ดังข้อสังเกตที่สังคมออนไลน์ได้อธิบายเทคนิคการแคช (cache) ไว้ว่าหมายถึง เป็นเทคนิคที่ช่วยให้เรียกดูข้อมูลได้รวดเร็วขึ้น โดยเก็บข้อมูลที่เคยเรียกดูแล้วไว้ในเครื่องคอมพิวเตอร์ เพื่อให้การดูครั้งต่อไปไม่ต้องโหลดซ้ำ ลักษณะข้อเท็จจริงเช่นนี้เป็นเรื่องของเทคโนโลยีคอมพิวเตอร์ทำงานด้วยตนเอง โดยที่ผู้ใช้คอมพิวเตอร์ไม่ได้ประสงค์ต่อผลหรือไม่ได้ย่อมเล็งเห็นผลของการกระทำ และข้อเท็จจริงคือผู้ใช้งานคอมพิวเตอร์จำนวนมากไม่รู้จักเทคนิคการแคช (cache) ที่เครื่องคอมพิวเตอร์ทำงานไปด้วยตัวเครื่องเอง เช่นนี้ ผู้ใช้คอมพิวเตอร์จึงไม่ได้เป็นผู้กระทำการสำเนาข้อมูลคอมพิวเตอร์ อีกทั้งผู้ใช้คอมพิวเตอร์ไม่รู้ข้อเท็จจริงที่เกิดการแคช (cache) เช่นนั้นจึงไม่อาจกล่าวได้ว่าผู้ใช้คอมพิวเตอร์มีเจตนาทำสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ย่อมไม่อาจมีความผิดและโทษตามมาตรา 16 ของร่างฯ ได้

กรณีที่สาม ถ้อยคำ **“น่าจะ”** ตามองค์ประกอบของฐานความผิดสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่น โดยมิชอบตามร่างฯ ของมาตรา 16 “น่าจะ” เป็นเพียงพฤติการณ์ประกอบการกระทำ หาใช่องค์ประกอบภายนอกที่จะต้องเกิดขึ้นและมีอยู่แล้ว พฤติการณ์ประกอบการกระทำเช่นนี้ มีอยู่ตามฐานความผิดทางอาญาของประมวลกฎหมายอาญาหลายมาตรา มีทั้งใช้คำว่า “น่าจะ” หรือ “อาจจะ” เช่น มาตรา 264 มาตรา 137 มาตรา 220 มาตรา 269/1 เป็นต้น อันเป็นองค์ประกอบความผิดที่ปกติธรรมดาของความผิดทางอาญา

3.4 แนวทางปรับปรุงมาตรการทางกฎหมายอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์

องค์ประกอบของฐานความผิดสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ตามร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... มาตรา 16 ผู้วิจัยมีข้อความเห็นสองประการ คือ ความไม่ครอบคลุมถึงผู้เกี่ยวข้องกับการกระทำความผิดกับความไม่ชัดเจนว่ามีเจตนารมณ์เอาผิดต่อการกระทำจากภายนอกองค์กรหรือทั้งจากภายนอกและภายในองค์กร

ประการแรก กรณีองค์ประกอบของความผิดไม่ครอบคลุมถึงผู้เกี่ยวข้องกับการกระทำความผิด หมายถึง ฐานความผิดกำหนดให้เป็นความผิดเฉพาะผู้ที่ลงมือกระทำการสำเนาข้อมูลคอมพิวเตอร์ด้วยตนเอง กรณีเช่นนี้ หากเป็นผู้อื่นที่มิได้ลงมือกระทำการสำเนา

ข้อมูลคอมพิวเตอร์ด้วยตนเอง แต่ได้รับจากผู้ลงมือกระทำการสำเนาอีกทอดหนึ่งหรือทอดต่อๆ ไป[99] ฐานความผิดตามมาตรา 16 ของร่างฯ จะไม่ครอบคลุมถึง ไม่อาจเอาผิดและโทษได้ และหากจะปรับใช้บทบัญญัติของประมวลกฎหมายอาญามาตรา 357 ข้อมูลคอมพิวเตอร์ก็มิใช่ทรัพย์ที่ได้จากการกระทำความผิดฐานต่างๆ ที่ระบุไว้ในมาตรา 357 อีกทั้งไม่มีบทบัญญัติของกฎหมายที่กำหนดความผิดและโทษทางอาญาใดจะบังคับแก่กรณีได้ ผู้วิจัยเห็นว่า องค์ประกอบของฐานความผิดควรเพิ่มวรรคสองขึ้น โดยกำหนดให้ผู้ที่เจตนารับข้อมูลคอมพิวเตอร์ที่ได้จากการกระทำความผิดฐานสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบต้องมีความผิดและโทษทางอาญาด้วย

ประการที่สอง ส่วนความไม่ชัดเจนว่ามีเจตนารมณ์เอาผิดต่อการกระทำจากภายนอกองค์กร หรือทั้งจากภายนอกและภายในองค์กร หมายถึง ตามร่างฯ มาตรา 16 มีความไม่ชัดเจนเพียงพอ ซึ่งอาจเกิดปัญหาให้ต้องใช้นิติวิธีตีความกฎหมายว่าเป็นบทบัญญัติที่มีเจตนารมณ์ต้องการเอาผิดกับผู้ที่กระทำสำเนาข้อมูลคอมพิวเตอร์จากภายนอกองค์กรเท่านั้น หรือมีเจตนารมณ์ต้องการเอาผิดทั้งการกระทำสำเนาข้อมูลคอมพิวเตอร์จากภายนอกองค์กรและภายในองค์กรด้วย ซึ่งอาจก่อให้เกิดปัญหาการบังคับใช้กฎหมายดังกรณีข้อเท็จจริงที่เกิดขึ้นในประเทศอังกฤษดังคดี DPP v Bignell [1998] โดยองค์กรผู้บังคับใช้กฎหมายไม่สามารถดำเนินคดีต่อการกระทำของจำเลย เพราะเหตุว่าการกระทำนั้นไม่ได้อยู่ในความหมายของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ.1990 (Computer Misuse Act 1990) มาตรา 1 ฐานเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งศาลยุติธรรมของประเทศอังกฤษวินิจฉัยตีความว่า **“ความผิดฐานนี้มีเจตนารมณ์เพื่อใช้กับแฮ็กเกอร์ (hacker) จากภายนอกองค์กร”** ดังนั้น ศาลยุติธรรมของประเทศอังกฤษจึงพิพากษายกฟ้องจำเลย[100] ผู้วิจัยจึงเห็นว่าควรกำหนดองค์ประกอบความผิดฐานสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบให้ชัดเจนว่ามีเจตนารมณ์เอาผิดการกระทำสำเนาข้อมูลคอมพิวเตอร์ทั้งจากภายนอกและภายในองค์กรในลักษณะเดียวกับบทบัญญัติของประมวลกฎหมายประเทศสหรัฐอเมริกา ตามรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) มาตรา 1030 แห่ง (United States Code : U.S.C.) บรรพที่ 18 (Title 18) หมวด 47 (Chapter 47) ซึ่งบังคับใช้ทั้งกรณีการกระทำผิดฐานสำเนาข้อมูลคอมพิวเตอร์ที่กระทำโดยบุคคลากรภายในองค์กร[101] และกระทำความผิดสำเนาข้อมูลคอมพิวเตอร์จากภายนอกองค์กร[102] เพื่อมิให้เกิดปัญหาช่องว่างทางกฎหมายและเป็นปัญหาไปถึงองค์กรผู้บังคับใช้กฎหมาย

