พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

นางสาวพิญดา เลิศกิตติกุล

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2550

THE COMPUTER-RELATED CRIME ACT 2007 : A CASE STUDY OF CRIMINAL LIABILITY IN ACCESS TO COMPUTER SYSTEM AND COMPUTER DATA

Miss Phinda Lertkitikul

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Laws Program in laws
Faculty of Law
Chulalongkorn University
Academic Year 2007

หัวข้อวิทยานิพนธ์	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์
โดย	นางสาวพิญดา เลิศกิตติกุล
สาขาวิชา	สาขาวิชานิติศาสตร์
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์ ดร. ปารีณา ศรีวนิชย์

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะนิติศาสตร์
(รองศาสตราจารย์ธิติพันธุ์ เชื้อบุญชัย)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร. อภิรัตน์ เพ็ชรศิริ)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์
(ผู้ช่วยศาสตราจารย์ ดร. ปารีณา ศรีวนิชย์)

..... กรรมการ
(อาจารย์นันทชัย เพียรสนอง)

..... กรรมการ
(รองศาสตราจารย์ ดร. ทวีเกียรติ มีนะกนิษฐ)

..... กรรมการ
(พันตำรวจเอกญาณพล ยั่งยืน)

พิญดา เลิศกิตติกุล : พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ศึกษากรณีความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์. (The Computer-Related Crime Act 2007 : a case study of criminal liability in access to computer system and computer data) อ. ที่ปรึกษา : ผู้ช่วยศาสตราจารย์ ดร. ปารีณา ศรีวนิชย์ , 208 หน้า.

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อที่จะศึกษาหาความหมายที่ชัดเจนของคำว่า "เข้าถึง" ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และหาคำตอบว่าควรที่จะตีความคำว่า "เข้าถึง" อย่างไรจึงจะมีผลใช้บังคับได้จริง ตลอดจนถึงปัญหาที่ว่าการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่จะเป็นความผิดอาญามีขอบเขตเช่นใด

ผลการวิจัยพบว่า ไม่มีนิยามคำว่า "เข้าถึง" ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ดังนั้นศาลจึงต้องมีการตีความคำว่า "เข้าถึง" เพื่อการบังคับใช้กฎหมาย จึงควรตีความอย่างกว้างเพื่อให้เหมาะสมกับพฤติกรรมการใช้คอมพิวเตอร์ที่หลากหลาย ทำให้สามารถนำตัวผู้กระทำความผิดมาลงโทษได้ เนื่องจากหากตีความอย่างแคบแล้วก็จะทำให้เกิดปัญหาว่ามีการเข้าถึงแล้วหรือยัง และอาจทำให้ไม่สามารถนำตัวผู้กระทำผิดมาลงโทษได้

สำหรับขอบเขตของการเข้าถึงที่จะต้องรับผิดทางอาญานั้น ควรที่จะปล่อยให้เป็นหน้าที่ของศาลที่จะพิจารณาว่าการเข้าถึงที่จะเป็นความผิดนั้นควรมีลักษณะอย่างไร โดยไม่จำกัดว่าต้องไม่ชอบด้วยกฎหมายหรือโดยปราศจากอำนาจเท่านั้น เนื่องจากมีลักษณะการกระทำอื่นที่เป็นการกระทำที่ไม่ถูกต้องหากแต่ไม่ผิดกฎหมายหรือทำโดยมีอำนาจ ซึ่งหากตีความอย่างแคบแล้วจะทำให้ผู้กระทำความผิดไม่ต้องรับโทษทางกฎหมาย

สาขาวิชา.....นิติศาสตร์..... ลายมือชื่อนิสิต.....

ปีการศึกษา 2550 ลายมือชื่ออาจารย์ที่ปรึกษา.....

4886256434 : MAJOR LAWS

KEY WORD: ACCESS / COMPUTER / COMPUTER-RELATED CRIME ACT

PHINDA LEARTKITIKUL : THE COMPUTER-RELATED CRIME ACT 2007 : A CASE STUDY OF CRIMINAL LIABILITY IN ACCESS TO COMPUTER SYSTEM AND COMPUTER DATA. THESIS ADVISOR : ASSOC. PROF. PAREENA SRIVANIT,Ph.D., 208 pp.

The objectives of this research is to clarify the term "access" in The Computer-Related Crime Act, 2007, to identify the conclusion of the interpretation of the term "access" in order to enforce the law efficiently, and to find to what extent the access to computer system and computer data may be liable.

The findings reveal that there is no definition of the term "access" in. therefore, the term "access" must be interpreted broadly by court. If the courts interpret "access" narrowly, it is cause a problem that in some cases, the person who commit the crime may not be punished according to law.

The scope of criminal liability in access to computer system and computer data is duty of the courts to consider that what kind of access that shall be punished. The court do not limit the scope of access by the term "illegal" or "unauthorized" access. Because the person can commit the crime just improper access. If interpret the criminal kind of access narrowly, person who make a crime may be not liable.

Field of study.....Laws..... Student's signature.....

Academic year 2007 Advisor's signature.....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้จะไม่สามารถสำเร็จลุล่วงไปได้ถ้าปราศจากความเมตตาและความช่วยเหลือจากผู้มีพระคุณดังต่อไปนี้

ดร. ปารีณา ศรีวนิชย์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ช่วยดูแลและให้คำปรึกษาตั้งแต่เริ่มต้นทำวิทยานิพนธ์ ชี้แนะวิธีการเขียนและเนื้อหาของวิทยานิพนธ์ แนะนำผู้เชี่ยวชาญทางด้านกฎหมายเยอรมันในการทำวิทยานิพนธ์ อีกทั้งให้เวลาผู้เขียนในการซักถามเมื่อมีปัญหาเสมอมา

รองศาสตราจารย์ ดร. อภิรัตน์ เพ็ชรศิริ ประธานกรรมการสอบวิทยานิพนธ์ อาจารย์นันทชัย เพียรสนอง รองศาสตราจารย์ ดร. ทวีเกียรติ มีนะกนิษฐ์ และพันตำรวจเอก ญาณพล ยั่งยืน กรรมการสอบวิทยานิพนธ์ ซึ่งได้กรุณาสละเวลามาเป็นประธานกรรมการและกรรมการในการสอบวิทยานิพนธ์และให้คำแนะนำในการทำวิทยานิพนธ์

ดร. ไพจิตร สวัสดิสาร ผู้พิพากษา ซึ่งได้กรุณาสละเวลามาช่วยแปลกฎหมายต่างประเทศที่เกี่ยวข้องและตอบคำถามทางกฎหมายที่ผู้เขียนสงสัย และดร. ราล์ฟ บาวมการ์เทน อาจารย์ประจำจุฬาลงกรณ์มหาวิทยาลัย ซึ่งได้ช่วยกรุณาแปลกฎหมายอาญาเยอรมันให้

อาจารย์ธงชัย โรจน์กังสดาล อาจารย์ประจำคณะวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย และดร. สันติธร บุญเจือ คณบดีคณะเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยอัสสัมชัญ ซึ่งได้กรุณาสละเวลามาให้ความรู้เกี่ยวกับคอมพิวเตอร์และการทำงานของคอมพิวเตอร์

ขอขอบพระคุณ คุณชัยวัฒน์ เลิศกิตติกุล และคุณนิตยา แตงจ๊อก ซึ่งได้ช่วยหาข้อมูลเกี่ยวกับคอมพิวเตอร์และการทำงานของคอมพิวเตอร์ รวมตลอดถึงท่านรองเลขาฯ เจ้าหน้าที่งานคำสั่งคำร้อง ศาลอุทธรณ์ภาค 9 และเพื่อนๆ ทุกท่านที่ให้การสนับสนุนและให้กำลังใจเสมอมา

เหนือสิ่งอื่นใด ผู้เขียนวิทยานิพนธ์ขอกราบขอบพระคุณ บิดา มารดา และคุณอาวรรณชัย สุรอมรรัตน์ ซึ่งสนับสนุนในด้านการเงินและให้ความรัก ความห่วงใย แก่ผู้เขียนมาโดยตลอด หากมีข้อบกพร่องใดในเนื้อหาของวิทยานิพนธ์ฉบับนี้ผู้เขียนขอน้อมรับไว้แต่เพียงผู้เดียว

สารบัญ

หน้า

หน้า

หน้า

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันคอมพิวเตอร์ได้เข้ามามีบทบาทในชีวิตและการทำงานของบุคคลทั่วไปเป็นอย่างมาก ทำให้พฤติกรรมการใช้ชีวิตของมนุษย์เปลี่ยนแปลงไปในแทบทุกด้าน ไม่ว่าจะเป็นด้านการทำงาน การพักผ่อน การเรียนรู้ หรือแม้กระทั่งการจับจ่ายซื้อของในชีวิตประจำวัน โดยเฉพาะอย่างยิ่งงานบางประเภทได้ถูกปรับปรุงและพัฒนาให้ควบคุมด้วยคอมพิวเตอร์อย่างสมบูรณ์แบบแทบทุกขั้นตอน เช่น การรักษาทางด้านการแพทย์ ระบบโทรศัพท์และการติดต่อสื่อสาร การเกษตร การจัดเก็บข้อมูล การทำธุรกรรมอิเล็กทรอนิกส์ หรือแม้กระทั่งการทำสงครามต่างก็มีคอมพิวเตอร์เข้าไปเกี่ยวข้องทั้งสิ้น ไม่ว่าในฐานะเป็นอุปกรณ์ เครื่องมือ หรือแม้แต่การนำระบบปฏิบัติการต่างๆ ของคอมพิวเตอร์ไปใช้ คอมพิวเตอร์จึงเข้ามามีบทบาทอย่างหลีกเลี่ยงไม่ได้ในการช่วยเหลือและทดแทนการทำงานของมนุษย์และเทคโนโลยีที่มีอยู่เดิม เครื่องมือหรืออุปกรณ์ที่ช่วยอำนวยความสะดวกที่มีในอดีต เช่น เครื่องพิมพ์ดีด โทรสาร โทรศัพท์ ถูกแทนที่ด้วยคอมพิวเตอร์ หรือนำระบบปฏิบัติการของคอมพิวเตอร์มาปรับปรุงหรือพัฒนาประสิทธิภาพของอุปกรณ์เหล่านั้น ทำให้หน่วยงานต่างๆ สามารถลดภาระในการทำงานหรือค่าใช้จ่ายลงได้ส่วนหนึ่งและใช้บุคคลากรในการทำงานน้อยลงแต่มีผลผลิตหรือชิ้นงานมากขึ้น

ดังนั้นไม่ว่าจะพิจารณาในแง่ของการเป็นอุปกรณ์การทำงาน อุปกรณ์สื่อสาร เครื่องมือในการบริหารงาน หรือเป็นสื่อบันเทิงต่างๆ อิทธิพลของคอมพิวเตอร์จึงกลายเป็นสิ่งที่บุคคลที่อาศัยอยู่ในสังคมปัจจุบันไม่สามารถปฏิเสธได้แม้บุคคลนั้นจะใช้คอมพิวเตอร์ไม่เป็นก็ตาม เพราะข้อมูลหรือการให้บริการที่บุคคลนั้นเข้าไปเกี่ยวข้องก็มักจะมีการจัดการด้วยระบบงานคอมพิวเตอร์แทบทั้งสิ้นโดยเฉพาะอย่างยิ่งการให้บริการในภาคเอกชน การใช้คอมพิวเตอร์จึงกลายเป็นทักษะที่จำเป็นส่วนหนึ่งในชีวิตของบุคคลทั่วไปไม่ว่าทางด้านการงานหรือส่วนตัว หน่วยงานหรือองค์กรต่างๆ พยายามให้บุคคลากรของตนเรียนรู้และใช้คอมพิวเตอร์ให้เป็น เพราะคอมพิวเตอร์ถูกนำมาใช้ประโยชน์อย่างหลากหลายและกลายเป็นองค์ประกอบสำคัญในการดำเนินงานไม่ว่าจะเป็นงานบริการหรืองานบริหารข้อมูล งานภาครัฐหรือภาคเอกชน หรือแม้กระทั่งงานอดิเรกส่วนบุคคล

ด้วยประสิทธิภาพของคอมพิวเตอร์ในบางด้านที่ทำได้ดีกว่ามนุษย์ เช่น ความจุของหน่วยความจำที่มีขนาดใหญ่และคงอยู่ตลอดไปหากไม่มีการลบล้างข้อมูลที่บรรจุไว้ การคิดคำนวณที่รวดเร็วและเที่ยงตรง สามารถทำงานได้โดยไม่ต้องหยุดพัก ทำให้มีการนำคอมพิวเตอร์

เข้าไปสนับสนุนการทำงานต่างๆ เพื่อให้เกิดประสิทธิภาพสูงสุดในการปฏิบัติงานนั้น โดยเฉพาะงานที่ต้องการความแม่นยำ เที่ยงตรง ตัวอย่างที่เห็นได้ชัดว่าคอมพิวเตอร์มีประโยชน์อย่างมหาศาลในการพัฒนาคุณภาพชีวิตของมนุษย์ คือ การนำคอมพิวเตอร์ไปใช้ในทางการแพทย์ ตั้งแต่โปรแกรมคำสั่งพื้นฐานที่ช่วยในการวินิจฉัยโรค จนกระทั่งถึงเครื่องคอมพิวเตอร์ที่ซับซ้อนที่สามารถถ่ายภาพและวิเคราะห์สมองของมนุษย์ได้ จนไปถึงมีการพยายามพัฒนาคอมพิวเตอร์ที่ช่วยในการผ่าตัด ซึ่งเครื่องมือในสมัยใหม่ต่างพยายามนำคอมพิวเตอร์เข้ามาใช้เพื่อให้มีความละเอียดแม่นยำมากที่สุดเท่าที่สามารถทำได้และทดแทนสิ่งที่อยู่เกินขอบเขตความสามารถของมนุษย์ที่จะกระทำได้ ดังนั้นในปัจจุบันคอมพิวเตอร์ได้กลายเป็นส่วนประกอบที่สำคัญอย่างยิ่งในวงการแพทย์สมัยใหม่ นอกจากนี้ระบบคอมพิวเตอร์ถูกนำไปใช้ส่งเสริมประสิทธิภาพของอุปกรณ์อื่นๆ เช่น รหัสแท่งและเครื่องคิดเงิน ระบบโทรศัพท์ งานออกแบบ และงานสิ่งพิมพ์ต่างๆ อุปกรณ์ในโรงงานอุตสาหกรรม เป็นต้น จึงเป็นได้ว่าอุปกรณ์หรือสิ่งประดิษฐ์ต่างๆ พยายามนำระบบปฏิบัติการแบบคอมพิวเตอร์เข้าไปใช้เพื่อพัฒนาการทำงานของอุปกรณ์ต่างๆ ซึ่งจะทำให้สามารถทำงานได้มากขึ้นและมีประสิทธิภาพยิ่งขึ้นกว่าอุปกรณ์แบบเดิม

เมื่อคอมพิวเตอร์ถูกนำมาใช้อย่างแพร่หลาย การใช้คอมพิวเตอร์ที่พบเห็นในหน่วยงานหรืองานด้านต่างๆ รวมถึงในชีวิตประจำวันของบุคคลทั่วไปมากที่สุดคือการนำคอมพิวเตอร์มาใช้ในการดำเนินการและเก็บรักษาข้อมูลในรูปแบบข้อมูลทางคอมพิวเตอร์ ซึ่งการเก็บรักษาข้อมูลในระหว่างดำเนินการหรือดำเนินการเสร็จสิ้นแล้วในรูปข้อมูลคอมพิวเตอร์เป็นสิ่งที่พบเห็นได้เป็นปกติในการทำงานและมีปริมาณเพิ่มมากขึ้นตามความต้องการของสังคม

ข้อมูลต่างๆ ที่เก็บรักษานั้นมีตั้งแต่ข้อมูลทั่วไปที่เปิดโอกาสให้บุคคลภายนอกอื่นๆ เข้าถึงได้ ไปจนถึงข้อมูลที่เป็นความลับส่วนบุคคล ความลับของทางบริษัทหรือทางราชการ เช่น หน่วยงานราชการอาจเก็บข้อมูลเกี่ยวกับประชาชนที่เข้ามาติดต่อ เอกสารหลักฐานต่างๆ รวมถึงการกำหนดวันนัดติดต่อทางราชการไว้ในรูปแบบข้อมูลทางคอมพิวเตอร์ หรือหน่วยงานเอกชนอาจเก็บข้อมูลของลูกค้าที่เข้ามาติดต่อกับตนไว้ในรูปแบบข้อมูลคอมพิวเตอร์เช่นกัน นอกจากนี้อาจมีการจัดทำข้อมูลพื้นฐานหรือข้อมูลที่เป็นความลับของบริษัทโดยเฉพาะ เช่น ความลับทางการค้าของบริษัทในรูปข้อมูลทางคอมพิวเตอร์ ในหลายๆหน่วยงานมีแนวคิดว่าควรมีการส่งเสริมให้มีการเก็บรักษาข้อมูลไว้ในลักษณะข้อมูลทางคอมพิวเตอร์มากยิ่งขึ้น ซึ่งอาจจะเกิดจากความคิดที่ว่าการเก็บรักษาข้อมูลต่างๆในรูปแบบกระดาษกลายเป็นสิ่งที่สิ้นเปลืองโดยเฉพาะข้อมูลที่ไม่มีความจำเป็นที่ต้องนำกลับมาใช้ซ้ำ นอกจากนั้นสำหรับข้อมูลสำคัญที่ต้องเก็บรักษาไว้ยังประสบความยุ่งยากที่จะทำการคัดลอกเก็บสำเนา สิ้นเปลืองเนื้อที่จัดเก็บ และยากต่อการ

ค้นหาอีกด้วย ดังนั้นหน่วยงานจำนวนมากโดยเฉพาะหน่วยงานภาคเอกชนจึงใช้คอมพิวเตอร์เป็นแนวทางในการแก้ไขปัญหาดังกล่าวโดยมีการเก็บรักษาข้อมูลไว้ในรูปแบบข้อมูลทางคอมพิวเตอร์ทำให้ลดค่าใช้จ่ายลงได้จำนวนหนึ่ง นอกจากนี้ยังง่ายต่อการนำไปดำเนินงานต่อและการค้นหาข้อมูลอีกด้วย

ดังนั้น เมื่อมีการใช้คอมพิวเตอร์ในงานต่างๆมากขึ้น และข้อมูลที่ถูกเก็บไว้ในรูปแบบข้อมูลทางคอมพิวเตอร์มีปริมาณมากขึ้น ขณะเดียวกันการใช้คอมพิวเตอร์เพื่อติดต่อสื่อสารทั้งภายในและภายนอกองค์กรก็เป็นสิ่งจำเป็นในการบริหารงานในปัจจุบัน การเข้าถึงระบบคอมพิวเตอร์โดยผ่านการเชื่อมโยงในระบบเครือข่ายสามารถทำได้ง่ายและข้อมูลที่มีอยู่ก็มักถูกแบ่งปันแลกเปลี่ยนเพื่อความสะดวกในการปฏิบัติงานและติดตามข้อมูลได้อย่างรวดเร็วเช่นกัน โดยเฉพาะเมื่อมีแนวความคิดในการจัดระบบเครือข่ายและจัดเก็บข้อมูลให้ครบวงจรดังที่หน่วยงานในปัจจุบันนิยมทำกันคือการบริหารข้อมูลแบบเบ็ดเสร็จเพื่อที่จะทำให้การทำงานเสร็จสิ้นภายในหน่วยงานเดียวและเชื่อมต่อข้อมูลใหม่ๆได้ตลอดเวลา เช่น อาจมีการเชื่อมต่อข้อมูลที่เป็นข้อมูลของแต่ละหน่วยงานที่ทำงานอยู่ในองค์กรเดียวกันหรือระหว่างหน่วยงานภายนอกในการทำงานเพื่อให้การติดตามทางเดินของข้อมูลเป็นไปด้วยความสะดวก การค้นหาข้อมูลสามารถทำได้อย่างรวดเร็วและไม่ต้องติดต่อหน่วยงานหลายหน่วยงานจนทำให้เกิดความล่าช้าและการทำงานซ้ำซ้อนโดยไม่จำเป็น

เมื่อข้อมูลมีการเชื่อมต่อและแลกเปลี่ยนกันมากขึ้น การเข้าถึงข้อมูลต่างๆเหล่านี้ก็สามารถทำได้ง่ายและสะดวกสบายยิ่งขึ้นในหลายช่องทาง แม้ระบบเครือข่ายและการแบ่งปันข้อมูลจะมีข้อดีที่ทำให้การทำงานเป็นระบบและรวดเร็ว แต่ปัญหาที่เกิดขึ้นคือ การเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมีเจตนาที่ไม่สุจริตเกิดขึ้นได้บ่อยครั้งและกระทำได้ง่ายกว่าการเก็บรักษาข้อมูลในรูปแบบเดิม เมื่อมีการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ก็มักจะก่อให้เกิดความเสียหายตามมา โดยความเสียหายที่เกิดขึ้นอาจจะเป็นเรื่องความเป็นส่วนตัวหรือความลับส่วนตัวที่มีความเสียหายเล็กน้อย ความเสียหายทางด้านธุรกิจและการแข่งขันทางการค้า ตลอดจนเรื่องความมั่นคงของประเทศชาติซึ่งเป็นเรื่องที่มีความสำคัญอย่างมาก ทำให้รัฐต่างๆ มีความจำเป็นต้องบัญญัติกฎหมายเพื่อลงโทษผู้กระทำผิดดังกล่าวขึ้น แต่เนื่องจากความรับผิดในเรื่องการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ เป็นเรื่องใหม่สำหรับนักกฎหมายและเกี่ยวพันกับศาสตร์ทางด้านคอมพิวเตอร์ซึ่งเป็นศาสตร์ที่ว่าด้วยสิ่งที่ไม่มีรูปร่าง ขณะที่กฎหมายโดยทั่วไปนั้นการกำหนดความผิดมักเป็นเรื่องของสิ่งที่มีรูปร่างที่สามารถจับต้องได้เป็นหลักโดยเฉพาะในกฎหมายอาญา ทำให้ยากจะนิยามศัพท์ทางกฎหมายที่เหมาะสมและ

ครอบคลุมกับเทคโนโลยีที่เกิดขึ้นและยากต่อการกำหนดขอบเขตความรับผิดในการกระทำที่เกิดขึ้นว่าการกระทำอย่างไรที่กฎหมายควรกำหนดให้เป็นความผิดทางอาญา และมีวัตถุประสงค์ขอบเขตความรับผิดแค่ไหน เพียงใด นอกจากนี้ยังมีปัญหาเกี่ยวข้องกับเทคโนโลยีที่เคลื่อนไหวไปข้างหน้าอย่างรวดเร็วตลอดเวลา ในขณะที่กฎหมายจะมีลักษณะหยุดนิ่งทำให้เกิดความยากลำบากในการบังคับใช้

แม้เทคโนโลยีที่ทันสมัยทำให้สังคมพัฒนาไปอย่างรวดเร็ว แต่ขณะเดียวกันก็ทำให้การกระทำผิดมีรูปแบบที่หลากหลายมากขึ้น โดยการกระทำบางอย่างแม้จะก่อให้เกิดความเสียหายแต่กฎหมายอาญาในลักษณะเดิมไม่สามารถนำตัวผู้กระทำผิดมาลงโทษได้ เนื่องจากไม่มีกฎหมายรองรับว่าการกระทำดังกล่าวเป็นความผิดอาญา จึงไม่สามารถที่จะลงโทษได้ ประเทศไทยก็เล็งเห็นถึงความสำคัญของปัญหาดังกล่าว จึงได้มีการออกกฎหมายเกี่ยวกับความรับผิดการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ขึ้น โดยปรากฏอยู่ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่อย่างไรก็ตามพระราชบัญญัติดังกล่าวได้มีการแก้ไขเปลี่ยนแปลงมาหลายครั้งก่อนออกมาเป็นกฎหมาย ซึ่งยังมีปัญหาที่เป็นข้อถกเถียงและมีความเห็นที่แตกต่างกันในเรื่องความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ ทำให้การกระทำความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์โดย ยังมีปัญหาที่เกิดจากการตีความและบังคับใช้กฎหมายได้ในอนาคต และอาจทำให้ไม่สามารถดำเนินการนำตัวผู้กระทำผิดมารับโทษตามกฎหมายได้ หรืออาจทำให้บุคคลทั่วไปอาจต้องรับผิดตามพระราชบัญญัตินี้โดยกระทำสิ่งที่ตนคิดว่าสามารถทำได้แต่เป็นความผิดตามพระราชบัญญัตินี้ได้เนื่องจากความรับผิดในเรื่องดังกล่าวยังเป็นสิ่งใหม่ที่นักกฎหมายไม่คุ้นเคยจึงยากที่จะพิจารณาความรับผิดได้อย่างถูกต้องไม่คลุมเครือและเหมาะสมกับสภาพสังคมในปัจจุบัน

เนื่องจากการกำหนดกฎหมายที่เกี่ยวข้องกับเทคโนโลยีในยุคสมัยใหม่เป็นสิ่งที่ทำได้ยาก เพราะการเปลี่ยนแปลงทางเทคโนโลยีในอดีตอาจใช้เวลาเป็นร้อยปีจึงจะถึงจุดที่ทำให้สภาพสังคมเปลี่ยนรูปแบบไป มนุษย์ต้องใช้ระยะเวลาหลายร้อยปีที่จะเปลี่ยนจากเทคโนโลยีทางการเกษตรมาสู่เทคโนโลยีทางอุตสาหกรรม แต่การพัฒนาทางด้านคอมพิวเตอร์ทำให้การเปลี่ยนแปลงทางเทคโนโลยีใช้เวลาไม่ถึงสิบปี ตัวอย่างที่เห็นได้ชัดคือเทคโนโลยีในการสื่อสารที่ในปัจจุบันเป็นสิ่งที่พัฒนาอย่างก้าวกระโดด ง่ายต่อการเข้าถึง และเปลี่ยนแปลงอยู่ตลอดเวลา ในเวลาไม่กี่สิบปีคอมพิวเตอร์ทำให้การติดต่อสื่อสารระหว่างมนุษย์ที่อยู่คนละซีกโลกเป็นสิ่งที่ทำได้ในเวลาไม่กี่นาทีโดยนั่งอยู่ที่บ้านของตนก็ได้ สิ่งเหล่านี้ทำให้วิถีชีวิตของคนในสังคมเปลี่ยนรูปแบบ

ไป จึงเห็นได้ชัดว่าในขณะที่เทคโนโลยีเปลี่ยนแปลงแทบทุกนาที แต่กฎหมายกลับไล่ตามความเปลี่ยนแปลงนั้นได้อย่างล่าช้า ทำให้เกิดปัญหาต่างๆ ขึ้น ในการกำหนดหลักเกณฑ์ความรับผิดและบทลงโทษผู้กระทำผิดในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่ประเทศไทยบัญญัติขึ้นเพื่อป้องกันและปราบปรามการกระทำผิดเกี่ยวกับคอมพิวเตอร์ก็เช่นกัน ต้องมีการกำหนดกฎเกณฑ์ให้เหมาะสมโดยพิจารณาขอบเขตความรับผิดตามกฎหมายโดยกฎหมายจำเป็นต้องแยกผู้กระทำผิดออกจากบุคคลที่เป็นผู้ใช้คอมพิวเตอร์โดยทั่วไปให้ชัดเจน โดยลงโทษเฉพาะผู้ที่กระทำผิดอย่างแท้จริงเท่านั้น

เมื่อพิจารณาถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แล้ว ความผิดทางอาญาในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์อาจกล่าวได้ว่าเป็นการกระทำพื้นฐานของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และเป็นความผิดหลักที่ต้องมีอยู่ในการกำหนดความรับผิดเกี่ยวกับคอมพิวเตอร์โดยทั่วไป เพราะการกระทำความผิดเกี่ยวกับคอมพิวเตอร์โดยทั่วไปนั้นมักจะเริ่มที่การเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์แทบทั้งสิ้น เป็นการกระทำเริ่มแรกที่ก่อให้เกิดการกระทำความผิดฐานอื่นตามมา เมื่อการกระทำดังกล่าวยังเป็นการกระทำที่ไม่สามารถกำหนดได้ว่าเป็นความผิดฐานใดในกฎหมายอาญาที่มีอยู่ เพราะองค์ประกอบและฐานความผิดที่เปลี่ยนแปลงไป และกฎหมายอาญาไม่สามารถที่จะตีความครอบคลุมไปถึงเพื่อที่จะบ่งชี้ว่าการกระทำดังกล่าวเป็นความผิดได้ ในขณะเดียวกันพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่ออกมาบังคับใช้ก็ยังเป็นเรื่องใหม่ในสังคมไทย ยังต้องมีการพิจารณาว่าการกระทำใดเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และต้องรับผิดแค่ไหน เพียงใด เนื่องจากมีลักษณะที่แตกต่างจากกฎหมายอาญาโดยทั่วไป ทำให้มีปัญหาในการตีความถ้อยคำตามกฎหมายว่าการกระทำใดที่ถือว่าเป็นการกระความผิดโดยการเข้าถึงโดยมิชอบตามที่กฎหมายกำหนด

ด้วยเหตุนี้จึงเป็นเหตุจูงใจให้ข้าพเจ้าได้ทำการศึกษาพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในความผิดเกี่ยวกับการเข้าถึงโดยมิชอบ โดยในวิทยานิพนธ์ฉบับนี้ผู้เขียนมุ่งที่จะศึกษาว่าการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมีความหมายครอบคลุมเพียงใด การกระทำจึงจะถือว่าเป็นการเข้าถึง และการกระทำใดเป็นการเข้าถึงโดยมิชอบที่เป็นความผิดตามกฎหมาย เนื่องจากผู้เขียนมีความเห็นว่าความรับผิดทางอาญาในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์เป็นความผิดพื้นฐานโดยทั่วไปของการกระทำความผิดทางคอมพิวเตอร์ที่เกิดขึ้น เพราะการกระทำผิดทางด้าน

คอมพิวเตอร์โดยมากมักจะเริ่มจากการเข้าไปในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์แทบทั้งสิ้น ซึ่งหลังจากการเข้าไปแล้วก็จะมีการกระทำความผิดต่างๆตามมา เช่น การขโมย การเปลี่ยนแปลง การทำลาย การกลั่นแกล้ง หรือแม้แต่การจับข้อมูลเป็นตัวประกันเพื่อเรียกร้องบางสิ่งบางอย่างจากเจ้าของข้อมูล

ดังนั้นผู้เขียนจึงมุ่งจะศึกษาเกี่ยวกับการกำหนดความรับผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ว่ามีองค์ประกอบความรับผิดเช่นใดตามกฎหมาย และการกำหนดองค์ประกอบดังกล่าวมีความเหมาะสมกับการกระทำผิดที่เกิดขึ้นในปัจจุบันหรือไม่ และมีขอบเขตความรับผิดเพียงใด การกระทำเช่นใดจึงถือว่าเป็นความผิดตามกฎหมายและควรมีการตีความอย่างไร ความผิดสำเร็จเมื่อใด บุคคลใดบ้างที่กฎหมายกำหนดให้ต้องรับผิดหรือต้องรับโทษ และสามารถตีความกฎหมายให้ใช้บังคับได้จริงเมื่อเกิดการกระทำความผิดขึ้นโดยสามารถแยกผู้กระทำผิดออกจากผู้ใช้คอมพิวเตอร์โดยทั่วไปเพื่อไม่ให้เกิดปัญหาในการใช้และตีความกฎหมายเนื่องจากความผิดดังกล่าวเป็นเรื่องใหม่ในกฎหมายซึ่งถ้าจะมีการบังคับใช้ก็ต้องมีการศึกษาเพื่อให้มีขอบเขตในการใช้กฎหมายที่ชัดเจนต่อไป

1.2 สมมติฐานของการวิจัย

ความรับผิดทางอาญาในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ยังมีปัญหาในการตีความกฎหมายเพื่อนำมาบังคับใช้และยังไม่สามารถแก้ไขปัญหาการตีความในความผิดเกี่ยวกับการเข้าถึง โดยเฉพาะอย่างยิ่งคำว่า “การเข้าถึง” และ “โดยมิชอบ” ได้ จึงจำเป็นต้องศึกษาหาแนวทางในการตีความให้ชัดเจนยิ่งขึ้น

1.3 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาวิเคราะห์ถึงแนวความคิดและทฤษฎีของการกำหนดความรับผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ว่ามีแนวคิดและทฤษฎีเช่นใด เหตุใดจึงควรมีการกำหนดเป็นความผิดทางอาญา

2. เพื่อศึกษาวิเคราะห์ถึงลักษณะความรับผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ว่าเป็นเช่นไร การกระทำเช่นใดจึงควรกำหนดเป็นความผิดทางอาญา

3. เพื่อศึกษาวิเคราะห์ถึงหลักเกณฑ์และขอบเขตความรับผิดของบุคคลที่การเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ว่าบุคคลใดบ้างที่ต้องรับผิดทางกฎหมาย และมีขอบเขตแค่ไหน เพียงใด

4. เพื่อศึกษาวิเคราะห์ถึงนโยบาย โครงสร้าง มาตรการทางกฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในส่วนของการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ขององค์การสหประชาชาติ (UN) ข้อตกลง (DIRECTIVE) ของกลุ่มประเทศยุโรป (EC) ประเทศสหรัฐอเมริกา ประเทศเยอรมัน และประเทศอังกฤษ เทียบเคียงกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

5. เพื่อศึกษาวิเคราะห์ถึงแนวทางในการกำหนดกฎเกณฑ์ทางกฎหมาย การตีความกฎหมายในความผิดเกี่ยวกับเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ว่าควรมีหลักเกณฑ์ความรับผิดอย่างไรและควรตีความอย่างไร และปัญหาที่อาจเกิดขึ้นจากการบัญญัติและการตีความในความผิดฐานเข้าถึงโดยมิชอบตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในอนาคต

1.4 ขอบเขตของการวิจัย

วิทยานิพนธ์ฉบับนี้จะศึกษาถึงนิยามศัพท์คอมพิวเตอร์ที่จะนำมาใช้กำหนดเป็นนิยามศัพท์ทางกฎหมาย ทฤษฎีต่างๆที่เกี่ยวข้องเพื่อกำหนดว่าความรับผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ควรมีลักษณะอย่างไร และการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์สามารถทำได้ในกรณีใดบ้าง ผู้กระทำต้องรับผิดเมื่อใด ศึกษาถึงกฎหมายต่างประเทศว่ามีอย่างไร โดยศึกษาข้อตกลงขององค์การสหประชาชาติ ข้อตกลงของกลุ่มสหภาพยุโรป กฎหมายของประเทศสหรัฐอเมริกา ประเทศเยอรมัน และประเทศอังกฤษ โดยนำมาเทียบเคียงกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550 ว่ามีส่วนใดที่ควรจะมีการแก้ไขเพิ่มเติมโดยคำนึงว่ากฎหมายไม่ควรจำกัดขอบเขตมากจนทำให้ประชาชนขาดความสนใจในเทคโนโลยีสมัยใหม่แต่ขณะเดียวกันต้องสามารถนำตัวผู้กระทำผิดมาลงโทษได้

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้เข้าใจแนวความคิดและทฤษฎีของการความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

2. ทำให้เข้าใจถึงลักษณะการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์มีลักษณะอย่างไร การกระทำเช่นใดจึงควรบัญญัติเป็นความผิด ทำให้เกิดความชัดเจนในการกำหนดกฎหมาย สามารถพิจารณาถึงลักษณะความผิดที่เกิดขึ้นได้ถูกต้อง

3. ทำให้เข้าใจว่าบุคคลใดบ้างที่ต้องรับผิดในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ และต้องรับผิดแค่ไหน เพียงใด

4. ทำให้เห็นถึงแนวทางในการกำหนดหลักเกณฑ์ ความรับผิดทางอาญาในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ของประเทศต่างๆ และการบังคับใช้กฎหมาย เพื่อเป็นแนวทางในการกำหนดและบังคับใช้ตามกฎหมายไทย ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

5. ทำให้เห็นถึงแนวทางในการกำหนดกฎเกณฑ์ทางกฎหมาย การตีความกฎหมายในความผิดเกี่ยวกับเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ว่าควรมีหลักเกณฑ์ความรับผิดอย่างไรและควรตีความอย่างไร ทำให้การบัญญัติและการตีความกฎหมายเพื่อบังคับเกิดความชัดเจนและมีความเหมาะสมกับสถานการณ์ในปัจจุบัน ไม่ก่อให้เกิดปัญหาจากการการบัญญัติและการตีความในความผิดฐานเข้าถึงโดยมิชอบตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในอนาคต

1.6 วิธีดำเนินการวิจัย

วิธีการวิจัยเป็นการวิจัยเอกสาร (Documentary Research) และการวิจัยเชิงคุณภาพ (Qualitative Research) โดยการสัมภาษณ์เชิงลึก (In-depth Interview) กล่าวคือ เป็นการวิจัยโดยการสัมภาษณ์ผู้เชี่ยวชาญ ศึกษาและวิเคราะห์ข้อมูลจากหนังสือ บทความ คำพิพากษาของศาลในต่างประเทศและเอกสารต่างๆที่เกี่ยวข้อง ตลอดจนกฎหมายที่เกี่ยวข้อง ทั้งนี้ไม่ว่าจะเป็นกฎหมายของประเทศต่างๆ และกฎหมายของประเทศไทย ในลักษณะการนำมาใช้โดยตรงและเปรียบเทียบประกอบกับความคิดเห็นของนักกฎหมายและบุคคลที่เกี่ยวข้องเพื่อให้การทำวิทยานิพนธ์นี้สมบูรณ์ที่สุด

บทที่ 2
ความหมายของการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

ตั้งแต่มนุษย์รู้จักคอมพิวเตอร์ในฐานะนวัตกรรมใหม่ที่พัฒนาขึ้นอย่างรวดเร็วในเวลาไม่กี่สิบปี คอมพิวเตอร์ได้ถูกประดิษฐ์ คิดค้น และเพิ่มประสิทธิภาพขึ้นอย่างกว้างขวางและต่อเนื่อง ทำให้เกิดเทคโนโลยีและอุปกรณ์อำนวยความสะดวกอื่นๆ เป็นจำนวนมาก ส่งผลให้มนุษย์เปลี่ยนแปลงพฤติกรรมการดำรงชีวิตในสังคมไปจากเดิมโดยสิ้นเชิง ทั้งในแง่การทำงานและการใช้ชีวิตประจำวันโดยทั่วไป เช่น ในการทำงานในปัจจุบันงานบางประเภทก็สามารถทำที่บ้านได้โดยไม่จำเป็นต้องไปที่ทำงาน การประชุมทางไกลโดยผ่านระบบคอมพิวเตอร์ทำให้ผู้ประชุมที่อยู่ในสถานที่ต่างกันสามารถทำการประชุมร่วมกันได้โดยไม่จำเป็นต้องอยู่ในห้องประชุมด้วยกัน ฯลฯ ระยะทางจึงไม่ใช่อุปสรรคในการติดต่อสื่อสารในโลกปัจจุบันอีกต่อไป

อาจกล่าวได้ว่าคอมพิวเตอร์ทำให้โลกเล็กและแคบลง มนุษย์สามารถติดต่อพูดคุยรวมถึงสามารถเห็นภาพของบุคคลที่อยู่ห่างกันเป็นซีกโลกได้ โดยภาพที่ปรากฏที่ไม่แตกต่างจากการติดต่อในโลกแห่งความเป็นจริงที่ต้องมีการพบปะพูดคุยกัน ทำให้มนุษย์มีปฏิสัมพันธ์กันทางโลกเสมือนผ่านคอมพิวเตอร์มากขึ้นจนกลายเป็นสังคมอีกสังคมหนึ่งที่เกิดขึ้น ซึ่งสังคมที่เกิดขึ้นใหม่นี้ยังมีปัญหามากมายที่ต้องได้รับการแก้ไข เนื่องจากเป็นสิ่งใหม่ที่มนุษย์ยังไม่เข้าใจและไม่สามารถจับต้องได้จริงหากแต่สามารถเห็นหรือมีส่วนร่วมได้ เมื่อยังไม่มีกฎเกณฑ์และกฎระเบียบที่เป็นที่ยอมรับกันโดยทั่วไป มนุษย์จึงพยายามหาเส้นแบ่งที่เหมาะสมสำหรับโลกที่เกิดขึ้นใหม่นี้ สิ่งหนึ่งที่กลายเป็นปัญหาหลักสำหรับสังคมใหม่ในโลกเสมือนนี้ คือ อาชญากรรม เพราะว่าที่ใดที่มีคนมาอยู่ร่วมกันย่อมมีการกระทบกระทั่งและมีการกระทำผิดขึ้น จึงต้องมีกฎหมายมาบังคับให้คนอยู่ร่วมกันอย่างปกติสุข แต่อย่างไรก็ตามยังมีความแตกต่างทางแนวคิดในมุมมองของโลกเสมือนนี้ว่าจะเหมือนหรือแตกต่างกับโลกแห่งความเป็นจริงอย่างไร สามารถนำวิธีการและหลักเกณฑ์ที่มีอยู่ในปัจจุบันมาใช้กับโลกเสมือนนี้ได้หรือไม่ และควรจะมีมาตรฐานอย่างไรจึงจะเหมาะสม

ในปัจจุบันจึงมีความพยายามที่จะกำหนดกฎเกณฑ์ใหม่ขึ้นสำหรับโลกเสมือนเหล่านี้ รวมถึงการควบคุมอาชญากรรมเช่นเดียวกัน มีความพยายามตั้งกฎเกณฑ์ว่าการกระทำใดที่ถือว่าเป็นอาชญากรรม และควรมีการกำหนดกฎเกณฑ์ทางกฎหมายอย่างไรเพื่อที่จะนำตัวผู้กระทำผิดมาลงโทษเนื่องจากสิ่งที่สำคัญในความคิดของคนทั่วไปในการมีตัวตนในโลกเสมือนคือการได้แสดงออกซึ่งสิทธิเสรีภาพของตนอย่างเต็มที่ สามารถทำอะไรก็ได้ โดยคิดว่าเป็นสิทธิส่วนบุคคล การกระทำสิ่งใดลงไปหรือรับรู้ข้อมูลผ่านคอมพิวเตอร์ของตนเองถือเป็นเรื่องส่วนตัว ซึ่งจะ

ทำให้เกิดความขัดแย้งเสมอว่าเป็นความจริงหรือไม่ เนื่องจากแม้จะเป็นคอมพิวเตอร์ส่วนตัวอยู่ในห้องส่วนตัวของตนเอง หากแต่สิ่งที่กระทำลงหรือได้รับรู้กลับไม่มีขอบเขต บุคคลไม่ว่าอยู่ที่ใดก็สามารถเข้าถึงข้อมูลต่างๆ ได้โดยปราศจากข้อจำกัดทางด้านกายภาพเหมือนในอดีต เช่น ในอดีตหากมีความต้องการหาข้อมูลทางด้านการแพทย์เบื้องต้น ก็ต้องเดินทางไปที่โรงพยาบาลเพื่อติดต่อสอบถามหรือไปซื้อหนังสือทางการแพทย์มาอ่าน แต่ในปัจจุบันเพียงแค่นั่งอยู่หน้าคอมพิวเตอร์ในบ้านและค้นหาทางอินเทอร์เน็ตก็สามารถหาข้อมูลเบื้องต้นได้เพียงพอโดยไม่ต้องเดินทางไปไหนและไม่มีข้อจำกัดเรื่องเวลา แต่ขณะที่คอมพิวเตอร์ให้ประโยชน์มหาศาล ในทางตรงกันข้ามการใช้คอมพิวเตอร์ในทางที่ไม่ดีก็ย่อมให้โทษได้เช่นกัน มีข้อมูลหลายประเภทที่อยู่ในอินเทอร์เน็ตที่เป็นข้อมูลส่วนตัวหรือมีความสำคัญที่อาจไม่ต้องการให้บุคคลทั่วไปรับรู้ หากแต่ก็มีบุคคลบางประเภทสามารถเข้าถึงข้อมูลต่างๆ เหล่านั้นได้ และอาจนำมาใช้ประโยชน์ส่วนตัวในทางที่ผิดจนอาจจะกลายเป็นอาชญากรรมขึ้น และทำให้รัฐต้องนำตัวผู้กระทำผิดมาลงโทษ

อย่างไรก็ตามสิ่งที่เป็นปัญหาสำหรับการกำหนดความรับผิดในการกระทำผิดเกี่ยวกับคอมพิวเตอร์นั้นเป็นสิ่งยุ่งยาก เนื่องจากปัญหาทางด้านทัศนคติของบุคคลที่ยากจะหาเส้นแบ่งระหว่างอาชญากรรมและสิทธิเสรีภาพส่วนบุคคล โดยการพัฒนาทางระบบคอมพิวเตอร์ก่อให้เกิดปัญหาอาชญากรรมใหม่ๆ ขึ้นอย่างที่ไม่เคยปรากฏมาก่อนในอดีต เดิมการก่ออาชญากรรมเป็นสิ่งที่เกิดขึ้นในสังคมภายนอก แต่ในสถานที่ที่เป็นส่วนตัว เช่น สถานที่ทำงานหรือที่บ้าน โดยทั่วไปแล้วมนุษย์จะรู้สึกปลอดภัยและเชื่อว่าไม่มีอันตราย แต่ด้วยพัฒนาการของคอมพิวเตอร์ ทำให้อาชญากรรมสามารถเกิดขึ้นได้แม้ในโต๊ะทำงานหรือห้องนอนของบุคคลนั้นเอง เช่น แฮกเกอร์สามารถกระทำความผิดได้โดยการเจาะเข้าไปในระบบของบุคคลอื่นผ่านระบบเครือข่ายโดยไม่มีความจำเป็นจะต้องอยู่ในสถานที่ที่ข้อมูลถูกเก็บอยู่ และสามารถทำความเสียหาย ขโมยข้อมูลหรือเปลี่ยนแปลงข้อมูลของบุคคลอื่นได้

โดยบุคคลที่ถูกเรียกว่า “แฮกเกอร์” เป็นถ้อยคำที่มีมาไม่กี่สิบปีนับแต่เกิดการพัฒนาทางด้านคอมพิวเตอร์ขึ้น แต่ได้กลายเป็นที่รู้จักกันอย่างแพร่หลาย และก่อให้เกิดความเสียหายอย่างมากในปัจจุบันโดยเฉพาะทางด้านเศรษฐกิจ เนื่องจากในปัจจุบันการทำธุรกรรมออนไลน์ต่างๆ ผ่านทางคอมพิวเตอร์เป็นสิ่งทำกันอย่างกว้างขวาง เพราะก่อให้เกิดความสะดวกสบายแก่ผู้ให้และผู้รับบริการ แต่ในขณะเดียวกันก็เปิดโอกาสให้ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลต่างๆได้ง่ายขึ้นเช่นกัน โดยผู้กระทำผิดสามารถกระทำผิดได้ทั้งที่อยู่ที่บ้านของตนเอง จึงทำให้การกระทำผิดทำได้อย่างสะดวก ใช้เวลาเท่าใดก็ได้ และยากจะติดตามหาผู้กระทำผิด ซึ่งทำให้เกิดปัญหาในการนำตัวผู้กระทำผิดมารับโทษ

ด้วยความจำเป็นดังกล่าวจึงต้องมีการบัญญัติกฎหมายเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ขึ้น แต่เนื่องจากคำว่า “คอมพิวเตอร์” เป็นสิ่งใหม่ในกฎหมายและเกี่ยวพันกับศาสตร์อื่นคือศาสตร์เกี่ยวกับคอมพิวเตอร์ จึงมีความจำเป็นต้องทำความเข้าใจความหมายของของคำต่างๆ ที่ปรากฏอยู่ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ว่ามีความหมายครอบคลุมเพียงใดทั้งในด้านศาสตร์ทางคอมพิวเตอร์และทางด้านกฎหมายเพื่อที่จะเปรียบเทียบหาความหมายที่ถูกต้องเหมาะสมในการบังคับใช้กฎหมายต่อไป โดยคำที่กฎหมายนำศัพท์ทางคอมพิวเตอร์มาใช้และให้นิยามไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 คือคำว่า “ระบบคอมพิวเตอร์” และ “ข้อมูลคอมพิวเตอร์” ซึ่งอาจพิจารณาได้ดังนี้

2.1 ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์เป็นศัพท์ทางศาสตร์เกี่ยวกับคอมพิวเตอร์ซึ่งมีลักษณะเป็นภาษาเทคนิคที่มีความหมายพิเศษต่างไปจากภาษาธรรมดา เมื่อกฎหมายนำมากำหนดเป็นคำนิยามในกฎหมาย จึงต้องทำความเข้าใจเกี่ยวกับลักษณะและความหมายของคำดังกล่าวเพื่อให้สามารถแยกแยะได้ว่าสิ่งใดคือระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ ทั้งในความหมายในทางศาสตร์เกี่ยวกับคอมพิวเตอร์และทางด้านกฎหมายเพื่อให้ทราบความหมายที่ถูกต้องจึงเป็นเรื่องสำคัญ แม้ว่าในภาษาที่ใช้กันอยู่ทั่วไปหรือในศาสตร์อื่นๆ นั้นการให้คำนิยามอาจจะไม่ใช่เรื่องสำคัญมากนัก แต่ในกฎหมายโดยเฉพาะในกฎหมายอาญาแล้วเป็นเรื่องสำคัญมากเนื่องจากกฎหมายอาญาคือกฎเกณฑ์ที่จะลงโทษบุคคลในสังคม หากไม่ชัดเจนหรือไม่เข้าหลักเกณฑ์ที่กำหนดห้ามไว้ก็ไม่สามารถลงโทษ และไม่สามารถที่จะอนุมานหรือตีความถ้อยคำในกฎหมายให้กว้างเพื่อลงโทษบุคคลใดๆ โดยไม่มีกฎหมายกำหนดไว้ชัดเจนได้ เนื่องจากเป็นการจำกัดอำนาจรัฐไม่ให้ล่วงล้ำสิทธิเสรีภาพของบุคคลได้อย่างไม่มีขอบเขตจำกัด

ดังนั้นก่อนที่จะไปพิจารณาถึงคำนิยามทางด้านกฎหมายต่อไป ผู้เขียนก็จะเริ่มพิจารณาจากคำว่า “ระบบคอมพิวเตอร์” ในศาสตร์ทางคอมพิวเตอร์ก่อนเพื่อความเข้าใจ ดังนี้

2.1.1 ระบบคอมพิวเตอร์

เนื่องจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่มีคำว่า “คอมพิวเตอร์” แต่มีคำว่า “ระบบคอมพิวเตอร์” แทน ซึ่งโดยปกติแล้วถ้อยคำที่คนทั่วไปคุ้นเคยคือคำว่า “คอมพิวเตอร์” ดังนั้นก่อนที่จะพิจารณาถึงคำว่า “ระบบคอมพิวเตอร์”

เราคงจะต้องมาพิจารณาคำว่า “คอมพิวเตอร์” ให้ชัดเจนในแง่ของศาสตร์ทางคอมพิวเตอร์ก่อน ว่า คำว่า “คอมพิวเตอร์” มีความหมายว่าอย่างไร ก่อนที่จะไปพิจารณาถึงคำว่า “ระบบคอมพิวเตอร์” ว่ามีความหมายว่าอย่างไร เพื่อที่จะสามารถพิจารณาว่าคำว่า “คอมพิวเตอร์” กับคำว่า ”ระบบคอมพิวเตอร์” ในศาสตร์ทางคอมพิวเตอร์ได้ว่ามีความหมายเหมือนกันหรือต่างกันอย่างไร

คำว่า “คอมพิวเตอร์” เป็นศัพท์ใหม่ที่เกิดมาไม่กี่สิบปี เป็นอุปกรณ์อิเล็กทรอนิกส์ที่ใช้เวลาพัฒนาไม่นานจนกลายเป็นอุปกรณ์ที่พบเห็นและใช้กับทั่วไป โดยในปัจจุบันได้เป็นที่ยอมรับและคนในสังคมก็คุ้นเคยกับคำว่า “คอมพิวเตอร์” พอสมควรจนมีการใช้ทับศัพท์ในภาษาไทยว่า “คอมพิวเตอร์” แทนคำว่า “computer” ในภาษาอังกฤษและใช้แพร่หลายทั่วไป ดังนั้นการที่จะเข้าใจว่าคอมพิวเตอร์คืออะไร คงจะต้องพิจารณาถึงความหมายในภาษาต่างประเทศ ลักษณะเฉพาะที่เป็นเครื่องบ่งชี้ว่าอุปกรณ์ใดถือเป็นคอมพิวเตอร์ และอุปกรณ์อิเล็กทรอนิกส์ที่ถือว่าเป็นคอมพิวเตอร์เสียก่อน เพื่อที่จะสามารถหาความหมายของคอมพิวเตอร์ได้

2.1.1.1 **ความหมายของระบบคอมพิวเตอร์**

จะเห็นได้ว่าคอมพิวเตอร์มีพัฒนาการมาอย่างรวดเร็วตามเทคโนโลยีที่พัฒนาขึ้น โดยมีความพยายามในการให้ความหมายของคำว่า “คอมพิวเตอร์” ขึ้น โดยคอมพิวเตอร์มาจากภาษาละตินว่า Computare ซึ่งหมายถึง การนับหรือการคำนวณ[1] และถ้าจะพิจารณาตามคำศัพท์ภาษาอังกฤษ คำว่า “คอมพิวเตอร์” (Computer) มีการให้ความหมายไว้หลากหลาย ดังต่อไปนี้

คอมพิวเตอร์ตามรูปศัพท์ภาษาอังกฤษ (Computer) หมายถึง ผู้คำนวณ ซึ่งหมายถึง อุปกรณ์ที่ใช้ในการคำนวณ เช่น การบวก ลบ คูณ หาร โดยหากจะพิจารณาเพียงเท่านี้คอมพิวเตอร์ก็เป็นแค่เครื่องคิดเลขธรรมดาเครื่องหนึ่ง และถ้ากล่าวอย่างกว้างๆ เครื่องคำนวณที่มีส่วนประกอบเป็นเครื่องกลไกหรือเครื่องไฟฟ้าต่างก็จัดเป็นคอมพิวเตอร์ได้ทั้งสิ้น ไม่ว่าจะเป็นลูกคิดที่เคยใช้กันในร้านค้า ไม้บรรทัดคำนวณ (slide rule) ซึ่งถือเป็นเครื่องมือประจำตัววิศวกรในยุคยี่สิบปีก่อน หรือเครื่องคิดเลข ล้วนเป็นคอมพิวเตอร์ได้ทั้งหมด แต่ในความเป็นจริงโดยทั่วไปคอมพิวเตอร์มีคุณลักษณะและความสามารถดีกว่าเครื่องคิดเลขหลายร้อยเท่าและมีความหมายเฉพาะเจาะจง ดังนั้นคอมพิวเตอร์จึงอาจให้ความหมายได้ว่า "เครื่องคำนวณอิเล็กทรอนิกส์ที่มี

---

[1] “ความหมายของคอมพิวเตอร์ Chapter 1,” E-learning [Online] แหล่งที่มา : http://isc.dopa.go.th/iad [15 ตุลาคม 2550]

การทำงานแบบอัตโนมัติ ทำหน้าที่เหมือนสมองกล สามารถแก้ปัญหาต่าง ๆ ทั้งที่ง่ายและซับซ้อนตามคำสั่งของโปรแกรม"

แต่ในพจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2525 ได้ให้คำจำกัดความของคอมพิวเตอร์ไว้ค่อนข้างกะทัดรัดว่า "เครื่องอิเล็กทรอนิกส์แบบอัตโนมัติ ทำหน้าที่เสมือนสมองกล ใช้สำหรับแก้ปัญหาต่าง ๆ ทั้งที่ง่ายและซับซ้อนโดยวิธีทางคณิตศาสตร์"

ในขณะที่พจนานุกรมศัพท์คอมพิวเตอร์ฉบับราชบัณฑิตยสถาน พ.ศ. 2540 ให้คำทับศัพท์คำว่า “คอมพิวเตอร์” ในภาษาอังกฤษที่กำหนดเป็นภาษาไทยว่า “คณิตกรณ์” ซึ่งก็คือ เครื่องอิเล็กทรอนิกส์แบบอัตโนมัติใช้สำหรับแก้ปัญหาต่างๆ โดยวิธีทางคณิตศาสตร์สมองกล[2]

ในขณะเดียวกันก็มีบุคคลให้คำนิยามคำว่า “คอมพิวเตอร์” ไว้หลากหลาย เช่น คอมพิวเตอร์ หมายถึง เครื่องอิเล็กทรอนิกส์ที่มีสมรรถนะในการประมวลผลของข้อมูลได้อย่างอัตโนมัติ โดยอาศัยคำสั่งหรือชุดคำสั่งที่เขียนขึ้นมาเป็นโปรแกรมกำหนดเงื่อนไขให้คอมพิวเตอร์ทำงานอย่างเป็นระบบด้วยความรวดเร็ว ถูกต้อง ในการจดจำข้อมูล คิดคำนวณทางคณิตศาสตร์ การเคลื่อนย้ายข้อมูล และการพิมพ์ผลลัพธ์ออกมา ไม่ว่าจะมีการกำหนดในเรื่องความจำข้อมูลหรือคำสั่งต่างๆสลับซับซ้อนเพียงใดก็ตาม เครื่องคอมพิวเตอร์สามารถทำงานให้ได้ผลออกมาอย่างถูกต้อง ถ้าข้อมูลและคำสั่งที่ป้อนเข้าไปในเครื่องนั้นมีความถูกต้อง[3]

ส่วนนิยามของคอมพิวเตอร์ ตามพจนานุกรมอิเล็กทรอนิกส์ของนายรูดอล์ฟ เอฟ แกรฟ ให้ความหมายไว้ว่า เป็นอุปกรณ์ใดๆ ก็ได้ที่สามารถรับข้อมูลเข้าไปประมวลผลแล้วให้ผลลัพธ์อยู่ในรูปแบบที่เราต้องการ ชิ้นส่วนหลักที่ประกอบขึ้นเป็นคอมพิวเตอร์จะประกอบด้วยหน่วยความจำ หน่วยควบคุม หน่วยคำนวณผล หน่วยรับข้อมูล และหน่วยแสดงผล[4]

จะเห็นได้ว่าคำว่า “คอมพิวเตอร์” มีคนให้ความหมายไว้อย่างหลากหลายโดยเป็นการขยายถึงรายละเอียดความสามารถของคอมพิวเตอร์ในการทำงาน ซึ่งในช่วงระยะเวลาที่

---

[2] วิทย์ เที่ยงบูรณธรรม, พจนานุกรม ไทย-อังกฤษ (กรุงเทพมหานคร : รวมสาสน์ (1977), 2535), หน้า 248.

[3] พีรพันธุ์ เปรมภูติ, “เอกสารประกอบการสัมมนาเรื่องสภาพปัญหาอาชญากรรมทางคอมพิวเตอร์,” 10 กันยายน 2539, หน้า 4.