---

[99] ดังข้อเท็จจริงในคดี United States v. Dimetriace Eva Lavon John (08-10459 No.) 2010

[100] เว็บไซต์อาจารย์นิติศาสตร์ดอทเน็ต *http://www.lawteacher.net/criminal-law/acts/computer-misuse-act-1990.php* และเว็บไซต์หน่วยงานพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ ประเทศอังกฤษ *http://www.computer evidence.co.uk/Cases/CMA.htm* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

[101] คดี United States v. Dimetriace Eva Lavon John (08-10459 No.) 2010

[102] คดี United States v. Batti (09-2050 No.) 2011

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

จากการศึกษาวิเคราะห์ข้อมูลถึงลักษณะและประเภทของข้อมูลคอมพิวเตอร์ ในฐานะวัตถุแห่งการกระทำ กับลักษณะแห่งการกระทำโจรกรรมข้อมูลคอมพิวเตอร์ กฎหมายอาญาของประเทศไทยและต่างประเทศบางประเทศ เช่น ประเทศอังกฤษ กับประเทศสหรัฐอเมริกา ซึ่งถือว่าประเทศสหรัฐอเมริกาเป็นประเทศที่มีกฎหมายเกี่ยวกับคอมพิวเตอร์ก้าวหน้าที่สุด ผู้วิจัยมีข้อสรุปและข้อเสนอแนะมาตรการทางกฎหมายอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์ ดังนี้

1. สรุปผลการวิจัย
2. ข้อเสนอแนะ

1. สรุปผลการวิจัย

ข้อสรุปที่ได้จากการศึกษาวิจัยสามารถวิเคราะห์ตอบวัตถุประสงค์ของการศึกษาวิจัย 2 ข้อแรก ของบทที่ 1 คือ ข้อ 2.1 ศึกษาลักษณะและประเภทของข้อมูลคอมพิวเตอร์ ในฐานะวัตถุแห่งการกระทำกับลักษณะแห่งการกระทำโจรกรรมข้อมูลคอมพิวเตอร์ กับข้อ 2.2 วิเคราะห์บทบัญญัติและอุปสรรคในการบังคับใช้กฎหมายทางอาญาเกี่ยวกับการคุ้มครองข้อมูลคอมพิวเตอร์จากการกระทำโจรกรรมข้อมูลคอมพิวเตอร์ ดังนี้

1.1 ข้อค้นพบตามวัตถุประสงค์ข้อ 2.1 ศึกษาลักษณะและประเภทของข้อมูลคอมพิวเตอร์ ในฐานะวัตถุแห่งการกระทำ กับลักษณะแห่งการกระทำโจรกรรมข้อมูลคอมพิวเตอร์ ดังนี้

จากความหมายของ “ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

ส่วนบทนิยามของ “การโจรกรรมข้อมูล” ซึ่งหมายถึง ลักษณะแห่งการกระทำสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ซึ่งอาจทำโดยการเจาะระบบหรือแฮ็ก (hack) โดยมิชอบ หรือเข้าถึงข้อมูลคอมพิวเตอร์โดยชอบ แต่สำเนาไปโดยมิชอบ หรืออาจเป็นการได้ไปด้วยวิธีสามัญ เช่น เห็นหน้าจอมอนิเตอร์คอมพิวเตอร์หรือสมาร์ทโฟน และจดจำไป เป็นต้น

บทนิยามทั้งสองข้างต้น ซึ่งปรากฏตามบทที่ 1 บ่งชี้ถึงลักษณะและประเภทของข้อมูลคอมพิวเตอร์ ส่วนลักษณะแห่งการกระทำสามารถแบ่งลักษณะแห่งการกระทำเกี่ยวกับการโจรกรรมข้อมูลคอมพิวเตอร์ออกเป็น 3 รูปแบบ ดังนี้

1) เจาะระบบ หรือที่เรียกกันว่าแฮ็ก (hack) ซึ่งเป็นการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยไม่มีสิทธิ ด้วยเทคนิคทางคอมพิวเตอร์ ซึ่งผู้กระทำอยู่ห่างโดยระยะทางกับข้อมูลคอมพิวเตอร์เป้าหมาย

2) โจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยเข้าถึงระบบคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์

รูปแบบแรก เข้าถึงโดยมีสิทธิ การเข้าถึงโดยมีสิทธิ หมายถึง ผู้กระทำเอาข้อมูลคอมพิวเตอร์ไปนั้น มีรหัสผ่าน หรือได้รับอนุญาตให้เข้าถึงข้อมูลคอมพิวเตอร์ได้ แต่ไม่มีสิทธิสำเนาข้อมูลคอมพิวเตอร์ไป ซึ่งอาจเป็นกรณีมีสิทธิเข้าถึงข้อมูลคอมพิวเตอร์ เพื่อใช้ประโยชน์ภายในองค์กร แต่ไม่มีสิทธินำหรือสำเนาข้อมูลคอมพิวเตอร์ไปใช้สำหรับประโยชน์ส่วนตัวหรือประโยชน์ขององค์กรอื่น

รูปแบบที่สอง เข้าถึงโดยไม่มีสิทธิ การเข้าถึงโดยไม่มีสิทธิ หมายถึง ผู้กระทำเอาข้อมูลคอมพิวเตอร์ไปนั้น ไม่มีรหัสผ่าน หรือไม่ได้รับอนุญาตให้เข้าถึงข้อมูลคอมพิวเตอร์ได้ แต่ผู้กระทำอาจมีอุปกรณ์อิเล็กทรอนิกส์บางชนิดที่สามารถ ดักจับหรือดูดข้อมูลคอมพิวเตอร์ เช่น เครื่องสกิมเมอร์ (skimmer เครื่องดูดหรือกวาดข้อมูล) ซึ่งเป็นการเข้าถึงและโจรกรรมข้อมูลคอมพิวเตอร์ไปโดยไม่มีสิทธิเข้าถึงข้อมูลคอมพิวเตอร์อย่างรูปแบบแรก

เครื่องสกิมเมอร์ (skimmer เครื่องดูดหรือกวาดข้อมูล) เป็นอุปกรณ์ที่ผู้กระทำเพื่อให้ได้ข้อมูลคอมพิวเตอร์ไปโดยไม่มีสิทธิ มักใช้กับการสำเนาหรือโจรกรรมข้อมูลคอมพิวเตอร์ที่เกี่ยวกับบัตรเครดิต หรือบัตร เอ.ที.เอ็ม เป็นต้น

3) โจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยวิธีสามัญ มีลักษณะแห่งการกระทำเกี่ยวกับข้อมูลคอมพิวเตอร์อย่างการกระทำสามัญธรรมดา ที่กล่าวว่าสามัญธรรมดา เช่น การจดจำซึ่งอาจจดจำจากการเห็นจากหน้าจอคอมพิวเตอร์ที่ผู้อื่นกำลังใช้งานตัวเครื่องหรือระบบคอมพิวเตอร์ หรืออาจจดจำจากที่ผู้ทรงสิทธิในการเข้าถึงตัวเครื่องหรือระบบคอมพิวเตอร์ หรืออุปกรณ์การเก็บข้อมูลคอมพิวเตอร์ที่จดใส่กระดาษไว้ เป็นต้น

กรณีการโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยวิธีสามัญ เป็นการโจรกรรมหรือได้ไปที่ไม่ใช่อาชญากรรมทางเทคโนโลยี (hitech crime) ต่อเมื่อผู้ได้ไปซึ่งข้อมูลเหล่านั้นนำไปพิมพ์และนำเข้าระบบคอมพิวเตอร์ก็จะเป็นข้อมูลคอมพิวเตอร์ที่ตนเองไม่ใช่ผู้ทรงสิทธิ แต่เจ้าของหรือผู้ทรงสิทธิที่ตนไปโจรกรรมมาจึงเป็นผู้มีสิทธิโดยชอบด้วยกฎหมาย

1.2 ข้อค้นพบตามวัตถุประสงค์ข้อ 2.2 วิเคราะห์บทบัญญัติและอุปสรรคในการบังคับใช้กฎหมายทางอาญาเกี่ยวกับการคุ้มครองข้อมูลคอมพิวเตอร์จากการกระทำโจรกรรมข้อมูลคอมพิวเตอร์

จาก **คำพิพากษาฎีกาที่ 4311/2557** ซึ่งวินิฉัยไว้ว่า ข้อมูลคอมพิวเตอร์เป็นเอกสารตามประมวลกฎหมายอาญา มาตรา 1 (7) นั้น ด้วยความเคารพ เมื่อวิเคราะห์บทนิยาม ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 *“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย* กับลักษณะเฉพาะของข้อมูลคอมพิวเตอร์จะเป็นสัญลักษณ์ที่ปรากฏบนฮาร์ดดิสก์ หรืออุปกรณ์อื่น เช่น ทรัมไดร์ฟ แผ่นซีดี แผ่นดีวีดี เป็นต้น ซึ่งสัญลักษณ์เหล่านั้นไม่ประจักษ์แก่สายตา และไม่มีสภาพเป็นภาษาหรือตัวอักษร หรือสัญลักษณ์ที่คนทั่วไปเข้าใจ หรืออ่านได้ หรือสื่อความหมายได้แต่อย่างใด

หากแต่ที่ปรากฏเป็นภาษาอันสื่อความหมายได้ เกิดจากการประมวลผลของอุปกรณ์อิเล็กทรอนิกส์ หรือเครื่องคอมพิวเตอร์แปลงสัญลักษณ์เหล่านั้นให้ปรากฏขึ้นบนจอมอนิเตอร์อีกชั้นหนึ่ง และเมื่อปิดเครื่องคอมพิวเตอร์ ข้อความที่สื่อความหมายได้ก็จะหายไป กลับไปเป็นสัญลักษณ์บนฮาร์ดดิสก์ ทรัมไดร์ฟ แผ่นซีดี แผ่นดีวีดี ซึ่งไม่ประจักษ์แก่สายตา และบุคคลทั่วไปไม่สามารถเข้าใจ หรืออ่านได้ หรือสื่อความหมายได้

ด้วยบทนิยามของ “ข้อมูลคอมพิวเตอร์” และสภาพข้อเท็จจริงของ “ข้อมูลคอมพิวเตอร์” จึงไม่สามารถเป็นเอกสารตามความหมายของประมวลกฎหมายอาญา มาตรา 1 (7)

ดังนั้น การกระทำแก้ไขเปลี่ยนแปลง “ข้อมูลคอมพิวเตอร์” จึงไม่สามารถครบองค์ประกอบความผิดฐานปลอมเอกสาร ตามประมวลกฎหมายอาญา มาตรา 264 อีกทั้งไม่สามารถเป็นความผิดฐานทำให้เสียหายซึ่งเอกสาร ตามประมวลกฎหมายอาญา มาตรา 188 ได้เช่นเดียวกัน

อย่างไรก็ตาม แม้มี**คำพิพากษาศาลฎีกาที่ 4311/2557** จะวินิจฉัยไว้ว่าข้อมูลคอมพิวเตอร์เป็นเอกสาร ก็เพียงส่งผลให้การกระทำที่ทำให้ข้อมูลคอมพิวเตอร์เสียหายเป็นความผิดฐานทำให้เสียหายซึ่งเอกสารตามประมวลกฎหมายอาญา มาตรา 188 หรือกรณีถูกแก้ไขเปลี่ยนแปลงก็เป็นความผิดในลักษณะการปลอมเอกสารตามประมวลกฎหมายอาญา มาตรา 264 ตามลำดับเท่านั้น