[4] ยืน ภู่วรวรรณ และคณะ, โปรแกรมคอมพิวเตอร์ภาษาเบสิค (กรุงเทพมหานคร : ซีเอ็ดยูเคชั่น, 2527), หน้า 7.

คอมพิวเตอร์เพิ่งเป็นที่รู้จัก รูปลักษณ์และระบบการทำงานมีความชัดเจนที่แตกต่างจากอุปกรณ์อิเล็กทรอนิกส์อื่น คงจะเป็นการง่ายที่จะกำหนดว่าสิ่งใดคือคอมพิวเตอร์และสิ่งใดไม่ใช่ หากแต่ในปัจจุบัน ระบบปฏิบัติการของคอมพิวเตอร์ถูกนำมาใช้เพื่อเพิ่มประสิทธิภาพในอุปกรณ์ต่างๆ เช่น โทรศัพท์มือถือ เครื่องโทรสาร เครื่องเล่นเกม ฯลฯ เพื่อให้สามารถเติมเต็มความต้องการของผู้บริโภคได้อย่างไม่มีขอบเขตจำกัด ดังจะเห็นได้จากโทรศัพท์มือถือในปัจจุบัน สามารถที่จะเล่นเกม ฟังเพลง ดูหนัง รวมไปถึงการเชื่อมต่ออินเทอร์เน็ต ซึ่งคุณสมบัติต่างๆดังที่กล่าวมาในอดีตเป็นสิ่งที่ต้องทำด้วยเครื่องคอมพิวเตอร์ จึงอาจมีคำถามตามมาว่า สิ่งเหล่านี้เป็นคอมพิวเตอร์หรือไม่

หากจะพิจารณาจากการวิเคราะห์ศัพท์คำว่า “คอมพิวเตอร์” ที่ได้กล่าวมาข้างต้นแล้ว แม้จะเป็นการยากที่จะชี้ชัดว่าสิ่งใดเป็นคอมพิวเตอร์ โดยเฉพาะหากจะพิจารณาจากคำนิยามที่มีผู้ให้นิยามไว้อย่างเดียว เนื่องจากการให้คำนิยามดังกล่าวค่อนข้างกว้างและอุปกรณ์อิเล็กทรอนิกส์ที่มีอยู่ทั่วไปมีจำนวนมาก ยากที่จะยกอุปกรณ์ทุกอย่างขึ้นมาพิจารณาว่าเป็นคอมพิวเตอร์หรือไม่ ดังนั้นหากจะแยกคอมพิวเตอร์ออกจากอุปกรณ์อิเล็กทรอนิกส์อื่นนั้น ผู้เขียนมีความเห็นว่า ควรพิจารณาจากคุณลักษณะบางอย่างที่เป็นคุณสมบัติพื้นฐานของคอมพิวเตอร์ โดยพิจารณาว่าหากอุปกรณ์มีคุณสมบัติพื้นฐานครบถ้วนตามหลักเกณฑ์แล้ว ก็จะถือว่าอุปกรณ์ดังกล่าวคือ คอมพิวเตอร์ โดยหลักเกณฑ์ที่จะนำมาแยกแยะว่าอุปกรณ์ใดเป็นคอมพิวเตอร์ออกจากอุปกรณ์อิเล็กทรอนิกส์อื่นๆ ได้นั้น ผู้เขียนเห็นว่า สิ่งที่จะเรียกว่าเป็นคอมพิวเตอร์ได้ ต้องพิจารณาจากระบบการทำงานของอุปกรณ์อิเล็กทรอนิกส์ดังกล่าวเป็นสำคัญ ดังนั้นก่อนที่จะไปพิจารณาว่าอุปกรณ์อิเล็กทรอนิกส์ใดเป็นคอมพิวเตอร์ คงต้องพิจารณาถึงระบบการทำงานและประเภทของคอมพิวเตอร์ก่อนว่ามีลักษณะอย่างไร เพื่อนำไปใช้แยกคอมพิวเตอร์ออกจากเครื่องใช้อิเล็กทรอนิกส์อื่นต่อไป โดยจะเริ่มจากระบบการทำงานของคอมพิวเตอร์ ซึ่งอาจพิจารณาได้ดังนี้

2.1.1.2 ระบบการทำงานของคอมพิวเตอร์[5]

[5] “หลักสูตรการใช้คอมพิวเตอร์ ตอนที่ 1,” ชุดการเรียนรู้ทางไกล ประเภทการศึกษาต่อเนื่อง [Online] แหล่งที่มา : http://202.143.141.237/etraining/courses/8/chap1.htm [20 ธันวาคม 2550]

คอมพิวเตอร์ไม่ว่าจะเป็นประเภทใดก็ตาม จะมีลักษณะการทำงานของส่วนต่างๆ ที่มีความสัมพันธ์กันเป็นกระบวนการ โดยมีองค์ประกอบพื้นฐานหลักคือ รับข้อมูลเข้า (Input) ประมวลผลข้อมูล (Process) และ แสดงผลลัพธ์ (Output) โดยมีขั้นตอนดังนี้

ขั้นตอนที่ 1 : **รับข้อมูลเข้า** (Input)

เริ่มต้นด้วยการนำข้อมูลเข้าเครื่องคอมพิวเตอร์ ซึ่งสามารถผ่านทางอุปกรณ์ชนิดต่างๆ แล้วแต่ชนิดของข้อมูลที่จะป้อนเข้าไป เช่น ถ้าเป็นการพิมพ์ข้อมูลจะใช้แผงแป้นพิมพ์ (Keyboard) เพื่อพิมพ์ข้อความหรือโปรแกรมเข้าเครื่อง ถ้าเป็นการเขียนภาพจะใช้เครื่องอ่านพิกัดภาพกราฟิก (Graphics Tablet) โดยมีปากกาชนิดพิเศษสำหรับเขียนภาพ หรือถ้าเป็นการเล่นเกมก็จะมีก้านควบคุม (Joystick) สำหรับเคลื่อนตำแหน่งของการเล่นบนจอภาพ เป็นต้น

ขั้นตอนที่ 2 : **ประมวลผลข้อมูล** (Process)

เมื่อนำข้อมูลเข้ามาแล้ว เครื่องจะดำเนินการกับข้อมูลตามคำสั่งที่ได้รับมาเพื่อให้ได้ผลลัพธ์ตามที่ต้องการ การประมวลผลอาจจะมีได้หลายอย่าง เช่น นำข้อมูลมาหาผลรวม นำข้อมูลมาจัดกลุ่มนำข้อมูลมาหาค่ามากที่สุดหรือน้อยที่สุด เป็นต้น

ขั้นตอนที่ 3 : **แสดงผลลัพธ์** (Output)

เป็นการนำผลลัพธ์จากการประมวลผลมาแสดงให้ทราบทางอุปกรณ์ที่กำหนดไว้ โดยทั่วไปจะแสดงผ่านทางจอภาพ หรือเรียกกันโดยทั่วไปว่า "จอมอนิเตอร์" (Monitor) หรือจะพิมพ์ข้อมูลออกทางกระดาษโดยใช้เครื่องพิมพ์ก็ได้

เมื่อพิจารณาถึงระบบการทำงานของคอมพิวเตอร์แล้ว อาจแยกประเภทของคอมพิวเตอร์ได้ ดังนี้

2.1.1.3 ประเภทของคอมพิวเตอร์

ประเภทของคอมพิวเตอร์สามารถแบ่งออกได้ 2 แบบ คือ แบ่งตามลักษณะของข้อมูล และแบ่งตามสมรรถนะและขนาดของคอมพิวเตอร์

การแบ่งตามลักษณะของข้อมูล สามารถแบ่งคอมพิวเตอร์ออกได้เป็น 3 ประเภท คือ[6]

1. อนาลอกคอมพิวเตอร์ (Analog Computer) เป็นเครื่องคอมพิวเตอร์ที่สร้างขึ้นเป็นพิเศษ เพื่อใช้กับงานเฉพาะด้าน มีการทำงานโดยใช้หลักในการวัด มีความละเอียดและสามารถคำนวณได้น้อยกว่าดิจิทัลคอมพิวเตอร์ ไม่สามารถเก็บข้อมูลได้เป็นจำนวนมากเหมือนกับดิจิทัลคอมพิวเตอร์ ได้แก่ เครื่องที่ใช้วัดปริมาณทางฟิสิกส์ ซึ่งผลลัพธ์ที่ได้จะออกมาในรูปของกราฟ เครื่องคอมพิวเตอร์ที่ตรวจสภาพอากาศและที่ใช้ในวงการแพทย์ เช่น เครื่องตรวจวัดสายตา ตรวจวัดคลื่นสมองและการเต้นของหัวใจ เป็นต้น

2. ดิจิทัลคอมพิวเตอร์ (Digital Computer) เป็นเครื่องคอมพิวเตอร์ที่ทำงานโดยใช้หลักในการคำนวณแบบลูกคิดหรือหลักการนับและทำงานกับข้อมูลแบบไม่ต่อเนื่อง มีความสามารถในการคำนวณและมีความแม่นยำมากกว่าอนาลอกคอมพิวเตอร์ สามารถเก็บข้อมูลได้เป็นจำนวนมากจึงต้องใช้สื่อในการบันทึกข้อมูล เช่น จานแม่เหล็กและเทปแม่เหล็ก เป็นต้น มีการพัฒนาให้สามารถทำงานได้เหมาะสมกับสภาพงานทั่วไป เช่น งานพิมพ์เอกสาร งานคำนวณ งานวิจัยเปรียบเทียบค่าทางสถิติ งานบันทึกนัดหมาย งานส่งข้อความในรูปเอกสาร ภาพและเสียง ตลอดจนงานกราฟิกเพื่อนำเสนอในรูปแบบต่างๆ เป็นต้น

3. ไฮบริดคอมพิวเตอร์ (Hybrid Computer) เป็นเครื่องคอมพิวเตอร์ที่ใช้กับงานเฉพาะด้าน มีประสิทธิภาพสูงและสามารถทำงานที่ซับซ้อนได้ เนื่องจากมีการนำเทคนิคการทำงานของอนาลอกคอมพิวเตอร์และดิจิทัลคอมพิวเตอร์มาใช้งานร่วมกัน เช่น การส่งยานอวกาศขององค์การนาซา จะใช้เทคนิคของอนาลอกคอมพิวเตอร์ในการควบคุมการหมุนของตัวยานอวกาศ ซึ่งเกี่ยวข้องกับความกดดันอากาศ อุณหภูมิ ความเร็ว และใช้เทคนิคของดิจิทัลคอมพิวเตอร์ในการคำนวณระยะทางจากพื้นผิวโลก เป็นต้น

ซึ่งการแบ่งคอมพิวเตอร์ตามลักษณะข้อมูลนั้นเป็นสิ่งที่ค่อนข้างเข้าใจยาก ส่วนการแบ่งตามสมรรถนะและขนาดของคอมพิวเตอร์นั้นสามารถเข้าใจได้ง่ายกว่า โดยสามารถแบ่งคอมพิวเตอร์ออกได้เป็น 5 ประเภท คือ[7]

---

[6] มหาวิทยาลัยราชภัฏสวนดุสิต, “วิชาเทคโนโลยีสารสนเทศเพื่อชีวิต,” E-learning [Online] แหล่งที่มา : http://dusithost.dusit.ac.th/~librarian/it107/C2.htm [16 ตุลาคม 2550]

[7] เรื่องเดียวกัน,

1. ซูเปอร์คอมพิวเตอร์ (Supercomputer) เป็นคอมพิวเตอร์ที่มีขนาดใหญ่ที่สุด ทำให้ทำงานได้รวดเร็วและมีประสิทธิภาพสูง เป็นเครื่องคอมพิวเตอร์ที่เหมาะกับงานคำนวณที่ต้องคำนวณตัวเลขจำนวนมหาศาลให้เสร็จภายในระยะเวลาอันสั้น มักใช้กับองค์กรที่มีขนาดใหญ่เท่านั้น เนื่องจากสามารถรองรับการใช้งานของผู้ใช้จำนวนมากพร้อมๆ กันได้ เรียกว่า มัลติโปรเซสซิ่ง (Multiprocessing) อันเป็นการใช้หน่วยประมวลผลหลายตัว เพื่อให้คอมพิวเตอร์สามารถทำงานหลายงานพร้อมๆ กันได้ จึงนิยมใช้กับงานที่การคำนวณที่ซับซ้อน เช่น การพยากรณ์อากาศ การทดสอบทางอวกาศ การคำนวณทางวิทยาศาสตร์ การบิน อุตสาหกรรมน้ำมัน ตลอดจนการวิจัยในห้องปฏิบัติการ ทั้งของภาครัฐบาลและเอกชน เป็นต้น

2. เมนเฟรมคอมพิวเตอร์ (Mainframe Computer) เป็นเครื่องคอมพิวเตอร์ขนาดใหญ่ มีความเร็วในการประมวลผลสูงรองลงมาจากซูเปอร์คอมพิวเตอร์ ได้รับการพัฒนาให้มีหน่วยประมวลผลหลายหน่วยทำงานพร้อมๆ กันเช่นเดียวกับซูเปอร์คอมพิวเตอร์ แต่มีจำนวนหน่วยประมวลผลที่น้อยกว่าระบบคอมพิวเตอร์ของเครื่องเมนเฟรมส่วนมากจะมีระบบคอมพิวเตอร์ย่อยๆ ประกอบอยู่ด้วย เพื่อช่วยในการทำงานบางประเภทให้กับเครื่องหลัก เหมาะกับงานที่มีข้อมูลที่มีปริมาณมากต้องประมวลผลพร้อมกันโดยผู้ใช้นับพันคน (Multi-user) ใช้กับองค์กรใหญ่ๆ ทั่วไป เช่น งานด้านวิศวกรรมคอมพิวเตอร์ วิทยาศาสตร์ การควบคุมระบบเครือข่าย งานพัฒนาระบบ งานด้านธุรกิจธนาคาร งานสำมะโนประชากร งานสายการบิน งานประกันชีวิต และมหาวิทยาลัย เป็นต้น

3. มินิคอมพิวเตอร์ (Minicomputer) เป็นเครื่องคอมพิวเตอร์ที่มีขนาดกลางที่มีประสิทธิภาพในการทำงานน้อยกว่าเมนเฟรมแต่สูงกว่าไมโครคอมพิวเตอร์ สามารถรองรับการทำงานจากผู้ใช้หลายร้อยคน (Multi-user) ในการทำงานที่แตกต่างกัน (Multi Programming) เช่นเดียวกับเครื่องเมนเฟรม แต่สิ่งที่แตกต่างกันระหว่างเครื่องเมนเฟรมและเครื่องมินิคอมพิวเตอร์ คือ ความเร็วในการทำงาน เนื่องจากมินิคอมพิวเตอร์ทำงานได้ช้ากว่าและควบคุมผู้ใช้งานต่าง ๆ ในจำนวนที่น้อยกว่า รวมทั้งสื่อที่เก็บข้อมูลมีความจุน้อยกว่าเมนเฟรม จึงเหมาะกับองค์กรขนาดกลางทำงานเฉพาะด้าน เช่น การคำนวณทางด้านวิศวกรรม การจองห้องพักของโรงแรม การทำงานด้านบัญชีขององค์การธุรกิจ เป็นต้น

4. เวิร์คสเตชันคอมพิวเตอร์ (Workstation Computer) เป็นเครื่องคอมพิวเตอร์แบบตั้งโต๊ะ ที่สนับสนุนการทำงานของคอมพิวเตอร์เครือข่ายซึ่งใช้ในการจัดสรรและใช้ทรัพยากร

ร่วมกัน เช่น แฟ้มข้อมูลโปรแกรมประยุกต์ อุปกรณ์คอมพิวเตอร์ เช่น เครื่องพิมพ์และอุปกรณ์อื่นๆ โดยการเชื่อมโยงกับเทอร์มินัล (Terminal) หลายๆ เครื่อง อีกทั้งได้ถูกออกแบบมาให้มีความสามารถในการคำนวณด้านวิศวกรรม สถาปัตยกรรม หรืองานอื่นๆ ที่เน้นการแสดงผลด้านกราฟิก เช่น การนำมาช่วยออกแบบภาพกราฟิกที่มีความละเอียดสูง ทำให้เวิร์คสเตชันใช้หน่วยประมวลผลที่มีประสิทธิภาพสูงและมีหน่วยเก็บข้อมูลสำรองจำนวนมากด้วย ผู้ใช้บางกลุ่มจะเรียกเครื่องระดับเวิร์คสเตชันนี้ว่า ซูเปอร์ไมโคร (Supermicro) เพราะถูกออกแบบให้ใช้งานแบบตั้งโต๊ะ

5. ไมโครคอมพิวเตอร์ (Microcomputer) เป็นเครื่องคอมพิวเตอร์ขนาดเล็ก สามารถเรียกได้อีกอย่างหนึ่งว่า เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer หรือ PC) สามารถใช้งานโดยใช้คนเดียว (Stand-alone) หรือเชื่อมต่อเป็นเครือข่ายเพื่อติดต่อสื่อสารกับคอมพิวเตอร์เครื่องอื่นได้ จากการที่เทคโนโลยีที่ก้าวนำสมัยทำให้ PC สามารถเชื่อมโยงเข้ากับระบบเครือข่ายอินเทอร์เน็ตติดต่อสื่อสารกับคนอื่นได้ทั่วโลกเหมาะกับงานทั่วไป เช่น การประมวลผลคำ (Word Processing) การคำนวณ (Spreadsheet) การบัญชี (Accounting) จัดทำสิ่งพิมพ์ (Desktop Publishing) และงานที่เกี่ยวข้องกับฐานข้อมูล เป็นต้น โดยอาจแบ่งคอมพิวเตอร์ส่วนบุคคล ได้ดังนี้

5.1 คอมพิวเตอร์แบบตั้งโต๊ะ (Desktop Computer) เป็นเครื่องคอมพิวเตอร์ขนาดเล็ก ใช้งานส่วนบุคคลโดยสามารถใช้งานโดยใช้คนเดียว (Stand-alone) หรือเชื่อมต่อเป็นเครือข่ายเพื่อติดต่อสื่อสารกับคอมพิวเตอร์เครื่องอื่น

5.2 โน๊ตบุ๊คคอมพิวเตอร์ (Notebook Computer) เป็นคอมพิวเตอร์ขนาดเล็ก มีน้ำหนักเบาประมาณ 2-4 กิโลกรัม และบางกว่าแบบตั้งโต๊ะ สามารถพกพาไปยังสถานที่ต่างๆ ได้สะดวก โดยมีหน้าจอและคีย์บอร์ดติดกัน ส่วนเมาส์ (Mouse) และลำโพงจะอยู่ติดกับตัวเครื่อง โดยสามารถหาอุปกรณ์ดังกล่าวติดตั้งภายนอกเพิ่มเติมก็ได้ มีเครื่องอ่านแผ่นดิสก์ (Floppy Disk Drive) และเครื่องอ่านแผ่นซีดีรอม (CD-ROM Drive) และพัฒนาให้มีขนาดเล็กกว่าเดิมในขนาดที่สามารถวางบนตักได้

5.3 ซับโน๊คบุ๊ค (Subnotebook computer) เป็นคอมพิวเตอร์พกพาที่มีขนาดเล็กกว่าคอมพิวเตอร์โน้ตบุ๊ค โดยทั่วไปมีน้ำหนักน้อยกว่า 2 กิโลกรัม เพื่อเป็นการลดขนาด

และน้ำหนัก ในบางครั้ง subnotebook จะไม่มีเครื่องอ่านแผ่นดิสก์ และจะใช้การ์ดบันทึกสำหรับงานเฉพาะอย่างแทน[8]

5.4 คอมพิวเตอร์แทปเลท (Tablet Computer) มีลักษณะคล้ายโน๊ตบุ๊ค คือ มีขนาดเล็ก มีน้ำหนักเบา มีความบาง และสามารถเคลื่อนย้ายและพกพาได้สะดวก แต่จะมีความแตกต่างกันที่แทปเลทสามารถป้อนข้อมูลทางจอภาพได้ตามเทคโนโลยีของผู้ผลิต เช่น การใช้ปากกาชนิดพิเศษที่สามารถเขียนลงบนจอภาพ และใช้โปรแกรมในการช่วยแปลงตัวเขียนเหล่านั้นให้เป็นตัวอักษรที่เหมือนกับการพิมพ์จากคีย์บอร์ด

5.5 คอมพิวเตอร์พกพา (Handheld Computer) มีขนาดเล็กกว่าโน๊ตบุ๊คและแทปเลท คือ มีขนาดเท่าฝ่ามือ ถือเพียงมือเดียวได้ และใช้อีกมือถือปากกาที่เรียกว่าสไตล์ลัส (Stylus) เขียนข้อความบนจอเพื่อป้อนข้อมูลเข้าสู่เครื่องได้ด้วยเทคโนโลยีการรับรู้ลายมือ (Hand writing recognition) พกพาสะดวกมากกว่า สามารถจัดเก็บข้อมูลได้มาก คีย์บอร์ดและหน้าจอมีขนาดเล็ก บางรุ่นใช้ปากกาชนิดพิเศษในการนำเข้าข้อมูล มีน้ำหนักเพียงร้อยกว่ากรัม และจอสีที่มีความละเอียดสูงถึง 320x320 และสามารถต่อเข้ากับอินเทอร์เน็ต และบางรุ่นสามารถใช้ฟังเพลง MP3 หรือใช้เป็นโทรศัพท์เคลื่อนที่ได้ด้วย คอมพิวเตอร์ชนิดนี้ถูกออกแบบมาเพื่อทำหน้าที่เป็นอุปกรณ์จัดเก็บและจัดการสารสนเทศส่วนบุคคล (Personal Information Manager: PIM หรือ Personal Organizer) เช่น ตารางเวลา ปฏิทินนัดหมาย สมุดโทรศัพท์ และสมุดบันทึก เป็นต้น คอมพิวเตอร์ชนิดนี้นิยมเรียกว่า PDA (Personal Digital Assistant) โดย PDA ในปัจจุบันที่นิยมได้แบ่งออกเป็นสองแบบ คือ พีดีเอในกลุ่มของปาล์ม (Palm) ซึ่งใช้ Palm OS จากบริษัทปาล์มต่างๆ และ PDA ในกลุ่มของพอกเกตพีซี (Pocket PC)

จะเห็นได้ว่าแม้ว่าจะเรียกว่าคอมพิวเตอร์เหมือนกันหากแต่มีรูปลักษณ์และลักษณะการใช้งานที่แตกต่างกันออกไปเพื่อจุดประสงค์ที่หลากหลาย และยิ่งมนุษย์นำคอมพิวเตอร์ไปในมากเท่าใด ก็ยิ่งทำให้คอมพิวเตอร์เปลี่ยนแปลงรูปแบบและการทำงานมากยิ่งขึ้นเท่านั้น ดังที่ได้แยกประเภทของคอมพิวเตอร์มาข้างต้นแล้ว แม้จะสามารถระบุถึงอุปกรณ์อิเล็กทรอนิกส์บางประเภทว่าเป็นคอมพิวเตอร์ได้ เช่น ปาล์ม พอกเกตพีซี หากแต่มีอุปกรณ์

---

[8] มหาวิทยาลัยราชภัฏสวนดุสิต, “วิชาเทคโนโลยีสารสนเทศเพื่อชีวิต บทที่ 3,” E-learning [Online] แหล่งที่มา : http://dusithost.dusit.ac.th/~librarian/myweb/Chapter3.html [16 ตุลาคม 2550]

อิเล็กทรอนิกส์อื่นๆ อีกที่มีความสามารถในการทำงานคล้ายคลึงกับคอมพิวเตอร์แต่ไม่ถูกเรียกชื่อว่าคอมพิวเตอร์ ทำให้อาจมีปัญหาว่าในศาสตร์ทางด้านคอมพิวเตอร์แล้ว อุปกรณ์เหล่านั้นเป็นคอมพิวเตอร์หรือไม่ จึงจำเป็นที่จะต้องหาหลักเกณฑ์ในการพิจารณาว่าอย่างไรจึงจะเรียกว่าคอมพิวเตอร์ซึ่งหากจะอาศัยจากนิยามหรือความหมายตามพจนานุกรมแล้วก็ไม่อาจให้เป็นหลักเกณฑ์ในการแยกแยะได้ชัดเจน ดังนั้นตามที่ผู้เขียนได้หาข้อมูลในการกำหนดกฎเกณฑ์ในการพิจารณาว่าสิ่งใดคือคอมพิวเตอร์ จึงได้ข้อสรุปว่าสิ่งที่จะสามารถเรียกว่าคอมพิวเตอร์ได้นั้นต้องมีคุณสมบัติสำคัญคือ[9]

1. การรับข้อมูลเข้า (Input) คือ การนำข้อมูลเข้าซึ่งสามารถผ่านทางอุปกรณ์ชนิดต่างๆ แล้วแต่ชนิดของข้อมูลที่จะป้อนเข้าไป

2. มีการประมวลผลข้อมูล (Process) โดยเมื่อนำข้อมูลเข้ามาแล้ว มีการดำเนินการกับข้อมูลตามคำสั่งที่ได้รับมาเพื่อให้ได้ผลลัพธ์ตามที่ต้องการ

3. มีชุดคำสั่ง (software) ที่สั่งให้เกิดการทำงานตามที่ได้กำหนดไว้ในชุดคำสั่งนั้น

4. มีหน่วยความจำ (memory) คือ มีแหล่งเก็บข้อมูล

5. มีการแสดงผลลัพธ์ (Output) เป็นการนำผลลัพธ์จากการประมวลผลมาแสดงให้ทราบทางอุปกรณ์ที่กำหนดไว้ โดยทั่วไปจะแสดงผ่านทางจอภาพหรือเรียกกันโดยทั่วไปว่า "จอมอนิเตอร์" (Monitor)

อย่างไรก็ตามหลักเกณฑ์ดังที่ได้กล่าวมาแล้วนั้นก็ยังมีข้อถกเถียงที่ก่อให้เกิดความเห็นที่แตกต่างกันเช่นกัน ในขณะที่มีผู้ให้ความเห็นว่า[10]เพียงแค่มีคุณสมบัติครบถ้วนดังที่ได้กล่าวมาข้างต้นก็ถือว่าเป็นคอมพิวเตอร์แล้ว ซึ่งในกรณีนี้อุปกรณ์อิเล็กทรอนิกส์อื่นที่มีคุณสมบัติ

---

[9] “What is computer?” [Online] Available from : www.webopedia.com/TERM/C/computer.html [25 ตุลาคม 2550]

[10] **สัมภาษณ์** ดร.สันติธร บุญเจือ, คณบดีคณะเทคโนโลยีสารสนเทศและการสื่อสาร วิทยาลัยการศึกษาทางไกลอินเทอร์เน็ต มหาวิทยาลัยอัสสัมชัญ ,วันที่ 24 ธันวาคม 2550.

ครบถ้วนก็คือคอมพิวเตอร์แล้ว เช่น เครื่องเล่น MP3 แต่มีผู้ให้ความเห็นว่า[11] แม้จะมีคุณสมบัติครบถ้วนตามที่กล่าวมาข้างต้นก็ยังไม่อาจเรียกว่าคอมพิวเตอร์ได้ เพียงแค่คุณสมบัติดังกล่าวข้างต้นยังไม่เพียงพอที่จะเรียกว่าเป็นคอมพิวเตอร์ สิ่งที่จะทำให้อุปกรณ์อิเล็กทรอนิกส์เป็นคอมพิวเตอร์ได้นั้น นอกจากคุณสมบัติเบื้องต้นดังที่ได้กล่าวมาแล้ว ยังต้องมีลักษณะพิเศษอีกอย่างคือ การใส่ชุดคำสั่งไปในอุปกรณ์นั้นต้องสามารถใส่ชุดคำสั่งเพิ่มเติมอีกได้ โดยไม่ถูกจำกัดอยู่กับชุดคำสั่งเดิมเท่านั้น กล่าวคือต้องสามารถใส่ชุดคำสั่งใหม่ๆ เพื่อให้อุปกรณ์นั้นสามารถทำสิ่งที่แตกต่างจากคุณสมบัติเดิมได้ ดังนั้นเครื่องเล่น MP3 จึงไม่ใช่คอมพิวเตอร์ในความหมายดังกล่าว

หากยึดถือแนวคิดแรกที่ว่าคอมพิวเตอร์คืออุปกรณ์ที่มีคุณสมบัติข้างต้นแล้ว ก็อาจกล่าวได้ว่าเป็นการให้แนวคิดการแยกแยะอุปกรณ์คอมพิวเตอร์ในความหมายอย่างกว้าง อุปกรณ์ที่มีคุณสมบัติดังกล่าวอาจกล่าวได้ว่าเป็นคอมพิวเตอร์ทั้งหมด รวมตลอดถึง เครื่องเล่น MP3 หรือโทรสาร ด้วย หากเทียบกับแนวคิดหลังแล้วเป็นการให้กรอบกำหนดที่แคบกว่า ซึ่งทำให้อุปกรณ์อิเล็กทรอนิกส์บางชนิดไม่ใช่คอมพิวเตอร์ ซึ่งอาจพิจารณาได้ดังต่อไปนี้

ดังที่ได้กล่าวมาข้างต้นว่าอุปกรณ์อิเล็กทรอนิกส์มีอยู่เป็นจำนวนมาก ผู้เขียนไม่สามารถที่จะนำอุปกรณ์อิเล็กทรอนิกส์ทุกประเภทมาแยกแยะว่าเป็นคอมพิวเตอร์ในแนวคิดที่สองได้ ในขณะที่อุปกรณ์อิเล็กทรอนิกส์บางประเภทสามารถแยกแยะได้ง่ายว่าไม่ใช่คอมพิวเตอร์ เช่น โทรทัศน์ วิทยุ โทรศัพท์ หรือโทรสาร หากแต่อุปกรณ์บางประเภทนั้นยากที่จะแยกแยะได้ด้วยเหตุที่มีคุณสมบัติที่ใกล้เคียงกับเครื่องคอมพิวเตอร์มาก แต่อย่างไรก็ตาม หากอาศัยหลักเกณฑ์ที่ได้กล่าวมาข้างต้นก็สามารถนำไปใช้แยกแยะอุปกรณ์อิเล็กทรอนิกส์อื่นออกจากคอมพิวเตอร์ได้ โดยผู้เขียนจะขอยกตัวอย่างอุปกรณ์อิเล็กทรอนิกส์ต่างๆ ที่ที่มีอยู่ทั่วไปเป็นตัวอย่างในการพิจารณาว่าเป็นคอมพิวเตอร์หรือไม่ จะขอยกตัวอย่างในการแยกแยะอุปกรณ์อิเล็กทรอนิกส์ที่ไม่ได้ถูกเรียกว่าคอมพิวเตอร์แต่โดยคุณสมบัติแล้วถือว่าเป็นคอมพิวเตอร์อย่างหนึ่ง กับอุปกรณ์อิเล็กทรอนิกส์ที่มีคุณสมบัติใกล้เคียงกับคอมพิวเตอร์แต่ไม่ใช่คอมพิวเตอร์ โดยอุปกรณ์อิเล็กทรอนิกส์ที่ถือว่าเป็นคอมพิวเตอร์[12] เช่น

---

[11]สัมภาษณ์ ธงชัย โรจน์กังสดาล, เลขานุการภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 30 มกราคม 2551.