แต่ไม่ทำให้ช่องว่างแห่งกฎหมายอาญาที่ไม่สามารถคุ้มครองข้อมูลคอมพิวเตอร์ได้รับการแก้ไขปัญหาจากกรณีการโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ลงได้ ไม่ว่าลักษณะแห่งการกระทำโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์จะกระทำโดยรูปแบบเจาะระบบ หรือที่เรียกกันว่าแฮ็ก (hack) หรือรูปแบบโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไป โดยเข้าถึงระบบคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ หรือรูปแบบโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยวิธี

สามัญก็ตาม ซึ่งตามคำพิพากษาฎีกาที่ 5161/2547 ก็ได้วินิจฉัยไว้ว่าการกระทำ “เอาไป” ตามประมวลกฎหมายอาญา มาตรา 334 ฐานลักทรัพย์ ต้องมีการพรากทรัพย์ไป แต่การโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยไม่มีสิทธิ ไม่ได้มีการพรากข้อมูลคอมพิวเตอร์ไป หากข้อมูลคอมพิวเตอร์ก็ยังคงอยู่กับผู้ทรงสิทธิดังเดิม เพียงมีการคัดลอก (copy) ข้อมูลคอมพิวเตอร์ หรือจดจำไปเท่านั้น ดังที่ศาลฎีกาได้วินิจฉัยไว้ตามคำพิพากษาฎีกาที่ 5161/2547 “ข้อมูลคอมพิวเตอร์” ไม่ได้อยู่ในความหมายของคำว่า “ทรัพย์” ซึ่งผู้เขียนเห็นพ้องด้วยกับศาลฎีกา กล่าวคือ ข้อมูลคอมพิวเตอร์ไม่ใช่วัตถุที่มีรูปร่างอันอาจมีรูปร่างโดยตัวข้อมูลคอมพิวเตอร์เองหรือโดยอาศัยสิ่งอื่นเป็นรูปร่าง[103] อีกทั้งลักษณะแห่งการกระทำเป็นเพียงการ **แบ่ง : Share** ข้อมูลคอมพิวเตอร์ **มิใช่เอาไปในลักษณะที่พรากการครอบครองข้อมูลคอมพิวเตอร์ไปเสียทีเดียว** ข้อมูลคอมพิวเตอร์ก็ยังคงอยู่กับฮาร์ดดีสก์หรือแผ่นบันทึกข้อมูลของเจ้าของข้อมูลคอมพิวเตอร์ เมื่อข้อมูลคอมพิวเตอร์มิได้อยู่ในความหมายของคำว่าทรัพย์ การกระทำของจำเลยจึงไม่เป็นความผิดฐานลักทรัพย์

เมื่อการโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยไม่มีสิทธิ **มิใช่เอาไปในลักษณะที่พรากการครอบครองข้อมูลคอมพิวเตอร์ไปเสียทีเดียว** กรณีจึงไม่อาจเป็นความผิดฐานเอาไปเสียซึ่งเอกสาร ตามประมวลกฎหมายอาญา มาตรา 188 เช่นเดียวกัน

2. ข้อเสนอแนะ

ข้อค้นพบตามวัตถุประสงค์ข้อ 2.3 ของบทที่ 1 คือ เพื่อเสนอแนะการปรับปรุงกฎหมายที่เกี่ยวข้องกับมาตรการทางกฎหมายอาญาในการคุ้มครองข้อมูลคอมพิวเตอร์ มีข้อเสนอแนะ ดังนี้

ผลการวิเคราะห์จากข้อสรุป ซึ่งบทบัญญัติของประมวลกฎหมายอาญา และกฎหมายอื่นที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 รวมถึงการบังคับใช้กฎหมายโดยหน่วยงานตามกระบวนการยุติธรรม ไม่สามารถทำให้ช่องว่างแห่งกฎหมายอาญาที่ไม่อาจคุ้มครองข้อมูลคอมพิวเตอร์ ได้รับการแก้ไขปัญหากรณีการโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ด้วย นิติวิธีการตีความที่สุ่มเสี่ยงหลักกฎหมายสำคัญ “ไม่มีกฎหมาย ไม่มีความผิดและไม่มีโทษ” หรือการเทียบเคียงหรือการอุดช่องว่างแห่งกฎหมายที่ไม่สามารถใช้กับกฎหมายที่มีความผิดและโทษทางอาญาได้ จึงจำเป็นต้องใช้นิติวิธีแก้ไขเพิ่มเติมกฎหมายที่เกี่ยวข้อง เพื่อให้ข้อมูลคอมพิวเตอร์ได้รับการคุ้มครองในฐานะวัตถุแห่งการกระทำด้วยมาตรการทางกฎหมายอาญา

---

[103] จิตติ ติงศภัทิย์, *กฎหมายอาญา ภาค 2 ตอน 2 และภาค 3* พิมพ์ครั้งที่ 3 กรุงเทพมหานคร:เนติบัณฑิตยสภา 2532, หน้า 2473-2477

เมื่อได้ศึกษาวิเคราะห์บทบัญญัติของกฎหมายอาญาของประเทศไทยและกฎหมายอาญาที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศอังกฤษ และประเทศสหรัฐอเมริกาตามบทที่ 2 และบทที่ 3 พบว่า บทบัญญัติตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มีโครงสร้างของกฎหมายทำนองเดียวกันกับกฎหมายของประเทศสหรัฐอเมริกา ตามรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์ และการทำละเมิด ค.ศ.1986 (Computer Fraud and Abuse Act 1986) อีกทั้งกฎหมายฉบับนี้ของประเทศสหรัฐอเมริกาเป็นกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ที่มีการแก้ไขเพิ่มเติมมาตลอด และมีความทันสมัยที่สุดในการคุ้มครองข้อมูลคอมพิวเตอร์ด้วยมาตรการทางกฎหมายอาญาจากการกระทำโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ รวมไปถึงการกำหนดความผิดแก่ผู้ที่ได้รับข้อมูลคอมพิวเตอร์จากการโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยมิชอบอีกด้วย

ส่วนกฎหมายคอมพิวเตอร์ของประเทศอังกฤษ คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) ซึ่งมีอยู่ 4 มาตรา เป็นบทบัญญัติที่วางองค์ประกอบกำหนดความผิดในลักษณะการเข้าถึง (access) กับการทำให้ข้อมูลคอมพิวเตอร์เสียหายเป็นหลัก ยังมีช่องว่างแห่งกฎหมายอาญาที่ไม่ครอบคลุมการกระทำสำหรับการเข้าถึง (access) ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์จากภายในองค์กร และไม่มีบทบัญญัติที่มีเจตนารมณ์มุ่งคุ้มครองข้อมูลคอมพิวเตอร์ในฐานะวัตถุแห่งการกระทำ การจะอาศัยนิติวิธีการตีความกฎหมายก็มีข้อจำกัดว่า การตีความกฎหมายอาญาต้องเคร่งครัด และประการสำคัญสุ่มเสี่ยงข้อห้ามหลักกฎหมายสำคัญ คือ **“ไม่มีกฎหมาย ไม่มีความผิด และไม่มีโทษ”** หากจะมีข้อเสนอแนะแก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ก็พึงร่างกฎหมายให้ชัดเจน ครอบคลุมและมีเจตนารมณ์มุ่งคุ้มครองข้อมูลคอมพิวเตอร์ในฐานะวัตถุแห่งการกระทำโดยตรงเช่นเดียวกับรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์ และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) จะได้ไม่เป็นปัญหาต้องตีความกฎหมายที่สุ่มเสี่ยงข้อห้ามหลักกฎหมายสำคัญดังกล่าวข้างต้นอีก

ดังตัวอย่างคดีที่เกิดขึ้นและเป็นคดีขึ้นสู่ศาลประเทศอังกฤษ ซึ่งผู้กระทำความผิดเข้าถึงระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์โดยมีสิทธิ แต่นำข้อมูลคอมพิวเตอร์ขององค์กรไปใช้ประโยชน์ส่วนตัว ซึ่งกฎหมายอาญาไทยและกฎหมายอาญาประเทศอังกฤษไม่สามารถเอาผิดได้ กล่าวคือ ในคดี DPP v Bignell [1998] จำเลยเป็นเจ้าหน้าที่ตำรวจของสำนักงานตำรวจแห่งชาติ ถูกดำเนินคดีฟ้องร้องข้อหาเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจตามมาตรา 1 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) โดยข้อเท็จจริงในคดีนี้ จำเลยซึ่งเป็นเจ้าหน้าที่ตำรวจของสำนักงานตำรวจแห่งชาติใช้คอมพิวเตอร์ขององค์กร เข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ขององค์กร เพื่อให้ได้ข้อมูล

สำหรับการใช้งานหรือเพื่อประโยชน์ส่วนตัว อย่างไรก็ตาม องค์กรผู้บังคับใช้กฎหมายไม่ สามารถดำเนินคดีต่อการกระทำของเขา เพราะเหตุว่าการกระทำนั้นไม่ได้อยู่ในความหมายของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ค.ศ. 1990 (Computer Misuse Act 1990) มาตรา 1 ฐานเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ความผิดฐานนี้มีเจตนารมณ์เพื่อใช้กับแฮ็กเกอร์ (hacker) จากภายนอก ดังนั้น ศาลยุติธรรมของประเทศอังกฤษจึงพิพากษายกฟ้องจำเลย[104]

ข้อสังเกต คดีนี้ จำเลยเป็นผู้มีสิทธิใช้รหัสผ่าน (password) เข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ขององค์กรได้ ซึ่งรหัสผ่านคือบัตรอิเล็กทรอนิกส์ตามมาตรา 1 (14) (ข) ตามประมวลกฎหมายอาญาของไทย แม้จำเลยจะใช้รหัสผ่านเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ขององค์กร เพื่อประโยชน์ส่วนตัว ก็เป็นเพียงการใช้ที่ผิดวัตถุประสงค์เท่านั้น หาได้ไม่มีสิทธิใช้ หรือใช้โดยปราศจากอำนาจไม่ เช่นนี้ หากเปรียบกับฐานความผิดมาตรา 269/5 ตามประมวลกฎหมายอาญาของไทย ฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบแล้ว นี่เป็นกรณีที่ไม่สามารถปรับบทลงโทษแก่จำเลยได้ เพราะจำเลยเป็นผู้ที่มีสิทธิ หรือมีอำนาจใช้บัตรอิเล็กทรอนิกส์นั้น

รัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) ฉบับนี้อยู่ในประมวลกฎหมายสหรัฐเมริกา (United States Code : U.S.C.) บรรพที่ 18 (Title 18) หมวด 47 (Chapter 47) มาตรา 1030 การฉ้อโกงและการกระทำที่เกี่ยวข้องกับการเชื่อมต่อกับระบบคอมพิวเตอร์ (Fraud and related activity in connection with computers)

อนุมาตรา (a) ผู้ใด..

อนุมาตราย่อย (2) จงใจหรือเจตนาเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบอำนาจ และได้รับไปซึ่ง..

(A) ข้อมูลที่มีอยู่ในบันทึกทางการเงินของสถาบันการเงินหรือของบริษัทผู้ออกบัตรตามที่กำหนดไว้ในมาตรา 1602 (n) ของบรรพที่ 15 (Title 15) หรือที่มีอยู่ในแฟ้มของผู้บริโภคในการรายงานหน่วยงานคุ้มครองผู้บริโภค ซึ่งมีการกำหนดไว้ในรัฐบัญญัติการรายงานเครดิตที่เป็นธรรม (the Fair Credit Reporting Act, Title 15 USC section 1681 et seq.)