[12] เรื่องเดียวกัน,

1. เครื่องเล่นเกม ในปัจจุบันเครื่องเล่นเกมมีคุณสมบัติที่ถูกพัฒนาขึ้นเพื่อตอบสนองความต้องการของผู้บริโภค โดยเฉพาะอย่างยิ่งเครื่องเล่นเกมยุคใหม่ เช่น เพลย์สเตชั่น 3 (PS3) เอ็กบอกซ์ 360 (Xbox 360) หรือแม้แต่เครื่องเล่นเกมวี (wii) ที่สามารถเล่นเกมออนไลน์ผ่านเครือข่ายอินเทอร์เน็ตได้ นอกจากนี้อาจปรับปรุงแก้ไขให้เครื่องเล่นเกมสามารถดูหนัง หรือแม้แต่เชื่อมต่ออินเทอร์เน็ตได้ ซึ่งเครื่องเล่นเกมดังกล่าวมีทั้ง การรับข้อมูลเข้า (Input) ประมวลผลข้อมูล (Process) มีชุดคำสั่ง (software) หน่วยความจำ (memory) และมีการแสดงผลลัพธ์ (Output) และอาจใส่ชุดคำสั่งอื่นเพื่อให้ทำงานอย่างอื่นได้ เช่น เอ็กบอกซ์ 360 นั้นมีระบบปฏิบัติการวินโดว์อยู่ ทำให้มีคุณสมบัติที่กล่าวได้ว่าเป็นคอมพิวเตอร์เช่นเดียวกัน หากแต่อาจเป็นคอมพิวเตอร์ที่มีจุดประสงค์เฉพาะด้าน (Special purpose) คือใช้สำหรับเล่นเกมเท่านั้น หากแต่ด้วยคุณสมบัติดังกล่าวก็สามารถทำอย่างอื่นได้เช่นกันหากใส่ชุดคำสั่งอื่นนอกจากการเล่นเกมลงไป ทำให้เครื่องเล่นเกมเป็นคอมพิวเตอร์

2. ตู้เอทีเอ็ม (รวมถึงตู้ให้บริการทางบัญชีต่างๆ ของธนาคารด้วย) ซึ่งโดยสภาพแล้วตู้เอทีเอ็มก็คือเครื่องคอมพิวเตอร์นั่นเอง หากแต่มาใส่รูปแบบที่มีลักษณะเป็นเครื่องเอทีเอ็ม และมีชุดคำสั่งเฉพาะเรื่องการเบิกถอนเงินเท่านั้น หากแต่ภายในนั้นเป็นเครื่องPC หากแต่ใส่กรอบไว้ให้เป็นหน้าจอเท่านั้น จึงอาจกล่าวได้ว่าตู้เอทีเอ็มเป็นคอมพิวเตอร์ที่มีจุดประสงค์เฉพาะด้าน (Special purpose) คือใช้สำหรับเบิกถอนเงินหรือดำเนินการอื่นๆ ที่ธนาคารกำหนดเท่านั้น

3. ไอโฟนหรือโทรศัพท์มือถือรุ่นใหม่ที่มีระบบปฏิบัติการ ซึ่งมีคุณสมบัติที่ไม่แตกต่างจากคอมพิวเตอร์ สามารถดูหนัง ฟังเพลง แปลงข้อมูล หรือแม้แต่เล่นอินเทอร์เน็ตได้ และสามารถนำชุดคำสั่งใหม่ๆ เพิ่มเข้าไปและทำงานตามชุดคำสั่งใหม่ได้ ซึ่งคุณสมบัติเหล่านี้เป็นคุณสมบัติของคอมพิวเตอร์ ดังนั้นจึงอาจกล่าวได้ว่าเป็นคอมพิวเตอร์อย่างหนึ่ง

นอกจากนี้เพื่อให้เกิดความชัดเจนยิ่งขึ้น ผู้เขียนจึงจะขอยกตัวอย่างอุปกรณ์อิเล็กทรอนิกส์อื่นๆ ที่ไม่จัดว่าเป็นคอมพิวเตอร์ ดังนี้

1. เครื่องคิดเลข ไม่เป็นคอมพิวเตอร์ เนื่องจากไม่มีหน่วยความจำ ไม่มีการประมวลผลโดยคำสั่งที่ทำงานได้เต็มรูปแบบ

2. เครื่องรับส่งโทรสาร ไม่ใช่คอมพิวเตอร์ เพราะไม่มีชุดคำสั่งให้ทำงานอื่นนอกเหนือจากการรับส่งโทรสารได้

3. โทรศัพท์มือถือรุ่นเก่าที่มีคุณสมบัติไม่ครบถ้วนที่จะเป็นคอมพิวเตอร์ เช่น ไม่มีหน่วยประมวลผล ไม่มีชุดคำสั่งที่จะกำหนดให้ทำงานได้

4. เครื่องเล่นเอ็มพี 3 หรือไอพอด ไม่ถือว่าเป็นคอมพิวเตอร์ เพราะคอมพิวเตอร์มีชุดคำสั่งที่สามารถสั่งการให้ทำงานตามที่ต้องการได้ หากแต่เครื่องเล่นเอ็มพี 3 แม้จะมีชุดคำสั่งแต่ไม่สามารถนำชุดคำสั่งใหม่ให้ทำงานนอกเหนือจากชุดคำสั่งเดิมได้

ดังนั้นอาจสรุปได้ว่า ในการกำหนดกรอบว่าสิ่งใดคือคอมพิวเตอร์ในแนวคิดที่สองแล้ว อาจกล่าวได้ว่านอกเหนือจากคุณสมบัติพื้นฐานที่เป็นองค์ประกอบที่กล่าวมาข้างต้นแล้ว แม้จะมีองค์ประกอบครบถ้วนหากแต่สิ่งที่เป็นสิ่งที่แบ่งแยกอุปกรณ์อิเล็กทรอนิกส์อื่นออกจากคอมพิวเตอร์คือ คอมพิวเตอร์ต้องสามารถใส่ชุดคำสั่งอื่นๆ นอกเหนือจากชุดคำสั่งเดิมได้ และทำงานได้นอกเหนือจากชุดคำสั่งเดิมที่มีอยู่ในอุปกรณ์นั้น โดยจะเห็นได้ว่า แม้ในศาสตร์ทางด้านคอมพิวเตอร์เองการที่จะกำหนดว่าสิ่งใดเป็นคอมพิวเตอร์ก็ยังมีความเห็นที่ไม่ตรงกันแล้วแต่ผู้ให้หลักเกณฑ์ขอบเขตนั้น

เมื่อกล่าวถึงคอมพิวเตอร์แล้ว สิ่งที่ต้องพิจารณาต่อมาคือ คำว่า “ระบบคอมพิวเตอร์” ในศาสตร์ทางด้านคอมพิวเตอร์นั้น คำว่าระบบคอมพิวเตอร์มีความแตกต่างจากคำว่า “คอมพิวเตอร์” ที่กล่าวมาข้างต้น โดยคำว่า ระบบ (System) หมายถึง ระเบียบวิธีการปฏิบัติที่รวมส่วนต่าง ๆ เข้าด้วยกันเพื่อปฏิบัติงานให้เกิดผลลัพธ์ตามที่ต้องการอย่างมีประสิทธิภาพมากที่สุด ดังนั้น คำว่า ระบบคอมพิวเตอร์ ในที่นี้มีความหมายกว้างกว่าคำว่า “เครื่องคอมพิวเตอร์” โดยระบบคอมพิวเตอร์หมายถึง ส่วนทุกส่วนที่รวมกันแล้ว ทำให้สามารถใช้เครื่องคอมพิวเตอร์ให้เป็นประโยชน์ได้[13]

ดังนั้นจะเห็นไว้ว่า คำว่า “คอมพิวเตอร์” และคำว่า “ระบบคอมพิวเตอร์” มีความแตกต่างกัน โดยอาจพิจารณาได้ง่ายๆ ว่า เมื่อพูดถึงคอมพิวเตอร์แล้ว โดยทั่วไปมักจะนึกถึงคอมพิวเตอร์เครื่องเดียว หากแต่ระบบคอมพิวเตอร์มักจะถูกกล่าวถึงในแง่ระบบรวมที่ใหญ่ขึ้น จะสังเกตได้ว่าจะไม่พูดกันว่าผู้ใช้มีระบบคอมพิวเตอร์ แต่มักจะกล่าวว่าในบริษัทมีการใช้งานคอมพิวเตอร์ในด้านใด เช่นมีคอมพิวเตอร์หลายเครื่องต่อกันเป็นเครือข่ายเพื่อใช้งานเฉพาะด้าน ดังนั้นอาจกล่าวคำว่าระบบคอมพิวเตอร์จึงเป็นคำรวมที่กว้าง โดยมากมักแสดงให้เห็นถึงการใช้งานโดยเฉพาะเจาะจงที่ใช้ในกลุ่มคนที่กว้างขึ้น มีจุดมุ่งหมายที่แตกต่างออกไปจากคอมพิวเตอร์ทั่วๆ ไป โดยระบบคอมพิวเตอร์อาจมีคอมพิวเตอร์เครื่องเดียวก็ได้ และทำงานตามจุดมุ่งหมายที่

---

[13] เรื่องเดียวกัน,

ต้องการ เช่น คอมพิวเตอร์เครื่องหนึ่งทำหน้าที่เป็น web browser ดังนั้นคำว่าระบบคอมพิวเตอร์จึงมีความหมายกว้างกว่าคำว่าคอมพิวเตอร์

เมื่อพิจารณาถึงคำว่าคอมพิวเตอร์และระบบคอมพิวเตอร์ในศาสตร์ทางด้านคอมพิวเตอร์แล้ว สิ่งที่จะต้องพิจารณาต่อไปคือ คำว่าคอมพิวเตอร์และระบบคอมพิวเตอร์ในแง่มุมทางด้านกฎหมาย

2.1.1.4 การให้คำนิยามทางด้านกฎหมาย

เมื่อมีการบัญญัติกฎหมายเกี่ยวกับการกระทำความผิดคอมพิวเตอร์ขึ้น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้กำหนดนิยามคำว่า “ระบบคอมพิวเตอร์” แต่เนื่องจากการบัญญัติกฎหมายที่เกี่ยวพันกับศาสตร์อื่นที่เป็นศาสตร์เฉพาะนั้น สิ่งที่สำคัญอย่างหนึ่งที่ต้องคำนึงถึงเป็นอย่างมากคือ ลักษณะของภาษาที่ใช้ในบทบัญญัติของกฎหมาย เนื่องจากภาษาที่ใช้ในบทบัญญัติของกฎหมายมีความแตกต่างกัน ที่สามารถแยกออกได้เป็น 4 ประเภท ดังนี้[14]

1. ภาษาธรรมดา

ถ้อยคำในกฎหมายโดยทั่วๆ ไป ย่อมมีความหมายตามที่ประชาชนทั่วไปเข้าใจ การตีความก็ต้องตีความไปตามความหมายของศัพท์เหล่านั้น เช่น คำว่า ฆ่า หมายถึง ทำให้ตาย ค่าจ้าง คือ สิ่งตอบแทนที่ทำงานให้ หรือคำว่า ศพ คือ ร่างของคนที่ตายแล้ว เป็นต้น หากคำใดมีปัญหาเกี่ยวกับความหมาย ก็ให้ค้นหาเอาได้จากพจนานุกรมฯ เช่น คำว่า “ลุแก่โทษ” ได้แก่ การปลดความผิดของตน เพื่อขอความกรุณา ดังนั้นการที่จำเลยมอบตัวแก่ตำรวจพร้อมปืนที่ใช้ยิง จึงเป็นการลุแก่โทษ[15]

2. ภาษาเทคนิค

หมายถึงภาษาที่มีความหมายพิเศษ กว้างขวางลึกซึ้ง ต่างไปจากภาษาธรรมดาอยู่บ้าง ใช้เข้าใจกันอยู่ในหมู่ของผู้ที่เกี่ยวข้อง ภาษาเทคนิคมีอยู่ทั่วไปในกลุ่มผู้ที่เป็นวิศวกร กลุ่มการเดินเรือ การบัญชี ฯลฯ ซึ่งศัพท์ธรรมดาๆในกลุ่มของบุคคลเหล่านี้ ก็จะมีความหมายที่เข้าใจ

---

[14] ทวีเกียรติ มีนะกนิษฐ์, “ปัจจัยสำคัญที่ทำให้กฎหมายขาดประสิทธิภาพ,” บทบัณฑิตย์ เล่มที่ 60 (มิถุนายน 2547) หน้า 96-103.

[15] คำพิพากษาฎีกาที่ 1499/2512.

แตกต่างกัน กว้างขวางออกไป ทางกฎหมายก็เช่นเดียวกัน ก็มีถ้อยคำที่ในหมู่นักกฎหมายเข้าใจโดยเฉพาะ คำว่า “วิ่งราวทรัพย์” ในความหายธรรมดาที่ชาวบ้านเข้าใจ หมายถึงต้องมีการวิ่งเอาทรัพย์ไป แต่ในหมู่นักกฎหมายแล้ว เป็นที่รู้กันว่า ได้แก่การ “ลักทรัพย์โดยฉกฉวยเอาซึ่งหน้า” ซึ่งอาจไม่มีการวิ่งเลยก็ได้ เช่น หยิบเอาของเขาไป แล้วก็เดินออกไปต่อหน้า ก็เป็นการวิ่งราวทรัพย์ก็ได้[16] ดังนั้น ภาษาเทคนิคจึงต้องมีการตีความให้ได้ความตามความหมายที่เข้าใจกัน ในกลุ่มคนที่เขาใช้ มิฉะนั้นการวินิจฉัยก็จะผิดพลาดไม่เป็นธรรมได้ เช่น หากโจทก์ฟ้องว่า นายแดงบุกเดี่ยวปล้นทรัพย์ ต้องหมายความว่า นายแดงชิงทรัพย์ไม่ใช่ปล้นทรัพย์ เป็นต้น

3. นิยามศัพท์

หมายถึงภาษาหรือถ้อยคำที่กฎหมายประสงค์จะให้มีความหมายเฉพาะแตกต่างจากภาษาธรรมดาทั่วไป หรือต้องการให้มีความหมายพิเศษครอบคลุมในสิ่งที่กฎหมายจะบังคับใช้ ก็ต้องใช้และตีความตามความหมายนั้นๆ อย่างเคร่งครัด[17] การกำหนดนิยามศัพท์มีได้ 2 ลักษณะ คือ

(ก) กำหนดเพื่อให้กระชับ โดยมิได้มุ่งหมายให้มีความหมายพิเศษแต่อย่างใด เช่น นิยามศัพท์คำว่า “รัฐมนตรี” หมายถึงรัฐมนตรีว่าการกระทรวงเกษตรและสหกรณ์การเกษตร เป็นต้น คำว่า รัฐมนตรีจึงหมายถึงรัฐมนตรีตามที่ระบุไว้ในพระราชบัญญัตินั้นๆ เท่านั้น ไม่ได้มีความหมายพิเศษแต่อย่างใด นิยามศัพท์เช่นนี้จึงไม่ค่อยมีปัญหาในเรื่องการตีความ

(ข) กำหนดเพื่อให้มีความหมายพิเศษ คำนิยามศัพท์มีขึ้น เพื่อใช้ในความมุ่งหมายเฉพาะของกฎหมายจึงมีความหมายของพระราชบัญญัตินั้นๆ เช่น คำว่า “ป่า” ตามพระราชบัญญัติป่าไม้ พ.ศ. 2484 หมายความว่า “ที่ดินที่ยังไม่ได้มีบุคคลได้มาตามกฎหมาย” ดังนั้นเมื่อพูดถึง “ป่า” คนทั่วไปย่อมนึกถึงต้นไม้ สายน้ำ ลำธาร แต่ป่าตามกฎหมายนี้อาจไม่มีต้นไม้แม้แต่ต้นเดียวเลยก็ได้ ความหมายของป่าจึงแตกต่างไปจากถ้อยคำธรรมดา หรือ

---

[16] คำพิพากษาศาลฎีกา 919/2503

[17] ธานินทร์ กรัยวิเชียรและวิชา มหาคุณ, การตีความกฎหมาย, พิมพ์ครั้งที่ 3 (กรุงเทพมหานคร : คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2539), หน้า 184.

ตามพระราชบัญญัติการประมง พ.ศ. 2490 มาตรา 4 (1) ซึ่งแก้ไขโดย มาตรา 3 แห่งพระราชบัญญัติการประมง (ฉบับที่ 3) พ.ศ.2528 ให้นิยามคำว่า "สัตว์น้ำ" หมายความว่า สัตว์ที่อาศัยอยู่ในน้ำหรือมีวงจรชีวิตส่วนหนึ่งอยู่ในน้ำหรืออาศัยอยู่ในบริเวณที่น้ำท่วมถึง เช่น ปลา กุ้ง ปู แมงดาทะเล หอย เต่า กระ ตะพาบน้ำ จระเข้ รวมทั้งไข่ของสัตว์น้ำนั้น สัตว์น้ำจำพวกเลี้ยงลูกด้วยนม ปลิงทะเล ฟองน้ำ หินปะการัง กัลปังหา และสาหร่ายทะเล ทั้งนี้ รวมทั้งซากหรือส่วนหนึ่งส่วนใดของสัตว์น้ำเหล่านั้น และหมายความรวมถึงพันธุ์ไม้น้ำตามที่ได้มีพระราชกฤษฎีการะบุชื่อ ดังนี้จะเห็นได้ว่า สาหร่ายทะเล ซึ่งภาษาธรรมดาเป็นพืช แต่พระราชบัญญัตินี้ หมายถึง สัตว์น้ำ ฉะนั้น การช้อนสาหร่ายทะเลไปก็เป็นการจับสัตว์น้ำตามพระราชบัญญัตินี้ รวมถึงพันธุ์ไม้อย่างอื่นที่ประกาศในพระราชกฤษฎีกาด้วย ถือว่าเป็นการกระทำต่อสัตว์น้ำ เมื่อมีการประกาศจับสัตว์น้ำ ซึ่งความหมายดังกล่าวแตกต่างจากความเข้าใจธรรมดาๆไปมาก การตีความก็ต้องเป็นไปตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ผู้ที่เอาสาหร่ายทะเลไป จะเอาความหมายธรรมดามาต่อสู้ให้พ้นความผิดไม่ได้ บางครั้งก็อาจมีความหมายแปลกไปมาก เช่น พระราชบัญญัติการขายยา พ.ศ. 2493 "ยา" หมายความว่า "วัตถุที่มุ่งหมายสำหรับใช้ในการพิเคราะห์ บำบัด รักษา หรือป้องกันโรค หรือความเจ็บปวดของมนุษย์หรือสัตว์"[18] คดีนี้จำเลยกับพวกได้โฆษณาขายกำไลวิทยาศาสตร์ว่าเป็นเครื่องบำบัดโรคต่างๆ ได้ จำเลยฎีกาในข้อกฎหมายว่า กำไลไม่ใช่ยา ศาลฎีกาวินิจฉัยว่า การเป็นยาตามพระราชบัญญัตินี้หรือไม่ ข้อสำคัญหาได้อยู่ที่ว่าวัตถุนั้นจะบำบัดรักษา หรือป้องกันโรคได้จริงหรือไม่ หากแต่อยู่ที่ความมุ่งหมายในการใช้ ถ้ามุ่งหมายให้ใช้วัตถุนั้นบำบัดโรค และป้องกันโรคแล้วก็ต้องถือว่าเป็นยา ศาลจึงเห็นว่ากำไลข้อมือเป็นยา[19]

---

[18] ข้อความทำนองเดียวกับพระราชบัญญัติยา พ.ศ. 2510 มาตรา 4.

[19] คำพิพากษาฎีกาที่ 201/2506.

4. ถ้อยคำกำกวม

แม้หลักการบัญญัติกฎหมาย โดยเฉพาะกฎหมายอาญาต้องบัญญัติชัดแจ้ง แต่ก็แทบจะเป็นไปไม่ได้เลยที่จะบัญญัติถ้อยคำที่ชัดเจนทั้งหมด เพราะภาษาแต่ละคำย่อมมีความหมายในทางอัตนัย (Subjective meaning) อยู่มาก กฎหมายจึงยังต้องใช้ถ้อยคำกำกวมไม่ชัดเจนอยู่ เช่น คำว่า “เดือดร้อนรำคาญ” น่าจะเป็นเหตุให้เกิดอันตราย (ประมวลกฎหมายอาญา มาตรา 226) หรือ “รับไว้โดยประการใด” (ประมวลกฎหมายอาญา มาตรา 357) ฯลฯ เป็นต้น ซึ่งถ้อยคำเหล่านี้จะมีความหมายเช่นใดต้องพิจารณาจากสถานการณ์เป็นเรื่องๆ ไป เช่น การส่งเสียงดังจะเป็นความเดือดร้อนรำคาญหรือไม่ก็ต้องดูว่า หากเป็นการกระทำในเวลากลางคืน หรือคนอื่นเขาหลับนอนกันแล้วก็เป็นการทำให้เดือดร้อนรำคาญ หรือคำว่า รับไว้โดยประการใด ในเรื่องรับของโจร ตามมาตรา 357 ไม่ใช่ว่า เมื่อรับของที่ตนรู้ว่าได้มาจากการกระทำความผิดจะเป็นการรับของโจทก์เสมอไป หากวิทยุของเพื่อนถูกขโมยไป ต่อมาไปพบเข้าจึงซื้อกลับมาคืนเพื่อน ดังนี้เป็นการซื้อโดยรู้ว่าเป็นการซื้อเพื่อเจ้าของเอง[20] ดังนี้ ถ้อยคำที่กำกวมจึงต้องมีการตีความให้ถูกต้องตามความประสงค์ มิฉะนั้นคนที่มิได้เป็นผู้กระทำผิดในความหมายของกฎหมายก็จะกลายเป็นผู้กระทำความผิดไปได้

ดังนั้นจะเห็นได้ว่า การบัญญัติถ้อยคำในกฎหมายต้องพิจารณาถึงความเหมาะสมและความเป็นจริงในความหมายของศาสตร์นั้น เช่น หากจะบัญญัติกฎหมายเกี่ยวกับการแพทย์ ผู้ร่างเองก็ต้องศึกษาเรียนรู้เกี่ยวกับศาสตร์ทางการแพทย์เพื่อที่จะได้เกิดความเข้าใจในศาสตร์นั้น และนำมาบัญญัติกฎหมายให้ถูกต้องเหมาะสมกับความเป็นจริง แม้ว่าในความเป็นจริงแล้วนิยามทางด้านกฎหมายไม่จำเป็นต้องมีความหมายเหมือนกับความหมายในศาสตร์อื่นๆ ก็ตาม หากแต่เพื่อความเข้าใจที่ถูกต้องตรงกันทำให้ประชาชนทั่วไปสามารถเข้าใจได้และสามารถแก้ปัญหาที่เกิดขึ้นจากศาสตร์นั้นได้อย่างเหมาะสมกับสภาพความเป็นจริงที่เกิดขึ้น การนิยามศัพท์ทางด้านกฎหมายที่เหมาะสมและสอดคล้องกับศาสตร์ที่เกี่ยวข้องก็เป็นสิ่งที่จำเป็นในการบัญญัติกฎหมายเช่นกัน

การบัญญัติกฎหมายเกี่ยวกับการกระทำผิดทางคอมพิวเตอร์ก็เช่นเดียวกัน ศาสตร์ทางคอมพิวเตอร์ก็มีคำศัพท์ทางเทคนิคที่แตกต่างจากภาษาทั่วไปและภาษาทางกฎหมาย การศึกษาความหมายและให้คำนิยามที่เหมาะสมสอดคล้องกับความเป็นจริงและศาสตร์ทางคอมพิวเตอร์ที่เกี่ยวข้องกับสิ่งที่กฎหมายมุ่งคุ้มครองก็เป็นสิ่งที่ควรจะกระทำ โดยในความผิด

---

[20] คำพิพากษาฎีกาที่ 2611/2527.

เกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ สิ่งที่ต้องพิจารณาเป็นอันดับแรกคือ นิยามความหมายของคำว่า “ระบบคอมพิวเตอร์” และ “ข้อมูลคอมพิวเตอร์” ที่ปรากฏอยู่ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ว่ามีความหมายครอบคลุมเพียงใดทั้งในด้านศาสตร์ทางคอมพิวเตอร์และทางด้านกฎหมายเพื่อที่จะเปรียบเทียบหาความหมายที่ถูกต้องเหมาะสมในการบังคับใช้กฎหมายต่อไป

โดยในพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้นิยามคำว่า “ระบบคอมพิวเตอร์” ไว้ในมาตรา 3 ว่า

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ”

ซึ่งอาจแยกองค์ประกอบของความหมายดังกล่าว ได้ดังนี้

1. เป็นอุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน ซึ่งคือ อุปกรณ์ต่างๆ ของคอมพิวเตอร์ที่เชื่อมเข้าด้วยกัน เช่น จอภาพ คีย์บอร์ด เม้าท์ หรือเคสซีพียู

2. มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลอัตโนมัติ คือการกำหนดชุดคำสั่งให้คอมพิวเตอร์ทำงานเช่น ระบบปฏิบัติการวินโดว์ หรือระบบปฏิบัติการลีนุ๊ก หรือระบบปฏิบัติการแม็ค

จะเห็นได้จากองค์ประกอบข้างต้นว่า คำว่า “ระบบคอมพิวเตอร์” ที่กล่าวถึงในกฎหมายนั้นเป็นการกล่าวอย่างกว้างๆ โดยเน้นไปที่ hardware เป็นหลักมากกว่า โดยเป็น hardware ที่มี software อยู่ ดังนั้นหากเป็นเครื่องคอมพิวเตอร์ที่ยังไม่มีการลงชุดคำสั่งจึงไม่เป็นคอมพิวเตอร์ในความหมายนี้ และอาจกล่าวอย่างง่ายๆ ได้ว่าระบบคอมพิวเตอร์ในความหมายของกฎหมายคือคอมพิวเตอร์ที่เชื่อมต่อกันนั่นเอง ไม่ใช่ความหมายเดียวกับระบบคอมพิวเตอร์ในแง่ศาสตร์ทางด้านคอมพิวเตอร์แต่อย่างใด

หลังจากพิจารณาถึงความหมายของระบบคอมพิวเตอร์ทั้งในแง่ศาสตร์ของคอมพิวเตอร์และในแง่ของกฎหมายแล้ว สิ่งที่จะต้องพิจารณาต่อไปคือความหมายของคำว่าข้อมูลคอมพิวเตอร์ในแง่ของศาสตร์ทางด้านคอมพิวเตอร์และทางด้านกฎหมาย ดังนี้

2.1.2 ข้อมูลคอมพิวเตอร์

ข้อมูลคอมพิวเตอร์นั้นเป็นอีกสิ่งหนึ่งที่มีความสำคัญในคอมพิวเตอร์ เนื่องจากการทำงานหลักของคอมพิวเตอร์นั้นก็คือการประมวลผลข้อมูลที่นำเข้าไปในคอมพิวเตอร์และทำการส่งผลลัพธ์ของการประมวลผลนั้นออกมายังผู้ใช้เพื่อนำข้อมูลที่นำเข้าไปทำงานต่อไป ดังนั้นจึงมีความจำเป็นที่จะต้องเข้าใจถึงความหมายของข้อมูลคอมพิวเตอร์เพื่อให้เกิดความเข้าใจในการพิจารณาความหมายในกฎหมายต่อไป

2.1.2.1 ความหมายของข้อมูลคอมพิวเตอร์

ในศาสตร์ทางด้านคอมพิวเตอร์นั้น คำว่า “ข้อมูลคอมพิวเตอร์” แทบไม่มีใช้ดังที่มีการให้คำนิยามไว้ในกฎหมาย[21] มีแต่คำว่า “ข้อมูล” (data) ซึ่งหมายถึง กลุ่มตัวอักขระที่เมื่อนำมารวมกันแล้วมีความหมายอย่างใดอย่างหนึ่งและมีสำคัญควรค่าแก่การจัดเก็บเพื่อนำไปใช้ในโอกาสต่อๆ ไป ข้อมูลมักเป็นข้อความที่อธิบายถึงสิ่งใดสิ่งหนึ่ง อาจเป็นตัวอักษร ตัวเลข หรือสัญลักษณ์ใด ๆ ที่สามารถนำไปประมวลผลด้วยคอมพิวเตอร์ได้[22] จึงอาจมีการให้คำจำกัดความที่แตกต่างกันออกไปตามการใช้งาน ดังนั้นไม่ว่าคำว่า “ข้อมูลคอมพิวเตอร์” หรือคำว่า “ข้อมูลอิเล็กทรอนิกส์” จึงไม่มีคำนิยามทางศาสตร์ทางด้านคอมพิวเตอร์แต่อย่างใด แต่หากจะให้กล่าวอย่างกว้างๆ แล้ว โดยปกติข้อมูลอิเล็กทรอนิกส์จะมีขอบเขตที่กว้างกว่า เนื่องจากโดยปกติคอมพิวเตอร์คืออุปกรณ์อิเล็กทรอนิกส์อย่างหนึ่ง ข้อมูลคอมพิวเตอร์จึงแคบกว่าข้อมูลอิเล็กทรอนิกส์ในความหมายโดยทั่วไป ดังนั้นที่จะต้องพิจารณาจึงเป็นการให้คำนิยามทางด้านกฎหมาย

2.1.2.2 การให้คำนิยามทางด้านกฎหมาย

เมื่อพิจารณาถึงความหมายของคำว่าข้อมูลในศาสตร์ทางด้านคอมพิวเตอร์แล้ว สิ่งที่ต้องพิจารณาต่อมาคือความหมายที่ปรากฏในแง่คำนิยามทางกฎหมาย โดยพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้นิยามคำว่า “ข้อมูลคอมพิวเตอร์” ไว้ในมาตรา 3 ว่า

---

[21] สัมภาษณ์ ธงชัย โรจน์กังสดาล, 30 มกราคม 2551.

[22] มหาวิทยาลัยราชภัฏสวนดุสิต, “วิชาเทคโนโลยีสารสนเทศเพื่อชีวิต บทที่ 1,” E-learning [Online] แหล่งที่มา : http://dusithost.dusit.ac.th/~librarian/it107/C1.html [20 ตุลาคม 2550]

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

เมื่อพิจารณาถึงนิยามของคำว่า “ข้อมูลคอมพิวเตอร์” แล้ว สิ่งที่จะต้องพิจารณาควบคู่ไปด้วยคือ ความหมายของคำว่า “ข้อมูลอิเล็กทรอนิกส์” เนื่องจากในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ให้ความหมายครอบคลุมไปถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

โดยในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 ซึ่งตราขึ้นเพื่อรับรองผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์อันเป็นการรับรองข้อความที่อยู่บนสื่ออิเล็กทรอนิกส์ให้เท่าเทียมกับข้อความที่อยู่บนกระดาษ และได้ให้ความหมายคำว่า “ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

อนึ่ง คำว่า “ข้อมูลอิเล็กทรอนิกส์” ตามกฎหมายฉบับนี้ไม่ได้จำกัดอยู่เฉพาะข้อมูลอิเล็กทรอนิกส์ที่ใช้ในการติดต่อสื่อสารเท่านั้น แต่มุ่งประสงค์ให้ครอบคลุมถึงข้อมูลหรือบันทึกที่สร้างขึ้นโดยคอมพิวเตอร์ แม้จะไม่ได้ใช้เป็นสื่อในการต่อต่อสื่อสารกับบุคคลอื่นก็ตาม และวิธีการทางอิเล็กทรอนิกส์ในที่นี้ให้รวมถึงพัฒนาการทางเทคโนโลยีในลักษณะอื่นที่คล้ายคลึงกันในอนาคต [23]

เมื่อพิจารณาถึงนิยามของคำว่า “ระบบคอมพิวเตอร์” และ “ข้อมูลคอมพิวเตอร์” แล้ว สิ่งที่จะต้องพิจารณาต่อมาคือการกระทำผิดทางอาญาเกี่ยวกับระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่เกิดขึ้น โดยการกระทำผิดทางอาญาที่เกี่ยวกับคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์นั้น มักเรียกกันว่าอาชญากรรมทางคอมพิวเตอร์ ซึ่งมีรายละเอียดดังนี้

2.1.3 อาชญากรรมทางคอมพิวเตอร์

---

[23] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, “คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544,” [Online] แหล่งที่มา : www.ecommerce.or.th/ictlaw [วันที่ 15 กันยายน 2550]

การกระทำความผิดทางคอมพิวเตอร์นั้นโดยมากแล้วมักจะเป็นการคุกคามหรือลักลอบเข้าไปในระบบโดยไม่ได้รับอนุญาตหรือโดยไม่มีอำนาจให้กระทำการดังกล่าว และนำไปสู่การกระทำผิดอื่นๆ ต่อไป เมื่อพิจารณาถึงความเป็นมาในการกระทำผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์แล้ว จะเห็นได้ว่าช่วงระหว่างปี 1950 – 1975 โปรแกรมคอมพิวเตอร์และข้อมูลจัดเก็บลงในแผ่นการ์ดที่เจาะรูเอาไว้ หากมีผู้บุกรุกเข้ามาไม่ว่าจะทำลายหรือลักเอาแผ่นการ์ดเหล่านี้ ผู้ที่กระทำเช่นนั้นสามารถที่จะถูกลงโทษในกฎหมายอาญาแบบเดิมในฐานความผิดบุกรุก ทำลาย หรือลักทรัพย์ได้

แต่หลังจากปี 1975 เป็นเรื่องธรรมดาที่จะเข้าสู่โปรแกรมและข้อมูลจากเครื่องคอมพิวเตอร์ที่อยู่ระยะไกลโดยใช้โมเด็มและสายโทรศัพท์ ทำให้ธนาคารเปิดบัญชีของลูกค้าจากส่วนกลางได้ และการค้าขายที่ทำรายการเก็บเงินโดยบัตรเครดิตปราศจากการส่งเอกสารที่เป็นกระดาษ การเปลี่ยนแปลงทางเทคโนโลยีเช่นนี้ทำให้อาชญากรสามารถเปลี่ยนแปลงข้อมูลและโปรแกรมในขณะที่อยู่ในบ้านโดยไม่ต้องเข้าไปในที่อยู่ของผู้เสียหายโดยทางกายภาพ ทำให้กฎหมายอาญาแบบเดิมไม่เพียงพอที่จะลงโทษอาชญากรได้อีกต่อไป จึงมีความจำเป็นจะต้องกำหนดกฎหมายเฉพาะขึ้นเพื่อที่จะลงโทษผู้กระทำผิดดังกล่าวต่อไป

ซึ่งการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้น โดยลักษณะของความผิดแล้วถูกจัดอยู่ในประเภทของอาชญากรรมทางคอมพิวเตอร์อย่างหนึ่ง ซึ่งหากจะให้นิยามความหมายของอาชญากรรมคอมพิวเตอร์แล้ว อาจจะให้ความหมายง่ายๆ ว่า อาชญากรรมคอมพิวเตอร์ คือ การใช้คอมพิวเตอร์เพื่ออำนวยความสะดวกหรือนำไปสู่การกระทำผิดทางอาญา ซึ่งอาชญากรรมคอมพิวเตอร์นั้นนักวิชาการจัดให้เป็นอาชญากรรมทางเศรษฐกิจประเภทหนึ่ง เนื่องจากบุคคลที่จะประกอบอาชญากรรมทางคอมพิวเตอร์ได้ต้องมีความรู้ความสามารถ ไม่ใช่อาชญากรรมโดยทั่วไปที่ไม่ต้องอาศัยเทคนิคหรือวิธีการที่เป็นพิเศษในการประกอบอาชญากรรมขึ้น

กระทรวงยุติธรรมของประเทศสหรัฐอเมริกาได้ให้คำนิยามคำว่า “อาชญากรรมคอมพิวเตอร์” ไว้ว่า เป็นการกระทำที่ต้องอาศัยประสบการณ์ทางคอมพิวเตอร์ โดยทั่วไปอาชญากรรมประเภทนี้จะเกิดขึ้นภายในเครื่องคอมพิวเตอร์ ส่วนคำว่า “อาชญากรรมที่เกี่ยวกับคอมพิวเตอร์” เป็นคำที่กว้างกว่า หมายความถึงการกระทำความผิดทางอาญาที่อาศัยความรู้ทางด้านเทคโนโลยีสารสนเทศเพื่อกระทำความผิด รวมทั้งการสืบสวนสอบสวนและฟ้องร้อง จึงอาจกล่าวได้ว่า คำว่า “การใช้คอมพิวเตอร์การกระทำความผิด” เป็นการรวมความหมายที่กว้าง คือ การกระทำโดยเจตนาที่เป็นความผิดอาญา ซึ่งเป็นการกระทำโดยเจตนาใดๆ ที่อาศัยความรู้

ทางด้านเทคโนโลยีสารสนเทศกระทำความผิดโดยบุคคลหนึ่งหรือมากกว่านั้น เพื่อที่จะให้เหยื่อได้รับความเสียหาย[24]

ในขณะที่สำนักงานตำรวจแห่งชาติได้ให้คำนิยามของคำว่า "อาชญากรรมคอมพิวเตอร์" ไว้ดังนี้[25]

1. การกระทำใดๆ ก็ตามที่เกี่ยวกับการใช้คอมพิวเตอร์อันทำให้คอมพิวเตอร์อันทำให้เหยื่อได้รับความเสียหายและผู้กระทำได้รับผลประโยชน์ตอบแทน

2. การกระทำผิดกฎหมายใดๆ ซึ่งใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือและในการสืบสวนสอบสวนของเจ้าหน้าที่เพื่อนำตัวผู้กระทำผิดมาดำเนินคดีก็ต้องใช้ความรู้ทางเทคโนโลยีคอมพิวเตอร์เช่นกัน

โดยปัจจุบันทั่วโลก ได้จำแนกประเภทอาชญากรรมทางคอมพิวเตอร์ได้ 9 ประเภท (ตามข้อมูลคณะอนุกรรมการเฉพาะกิจร่างกฎหมายอาชญากรรมทางคอมพิวเตอร์) ดังนี้

1. การขโมยข้อมูลทางอินเตอร์เน็ต รวมถึงการขโมยประโยชน์ในการลักลอบใช้บริการ

2. การปกปิดความผิดของตัวเอง โดยใช้ระบบการสื่อสาร

3. การละเมิดลิขสิทธิ์ ปลอมแปลงรูปแบบเลียนแบระบบซอฟแวร์โดยมิชอบ

4. การเผยแพร่ภาพ เสียง ลามก อนาจาร และข้อมูลที่ไม่เหมาะสม

5. การฟอกเงิน

6. การก่อกวนระบบคอมพิวเตอร์ เช่น ทำลายระบบสาธารณูปโภค เช่น ระบบจ่ายน้ำ จ่ายไฟ จราจร

7. การหลอกลวงให้ร่วมค้าขาย หรือ ลงทุนปลอม (การทำธุรกิจที่ไม่ชอบด้วยกฎหมาย)

---

[24] Parker,D.B. and Nycum, S.H., Computer abuse, (California: Standford Research Institute, 1973) อ้างถึงใน เลิศชาย สุธรรมพร, "อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีความปลอดภัยของข้อมูล," (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2541), หน้า 36.

[25] สำนักงานตำรวจแห่งชาติ,"อาชญากรรมคอมพิวเตอร์," [Online] แหล่งที่มา : www.royalthaipolice.go.th [วันที่ 12 มกราคม 2551]

8. การลักลอบใช้ข้อมูลเพื่อแสวงหาผลประโยชน์ในทางมิชอบเช่น การขโมยรหัสบัตรเครดิต

9. การใช้คอมพิวเตอร์ในการโอนบัญชีผู้อื่นเป็นของตัวเอง

ซึ่งลักษณะของอาชญากรทางคอมพิวเตอร์ อาจจำแนกประเภท ได้ดังต่อไปนี้[26]

1. **พวกเด็กหัดใหม่** (Novice)

เป็นพวกที่เพิ่มเริ่มเข้าสู่วงการ หัดใช้คอมพิวเตอร์ หรืออาจเป็นพวกที่เพิ่งเข้าสู่ตำแหน่งที่มีอำนาจหรือเพิ่งได้รับความไว้วางใจให้เข้าสู่ระบบเครือข่ายคอมพิวเตอร์

2. **พวกจิตวิปริต** (Deranged persons)

มักเป็นพวกที่มีจิตใจวิปริต ผิดปกติ มีลักษณะเป็นพวกที่ชอบความรุนแรง และอันตราย มักเป็นผู้ที่ชอบทำลายไม่ว่าจะเป็นการทำลายข้าวของหรือบุคคล เช่น พวก UNA Bomber แต่เนื่องจากจำนวนอาชญากรประเภทนี้มีไม่มากนัก จึงทำให้ผู้รักษากฎหมายไม่ได้ให้ความสนใจ

3. **เป็นกลุ่มที่ประกอบอาชญากรรมในลักษณะองค์กร** (Organized crime)

องค์กรอาชญากรรมจะใช้คอมพิวเตอร์ในลักษณะที่แตกต่างกัน โดยส่วนหนึ่งอาจใช้เป็นเครื่องมือในการหาข่าวสาร เช่นเดียวกับองค์กรธุรกิจทั่วไป หรืออาจใช้เทคโนโลยีของคอมพิวเตอร์นี้เป็นตัวประกอบสำคัญในการก่ออาชญากรรม หรืออาจใช้เทคโนโลยีคอมพิวเตอร์นี้ในการที่ทำให้เจ้าหน้าที่ตามไม่ทันอาชญากรรมที่ตนก่อขึ้น

4. **อาชญากรอาชีพ** (Carriere Criminal)

เป็นกลุ่มอาชญากรรมคอมพิวเตอร์ที่ทวีจำนวนมากขึ้นเรื่อยๆ เป็นผู้ก่ออาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์นี้ครั้งแล้วครั้งเล่า โดยอาชญากรประเภทนี้อาจจะเคยถูกจับกุมในความผิดประเภทนี้มาก่อนแล้ว เป็นผู้ที่กระทำผิดโดยสันดาน

แบ่งเป็น 4 กลุ่ม

- ทำลายเวปคู่แข่ง

---

[26] พันตำรวจเอกญาณพล ยั่งยืน, “อาชญากรรมคอมพิวเตอร์,” เอกสารประกอบการสัมมนาโครงการเพิ่มศักยภาพข้าราชการฝ่ายตุลาการศาลอุทธรณ์ภาค 9 ประจำปี พ.ศ. 2550, 20 กรกฎาคม 2550.

- เจาะระบบเพื่อขโมยข้อมูล
- พยายามเจาะระบบของผู้จ้างเพื่อหาจุดอ่อน
- เจาะระบบก่อนไปเสนอขายระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์

5. **พวกหัวพัฒนา มีความก้าวหน้า** (Conartists)

เป็นพวกที่ชอบใช้ความก้าวหน้าทางคอมพิวเตอร์เพื่อให้ได้มาเพื่อผลประโยชน์มาสู่ตน อาชญากรประเภทนี้จะใช้ความรู้ด้านเทคโนโลยีและระบบคอมพิวเตอร์ที่ตนมีอยู่ในการที่จะหาเงินให้กับตนเองโดยมิชอบด้วยกฎหมาย

6.**พวกคลั่งลัทธิ**(Dremer) / **พวกช่างคิดช่างฝัน**(Ideologues)

เป็นผู้ที่กระทำผิดเนื่องจากมีความเชื่อถือสิ่งใดสิ่งหนึ่งอย่างรุนแรง

7. **ผู้ที่มีความรู้และทักษะด้านคอมพิวเตอร์อย่างดี** (Hacker/Cracker)

โดย Hacker หมายถึง บุคคลผู้ที่เป็นอัจฉริยะ มีความรู้ในระบบคอมพิวเตอร์เป็นอย่างดี สามารถเข้าไปถึงข้อมูลในคอมพิวเตอร์โดยเจาะผ่านระบบ รักษาความปลอดภัยของคอมพิวเตอร์ได้ แต่อาจไม่แสวงหาผลประโยชน์

และอีกคำหนึ่งคือ Cracker ซึ่งหมายถึง ผู้ที่มีความรู้และทักษะทางคอมพิวเตอร์เป็นอย่างดี จนสามารถเข้าสู่ระบบได้ เพื่อเข้าไปทำลายหรือลบแฟ้มข้อมูล หรือทำให้เครื่องคอมพิวเตอร์ เสียหายรวมทั้งการทำลายระบบปฏิบัติการของเครื่องคอมพิวเตอร์

ดังจะเห็นได้ว่าอาชญากรรมทางคอมพิวเตอร์มีหลายประเภท โดยวิทยานิพนธ์ฉบับนี้จะขอกล่าวถึงอาชญากรรมทางคอมพิวเตอร์ที่เกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์เท่านั้น โดยการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ในแง่ความผิดอาญา อาจแบ่งเป็น 4 ลักษณะ คือ

1. การเจาะระบบรักษาความปลอดภัยทางกายภาพ ได้แก่ ตัวอาคาร อุปกรณ์และสื่อต่างๆ

2. การเจาะเข้าไปในระบบสื่อสารและการรักษาความปลอดภัยของซอฟต์แวร์ข้อมูลต่างๆ เช่น กรณีที่มี firewall หรือ anti-virus

3. เป็นการเจาะเข้าสู่ระบบรักษาความปลอดภัยของระบบปฏิบัติการ (Operating System) เช่น การกำหนดรหัสผ่านหรือแสกน

4. เป็นการเจาะผ่านระบบรักษาความปลอดภัยส่วนบุคคลโดยใช้อินเทอร์เน็ตเป็นช่องทางในการกระทำความผิด

ซึ่งการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ อาจพิจารณาได้ดังนี้

2.2 การเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

การเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นเป็นการกระทำผิดโดยใช้คอมพิวเตอร์ในฐานะที่เป็นเป้าหมายหรือวัตถุแห่งการกระทำความผิด (Computers as the target of the crime) โดยผู้กระทำความผิดมีเป้าหมายอยู่ที่ระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์เป็นสำคัญ ทั้งนี้อาจเป็นการเข้าถึง ทำลาย เปลี่ยนแปลง หรือกระทำด้วยประการใด ๆ เพื่อให้ระบบและข้อมูลดังกล่าวได้รับความเสียหาย เปลี่ยนแปลงไปจากเดิม โดยตนเองอาจได้รับประโยชน์จากการกระทำดังกล่าวด้วยหรือไม่ก็ตาม

ซึ่งการกระทำดังกล่าวเป็นการกระทำที่มีลักษณะใหม่โดยอาศัยเทคโนโลยีที่พัฒนาไปเป็นเครื่องมือส่งเสริมการกระทำผิด โดยมีรูปแบบการกระทำความผิดแบบใหม่ทั้งหมดไม่ว่าจะเป็น วิธีการ หรือวัตถุที่ถูกกระทำต่อ จนไม่อาจตีความกฎหมายเดิมที่มีอยู่ให้ครอบคลุมได้ และจำเป็นต้องบัญญัติกฎหมายใหม่เพื่อกำหนดฐานความผิดใหม่ขึ้น

2.2.1 ความหมายของการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

การเข้าถึง (access) คอมพิวเตอร์นั้น อาจแยกออกได้เป็น 2 กรณี คือ การเข้าถึงในความหมายอย่างแคบ คือการเข้าไปโดยเทียบเคียงกับลักษณะของการบุกรุกที่เกิดขึ้นในโลกทางกายภาพ กล่าวคือมีการเข้าไป (inside) ในคอมพิวเตอร์ โดยได้มีการล่วงล้ำเข้าไปอย่างแท้จริงโดยเทียบกับการบุกรุกที่มีการเข้าถึงสถานที่นั้น แต่การเข้าถึงคอมพิวเตอร์ในความหมายอย่างกว้างนั้นมีแนวคิดที่อ้างอิงกับการทำงานของคอมพิวเตอร์เป็นหลัก โดยมุ่งเน้นที่ไปการทำงานของคอมพิวเตอร์ที่เกิดขึ้นโดยเห็นว่าการเข้าถึงนั้นคือการทำให้คอมพิวเตอร์ทำงาน หากทำให้คอมพิวเตอร์มีการตอบสนอง (response) กับคำสั่งที่ได้มีการสั่ง (input) นั้น

นอกจากนี้ ได้มีผู้ให้คำนิยามของคำว่า "การเข้าถึง" (Access) ไว้ว่าเป็นการเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้ ดังนั้น จึงอาจหมายถึง การเข้าถึงฮาร์ดแวร์หรือส่วนประกอบต่างๆ ของคอมพิวเตอร์ หรือข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง เช่น ข้อมูลจราจร เป็นต้น

โดย "การเข้าถึง" ยังสามารถหมายถึงการเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต อันเป็นการเชื่อมโยงระหว่างเครือข่ายหลายๆ เครือข่ายเข้าด้วยกัน และยังหมายถึง การเข้าถึงโดยผ่านระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบ LAN (Local Area Network) อันเป็นเครือข่ายที่เชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้ๆ กันเข้าด้วยกัน

การที่กำหนดให้การเข้าถึงโดยปราศจากอำนาจหรือโดยฝ่าฝืนกฎหมาย และการใช้คอมพิวเตอร์ในทางมิชอบการกระทำความผิดด้วยการเข้าถึงโดยไม่มีอำนาจหรือโดยฝ่าฝืนกฎหมาย และการใช้คอมพิวเตอร์ในทางมิชอบ ถือเป็นการกระทำที่คุกคามหรือเป็นภัยต่อความปลอดภัย (Security) ของระบบคอมพิวเตอร์และระบบข้อมูลที่มีผลกระทบต่อความครบถ้วน (Integrity) การรักษาความลับ (Confidential) และเสถียรภาพในการใช้งาน (Availability) ของระบบข้อมูลและระบบคอมพิวเตอร์ ซึ่งจะนำมาซึ่งความเสียหายหรือการกระทำผิดอื่นต่อไป ดังนั้นในหลายประเทศจึงได้มีการกำหนดให้การเข้าถึงโดยมิชอบเป็นความผิดขึ้น การเข้าถึงโดยมิได้รับอนุญาตนี้เกิดขึ้นเมื่อผู้กระทำประสบความสำเร็จในการเข้าสู่เป้าหมาย ซึ่งเป็นโปรแกรมหรือไฟล์คอมพิวเตอร์ ผู้กระทำอาจเป็นบุคคล หรือ เป็นคอมพิวเตอร์ที่ถูกสั่งการให้กระทำโดยการโปรแกรม การเข้าถึงอาจจะสำเร็จได้ด้วยทางอิเล็กทรอนิกส์ เช่น ผ่านทางรหัส/password และโดยกลไกอื่น ๆ หรือ สำเร็จได้ด้วยทางกายภาพ เช่น การลักรหัสประจำตัว /personal identification passwords (PIN)[27]

การเข้าถึงระบบโดยมิชอบนี้ สามารถก่อให้เกิดความเสียหายแก่บุคคลเป็นส่วนตัว หรือแก่องค์กรโดยรวม เช่น การเข้าถึงข้อมูลส่วนบุคคลย่อมเป็นอันตรายต่อสิทธิส่วนบุคคล (privacy) ของเหยื่อ หากว่า ผู้กระทำนำเข้ามูลส่วนบุคคลนั้นไปเผยแพร่หรือจำหน่ายต่อให้แก่บุคคลที่สาม

ในขณะที่การเข้าถึงระบบทางการค้า ข้อมูล หรือความลับทางการค้าของบริษัทเหยื่อย่อมเป็นอันตรายต่อการล่วงรู้โดยมิชอบต่อความลับทางการค้าของธุรกิจคู่แข่ง หากผู้กระทำนำข้อมูลดังกล่าวไปเผยแพร่หรือจำหน่ายต่อคู่แข่งทางการค้าของเหยื่อ แน่นอนว่าในกรณีนี้ผู้กระทำหวังผลประโยชน์ทางการเงินจากการเข้าถึงข้อมูลดังกล่าว

---

[27] นพมาศ ประสิทธิ์มณฑล, “อาชญากรรมคอมพิวเตอร์ ตามกฎหมายสหรัฐอเมริกา,” กฎหมายอิเล็กทรอนิกส์เพื่อการศึกษา [Online] แหล่งที่มา : www.geocities.com/elaw007 [14 กันยายน 2550]

โดยทั่วไปผู้กระทำในลักษณะนี้จะมีมูลเหตุจูงใจที่แตกต่างกันไปในการเลือกที่จะเข้าถึงแต่ละประเภท เช่น พวกที่มีมูลเหตุจูงใจทางการเงิน (จารกรรมลิขสิทธิ์ หรือความลับทางการค้า) พวกค้ากำไรจากศัตรูของเหยื่อ (จารกรรมข้อมูล) พวกทำเพื่อสนองความพอใจส่วนตัว (สืบความลับคู่รักหรือศัตรู) รวมไปถึงต้องการท้าทายกฎหมาย (แอบอ้างตัว) หรือพวกที่มีความแค้นต้องการเอาคืน ซึ่งโดยมากเป็นลูกจ้างหรืออดีตลูกจ้างที่ต้องการแก้แค้นนายจ้างตัวเอง [28]

2.2.2 ลักษณะของการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

ลักษณะของการเข้าถึงโดยปราศจากอำนาจ (Computer hacking) ในช่วงระยะเวลาเริ่มต้นนั้น อาจกล่าวได้ว่า ความผิดรูปแบบนี้ในระยะแรกๆ ผู้กระทำส่วนใหญ่ไม่ได้มีเป้าหมายในการกระทำความผิดอย่างอื่น อาทิ เปลี่ยนแปลงข้อมูลเพื่อหลอกลวง ทำลายระบบหรือจารกรรมข้อมูลด้วยเลย ผู้กระทำต้องการเพียงทดลองหรือทดสอบความสามารถของตนในการฝ่าระบบรักษาความปลอดภัยของผู้อื่นเท่านั้น โดยการเจาะระบบคอมพิวเตอร์นี้ คาดว่าเกิดขึ้นครั้งแรกในราวปี 1980 โดย Mitnick Kevin ซึ่งทำการเจาะเข้าไปในระบบคอมพิวเตอร์ของบริษัท US-Leasing[29]

ความผิดลักษณะนี้เกิดขึ้นบ่อยครั้งทั้งจากนักเจาะระบบมืออาชีพและแบบสมัครเล่น ความเสียหายจึงอาจแตกต่างกันไป และแม้คดีส่วนใหญ่ที่เกิดขึ้นจะเป็นกรณีที่สร้างความเสียหายต่อระบบรักษาความปลอดภัยของบริษัทหรือหน่วยงานที่ถูกเจาะระบบเท่านั้น แต่ในหลายคดีก็สร้างความเสียหายอื่นๆตามมาด้วย เมื่อปรากฏว่าผู้เจาะระบบนั้นนำเทคนิควิธีการที่ตนใช้ไปเผยแพร่ต่อยังบุคคลอื่นซึ่งอาจนำไปใช้ในการกระทำความผิดอื่นๆ ต่อไปอีก

โดยตัวอย่างคดีสำคัญที่เกิดขึ้นมาแล้ว ได้แก่ คดีในปี 1985 ในมลรัฐ New Jersey มีเด็กนักเรียนชาย 7 คน ได้ทำการเจาะระบบเข้าไปที่คอมพิวเตอร์ของหน่วยงานเพนทากอน และมีรายงานว่าตั้งแต่ปี 1986 เป็นต้นมาระบบคอมพิวเตอร์ตามหน่วยงานสำคัญ ๆ ของประเทศสหรัฐอเมริกาโดนเจาะระบบบ่อยครั้ง ดังเช่น ปี 1995 เพนทากอนรายงานว่า ระบบคอมพิวเตอร์ของหน่วยงานถูกโจมตีถึง 250,000 ครั้ง จนคาดกันว่า ข้อมูล หรือเทคนิคการเข้าถึง

---

[28] เรื่องเดียวกัน,

[29] สาวตรี สุขศรี, “ประวัติศาสตร์อาชญากรรมคอมพิวเตอร์,” [Online] แหล่งที่มา : www.biolawcom.de [19 สิงหาคม 2550]

ดังกล่าว อาจถูกนำไปขายต่อให้ KGB หรือ หน่วยรักษาความมั่นคง และหน่วยสืบราชการลับของรัสเซียด้วย[30]

2.2.3 ประเภทของการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

เครื่องคอมพิวเตอร์เครื่องเดียว เรียกว่า Stand Alone Computer ซึ่งแปลตรงตัวว่า เครื่องคอมพิวเตอร์ที่อยู่โดดเดี่ยว ซึ่งแต่เดิมเครื่องคอมพิวเตอร์แต่ละเครื่องจะมีการทำงานที่แยกจากกัน แต่เมื่อมนุษย์มีการพัฒนาการติดต่อสื่อสารมากขึ้นการเคลื่อนย้ายข้อมูลจำนวนมากจากที่หนึ่งไปยังอีกที่หนึ่งกลายเป็นสิ่งจำเป็น จึงได้เกิดแนวความคิดที่จะนำเอาเครื่องคอมพิวเตอร์มาเชื่อมต่อกันผ่านสายสัญญาณ (Signal Cable) ซึ่งจะทำให้เกิดการส่งผ่านข้อมูลระหว่างเครื่องคอมพิวเตอร์เร็วกว่าการบันทึกข้อมูลใส่อุปกรณ์บันทึกข้อมูลแล้วนำไปยังเครื่องอื่นๆ เป็นอย่างมาก โดยเรียกการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์เช่นนี้ว่า “ระบบเครือข่ายคอมพิวเตอร์” (Computer Networks) ซึ่งพัฒนาการนี้เองที่ทำให้การเจาะระบบคอมพิวเตอร์สามารถทำได้ง่าย รวดเร็ว และเกิดผลกระทบเป็นลูกโซ่