(B) ข้อมูลจากหน่วยงานใดหรือหน่วยงานของประเทศสหรัฐอเมริกา หรือ

(C) ข้อมูลจากคอมพิวเตอร์เครื่องใดๆ ที่ได้รับการคุ้มครอง

---

[104] เว็บไซต์อาจารย์นิติศาสตร์ดอทเน็ต *http://www.lawteacher.net/criminal-law/acts/computer-misuse-act-1990.php* และเว็บไซต์หน่วยงานพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ ประเทศอังกฤษ *http://www.computer evidence.co.uk/Cases/CMA.htm* สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

อนุมาตราย่อย (4) รู้อยู่แล้วและมีเจตนาที่จะฉ้อโกง เข้าถึงระบบคอมพิวเตอร์ที่มีการป้องกันการเข้าถึงโดยปราศจากอำนาจหรือเกินขอบอำนาจ และด้วยวิธีการเช่นว่านั้นการกระทำดังกล่าวมีเจตนาฉ้อโกง และได้รับสิ่งใดๆ ที่มีมูลค่าไป เว้นแต่วัตถุประสงค์ของการฉ้อโกงและสิ่งที่ได้มานั้นเป็นเพียงเพื่อการใช้งานคอมพิวเตอร์และมูลค่าการใช้งานดังกล่าวไม่เกิน 5,000 ดอลล่าห์สหรัฐอเมริกาในช่วงระยะเวลา 1 ปี

อนุมาตราย่อย (6) รู้อยู่แล้วและมีเจตนาที่จะฉ้อโกง ลักลอบค้า (ตามที่ระบุไว้ในมาตรา 1029)[105] รหัสผ่าน (password) หรือข้อมูลที่คล้ายคลึงกัน ซึ่งใช้สำหรับการเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจ ถ้า..

(A) การค้าดังกล่าวมีผลกระทบต่อการค้าระหว่างมลรัฐหรือระหว่างประเทศ หรือ

(B) ระบบคอมพิวเตอร์ดังกล่าวถูกใช้โดยหรือสำหรับรัฐบาลของประเทศสหรัฐอเมริกา

จากบทบัญญัติของรัฐบัญญัติเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์และการทำละเมิด ค.ศ. 1986 (Computer Fraud and Abuse Act 1986) เมื่อวิเคราะห์ปรับให้เข้ากับบทบัญญัติของกฎหมายไทยตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 การแก้ไขเพิ่มเติมสามารถเพิ่มบทบัญญัติขึ้นใหม่ 2 ฐานความผิด ด้วยการบัญญัติเพิ่มขึ้นหนึ่งมาตราให้มีสองวรรค ซึ่งแก้ไขเพิ่มเติมด้วยการให้มีความผิดฐาน **“สำเนาข้อมูลคอมพิวเตอร์โดยมิชอบ”** กับความผิดฐาน **“ได้รับข้อมูลคอมพิวเตอร์โดยมิชอบ”** โดยบัญญัติแก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพิ่มมาตรา 14/1 ด้วยการมีสองวรรค ดังนี้

“ผู้ใดสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นไปโดยมิชอบ โดยประการที่น่าจะทำให้ผู้อื่นหรือประชาชนเสียหาย ต้องระวางโทษ.....”

“ผู้ใดได้รับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ โดยรู้อยู่ว่าข้อมูลคอมพิวเตอร์นั้นได้มาจากการกระทำความผิดตามวรรคหนึ่ง ต้องระวางโทษ.....”

การแก้ไขเพิ่มเติมให้มีมาตรา 14/1 ดังกล่าวข้างต้นนอกจากการคุ้มครองข้อมูลจากการโจรกรรม หรือสำเนาข้อมูลคอมพิวเตอร์ทั้ง 3 รูปแบบ ไม่ว่าด้วยการเจาะระบบ หรือที่เรียกกันว่าแฮ็ก (hack) หรือโจรกรรมหรือสำเนาข้อมูลคอมพิวเตอร์ไปโดยเข้าถึงระบบคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ทั้งการเข้าถึงโดยมีสิทธิ และการเข้าถึงโดยไม่มีสิทธิ รวมถึงโจรกรรมหรือ

---

[105] รัฐบัญญัติเกี่ยวกับการฉ้อโกงโดยบัตรเครดิต ค.ศ. 1984 (The credit card fraud act 1984) มาตรา 1029 (e) (5) บัญญัติว่า *the term “traffic” means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of* เว็บไซด์คณะนิติศาสตร์ มหาวิทยาลัยคอร์แนล https://www.law.cornell.edu/uscode/text/18/1029 สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561

สำเนาข้อมูลคอมพิวเตอร์ไปโดยวิธีสามัญ ตามที่ได้จากการศึกษาในบทที่ 2 และกล่าวถึงในข้อ 1 ข้างต้น

ปัญหานี้จะได้รับการแก้ไขลงได้ด้วยการแก้ไขเพิ่มเติม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยเพิ่มมาตรา 14/1

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

เกียรติขจร วัจนะสวัสดิ์.(2551) *กฎหมายอาญา ภาคความผิด เล่ม 2* พิมพ์ครั้งที่ 5 กรุงเทพมหานคร: หจก.จิรรัชการพิมพ์.

จตุชัย แพงจันทร์ น.ต. (2550) *Master in Security* ไอดีซีอินโฟดิสทริบิวเตอร์เซ็นเตอร์ จก.

จิตติ ติงศภัทิย์. (2532) *กฎหมายอาญา ภาค 2 ตอน 2 และภาค 3* พิมพ์ครั้งที่ 3 กรุงเทพมหานคร: สำนักอบรมศึกษาแห่งเนติบัณฑิตยสภา.

ธานินทร์ กรัยวิเชียร และวิชา มหาคุณ. (2521) *การตีความกฎหมาย* พิมพ์ครั้งที่ 2 กรุงเทพมหานคร:โรงพิมพ์ชวนพิมพ์

มหาวิทยาลัยสุโขทัยธรรมาธิราช. (2552) *เอกสารการสอนชุดวิชากฎหมายอาญา 2 : ภาคความผิด* หน่วยที่ 1-5 (ฉบับปรับปรุงครั้งที่ 2) กรุงเทพมหานคร:สำนักพิมพ์มหาวิทยาลัยสุโขทัยธรรมาธิราช

สมศักดิ์ เธียรจรูญกุล (มิถุนายน 2554) *ความรับผิดทางอาญาของการลักลอบจูนโทรศัพท์เคลื่อนที่* วารสารกฎหมายสุโขทัยธรรมาธิราช ปีที่ 23 ฉบับที่ 1

สมศักดิ์ เธียรจรูญกุล (ก.ย. 2559 - มี.ค. 2560) *ความสำคัญของนิยามบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา* วารสารกฎหมายสุโขทัยธรรมาธิราช ปีที่ 28 ฉบับที่ 1

สมศักดิ์ เธียรจรูญกุล (ม.ค.-มิ.ย. 2560) *ความหมายของบัตรอิเล็กทรอนิกส์อันเป็นองค์ประกอบของฐานความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา* วารสารสุโขทัยธรรมาธิราช ปีที่ 30 ฉบับที่ 1

สมศักดิ์ เธียรจรูญกุล (2559) รายงานการวิจัยเรื่อง *ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา* ทุนอุดหนุนการวิจัยจากกองทุนรัตนโกสินทร์สมโภช 200 ปี มหาวิทยาลัยสุโขทัยธรรมาธิราช.