เนื่องจากในอดีตการที่คอมพิวเตอร์ทำงานแยกจากกัน การเจาะระบบก็จะทำได้เฉพาะเครื่องนั้นเท่านั้นเป็นมักเป็นทางด้านกายภาพไม่สามารถทำได้จากระยะห่างไกล แม้ทำให้จะเกิดความเสียหาย หากแต่ผลกระทบยังไม่ขยายเป็นวงกว้างและการเจาะระบบก็มีข้อจำกัดทั้งในเรื่องเวลาหรือระยะทาง แต่เทคโนโลยีในระบบเครือข่ายทำให้การเจาะระบบสามารถเกิดได้ทุกที่และสามารถใช้เวลาเท่าใดก็ได้ นอกจากนี้เมื่อทำการเจาะระบบได้แล้ว การที่จะเชื่อมต่อไปยังเครื่องคอมพิวเตอร์เครื่องอื่นก็สามารถทำได้ ซึ่งก่อนที่จะพิจารณาถึงการเข้าถึงระบบคอมพิวเตอร์นั้น ก่อนอื่นต้องทำความเข้าใจในเรื่องระบบเครือข่ายคอมพิวเตอร์ก่อนเพื่อให้เกิดความเข้าใจในประเภทและลักษณะการเข้าถึงระบบคอมพิวเตอร์ต่อไป

ระบบเครือข่ายคอมพิวเตอร์ (Computer Networks) หมายถึงการนำเอาเครื่องคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไปมาเชื่อมโยงต่อเข้าด้วยกันโดยอาศัยสายเคเบิลชนิดต่างๆ และมีเครื่องคอมพิวเตอร์ขนาดใหญ่เป็นศูนย์กลางในการจัดเก็บและประมวลผลข้อมูลเครื่องคอมพิวเตอร์ศูนย์กลางนี้เรียกว่า “แม่ข่าย” เพื่อประโยชน์ในการใช้โปรแกรมซอฟต์แวร์และข้อมูลร่วมกันในการติดต่อสื่อสารและการแลกเปลี่ยนข้อมูลข่าวสารระหว่างผู้ใช้คอมพิวเตอร์ในเครือข่ายอีกด้วย โดยผู้ใช้คอมพิวเตอร์สามารถใช้งานผ่านคอมพิวเตอร์เครื่องใดๆ ก็ได้ในเครือข่าย

---

[30] เรื่องเดียวกัน,

หากจำแนกระบบเครือข่ายคอมพิวเตอร์ตามระยะทางการเชื่อมต่อระหว่างอุปกรณ์สื่อสาร สามารถแบ่งออกได้เป็น 3 ลักษณะ ดังนี้[31]

1. **Local Area Network (LAN)** ระบบเครือข่ายแบบนี้จะเป็นเครือข่ายคอมพิวเตอร์ที่มีการเชื่อมต่ออุปกรณ์สื่อสารในระยะทางที่จำกัด ซึ่งมีความเร็วในการแลกเปลี่ยนข้อมูลสูงเป็นเครือข่ายที่ใช้ในหน่วยงานต่างๆ เฉพาะกลุ่ม จึงเป็นระบบเครือข่ายแบบปิด (Close Network) เช่น ระบบอินทราเน็ต (Intranet) เป็นต้น

2. **Metropolitan Area Network (MAN)** เป็นระบบเครือข่ายคอมพิวเตอร์ขนาดใหญ่ครอบคลุมพื้นที่มากกว่าระบบเครือข่ายแบบ LAN เครือข่ายนี้เกิดจากการเชื่อมต่อของเครือข่ายคอมพิวเตอร์แบบ LAN ตั้งแต่ 2 เครื่องเข้าด้วยกัน

3. **Wide Area Network (WAN)** เป็นระบบเครือข่ายคอมพิวเตอร์ที่มีขนาดใหญ่ประกอบด้วยระบบเครือข่ายคอมพิวเตอร์ทั้งแบบ LAN และเครือข่ายคอมพิวเตอร์แบบ MAN พื้นที่ของเครือข่ายสามารถครอบคลุมพื้นที่ได้ในระดับประเทศหรือระดับโลก และเป็นระบบเครือข่ายแบบเปิด (Open Network) ซึ่งระบบเครือข่ายอินเทอร์เน็ต (Internet) ก็เป็นระบบเครือข่ายแบบ WAN เช่นกัน

ดังกล่าวมาแล้วว่า เมื่อเทคโนโลยีด้านนี้ยังได้รับการพัฒนาต่อ รูปแบบการกระทำความผิด ก็ย่อมมีการพัฒนา และขยายตัวไปด้วย การเจาะระบบก็เช่นเดียวกัน ปัจจุบันไม่เฉพาะแต่ระบบคอมพิวเตอร์เท่านั้นที่เป็นเป้าหมายของการกระทำความผิด ระบบให้บริการอื่น ๆ โดยเฉพาะอย่างยิ่ง บริการโทรศัพท์ทางอินเทอร์เน็ต โทรศัพท์ทางไกล บริการจดหมายเสียง ได้กลายเป็นเป้าหมายใหญ่ของนักเจาะระบบ และการเข้าถึงต่าง ๆ ดังกล่าวย่อมมิใช่เพียงแค่การได้ทำลายระบบป้องกัน หรือรักษาความปลอดภัยอย่างเดียวแบบเดิม ๆ แต่ผู้กระทำยังมีเป้าหมายเพื่อลักลอบใช้บริการเหล่านั้นโดยไม่ต้องเสียเงินอีกด้วย ดังนั้น จากที่แต่เดิมความผิดในฐานนี้อาจ

---

[31] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, <u>กฎหมายธุรกรรมทางอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์</u> (กรุงเทพฯ : สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศ แห่งชาติ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, 2544), หน้า 36-37.

ไม่ได้เป็นภัยต่อเศรษฐกิจมากนัก แต่ปัจจุบันการกระทำดังกล่าวได้สร้างความเสียหายอย่างกว้างขวางไม่แพ้ความผิดในรูปแบบอื่น ๆ[32]

โดยลักษณะของความผิดที่สำคัญและเป็นที่รู้จักกันเป็นอย่างดี คือ การเจาะระบบ (Hacking and Cracking) หมายถึง การเข้าไปในระบบคอมพิวเตอร์โดยไม่มีอำนาจ ซึ่งอาจเป็นกรณีการเข้าถึงในระดับกายภาพ คือ กรณีผู้กระทำความดำเนินการโดยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านและใช้เครื่องคอมพิวเตอร์ของผู้อื่นนั้นโดยตรงหรืออาจเป็นกรณีการเข้าถึงโดยผู้กระทำอยู่ห่างโดยระยะทาง เช่น การเจาะระบบผ่านทางเครือข่ายอินเทอร์เน็ต อินทราเน็ต หรือ ระบบ LAN การเข้าถึงระบบหรือข้อมูลคอมพิวเตอร์โดยผู้กระทำมิได้มีเหตุจูงใจหรือต้องการทำให้เกิดความเสียหายต่อระบบ หรือข้อมูลเลย เรียกว่า Hacking ส่วนกรณีที่เข้าไปโดยมีมูลเหตุเพื่อทำลาย หรือก่อให้เกิดความเสียหายต่อระบบ หรือข้อมูลด้วย จะเรียกว่า Cracking นอกจากนี้ยังมีวิธีการอื่นๆ อีก เช่น

1 Superzapping คือ การกระทำความผิดด้วยการใช้เครื่องมือของระบบที่ทำให้สามารถเข้าไปในระบบคอมพิวเตอร์ได้ในกรณีฉุกเฉิน เปรียบเสมือนกุญแจผีที่จะนำมาใช้ก็ต่อเมื่อกุญแจดอกหลักหายหรือมีปัญหา มาจากคำว่า Superzap ซึ่งเป็นโปรแกรม macro-utility ที่นิยมใช้มากในศูนย์คอมพิวเตอร์ของบริษัท IBM ตัวอย่างความผิดที่พบ คือ กรณีผู้ครอบครองหรือรู้วิธีใช้ system tool ดังกล่าว เข้าไปในระบบ แล้วเปลี่ยนแปลงเงินในกองทุน หรือเปลี่ยนข้อมูลบางอย่างเพื่อประโยชน์ต่อตนเอง

2 Piggybacking ซึ่งมี 2 ลักษณะด้วยกันคือ

2.1 Physical (ทางกายภาพ) ผู้กระทำความผิดจะลักลอบ หรือหาวิธีเข้าไปในเขตควบคุม ซึ่งอาจควบคุมด้วยประตู ไฟฟ้า หรือเครื่องกล โดยรอให้บุคคลที่มีอำนาจมาใช้ประตู เมื่อประตูเปิดผู้กระทำความผิดจะฉวยโอกาส ตอนประตูยังไม่ปิดสนิทเข้าไปด้วย เป็นต้น และ

2.2 Electronic (ทางอิเล็กทรอนิกส์) ซึ่งอาจเกิดขึ้นได้กรณีที่เมื่อมีการใช้สายการสื่อสารเดียวกันกับผู้ได้รับอนุญาต เช่น ใช้สายเคเบิล หรือผ่านโมเด็ม เป็นต้น[33]

---

[32] สาวตรี สุขศรี, ประวัติศาสตร์อาชญากรรมคอมพิวเตอร์ [Online]

[33] แหล่งที่มา : www.siamsewana.org [15 ตุลาคม 2550]

3 Cracking Passwords, Codes and Keys ระบบที่ใช้ระบบรักษาความปลอดภัยแบบมีรหัสเข้า หรือกระบวนการเข้ารหัสข้อมูลจะถูกโจมตีโดยการเดาหรือการค้นหารหัสหรือกุญแจการเข้ารหัสข้อมูล ที่เรียกกันทั่วไปว่า มีรอยแตก (Cracking)

4 Exploiting Flaws in Design, Implementation or Operation เป็นการเข้าถึงโดยไม่ได้รับอนุญาต โดยการใช้ประโยชน์จากจุดบกพร่องของการออกแบบ การสนับสนุนและการปฏิบัติการของระบบรักษาความปลอดภัยที่ไม่ได้ป้องกันเอาไว้ ซึ่งเกิดจากข้อผิดพลาดจากการเขียนโปรแกรม หรือขาดความตั้งใจในการรักษาความปลอดภัย หรือโครงสร้างไม่ดีระบบการปฏิบัติการใหม่หรือสถาปัตยกรรมใหม่เช่น JAVA เป็นจุดที่ถูกโจมตีได้[34]

2.2.4 รูปแบบของการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

การเข้าถึง[35] (Access) หมายถึง เข้าไปสู่ สั่ง สื่อสารกับ ใส่ข้อมูลเข้าไปเก็บไว้ ล้วงข้อมูลมาจาก หรืออีกนัยหนึ่ง เอาประโยชน์ใดๆ ของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข่ายงานคอมพิวเตอร์มาใช้ ดังนั้นการเข้าถึงโดยไม่มีอำนาจจะหมายถึง การกระทำที่ผู้กระทำไม่ได้รับอนุญาตให้ผ่านเข้าไปในระบบ หรือข้อมูลาคอมพิวเตอร์ที่มีการรักษาความปลอดภัย เช่น การตั้งรหัสผ่านไว้ (Password) หรือ Firewalls[36] ซึ่งอาจเกิดขึ้นได้หลายวิธี เช่น การเจาะระบบ (hacking หรือ cracking) โดยจะเรียกผู้กระทำผิดในลักษณะนี้ว่า Hacker ซึ่งหมายถึงบุคคลผู้เจาะระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต[37]

2.2.4.1 ทางกายภาพ

---

[34] ดร. ไพจิตร สวัสดิสาร, การใช้คอมพิวเตอร์ทางกฎหมายและกฎหมายเกี่ยวกับคอมพิวเตอร์ (กรุงเทพมหานคร : โรงพิมพ์ ชวนพิมพ์ 50, 2550), หน้า 105-108.

[35] ภานุ รังสีสหัส, “การกระทำความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์,” (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2533), หน้า 53.

[36] เป็นอุปสรรคที่ใช้ในระบบรักษาความปลอดภัย โดยจะทำการตรวจสอบเพื่อบ่งชี้ว่าผู้ใดเป็นผู้ใช้คอมพิวเตอร์ก่อนที่จะอนุญาตให้ผู้ใช้ดังกล่าวผ่านเข้าสู่ระบบ

[37] เชิดพันธ์ อุปนิสากร, “ความรับผิดทางอาญาของผู้เข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต,” (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2542), หน้า 53.

การเข้าถึงในแง่ทางกายภาพคือการเข้าถึงโดยสัมผัสกับเครื่องคอมพิวเตอร์เครื่องนั้นโดยตรง เช่น การเข้าถึงผ่านเมาส์หรือคีย์บอร์ดของเครื่องคอมพิวเตอร์เครื่องนั้น การเข้าถึงในแง่นี้มักเกิดจากผู้ที่ใช้เครื่องคอมพิวเตอร์เครื่องนั้นอยู่แล้ว หรือเป็นผู้ที่ทำงานหรืออยู่ในหน่วยงานหรือองค์กรนั้น เพราะเป็นการยากที่บุคคลภายนอกหน่วยงานหรือองค์กรจะสามารถเข้าเครื่องคอมพิวเตอร์โดยตรงได้ ดังนั้นคดีที่เกิดขึ้นโดยทั่วไปในกรณีเช่นนี้มักจะพบว่าผู้กระทำเป็นลูกจ้าง ข้าราชการ หรือพนักงานในองค์กรนั้นๆ เป็นผู้กระทำความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ขึ้น

2.2.4.2 **ทางระบบเครือข่าย**

ดังที่ได้กล่าวมาแล้วข้างต้นว่าระบบเครือข่ายคอมพิวเตอร์คือการนำเอาเครื่องคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไปมาเชื่อมโยงต่อเข้าด้วยกัน โดยความสามารถในการเชื่อมต่อแล้วแต่ประเภทของระบบเครือข่ายที่ใช้ ซึ่งเมื่อมีการเชื่อมต่อก็ทำให้การเจาะระบบก็สามารถทำได้ผ่านระบบเครือข่ายดังกล่าวด้วยเช่นกัน สามารถเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ผ่านเครือข่ายได้ในระยะทางไกล ไม่จำเป็นต้องสัมผัสกับเครื่องคอมพิวเตอร์เครื่องนั้นโดยตรง ซึ่งผู้กระทำความผิดในลักษณะเช่นนี้อาจเป็นได้ทั้งผู้ที่ทำงานในหน่วยงานหรือองค์กรนั้นที่เจาะระบบโดยผ่านระบบเครือข่ายของหน่วยงานหรือบริษัท เช่น ระบบ LAN หรือเป็นบุคคลภายนอกที่เจาะระบบเข้ามาโดยผ่านเครือข่ายในระบบอินเทอร์เน็ต โดยเฉพาะระบบอินเทอร์เน็ตนั้นมีการใช้อย่างแพร่หลายทั่วโลกทำให้เกิดช่องทางสำหรับแฮกเกอร์ที่ใช้ในการเจาะระบบได้เป็นจำนวนมาก ซึ่งการเจาะระบบนั้นมีวิธีการหลากหลายซึ่งอาจยกตัวอย่างวิธีการเจาะระบบโดยทั่วไป ได้ดังนี้

1. **การแกะรอย** (Foot Printing)

เป็นวิธีการค้นหา และดึงข้อมูลมาใช้เพื่อหาช่องโหว่ และสิ่งที่ต้องการ เช่น ชื่อโดเมน หมายเลขเครือข่าย รูปแบบการติดต่อเครือข่าย เพื่อรวบรวมข้อมูล โดยจะตรวจสอบสิ่งต่างๆไม่ว่าจะเป็นเรื่องความปลอดภัยหรือพฤติกรรมการใช้งาน (Profile) การตรวจสอบนี้จะแยกทั้งในเครือข่ายภายใน และเครือข่ายภายนอก

2. **การตรวจสอบหรือสแกน** (Scan)

การแกะรอยเป็นเสมือนการเคาะประตูบ้าน โดยผู้เจาะระบบได้ตรวจสอบข้อมูลก่อนเริ่มโจมตี และในการสแกนนี้เป็นการตรวจสอบเพื่อเข้าไปดูข้อมูล หรือรายละเอียดภายในอีกขั้นหนึ่ง ซึ่งอาจทำได้โดยการ Ping Sweeps, ICMP Queries หรือ Port scanning

3. **การเจาะระบบ** (Hacking)

การเจาะระบบที่ง่ายที่สุดตั้งแต่ในระดับกายภาพคือการเข้าไปถึงตัวเครื่อง โดยส่วนใหญ่ผู้เจาะระบบจะเริ่มจากการล้วงข้อมูลในระดับเครื่องก่อน ซึ่งจะรวบรวมรหัสผ่านจากไฟล์ PW หรือการแครกรหัสผ่านจากโปรแกรมสำเร็จรูปต่างๆจากเครือข่ายภายใน หรือจากเครื่องนั้นๆ

ซึ่งจะพบว่าผู้ใช้ต้องมีการล็อกผ่านเครือข่าย ซึ่งจะมี User name และ Password ซึ่งโดยระบบของคอมพิวเตอร์นั้นเมื่อผู้ใช้ทำการเข้าสู่ระบบจะมีไฟล์ PW ขึ้นจากเครื่องแม่ข่าย และจุดนี้จะเป็นโอกาสของการเจาะระบบระบบปฏิบัติการเช่น Microsoft Network Unix เป็นต้น ซึ่งไฟล์ PW จะถูกเข้ารหัสด้วยอัลกอริทึมที่เข้ารหัสนี้ไม่ยากต่อการถอดรหัสทั้ง Unix และ Windows NT ซึ่งผู้ปรารถนาร้ายสามารถทำได้เพียงแค่ก๊อปปี้ไฟล์ดังกล่าวในเครื่องที่เข้าใช้แม่ข่าย และก๊อปปี้ไฟล์ลงแผ่นดิสก์ หรือส่งไฟล์ผ่าน e-mail เท่านั้น และบุคคลทั่วไปสามารถที่จะแครกโปรแกรม PW ที่บ้าน หรือใช้ผ่านเว็บก็ได้ ซึ่งถ้าได้ไฟล์ PW ก็สามารถแครกหรือควบคุมระบบใดๆได้

สำหรับเครื่องคอมพิวเตอร์ส่วนตัวที่ถูกแฮกนั้นผู้แฮกสามารถที่จะดูได้ทั้งจากการล็อกอิน หรือเกิดจากการพูดคุยโดยสังเกตได้จากคีย์บอร์ด (เมื่อเจ้าของเครื่องไม่อยู่) ถ้าผู้เจาะระบบได้รับ root หรือ Administrator ผู้เจาะระบบสามารถติดตั้งโปรแกรมที่อนุญาตให้เก็บคีย์บนเครื่องลูกข่าย และส่งผ่านทางไกลได้ด้วย

เมื่อควบคุมเครือข่ายได้โดยได้ไฟล์ PW เพราะว่าเป็น PW ของ Administrator และสามารถทำทุกอย่างบนเครือข่ายได้ก็สามารถที่ทำการเปลี่ยน Permissions ลบหรือติดตั้งโปรแกรมไฟล์ หรือบริการสำหรับการแฮกต่อไป โดยสามารถที่จะใช้จากทางไกลเพื่อให้ทำงานแบบออนไลน์ได้ คีย์สำคัญของการแฮกคือการควบคุมเครื่องแม่ข่าย แล้วใช้ไปเจาะระบบจากที่อื่นเพื่อให้ตามรอยไม่ได้ เครื่องแม่ข่ายที่เป็นเจ้าของระบบหรือมีศักยภาพมาก เรียกว่าแฮกได้ และควบคุมเครือข่ายได้

นอกจากวิธีการแฮกตามปกติแล้ว การแฮกที่เป็นที่นิยมในปัจจุบันคือการแฮกโดยผ่านระบบสืบค้นข้อมูล โดยเฉพาะ Google ซึ่งมักเรียกกันว่า Google for Hacker[38] สาเหตุที่ Google เป็นระบบค้นหาที่แฮกเกอร์นิยมใช้ ก็คือ Google มีฐานข้อมูลที่เป็น

---

[38] “Hack ระบบผ่าน Google ง่ายจริงหรือ??” [Online] แหล่งที่มา : www.arip.co.th/2006/blogs.php?g1=0&blogger=anantayut&id=406155 [วันที่ 30 ตุลาคม 2550]

ของเว็บไซต์ต่างๆ ทั่วโลกประมาณ 1 หมื่นล้านเว็บไซต์ ระบบค้นหารองรับคีย์เวิร์ดที่เป็นข้อความ Text ได้สมบูรณ์มาก สามารถใส่เงื่อนไขหรือพารามิเตอร์ในการค้นหาได้อย่างละเอียด ทำให้ผลลัพธ์ที่ได้คือข้อมูลที่มีความแม่นยำหรือตรงกับที่ต้องการมากที่สุด

นอกจากนี้ Google ยังเป็นของสาธารณะที่อนุญาตให้ใช้งานกันโดยไม่เสียค่าใช้จ่าย ทำให้เว็บไซต์หลายแห่งผูกตัวเองเข้ากับระบบค้นหาของ Google เพื่อที่จะได้ถูกค้นเจอเป็นอันดับต้นๆ รวมถึงยังฟรี Pop-Up ต่างๆ ด้วย เห็นได้ชัดว่า Google เกี่ยวข้องกับคนจำนวนมากอย่างแท้จริง

สำหรับแฮกเกอร์แล้ว การได้มาซึ่งข้อมูลส่วนตัวของเป้ามายเป็นสิ่งสำคัญที่สุด โดยเฉพาะอีเมล์แอดเดรสนั้น หากแฮกเกอร์ต้องการเจาะเข้าไปยังหน่วยงานราชการหรือองค์กรธุรกิจ สิ่งแรกที่ต้องทำคือ ค้นหาอีเมล์แอ็กเคานต์ของบุคลากรในหน่วยงานนั้นให้ได้ ซึ่งก็คือรายชื่ออีเมล์ของพนักงานนั่นเอง โดยเฉพาะระดับหัวหน้าหรือฝ่ายที่เกี่ยวข้องกับบัญชีและการเงินนั้น หากเป็นองค์กรใหญ่ๆ อีเมล์แอดเดรสของคนเหล่านี้จะมีค่ามาก หากแฮกเกอร์สามารถเจาะเข้าไปเพื่ออ่านข้อมูลในอีเมล์ได้จะเป็นช่องทางที่ทำให้เกิดปัญหาได้มากมาย ทำให้เห็นได้ชัดว่ายิ่ง Google หรือแม้แต่เว็บค้นหาอื่นๆ มีความสามารถหรือมีสมรรถนะในการสืบค้นข้อมูลได้ละเอียดและถูกต้องแม่นยำมากขึ้นเท่าไร การนำไปใช้ของแฮกเกอร์ก็มีแต่จะเอื้ออำนวยประโยชน์ให้มากขึ้นไปอีก

2.2.5 **ความเสียหายและผลกระทบจากการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์**

ความเสียหายที่เกิดจากการการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบนั้น เป็นได้ทั้งความเสียหายต่อบุคคลโดยส่วนตัว หรือเป็นความเสียหายที่เกิดกับองค์กรหรือหน่วยงานต่างๆ ซึ่งเป็นได้ทั้งความเสียหายทางด้านตัวเงินหรือข้อมูลทางการค้า และรวมไปถึงความมั่นคงด้วย เช่น การเข้าถึงข้อมูลส่วนบุคคล ย่อมเป็นอันตรายต่อสิทธิส่วนบุคคล (Privacy) หากว่าผู้กระทำนั้นนำเอาข้อมูลส่วนบุคคลไปเผยแพร่หรือจำหน่ายต่อให้แก่บุคคลที่สาม ในขณะที่การเข้าถึงระบบการค้า ข้อมูลหรือความลับทางการค้าของบริษัทต่างๆ ย่อมเป็นอันตรายต่อการล่วงรู้โดยมิชอบต่อความลับทางการค้าของธุรกิจคู่แข่ง หากผู้กระทำนำข้อมูลดังกล่าวไปเผยแพร่หรือจำหน่ายต่อคู่แข่งทางการค้า นอกไปจากนี้อาจเป็นข้อมูลเรื่องความมั่นคงของหน่วยงานหรือประเทศซึ่งก็มีความเป็นไปได้ เนื่องจากในปัจจุบันการเก็บรักษาข้อมูลและเข้าถึงข้อมูลในรูปคอมพิวเตอร์เป็นสิ่งที่พบเห็นได้ทั่วไป ซึ่งอาจแยกประเภทของความเสียหายที่เกิดขึ้น ได้ดังนี้

2.2.5.1 **ด้านเศรษฐกิจ**

ความเสียหายทางด้านเศรษฐกิจนั้น เป็นความเสียหายที่มองเห็นได้ชัดเจนที่สุด เนื่องจากมีความเสียหายที่ปรากฏออกมาเป็นตัวเลขที่เห็นได้ชัดถึงความเสียหายที่เกิดขึ้นและมีความเสียหายอย่างมหาศาลเนื่องจากความเสียหายประเภทนี้มักเกิดแก่บริษัทเอกชนในการทำธุรกิจ โดยเฉพาะธนาคารต่างๆ นอกจากนี้ความเสียหายทางเศรษฐกิจยังมีทั้งความเสียหายที่สามารถสำรวจได้ เช่น การถูกปรับเปลี่ยนจำนวนเงินของบริษัทและยักยอกเงินไป การเข้าไปทำลายระบบคอมพิวเตอร์ของบริษัทเอกชนทำให้ไม่สามารถดำเนินการได้อีกต่อไป ตัวอย่างเช่น ในประเทศสหรัฐอเมริกา พบว่ายอดความเสียหายจากอาชญากรรมคอมพิวเตอร์ในปี ค.ศ. 2004 มีจำนวนถึง 141,496,560 ดอลลาร์สหรัฐ ส่วนในประเทศออสเตรเลียพบว่ายอดความเสียหายจากภัยคุกคามจากระบบคอมพิวเตอร์มีค่าเสียหายประมาณ 15,921,064 ดอลลาร์ออสเตรเลีย จำนวนเงินที่ปรากฏเป็นเพียงตัวเลขมูลค่าความเสียหายที่เกิดขึ้นเท่านั้น ยังไม่รวมถึงจำนวนเงินที่แต่ละองค์กรจำต้องจ่ายออกไปเพื่อจัดหามาตรการในการดูแลระบบคอมพิวเตอร์ของตน

นอกจากนี้ ความเสียหายที่เกิดจากการถูกล่วงรู้ข้อมูลล่วงหน้าที่ไม่มีตัวเลขความเสียหายที่ชัดเจนหากแต่ก่อให้เกิดความเสียหายทางด้านผลกำไรหรือการทำงานของบริษัทต่างๆ ได้อย่างมหาศาล โดยหากจะพิจารณาถึงสถานการณ์อย่างง่ายแล้ว ถ้าเป็นบริษัทที่มีการแข่งขันกันอย่างการประมูลราคางานต่างๆ หากสามารถเข้าไปดูไฟล์ที่บริษัทคู่แข่งส่งประมูลได้ จะก่อให้เกิดความได้เปรียบอย่างเห็นได้ชัด โดยเฉพาะเวลายื่นซองประมูลงาน เงินที่ประมูลอาจต่างจากบริษัทคู่แข่งแค่หลักพัน แต่เพียงแค่นี้ก็สามารถชนะการประมูลบริษัทคู่แข่งได้แล้ว ดังนั้นในเรื่องข้อมูลนั้นถือว่าสำคัญมากหากใครมีข้อมูลมากกว่าและแม่นยำกว่าก็จะได้เปรียบมากกว่าอย่างเห็นได้ชัด

2.5.1.2 **ด้านความมั่นคง**

ความเสียหายที่เกี่ยวกับการความมั่นคงนั้นเป็นเรื่องที่สำคัญในระดับประเทศและระดับนานาชาติอย่างหลีกเลี่ยงไม่ได้ ในอดีตคงไม่มีใครคาดคิดเกี่ยวกับสงครามทางอินเทอร์เน็ตว่าจะกลายเป็นสงครามประเภทหนึ่ง และการก่อการร้ายทางอินเทอร์เน็ตเป็นเรื่องที่ไม่เคยคาดคิดว่าจะได้ยิน หากแต่ในปัจจุบัน คงไม่มีใครปฏิเสธถึงความร้ายแรงที่เกิดขึ้นจากการก่อการร้ายทางอินเทอร์เน็ตได้ การพยายามจู่โจมเจาะระบบคอมพิวเตอร์และข้อมูลต่างๆ ของทางการทหาร หน่วยสืบสวนสอบสวนต่างๆ ที่เก็บความลับทางการทหารและความมั่นคง เป็นสิ่งที่รับรู้กันทั่วไป การพยายามเจาะระบบเพื่อทำลายระบบหรือหาข้อมูลดังกล่าวของผู้ก่อการร้ายทางอินเทอร์เน็ตเป็นเรื่องที่สำคัญต่อความมั่นคงของประเทศอย่างหลีกเลี่ยงไม่ได้ โดยผู้ก่อการร้ายมีแนวโน้มที่ใช้

อินเทอร์เน็ตและคอมพิวเตอร์ในการก่ออาชญากรรมมากขึ้นเพื่อเป็นเครื่องมือเผยแพร่ข้อมูลระหว่างสมาชิกโดยมี 4 รูปแบบ 1.โฆษณาชวนเชื่อให้เข้ากลุ่ม 2.ใช้เพื่อปฏิบัติการเป็นเครื่องมือเผยแพร่กดดันข่มขู่ภาครัฐ 3.เป็นเครื่องมือขโมยข้อมูลที่สำคัญและจำเป็นของภาครัฐและเอกชน 4.การใช้เป็นช่องทางโจมตีระบบ[39] ซึ่งอาจแบ่งความเสียหายที่กระทบต่อความมั่นคงของประเทศได้ใน 4 ลักษณะใหญ่ๆ คือ ความเสียหายทางการเมือง ความเสียหายทางการทหาร ความเสียหายจากผู้ก่อการร้าย และความเสียหายต่อความสัมพันธ์ระหว่างประเทศ[40]

ก. ความเสียหายทางด้านการเมือง เป็นการใช้ระบบคอมพิวเตอร์เป็นช่องทางในการสืบค้นข้อมูลของพรรคการเมืองฝ่ายตรงข้าม โดยเฉพาะการเจาะระบบเข้าไปสู่ฐานข้อมูลของฝ่ายตรงข้าม เพื่อตรวจสอบพฤติกรรมการกระทำการทุจริตต่อหน้าที่ หรือค้นหาข้อมูลเพื่อใช้ในการอภิปราย

ข. ความเสียหายทางการทหาร การโจมตีระบบคอมพิวเตอร์ที่เกิดจากการกระทำของรัฐนั้น โดยส่วนใหญ่จะมุ่งเน้นเครือข่ายทางทหาร เนื่องจากแต่ละรัฐต้องการสร้างความได้เปรียบสูงสุดเมื่อเกิดสงครามขึ้น การกระทำการโจมตีเครือข่ายระบบคอมพิวเตอร์ของรัฐไม่ว่าจะเป็นการเจาะระบบเพื่อเข้าสู่ฐานข้อมูลของรัฐฝ่ายตรงข้ามเพื่อให้ได้มาซึ่งข้อมูลด้านกำลังพล อาวุธยุทโธปกรณ์ สถานที่ตั้งทางทหาร ยุทธวิธีการรบ หรือสภาพภูมิศาสตร์ เพราะข้อมูลเหล่านี้เป็นข้อมูลที่สำคัญในการสงคราม และสร้างโอกาสในการเป็นผู้ชนะสงครามให้แก่ฝ่ายของตน หรือมุ่งที่จะทำลายระบบเครือข่ายคอมพิวเตอร์หรือระบบสาธารณูปโภคเพื่อขัดขวางไม่ให้มีการติดต่อสื่อสาร แม้ในปัจจุบัน ประเทศที่ไม่มีสงครามก็ให้ความระมัดระวังในกรณีดังที่ว่ามานี้ เช่น มีหลายครั้งที่สหรัฐอเมริกากล่าวหาว่าจีนส่งแฮกเกอร์ไปเจาะระบบความมั่นคงของตน ซึ่งแสดงให้เห็นว่าความลับทางการทหารก็เป็นเป้าหมายหนึ่งของแฮกเกอร์ที่ส่งผลกระทบต่อรัฐอย่างมาก

ค. ความเสียหายจากการก่อการร้าย ในปัจจุบันผู้ก่อการร้ายได้ใช้ประโยชน์จากระบบคอมพิวเตอร์เป็นช่องทางอำนวยความสะดวกแก่พวกตนในการวางแผนและวินาศกรรม เช่น

---

[39] “ปลุกกระแสรับมือภัยมืดโลกไซเบอร์ ...15 วินาทีก็มีสิทธิ์โดนแฮก” [Online] แหล่งที่มา : www.ee-art.com/news/1448 [วันที่ 17 ตุลาคม 2550]

[40] กรุง เหลืองมโนธรรม, “การศึกษาประเด็นทางกฎหมายเกี่ยวกับการจัดการความไม่มั่นคงของระบบคอมพิวเตอร์ในสังคมไทย : ศึกษาเฉพาะภัยไวรัสคอมพิวเตอร์ แฮกเกอร์ และสแปมเมล์,” (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2548), หน้า 27-28.

การโจมตีทางคอมพิวเตอร์ โดยผู้ก่อการร้ายจะมุ่งโจมตีระบบคอมพิวเตอร์ขนาดใหญ่มากกว่าขนาดเล็ก โดยเฉพาะระบบสาธารณูปโภคไม่ว่าจะเป็นโรงงานไฟฟ้า เขื่อน หรือระบบคอมพิวเตอร์ขนส่ง เพื่อให้เกิดความปั่นป่วนภายในประเทศ

ง. ความเสียหายต่อความสัมพันธ์ระหว่างประเทศ ภัยจากแฮกเกอร์มีลักษณะข้ามชาติ เนื่องจากผู้กระทำและผลแห่งการกระทำไม่จำเป็นต้องเกิดเฉพาะรัฐเจ้าของสัญชาติหรือรัฐที่ผู้กระทำความผิดอาศัยอยู่เท่านั้น แต่จะกระทบต่อทุกรัฐที่มีการเชื่อมต่อโครงข่ายระบบคอมพิวเตอร์เข้าด้วยกัน หากรัฐใดรัฐหนึ่งปล่อยปละละเลยมิควบคุมดูแลภัยจากแฮกเกอร์ในรัฐของตน ให้กระทำการสร้างความเสียหายต่อระบบคอมพิวเตอร์ของรัฐอื่นๆ แล้ว ย่อมสร้างความไม่พึงพอใจต่อรัฐผู้ได้รับความเสียหายอันอาจจะนำมาซึ่งผลกระทบต่อความสัมพันธ์ระหว่างประเทศ หรืออาจเกิดความขัดแย้งทางการเมืองระหว่างประเทศขึ้น

นอกจากนี้ผลกระทบทางอ้อมของภัยอินเทอร์เน็ตนั้นยังทำให้ประเทศชาติขาดความเชื่อถือในด้านความมั่นคงของระบบโครงสร้างพื้นฐานสารสนเทศซึ่งเป็นสิ่งสำคัญในการพัฒนาประเทศอีกด้วย ดูจากตัวอย่างสถิติเว็บไซต์ของประเทศไทยที่ถูกแฮกเกอร์โจมตีที่เว็บ www.zone-h.org จะเห็นได้ว่าเว็บไซต์ของประเทศไทยถูกโจมตีมากกว่าหนึ่งพันเว็บไซต์ในปี 2006 ทั้งภาครัฐและเอกชน ซึ่งสะท้อนให้เห็นปัญหาด้านความปลอดภัยข้อมูลของประเทศ[41]

2.5.1.3 ด้านความเป็นส่วนตัว

ความเป็นส่วนตัวของบุคคลในยุคอินเทอร์เน็ตนั้นเป็นสิ่งที่ยากจะปกปิดได้อีกต่อไป โดยเฉพาะข้อมูลที่ให้ไว้กับหน่วยงานต่างๆ ไม่ว่าเป็นภาครัฐหรือภาคเอกชน โดยข้อมูลส่วนตัวนั้นมีทั้งข้อมูลที่มีค่าทางเศรษฐกิจ เช่น หมายเลขบัตรเครดิต หมายเลขบัตรประจำตัวประชาชน และข้อมูลที่ไม่มีค่าทางเศรษฐกิจ เช่น การสนทนาที่เป็นส่วนตัว ประวัติโดยทั่วไป ซึ่งการติดต่อสื่อสารทางคอมพิวเตอร์และอินเทอร์เน็ตที่มีการเก็บข้อมูลที่ติดต่อไว้ในฐานข้อมูลทางอินเทอร์เน็ตที่เข้าไปใช้บริการก่อให้เกิดความเสี่ยงที่จะมีบุคคลอื่นเข้ามาดูได้

หน่วยงานของทางรัฐโดยมากในปัจจุบันรวมถึงบริษัทเอกชนต่างๆ ต่างเก็บข้อมูลของประชาชนที่มาติดต่อไว้ในฐานข้อมูลที่เชื่อมต่อกับระบบเครือข่าย หากจะให้เปรียบเทียบแล้วก็เหมือนกับการเก็บจดหมายในตู้ไปรษณีย์ที่มีกุญแจ อาจจะมีบุคคลที่มีกุญแจผีไขเข้ามาดูข้อมูล

---

[41] ACIS, “10 ภัยมืดยุคอินเทอร์เน็ตปี คศ. 2007,” [Online] แหล่งที่มา : www.acisonline.net/article_prinya_eweek_010150.htm [15 ธันวาคม 2550]

เมื่อไรก็ได้ หากแต่ร้ายแรงกว่าเนื่องจากคนที่พยายามไขตู้ไปรษณีย์อาจมีคนพบเห็นได้ง่าย เนื่องจากต้องลงมือในที่สาธารณะ หากแต่การพยายามเจาะระบบหรือข้อมูลไม่ได้ทำในที่สาธารณะ แต่ทำในที่เป็นส่วนตัวและใช้เวลาเท่าใดก็ได้ ความเสียหายที่เกิดขึ้นจึงมักจะพบเมื่อความผิดสำเร็จแล้ว แม้ความเสียหายในลักษณะนี้บางส่วนอาจไม่สามารถประมาณค่าเป็นตัวเลขทางเศรษฐกิจได้ หากแต่ก็มีความสำคัญในแง่สิทธิเสรีภาพส่วนบุคคลที่ไม่ควรให้บุคคลอื่นที่ไม่มีส่วนเกี่ยวข้องเข้าถึงได้

ความเสียหายที่เกิดขึ้นและมีผลกระทบทั้งความเป็นส่วนตัวและเศรษฐกิจยกตัวอย่าง เช่น ภัยจากการถูกขโมยเงินผ่านทางอินเทอร์เน็ตแบงค์กิ้ง หรือ ผ่านทางการปลอมแปลงบัตรเอทีเอ็ม หรือ บัตรเครดิต ตลอดจนการถูกขโมยความเป็นตัวตน หรือ "Identity Theft" โดยแฮกเกอร์ หรือ ผู้ไม่หวังดีนิยมขโมยชื่อผู้ใช้และรหัสผ่านของเหยื่อ แล้วนำไปใช้ในทางที่ไม่ถูกต้องและขัดต่อกฎหมาย สร้างปัญหาให้กับผู้เป็นเจ้าของชื่อดังกล่าว และอาจถูกตำรวจสอบสวนในฐานะผู้ต้องหาในคดีอาชญากรรมคอมพิวเตอร์ ซึ่งทำให้เสียเวลาและเสียชื่อเสียงจากการขโมยความเป็นตัวตนดังกล่าว[42]

นอกจากนี้ ความเสียหายต่อสิทธิเสรีภาพของบุคคลทั่วไปที่เกิดจากการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลโดยปราศจากอำนาจนั้น แม้แฮกเกอร์จะมิได้ประสงค์ที่จะก่อภัยใดๆ ต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ เพียงแต่เข้ามาในระบบคอมพิวเตอร์เท่านั้น อย่างไรก็ตาม แม้ว่าจะมิได้ก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ ข้อมูลสารสนเทศ หรือระบบเครือข่ายก็ตาม แฮกเกอร์ก็สามารถเรียกร้องทรัพย์สินจากเจ้าของระบบได้เช่นกัน เช่น กรณีที่นักเจาะข้อมูลชาวคาซัคสถานได้เจาะระบบการป้องกันของบริษัทบลูมเบิร์กเข้าไปสำเร็จแล้วได้ส่งไปรษณีย์อิเล็กทรอนิกส์มาเรียกร้องเงินจากทางบริษัทว่าหากไม่จ่ายเงินจะนำวิธีการเจาะระบบไปเปิดเผย หรือผู้เจาะระบบอาจนำสิ่งที่รู้จากการเจาะข้อมูลเป็นเครื่องต่อรองเรียกร้องทรัพย์สินจากผู้ที่ถูกเจาะระบบคอมพิวเตอร์ได้

นอกจากนี้ มีหลายกรณีที่ละเมิดสิทธิส่วนบุคคลของผู้เสียหาย ไม่ว่าจะเป็นการเข้าถึงข้อมูลส่วนตัวของบุคคลอื่นโดยมิได้รับอนุญาต การติดตามพฤติการณ์ของผู้ใช้อินเทอร์เน็ตหรือใช้เทคโนโลยีเพื่อติดตามหรือสอดส่องชีวิตของผู้เสียหาย เช่น ในกรณีหญิงคนหนึ่งได้สนทนาผ่านอินเทอร์เน็ตกับชายชาวอเมริกัน และได้ใช้เว็บแคมเพื่อเห็นภาพผู้ที่สนทนาด้วย ผลปรากฏว่าชายชาวอเมริกันสามารถเจาะระบบเว็บแคมของผู้หญิงได้ และสามารถควบคุมการเปิดปิดเว็บ

---

[42] เรื่องเดียวกัน,

แคมได้โดยอัตโนมัติแม้จะไม่ได้ออนไลน์อยู่ก็ตาม ซึ่งถือว่าเป็นการล่วงละเมิดสิทธิส่วนบุคคลของผู้หญิงโดยที่เจ้าตัวไม่รู้[43]

2.5.1.4 **ด้านสังคม**

เมื่อคอมพิวเตอร์เข้ามามีบทบาทในสังคมพฤติกรรมของบุคคลก็เปลี่ยนแปลงไปเป็นอย่างมาก การติดต่อสื่อสาร การทำงาน หรือสื่อบันเทิงเปลี่ยนไปอย่างเห็นได้ชัด เมื่อคอมพิวเตอร์ทำให้พฤติกรรมของคนในสังคมเปลี่ยนแปลงไป ทำให้มนุษย์มีโลกอีกโลกหนึ่งที่ผ่านคอมพิวเตอร์เป็นสังคมใหม่ที่เกิดขึ้น และสิ่งที่ตามมาคืออาชญากรรมที่เกิดเทคโนโลยีสมัยใหม่ทำให้การกระทำผิดเปลี่ยนแปลงไป เกิดอาชญากรไซเบอร์ขึ้น โดยเฉพาะแฮกเกอร์หรือนักเจาะระบบกลายเป็นอาชญากรรมประเภทใหม่ที่เกิดขึ้นในสังคมพร้อมเทคโนโลยี และทำให้ประชาชนหวาดกลัวหรือหวั่นระแวงได้มากกว่าอาชญากรรมโดยทั่วไป เนื่องจากเป็นเรื่องยากที่จะระมัดระวังและป้องกันตนเองจากการกระทำผิดดังกล่าวและผู้กระทำผิดสามารถทำได้โดยไม่มีข้อจำกัดเรื่องเวลาหรือสถานที่ สำนักวิจัยไอซีเอ็มได้สำรวจกลุ่มตัวอย่างผู้ใช้อินเทอร์เน็ต 1,317 ราย ในปี พ.ศ. 2549 พบว่า ร้อยละ 21 รู้สึกกลัวอาชญากรรมไซเบอร์มากกว่าอาชญากรรมประเภทอื่นๆ ร้อยละ 27 รู้สึกกลัวที่จะใช้บัตรเครดิตซื้อสินค้าผ่านทางอินเทอร์เน็ต ส่วนในประเทศอังกฤษ รัฐบาลได้แถลงว่า ประชาชนจำนวนมากกำลังเกรงกลัวว่าจะเป็นเหยื่ออาชญากรรมไซเบอร์มากกว่ากลัวที่จะถูกตัดช่องย่องเบาหรือจี้ปล้น ส่วนสำนักข่าวบีบีซีก็ได้วิเคราะห์และประกาศว่าผู้ใช้อินเทอร์เน็ตควรจะระมัดระวังแฮกเกอร์ ในการศึกษานี้บีบีซีได้ลองทำพีซีเครื่องหนึ่งเป็นเหยื่อปรากฏว่า ถูกโจมตีโดยเฉลี่ยทุก 15 นาที โดยการโจมตีส่วนมากเป็นการก่อกวนแต่การโจมตีบางรายก็เป็นการโจมตีที่รุนแรง[44]

2.2.6 **สถิติคดีและความเสียหายในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์**

---

[43] กรุง เหลืองมโนธรรม, “การศึกษาประเด็นทางกฎหมายเกี่ยวกับการจัดการความไม่มั่นคงของระบบคอมพิวเตอร์ในสังคมไทย : ศึกษาเฉพาะภัยไวรัสคอมพิวเตอร์ แฮกเกอร์ และสแปมเมล์,” หน้า 32-33.

[44] ศรีศักดิ์ จามรมาน, “มีการขโมยข้อมูลส่วนตัวทางอินเทอร์เน็ตในสหรัฐถึง 26 ล้านราย,” หนังสือพิมพ์เทเลคอมเจอร์นัล ปีที่ 16 ฉบับที่ 650 หน้า 20 วันที่ 1 - 7 ม.ค. 2550 [Online] แหล่งที่มา : www.charm.ksc.au.edu/index_th.htm [20 มกราคม 2551]

การบุกรุกเข้าสู่ระบบคอมพิวเตอร์ต่างๆ มักเป็นข่าวที่ปรากฏขึ้นบ่อยครั้งในปัจจุบันและก่อให้เกิดความเสียหายอย่างมหาศาล แต่ข่าวเหล่านั้นเป็นเพียงส่วนหนึ่งของเหตุการณ์ที่เกิดขึ้นจริงทั้งหมดซึ่งเกิดขึ้นไม่เว้นแต่ละวัน โดยมีข้อที่น่าสังเกตในประเทศสหรัฐอเมริกา คือ ถ้าหากมีโจรบุกเข้าปล้นธนาคารด้วยอาวุธปืน ผู้ร้ายรายนั้นก็จะถูกทางการหรือตำรวจตามหาตัวไปตลอดจนกว่าจะถูกจับกุมตัวได้ แต่ถ้าเปลี่ยนอุปกรณ์ที่ใช้ในการปล้นมาเป็นคอมพิวเตอร์แล้ว นอกจากจะไม่เกิดอะไรขึ้นกับตัวคนร้ายแล้ว ทางธนาคารอาจจะไม่ยอมรับว่าเกิดการปล้นขึ้นแต่อย่างใดเพราะห่วงเรื่องชื่อเสียงที่อาจเสื่อมเสียไป โดยอาจพิจารณาจากสถิติง่ายๆ ดังนี้

โดยเฉลี่ยคนร้ายที่บุกเข้าปล้นธนาคารจะปล้นเงินไปได้ประมาณ 2,500 ถึง 7,500 เหรียญต่อครั้ง เพื่อแลกกับความเสี่ยงถูกยิงตาย ตามสถิติของการปล้นธนาคารโดยใช้อาวุธทางการจับคนร้ายได้ประมาณ 50-60 เปอร์เซ็นต์ของคนร้ายทั้งหมดที่ก่อเหตุ 80 เปอร์เซ็นต์ของคนร้ายที่จับได้ถูกตัดสินลงโทษจำคุก 5 ปี โดยเฉลี่ย ในขณะที่การปล้นธนาคารในรูปของอาชญากรรมคอมพิวเตอร์จะนำเงินไปได้คราวละประมาณ 50,000 ถึง 500,000 เหรียญโดยไม่ต้องเสี่ยงกับลูกกระสุนแม้แต่นัดเดียว มีเพียง 10 เปอร์เซ็นต์ของการปล้นทางคอมพิวเตอร์ที่สามารถสาวไปถึงตัวคนร้ายได้ และในบรรดาคนร้ายเหล่านั้น มีเพียง 15 เปอร์เซ็นต์ที่ถูกส่งดำเนินคดี แต่ไม่ใช่ทั้งหมดที่ถูกลงโทษ เพราะมีถึง 50 เปอร์เซ็นต์ที่ถูกปล่อยตัวไปเพราะขาดพยานหลักฐานที่แน่นหนา หรือไม่ก็ด้วยเหตุผลที่เจ้าทุกข์ไม่อยากตกเป็นข่าว เหลืออยู่เพียง 50 เปอร์เซ็นต์ที่ถูกลงโทษด้วยบทลงโทษ 5 ปีโดยเฉลี่ย

จากตัวเลขสถิติข้างบนแสดงให้เห็นชัดแล้วว่า ผู้กระทำผิดมักไม่ถูกลงโทษ ทำให้คนร้ายไม่รู้สึกเกรงกลัวกฎหมายแต่อย่างใด ดังนั้น การฟ้องร้องและการทำให้คดีปรากฏต่อสาธารณชนจึงเป็นหนทางที่จะช่วยให้อาชญากรรมคอมพิวเตอร์ลดน้อยลงได้ อย่างน้อยที่สุด ผู้ที่กำลังจะลงมือคงต้องคิดหนักขึ้นก่อนที่จะทำอะไรลงไปเมื่อมีเหตุการณ์บุกรุกระบบคอมพิวเตอร์เกิดขึ้น โดยผู้เสียหายต้องออกมาให้ข้อมูลกับเจ้าหน้าที่ของรัฐเพื่อติดตามผู้กระทำผิดต่อไป ดังนั้นจะเห็นได้ว่าการเจาะเข้าสู่ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ก่อให้เกิดความเสียหายอย่างไร โดยอาจพิจารณาได้ดังนี้

2.2.6.1 **สถิติคดีและความเสียหายในประเทศไทย**

ถึงแม้ว่าในปัจจุบัน ThaiCERT จะไม่ได้มีการสำรวจความเสียหายที่เกิดขึ้นจากการก่ออาชญากรรมทางคอมพิวเตอร์ไว้ก็ตาม แต่ได้มีการรวบรวมสถิติเกี่ยวกับการร้องเรียนที่

เกิดขึ้นเกี่ยวกับการละเมิดความมั่นคงบนเครือข่ายไว้ ตั้งแต่ปี พ.ศ. 2544-2550 [45] ทั้งนี้ จำนวนผู้แจ้งเหตุในปี 2544 มีจำนวน 150 ราย โดยเป็นการแจ้งในเรื่อง Spam Mail จำนวน 66 ราย เรื่อง Port Scan จำนวน 38 ราย และไวรัสคอมพิวเตอร์ 34 ราย และการแฮกหรือเจาะระบบจำนวน 12 คดี จำนวนผู้แจ้งเหตุในปี 2545 มีจำนวน 355 ราย โดยเป็นการแจ้งในเรื่อง Spam Mail จำนวน 183 ราย เรื่อง Port Scan จำนวน 90 ราย และไวรัสคอมพิวเตอร์ 55 ราย และการแฮกหรือเจาะระบบจำนวน 27 คดี [46] จำนวนผู้แจ้งเหตุในปี 2546 มีจำนวน 389 ราย โดยเป็นการแจ้งในเรื่อง Spam Mail จำนวน 30 ราย เรื่อง Port Scan จำนวน 170 ราย และไวรัสคอมพิวเตอร์ 171 ราย และการแฮกหรือเจาะระบบจำนวน 17 คดี

จำนวนผู้แจ้งเหตุในปี 2547 มีจำนวน 400 ราย โดยเป็นการแจ้งในเรื่อง Spam Mail จำนวน 48 ราย เรื่อง Port Scan จำนวน 132 ราย และไวรัสคอมพิวเตอร์ 210 ราย และการแฮกหรือเจาะระบบจำนวน 10 คดี โดยในช่วงเดือน มกราคม 2547 - 22 กันยายน 2547 สำรวจพบการก่ออาชญากรรมคอมพิวเตอร์ทั้งสิ้น 340 คดี แตกต่างจากปี 2546 ทั้งปี ที่สำรวจพบเพียง 260 คดี โดยคดีอาชญากรรมคอมพิวเตอร์ที่สำรวจพบแบ่งออกเป็นไวรัสและหนอนคอมพิวเตอร์ จำนวน 161 คดี สแกนพอร์ตจำนวน 129 คดี สแปมเมล์จำนวน 43 คดีและการแฮกหรือเจาะระบบจำนวน 7 คดี นอกจากนี้ ยังพบไวรัสคอมพิวเตอร์ติดมาพร้อมอีเมล์มากกว่า 50% ของอีเมล์ทั้งหมด แตกต่างจากปี 2546 ที่มีคดีจากไวรัสและหนอนคอมพิวเตอร์จำนวน 31 คดีสแกนพอร์ตจำนวน 170 คดี สแปมเมล์จำนวน 42 คดี และการเจาะระบบจำนวน 17 คดี[47]

จำนวนผู้แจ้งเหตุในปี 2548 มีจำนวน 453 ราย โดยเป็นการแจ้งในเรื่อง Spam Mail จำนวน 24 ราย เรื่อง Port Scan จำนวน 56 ราย และไวรัสคอมพิวเตอร์ 307 ราย การฟิชชิ่ง 20 ราย และการแฮกหรือเจาะระบบจำนวน 46 คดี จำนวนผู้แจ้งเหตุในปี 2549

---

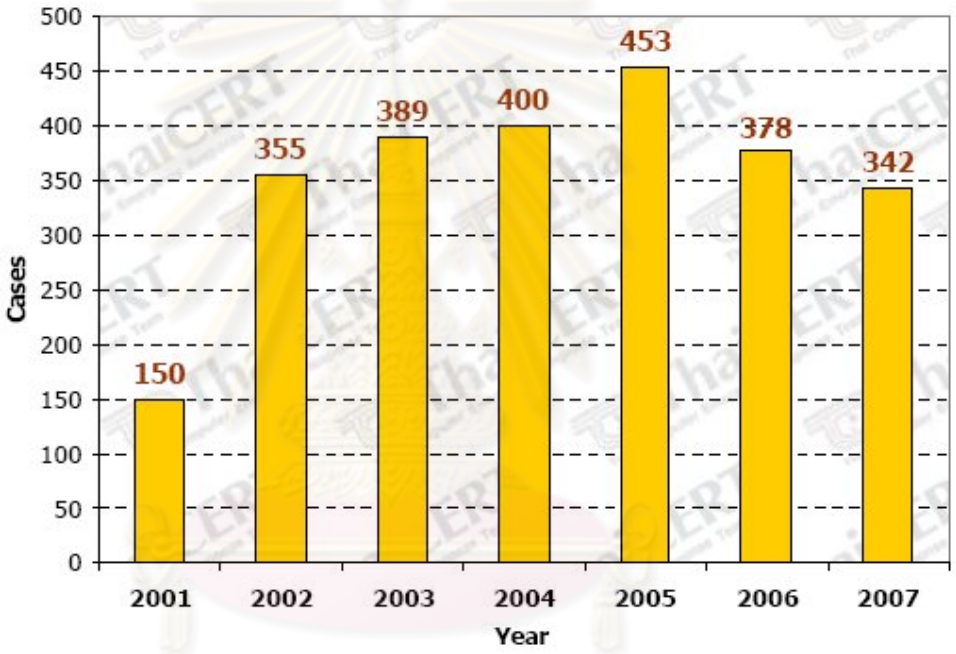
[45] ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย, “รายงานสรุปผลการตอบสนองเหตุละเมิดความปลอดภัยคอมพิวเตอร์ปี 2550,” [Online] แหล่งที่มา : www.thaicert.nectec.or.th [วันที่ 25 กุมภาพันธ์ 2551]

[46] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, “แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์,” [Online] แหล่งที่มา : www.etcommission.go.th/books/Cyber_crime.pdf [วันที่ 21 กรกฎาคม 2550]

[47] หนังสือพิมพ์ไทยรัฐ, “เร่งล้อมคอกก่อนวัวหาย...หลังสถิติอาชญากรรมคอมฯปี 47 ไม่ลด,” [Online] แหล่งที่มา : www.thaitelecom.com [วันที่ 2 กรกฎาคม 2548]

มีจำนวน 378 ราย โดยเป็นการแจ้งในเรื่อง Spam Mail จำนวน 17 ราย เรื่อง Port Scan จำนวน 29 ราย และไวรัสคอมพิวเตอร์ 162 ราย การฟิชชิ่ง 154 ราย และการแฮกหรือเจาะระบบจำนวน 16 คดี และในปี 2550 มีจำนวนผู้แจ้งเหตุในปี 2550 มีจำนวน 342 ราย โดยเป็นการแจ้งในเรื่อง Port Scan จำนวน 7 ราย และไวรัสคอมพิวเตอร์ 38 ราย การฟิชชิ่ง 262 ราย และการแฮกหรือเจาะระบบจำนวน 35 คดี

โดยอาจพิจารณาสถิติคดีในการก่ออาชญากรรมคอมพิวเตอร์ได้จากรายงานสรุปผลการตอบสนองเหตุละเมิดความปลอดภัยคอมพิวเตอร์ ปี 2550 โดย ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย ดังนี้[48]

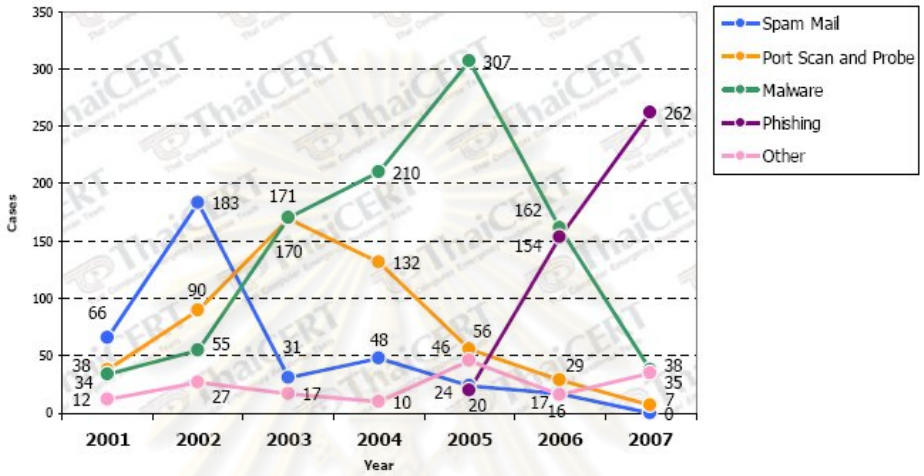


จำนวนเหตุละเมิดความปลอดภัยที่ ThaiCERT ได้รับและดำเนินการ ตั้งแต่ปี 2544 ถึงปี 2550 และอาจแยกตามเหตุและประเภทได้ ดังนี้[49]