สมศักดิ์ เธียรจรูญกุล (ธันวาคม 2554) *สำเนาข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ* วารสารกฎหมายสุโขทัยธรรมาธิราช ปีที่ 23 ฉบับที่ 2

สำนักงานคณะกรรมการกฤษฎีกา *วิเคราะห์ร่างพระราชบัญญัติการประกอบธุรกิจบัตรเครดิต พ.ศ. ....* เรื่องเสร็จที่ 592/2543

หยุด แสงอุทัย (2525) *กฎหมายอาญา ภาค 1* กรุงเทพมหานคร:มหาวิทยาลัยธรรมศาสตร์, อ้างในมหาวิทยาลัยสุโขทัยธรรมาธิราช *เอกสารการสอนชุดวิชากฎหมายอาญา 1: ภาคบทบัญญัติทั่วไป* กรุงเทพมหานคร:สำนักพิมพ์มหาวิทยาลัยสุโขทัยธรรมาธิราช.

สื่ออิเล็กทรอนิกส์ภาษาไทย

เกียรติขจร วัจนะสวัสดิ์ วันที่ 17 มิถุนายน 2559 *คำบรรยายเนติบัณฑิตกฎหมายอาญา มาตรา 59-106* เล่ม 4 สืบค้นเมื่อวันที่ 28 พฤศจิกายน 2560 จาก *https://web.facebook.com/permalink.php?story_fbid=156796628063950&id=136630040080609&hc_location=ufi*

พรเพชร วิชิตชลชัย *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550* เว็บไซต์มหาวิทยาลัยเชียงใหม่ สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561 จาก *http://www.med.cmu.ac.th/home/file/cc_act_exp.pdf*

เว็บไซต์เวิลด์เพรสดอทคอม สืบค้นเมื่อวันที่ 8 พฤษภาคม 2560 จาก *https://neay999.wordpress.com/บทที่-7-การเจาะระบบและวิ/*

เว็บไซต์บ้านมหาดอทคอม สืบค้นเมื่อวันที่ 10 สิงหาคม พ.ศ. 2561 จาก *http://www.baanmaha.com/community/thread40335.html*

ภาษาต่างประเทศ

Caminer, B. F., (1985) *Comment, Credit Card Fraud : Neglected Crime* Jouenal of Criminal Law and Criminology.

Maffly, D.H. and Mcdonald, A.C. (1960) *The Triparties Credit Card Transaction : A Legal Infant* 48 Californai Law Review, Vol. 489

Melhem, Ahmed Al (1990) *“The Legal Regime of Payment Cards:A comparative Study between American, British and Kuwaiti Laws, With Particular reference to Credit Cards.”* Ph.D. thesis The University of Exeter England.

National Criminal Justice Information and Statistics Service, Law Enforcement Assistance Administration, U.S. Department of Justice (1979) *COMPUTER CRIME:Criminal Justice Resource Manual* Washington D.C.:U.S. Government Printing Office.

Sayer, P.E. (1988) *Credit Cards and the Law : An Introduction* London : Fourmat Publishing.

Smith, J. C., (1980) Obtaining by Ceception R.v. Lambei *Criminal Law Review*.

Smith & Hogan (1988) *Criminal law* 6th ed., Butterworths.

สื่ออิเล็กทรอนิกส์ภาษาต่างประเทศ

Aggravated identity theft, Retrieved August 10, 2018,/form/ *https://www.law.cornell.edu/search/site/1028*

ARC Airlines Tackle, Retrieved August 10, 2018,/form/ *http://nvflyer.wordpress.com/2010/12/05/the-computer-fraud-and-abuse-act-revenue-protection-weapon-for-airlines/*

Congress, *Identity Theft Enforcement and Restitution Act of 2007*, Retrieved August 10, 2018,/form/ *http://www.govtrack.us/congress/billtext.xpd?bill=s110-2168*

Congress, *Theft Act 1968*, Retrieved August 10, 2018,/form/ *http://www.policeoracle.com/acts_of_parliament/THEFT_ACT_1968.doc*

Congress, *Theft Act 1978*, Retrieved August 10, 2018,/form/ *http://www.policeoracle.com/acts_of_parliament/Theft_Act_1978.doc*

Crown Prosecution Service, Retrieved August 10, 2018,/form/ *https://www.cps.gov.uk/legal-guidance/computer-misuse-act-1990*

Findlaw.com, *Fraud and related activity in connection with identification documents, authentication features, and information*, Retrieved August 10, 2018,/form/ *http://codes.lp.findlaw.com/uscode/18/I/47/1028*

Findlaw.com, Law Cornell, Ehow.com, *Identity theft and Assumption Deterrence Act 1998*, Retrieved August 10, 2018,/form/ *http://codes.lp.findlaw.com/uscode/18/I/47/1028* and *https://www.law.cornell.edu/search/site/1028* and *http://www.ehow.com/about_6661635_identity-theft-restitution-act.html*

Findlaw.com, Law Cornell, U.S. Government Publishing Office, *The credit card fraud act 1984*, Retrieved August 10, 2018,/form/ *http://codes.lp.findlaw.com/uscode/18/I/47/1029/notes* and https://www.law.cornell.edu/uscode/text/18/1029 and https://www.gpo.gov/fdsys/granule/USCODE-2011-title18/USCODE-2011-title18-partI-chap47-sec1029

Legislation GOV UK, *Forgery and Counterfeiting Act 1981*, Retrieved August 10, 2018,/form/ *http://www.legislation.gov.uk/ukpga/1981/45*

Legislation GOV UK, *Theft Act 1996*, Retrieved August 10, 2018,/form/ *http://www.legislation.gov.uk/ukpga/1996/62/pdfs/ukpga_19960062_en.pdf*

Law cornel, *Computer Fraud and Abuse Act 1986*, Retrieved August 10, 2018,/form/ https://www.law.cornell.edu/uscode/text/18/1030

Lawteacher.net *Describe the origins and function of the Computer Misuse Act 1990 Evaluate the extent to which it is intended to serve as a deterrent to 'hacking'* Retrieved August 10, 2018,/form/ *http://www.lawteacher.net/criminal-law/acts/computer-misuse-act-1990.php*

Law Cornell, *U.S.C.* , Retrieved August 10, 2018,/form/ https://www.law.cornell.edu/uscode/text/18/1029

Panix.com, Retrieved August 10, 2018,/form/ *http://www.panix.com/~eck/computer-fraud-act.html*

Statutelaw GOV UK, *Police and Justice Act 2006*, Retrieved August 10, 2018,/form/ *http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=1353366*

Statutelaw GOV UK, *Computer misuse act 1990*, Retrieved August 10, 2018,/form/ *http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=1353366*

UNCITRAL, *Model Law on Electronic Commerce with Guide to Enactment 1996*, Retrieved August 10, 2018,/form/ *http://www.uncitral.org*

United States Code : U.S.C., Retrieved August 10, 2018,/form/ *http://uscode.house.gov/download/pls/15C41.txt* and Retrieved April 28, 2011,/form/*http://law.onecle.com/uscode/15/1602.html*

Yaman Akdeniz Faculty of Law University of Leeds, *Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!*, Retrieved August 10, 2018, /form/ *http://www.bailii.org/cgi-bin/format.cgi?doc=/uk/other/journals/WebJCLI/1996/issue3/akdeniz3.html&query=(Yaman)+AND+(Akdeniz)*

Case Law

Case. DPP v Bignell [1998], Retrieved August 10, 2018,/form/ *http://www.lawteacher.net/criminal-law/acts/computer-misuse-act-1990.php* and *http://www.computerevidence.co.uk/Cases/CMA.htm*

Case. Cox v Riley (1986) 54, Yaman Akdeniz Faculty of Law University of Leeds, *Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!*, Retrieved August 10, 2018,/form/ *http://www.bailii.org/cgi-bin/format.cgi?doc=/uk/other/journals/WebJCLI/1996/issue3/akdeniz3.html&query=(Yaman)+AND+(Akdeniz)*

Case. Ellis v DPP [2001], Retrieved August 10, 2018,/form/ *http://books.google.co.th/books?id=-VtTiR8niBEC&pg=PR16&lpg=PR16&dq=Ellis+v+DPP+%5B2001%5D&source=bl&ots=6zt68mcNJk&sig=LvD2CsrelerffCv1Yfw0-u5yXRE&hl=th&ei=FK89TcGgLYbIuAPH-p3fCg&sa=X&oi=book_result&ct=result&resnum=5&ved=0CDQQ6AEwBA#v=on epage&q=Ellis%20v%20DPP%20%5B2001%5D&f=false* pp. 442

Case. Whiteley (1991), Yaman Akdeniz, Faculty of Law University of Leeds, *Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!*, Retrieved August 10, 2018,/form/ *http://www.bailii.org/cgi-bin/format.cgi?doc=/uk/other/journals/WebJCLI/1996/issue3/akdeniz3.html&query=(Yaman)+AND+(Akdeniz)*

R v. Abdulla, in Melhem, Ahmed Al (1990), *"The Legal Regime of Payment Cards:A comparative Study between American, British and Kuwaiti Laws, With Particular reference to Credit Cards."* Ph.D. thesis The University of Exeter England.,

R v. Gold (1988), *Describe the origins and function of the Computer Misuse Act 1990 Evaluate the extent to which it is intended to serve as a deterrent to 'hacking'*, Retrieved August 10, 2018,/form/ *http://www.lawteacher.net/criminal-law/acts/computer-misuse-act-1990.php* and *http://www.lawteacher.net/criminal-law/acts/computer-misuse-act-1990.php*

R v. Malcolm Farquharson (09/12/1993), Retrieved August 10, 2018,/form/ *http://www.computerevidence.co.uk/Cases/CMA.htm*

R v. Paul Bedworth, Retrieved August 10, 2018, 2010,/form/ *http://www.lawteacher.net/criminal-law/acts/computer-misuse-act-*

1990.php and *http://www.computerevidence.co.uk/Cases/CMA.htm* and Yaman Akdeniz *Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!*, Retrieved August 10, 2018,/form/ *http://www.bailii.org/cgi-bin/format.cgi?doc=/uk/other/journals/WebJCLI/1996/issue3/akdeniz3.html&query=(Yaman)+AND+(Akdeniz)*

R v. Richard Goulden [June 10, 1992], Yaman Akdeniz, *Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!*, Retrieved August 10, 2018,/form/ *http://www.bailii.org/cgi-bin/format.cgi?doc=/uk/other/journals/WebJCLI/1996/issue3/akdeniz3.html&query=(Yaman)+AND+(Akdeniz)*

R v. Ross Pearlstone [1991], Retrieved August 10, 2018,/form/ *http://www.computerevidence.co.uk/Cases/CMA.htm* and *http://www.cs.bris.ac.uk/Teaching/Resources/COMSM2005/Lecture14.pdf*

R v. Strickland, R v. Woods [May 21, 1993], Yaman Akdeniz, *Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!*, Retrieved August 10, 2018,/form/ *http://www.bailii.org/cgi-bin/format.cgi?doc=/uk/other/journals/WebJCLI/1996/issue3/akdeniz3.html&query=(Yaman)+AND+(Akdeniz)*

R v. Susan Holmes [15/02/2008], John Leyden, Retrieved August 10, 2018,/form/ *http://www.theregister.co.uk/2008/02/18/nanny_agency_hack_conviction/*

United States v. Batti (09-2050 No.) 2011, Retrieved August 10, 2018,/form/ *http://caselaw.findlaw.com/us-6th-circuit/1552671.html*

United States v. Czubinski (96-1317 No.) 1997, Retrieved August 10, 2018,/form/ *http://caselaw.findlaw.com/us-1st-circuit/1061981.html*

United States v. Dimetriace Eva Lavon John (08-10459 No.) 2010, Retrieved August 10, 2018,/form/ *http://caselaw.findlaw.com/us-5th-circuit/1507168.html*

United States of America, Plaintiff-Appellee, v. Castellanos Ruben, Retrieved August 10, 2018,/form/ *https://caselaw.findlaw.com/us-7th-circuit/1436041.html*