[48] ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย, “รายงานสรุปผลการตอบสนองเหตุละเมิดความปลอดภัยคอมพิวเตอร์ปี 2550,” [Online]

[49] เรื่องเดียวกัน,

Year \ Type of Incident	Spam Mail	Port Scan and Probe	Malware	Phishing	Others (Hack, DDos etc.)
2001	66	38	34	-	12
2002	183	90	55	-	27
2003	31	170	171	-	17
2004	48	132	210	-	10
2005	24	56	307	20	46
2006	17	29	162	154	16
2007	**0**	**7**	**38**	**262**	**35**



2.2.6.2 สถิติคดีและความเสียหายในต่างประเทศ

แม้ในประเทศไทยจะไม่มีการจัดทำสถิติคดีและความเสียหายที่ชัดเจน แต่ในต่างประเทศซึ่งให้ความสำคัญกับการก่ออาชญากรรมทางคอมพิวเตอร์แล้ว ได้มีการสำรวจความเสียหายและจัดทำสถิติในหลายองค์กรในต่างประเทศ โดยปัจจุบันมีหน่วยงานของต่างประเทศหลายหน่วยงานที่ทำการสำรวจข้อมูลเกี่ยวกับสถิติความเสียหายที่เกิดขึ้นจากการก่ออาชญากรรมทางคอมพิวเตอร์ อาทิ AusCert , CSI, IPRI เป็นต้น และบริษัทเอกชนที่ทำธุรกิจเกี่ยวข้องกับความปลอดภัยของคอมพิวเตอร์ เช่น ไซแมนเทค โดยรายงานภัยคุกคามด้านความปลอดภัยบนอินเทอร์เน็ต (Internet Security Threat Report) ฉบับล่าสุด จากไซแมนเทค[50] แสดงรูปแบบภัยร้ายออนไลน์ในปัจจุบันที่มุ่งเน้นการขโมยข้อมูล การรั่วไหลของข้อมูล และใช้โค้ดอันตรายเพื่อจารกรรมข้อมูลสำคัญแบบเจาะจง เพื่อหาผลประโยชน์ด้านการเงิน นอกจากนี้อาชญากรออนไลน์ยังได้ปรับเปลี่ยนรูปแบบการโจมตีระบบให้ยากต่อการตรวจจับ และสร้างเครือข่ายระดับโลกเพื่อรองรับอาชญากรรมต่างๆ ด้วย

---

[50] “Positioning Magazine” [Online] แหล่งที่มา : www.positioningmag.com/index.aspx [วันที่ 27 กุมภาพันธ์ 2551]

โดยการจำหน่ายข้อมูลลับที่ถูกจารกรรมมาและถูกเผยแพร่บนเซิร์ฟเวอร์ใต้ดินราคาประหยัด โดยเซิร์ฟเวอร์เหล่านี้ถูกใช้เป็นทางผ่านในการจำหน่ายข้อมูลสำคัญต่างๆ เช่น หมายเลขประกันสังคม ข้อมูลบัตรเครดิต เลขรหัสลับส่วนบุคคล (PIN) และรายชื่ออีเมล์แอดเดรส โดยในช่วงครึ่งหลังของปี 2549 มีเซิร์ฟเวอร์ใต้ดินลักษณะนี้ในสหรัฐอเมริกา คิดเป็น 51 เปอร์เซ็นต์ของเซิร์ฟเวอร์ใต้ดินทั้งหมด และสนนราคาข้อมูลบัตรเครดิตสัญชาติอเมริกันในราคา 1-6 ดอลลาร์ ในขณะที่ข้อมูลส่วนบุคคลอื่นๆ แบบครบชุด ตั้งแต่ หมายเลขบัญชีธนาคาร หมายเลขบัตรเครดิต วันเดือนปีเกิด หมายเลขประจำตัวที่ออกโดยทางราชการ ฯลฯ จะถูกจำหน่ายในราคาตั้งแต่ 14-18 ดอลลาร์

นอกจากนี้ ยังมีการเพิ่มขึ้นของภัยคุกคามที่เกี่ยวข้องกับการจารกรรมข้อมูลลับ อันมีสาเหตุมาจากโทรจันและเครือข่ายบ็อต (bot networks) ที่ผู้ประสงค์ร้ายใช้เป็นเครื่องมือในการเจาะเข้าระบบคอมพิวเตอร์ของผู้อื่น ซึ่งการโจมตีเพื่อลอบขโมยข้อมูลสำคัญบนเครื่องคอมพิวเตอร์นั้นได้สร้างความเสียหายทางการเงินมากมาย โดยเฉพาะอย่างยิ่งหากข้อมูลบัญชีธนาคารและบัตรเครดิตถูกลอบขโมยไปได้ โดยภัยคุกคามที่เกี่ยวข้องกับข้อมูลลับนั้นคิดเป็น 66 เปอร์เซ็นต์ของภัยอันเกิดจาก 50 อันดับแรกของโค้ดอันตราย ซึ่งเพิ่มขึ้นกว่าเมื่อช่วงที่ผ่านมาถึง 48 เปอร์เซ็นต์ ส่วนภัยคุกคามที่สามารถส่งข้อมูลผู้ใช้ เช่น ชื่อผู้ใช้และรหัสผ่าน ออกไปยังปลายทางที่กำหนด คิดเป็น 62 เปอร์เซ็นต์ของภัยคุกคามที่เกี่ยวข้องกับข้อมูลลับในช่วงครึ่งหลังของปี 2549 และเพิ่มขึ้นจากครึ่งแรกของปีกว่า 38 เปอร์เซ็นต์

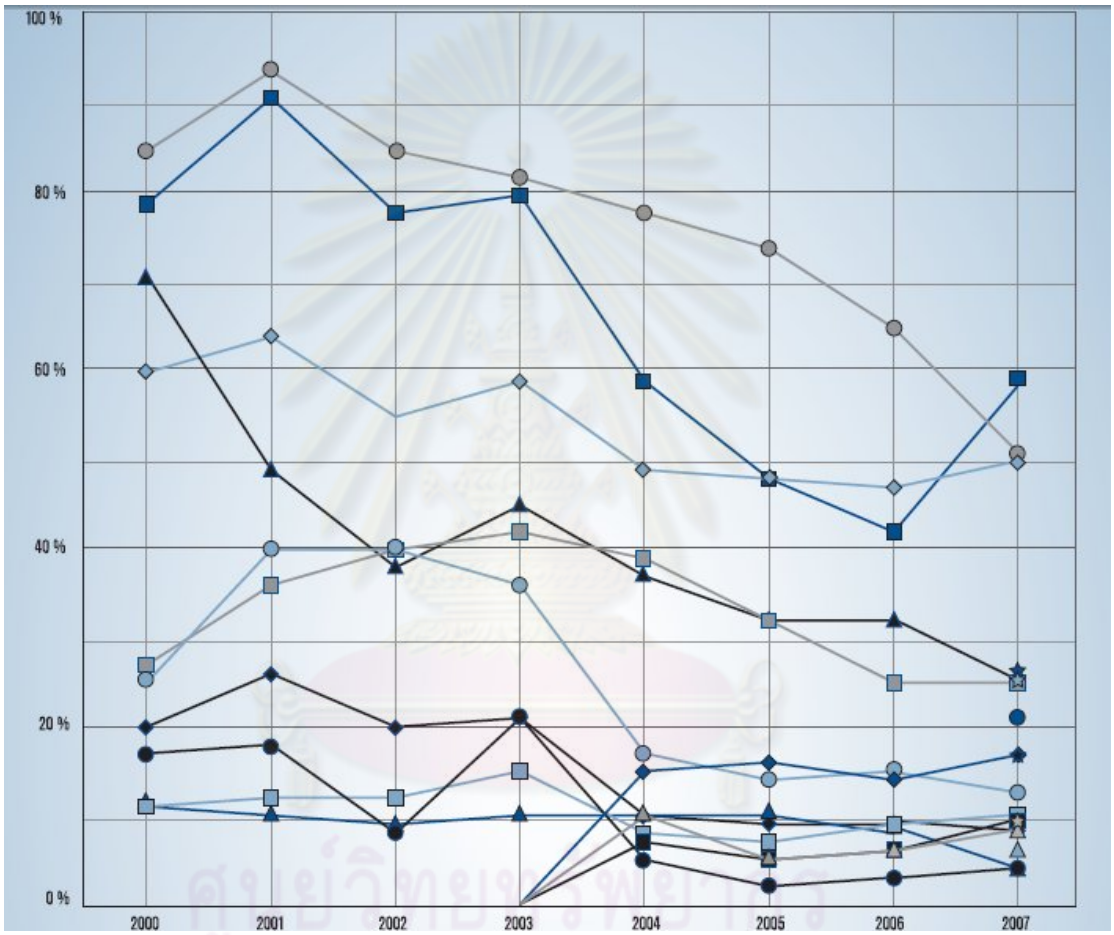
นอกจากนี้ยังมีสถิติความเสียหายของประเทศต่างๆ ที่เกิดจากอาชญากรรมทางคอมพิวเตอร์ เช่น

ประเทศสหรัฐอเมริกา

จากการสำรวจความเสียหายที่เกิดขึ้นจากการก่ออาชญากรรมทางคอมพิวเตอร์ในปี 2002 โดย Computer Security Institute (CSI) ซึ่งเป็นหน่วยงานหนึ่งใน FBI ของสหรัฐอเมริกา พบว่าความเสียหายที่เกิดขึ้นจากการขโมยข้อมูลทางคอมพิวเตอร์มีมูลค่าสูงที่สุด รองลงมาก็คือการฉ้อโกงทางคอมพิวเตอร์ และการปล่อยไวรัส ตามลำดับ โดยรายงานผลการสำรวจการก่ออาชญากรรมคอมพิวเตอร์ของ สำนักงานสืบสวนสอบสวนกลาง (เอฟบีไอ) และสถาบันความปลอดภัยบนคอมพิวเตอร์ หรือ ซีเอสไอ (Computer Security Institute) ของสหรัฐฯ ในปี 2547 พบว่า มีมูลค่าความเสียหายจากบริษัทต่างๆ จำนวน 489 ราย คิดเป็นมูลค่ากว่า 141 ล้านดอลลาร์สหรัฐ โดย 79% ของหน่วยงานทั้งหมดระบุว่า การต่อเชื่อมอินเทอร์เน็ต ถูกโจมตี

ระบบบ่อยครั้งขึ้นจากเดิมในปี 2544 ที่มีสัดส่วนเพียง 59% ที่ถูกโจมตีผ่านอินเทอร์เน็ต[51] ในขณะที่รายงานความเสียหายล่าสุดประจำปี 2550 ของ CSI ระบุว่ามีความเสียหายโดยเฉลี่ยต่อรายสูงถึง 350,424 ดอลลาร์ เมื่อเทียบกับความเสียหายโดยเฉลี่ย 168,000 ดอลลาร์จากปี 2549[52] โดยสถิติของอาชญากรรมคอมพิวเตอร์ในปี 2007 ของประเทศสหรัฐอเมริกา อาจพิจารณาได้ ดังนี้

Type of Attacks or Misuse Detected in the last 12 months[53]



[51] แหล่งที่มา : www.thaicleannet.com [วันที่ 27 กันยายน 2550]

[52] CSI, “2007 CSI Computer Crime and Security Survey,” [Online] Available from : www.gocsi.com [วันที่ 27 กุมภาพันธ์ 2551]

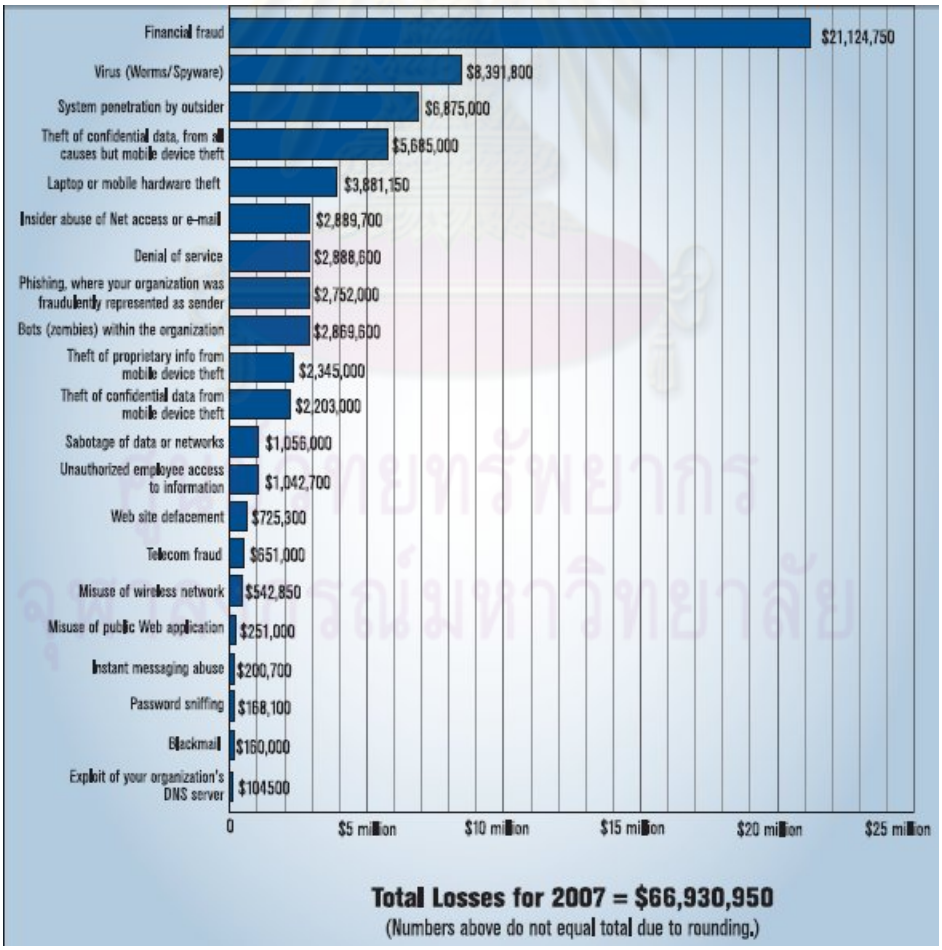
[53] เรื่องเดียวกัน,

TYPE OF ATTACK	2007
Insider abuse of Net access	59%
Virus	52%
Laptop / mobile device theft	50%
Phishing where your organization was fraudulently represented as sender**	26%
Instant messaging misuse**	25%
Denial of service	25%
Unauthorized access to information	25%
Bots within the organization**	21%
Theft of customer / employee data**	17%
Abuse of wireless network*	17%
System penetration	13%

TYPE OF ATTACK	2007
Financial fraud	12%
Password sniffing**	10%
Web site defacement*	10%
Misuse of public Web application*	9%
Theft of proprietary information (intellectual property)	8%
Exploit of the organization's DNS server**	6%
Telecom fraud	5%
Sabotage	4%

*Added in 2004 survey
**Added in 2007 survey

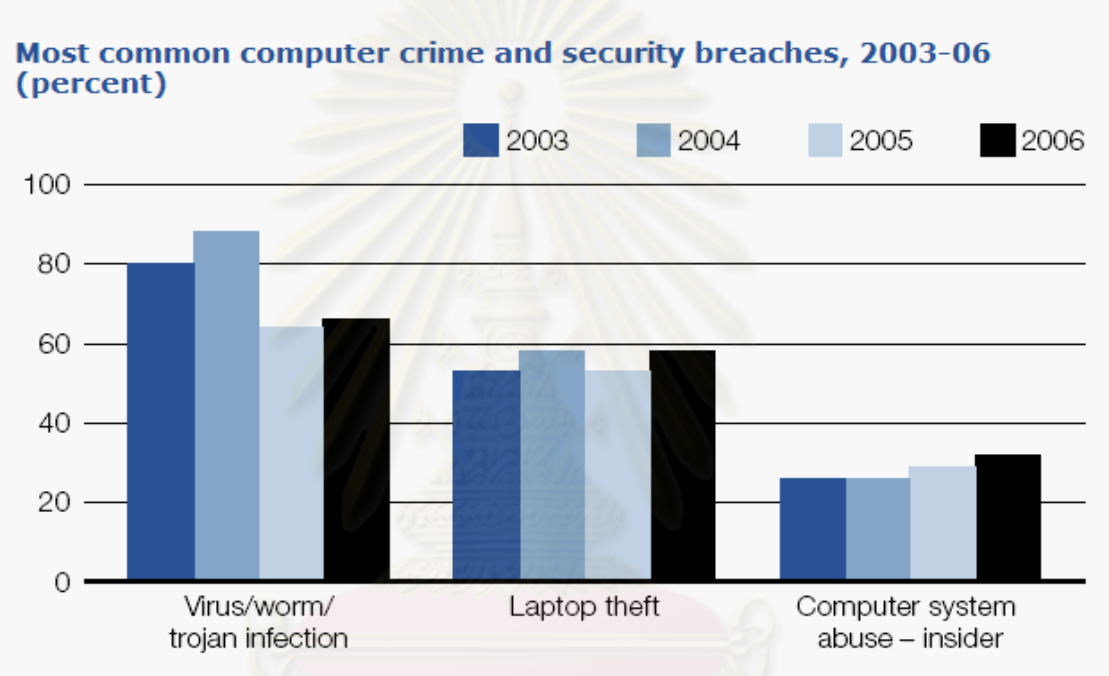
โดยอาจแยกความเสียหายจากการกระทำความผิดเป็นประเภทต่างๆ ได้ดังนี้[54]



[54] เรื่องเดียวกัน,

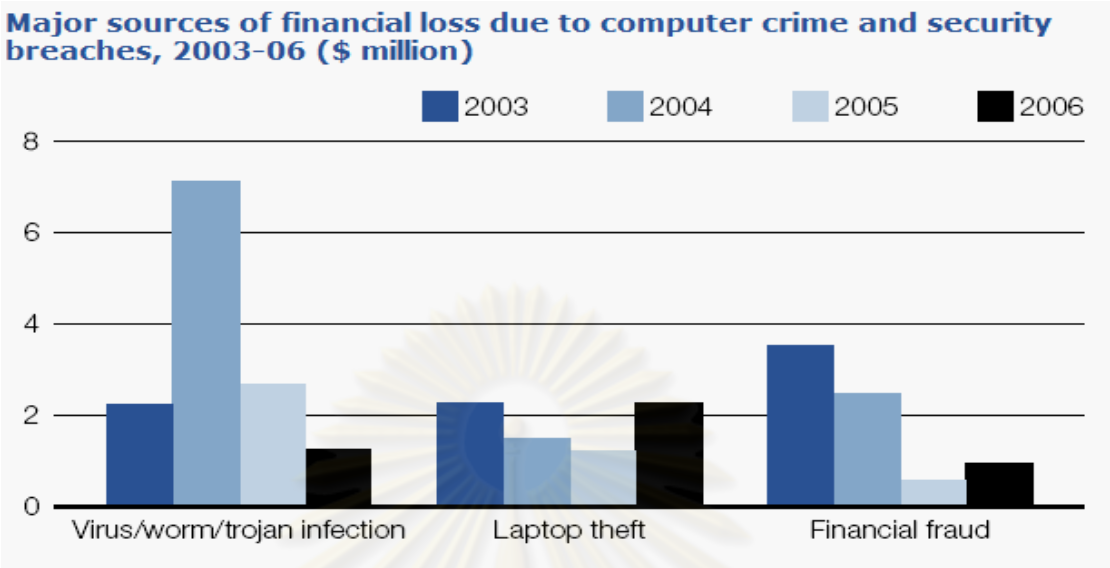
ประเทศออสเตรเลีย

ประเทศออสเตรเลีย ก็ได้ทำการสำรวจความเสียหายที่เกิดขึ้นจากการก่ออาชญากรรมทางคอมพิวเตอร์ตั้งแต่ในปี 2002 เช่นเดียวกัน โดยพบว่า ความเสียหายที่เกิดขึ้นจากการขโมยคอมพิวเตอร์ มีมูลค่าสูงที่สุด รองลงมาก็คือการปล่อยไวรัส และการเข้าถึงอินเทอร์เน็ตหรืออีเมล์โดยไม่ได้รับอนุญาตจากคนภายในองค์กรตามลำดับ และมีสถิติคดีในปี 2003-2006 ดังนี้[55]



[55] AusCert, “Crime and criminal justice statistics,” [Online] Available from : www.aic.gov.au/stats/crime/cybercrime.html [วันที่ 27 กุมภาพันธ์ 2551]

ซึ่งนอกเหนือจากสถิติคดีแล้ว AusCert ยังได้มีการสำรวจความเสียหายที่เกิดขึ้น ดังนี้



ประเทศเกาหลีใต้

เกาหลีใต้เป็นอีกประเทศหนึ่งที่มีความพยายามในการพัฒนาคอมพิวเตอร์เป็นอย่างมากและประสบความสำเร็จในการใช้คอมพิวเตอร์ทำธุรกิจต่างๆ โดยเฉพาะเกมออนไลน์ แต่เมื่อคนมีความรู้เกี่ยวกับคอมพิวเตอร์มากขึ้นก็มีการใช้คอมพิวเตอร์ในการกระทำความผิดมากขึ้นเช่นกัน โดยจำนวนคดีด้านอาชญากรรมในประเทศเกาหลีใต้มีจำนวนทั้งหมด 77,099 คดี ในปี 2547 และเพิ่มเป็น 88,731 คดี ในปี 2548 โดยโครงสร้างของหน่วยงานทางกระบวนการยุติธรรมของเกาหลีใต้นั้น มีสองหน่วยงานที่มีศูนย์พิสูจน์หลักฐานทางดิจิตอล (Digital Forensic Center) คือ สำนักงานอัยการสูงสุด (Supreme Prosecutor's Office) และ กรมตำรวจแห่งชาติฝ่ายปราบปรามอาชญากรรมคอมพิวเตอร์ (National Korean Cyber Police) โดยกรมตำรวจเป็น

หน่วยงานที่ควบคุมโดยสำนักงานอัยการสูงสุดอีกทีหนึ่ง[56] โดยอาชญากรรมคอมพิวเตอร์ในประเทศเกาหลีใต้แบ่งตามประเภทปี 2002-2007 มีสถิติดังนี้[57]

• **Cyber crime statistics (by type) Cyber crime statistics** (Dec. 31, 2007)

Year	Total	Hacking virus	Internet fraud	Cyber violence	Illegal website operation	Illegal copying and sales	Other
02	41,900	9,707	19,395	4,726	862	1,778	5,432
03	51,722	8,891	26,875	4,991	1,719	677	8,569
04	63,384	10,993	30,288	5,816	2,410	1,244	12,633
05	72,421	15,874	33,112	9,227	1,850	1,233	11,125
06	70,545	15,979	26,711	9,436	7,322	2,284	8,813
07	78,890	14,037	28,081	12,905	5,505	8,167	10,195

โดยสถิติจากอาชญากรรมคอมพิวเตอร์ที่เกิดและสามารถจับกุมได้ ตั้งแต่ ปี 2001-2007 คือ[58]

• **Status for cyber crime arrest Status for cyber crime arrest** (Dec. 31, 2007)

Year	Total			Cyber terror crimes			General cyber crimes		
	Occurred	Arrested		Occurred	Arrested		Occurred	Arrested	
		Cases	People		Cases	People		Cases	People
01	33,289	22,693	24,455	10,638	7,595	8,099	22,651	15,098	16,356
02	60,068	41,900	47,252	14,159	9,707	10,762	45,909	32,193	36,490
03	68,445	51,722	56,724	14,241	8,891	10,047	54,204	42,831	46,677
04	77,099	63,384	70,143	15,390	10,993	11,892	61,709	52,391	58,251
05	88,731	72,421	81,338	21,389	15,874	17,371	67,342	56,547	63,967
06	82,186	70,545	89,248	20,186	15,979	17,498	62,000	54,566	71,750
07	88,847	78,890	88,549	17,671	14,037	15,302	71,176	64,853	73,247

---

[56] ACIS, “กรณีศึกษาเกี่ยวกับอาชญากรรมคอมพิวเตอร์และการใช้กฎหมายการกระทำผิดเกี่ยวกับคอมพิวเตอร์ในกระบวนการยุติธรรมของประเทศเกาหลีใต้,” [Online] แหล่งที่มา : www.topsecure.net/article_prinya_eweek_150749.html [วันที่ 28 กุมภาพันธ์ 2551]

[57] Korean National Police Agency, “Cyber crime statistics,” [Online] Available from : www.police.go.kr/KNPA/statistics [วันที่ 28 กุมภาพันธ์ 2551]

[58] เรื่องเดียวกัน,

บทที่ 3
กฎหมายต่างประเทศที่เกี่ยวข้องกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

เมื่อการกระทำความผิดเนื่องจากการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ส่งผลกระทบต่อประชาชนทั่วไปเป็นจำนวนมาก และก่อให้เกิดความเสียหายที่ร้ายแรงต่างๆ เช่นทางเศรษฐกิจ ความมั่นคง หรือแม้แต่ในเรื่องความเป็นส่วนตัว ดังนั้นประเทศต่างๆ รวมถึงประเทศไทย จึงเล็งเห็นความสำคัญในการออกกฎหมายมาป้องกันและปราบปรามการกระทำผิดในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ขึ้น โดยจะเห็นได้จากความพยายามขององค์การระหว่างประเทศที่จะผลักดันให้ประเทศต่างๆ มีกฎหมายที่เกี่ยวข้องกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์โดยกำหนดให้เป็นความผิดอาญา

3.1 ความร่วมมือระหว่างประเทศในความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

ประชาคมโลกต่างเห็นความสำคัญของการกระทำความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ว่าเป็นอาชญากรรมทางคอมพิวเตอร์ประเภทหนึ่งที่มีความร้ายแรงและจำเป็นต้องมีกฎหมายควบคุม นอกจากนี้การกระทำผิดดังกล่าวทำให้เกิดปัญหาในการนำตัวผู้กระทำผิดมาลงโทษและการบังคับใช้กฎหมาย เนื่องจากการกระทำผิดดังกล่าวสามารถกระทำได้ทุกสถานที่ ทุกเวลา และผลของการกระทำความผิดอาจจะเกิดที่ใดก็ได้ในโลก ทำให้องค์การระหว่างประเทศต่างๆ เห็นถึงความสำคัญและความจำเป็นที่จะต้องมีกฎหมายหรือความร่วมมือกันเพื่อควบคุมการกระทำผิดดังกล่าว ซึ่งองค์การที่เห็นความสำคัญในเรื่องดังกล่าว เช่น สหประชาชาติ (UN) สหภาพยุโรป (EU) หรือองค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD)

3.1.1 สหประชาชาติ (UN)

องค์การสหประชาชาติได้เล็งเห็นความสำคัญในการกระทำผิดเกี่ยวกับคอมพิวเตอร์ โดยในการประชุมสหประชาชาติครั้งที่ 10 ว่าด้วยการป้องกันอาชญากรรมและการปฏิบัติต่อผู้กระทำผิด (The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders) ซึ่งจัดขึ้นที่กรุงเวียนนา เมื่อวันที่ 10-17 เมษายน 2543 ได้มีการจำแนกประเภทของอาชญากรรมทางคอมพิวเตอร์ โดยแบ่งเป็น 5 ประเภท คือ การเข้าถึงโดยไม่ได้รับอนุญาต การสร้างความเสียหายแก่ข้อมูลหรือโปรแกรมคอมพิวเตอร์ การก่อกวนการทำงานของ

ระบบคอมพิวเตอร์หรือเครือข่าย การยับยั้งข้อมูลที่ส่งถึง/จากและภายในระบบหรือเครือข่ายโดยไม่ได้รับอนุญาต และการจารกรรมข้อมูลบนคอมพิวเตอร์[1]

3.1.2 กลุ่มสหภาพยุโรป (EU)

กลุ่มสหภาพยุโรปได้มีการจัดตั้งกรรมาธิการผู้เชี่ยวชาญด้านอาชญากรรมทางคอมพิวเตอร์ขึ้นในปี 1985 เพื่อกำหนดแนวทางในการบัญญัติกฎหมายให้ครอบคลุมถึงลักษณะการกระทำที่สมควรบัญญัติเป็นความผิดซึ่งมีอย่างน้อย 8 ฐานความผิด ได้แก่ การฉ้อโกงทางคอมพิวเตอร์ การปลอมแปลงทางคอมพิวเตอร์ การทำลายข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ การรบกวนการทำงานของคอมพิวเตอร์หรือระบบคมนาคม การเข้าถึงโดยมิชอบ การดักข้อมูลโดยมิชอบ และการทำซ้ำลายพิมพ์วงจรโดยมิชอบ และยังมีความผิดอื่นที่กำหนดให้เป็นทางเลือกที่จะบัญญัติเป็นกฎหมายภายใน 4 ฐานความผิด ได้แก่ การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ การจารกรรมทางคอมพิวเตอร์ การใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยมิชอบ และการใช้โปรแกรมคอมพิวเตอร์ที่ได้รับการคุ้มครองโดยมิชอบ

โดยต่อมา Council of Europe ได้จัดทำอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์[2] (Convention on Cybercrime : ETS No. 185) ซึ่งนับเป็นอนุสัญญาฉบับแรกเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ โดยอนุสัญญานี้มีวัตถุประสงค์ที่สำคัญ 3 ประการ คือ

1. เพื่อให้กฎหมายสารบัญญัติภายในประเทศต่างๆ ที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์มีความสอดคล้องและเป็นไปในทิศทางเดียวกัน
2. เพื่อให้กฎหมายวิธีพิจารณาความอาญาตามกฎหมายภายในให้อำนาจที่จำเป็นเพื่อการสืบสวนสอบสวนและฟ้องร้องการกระทำความผิดที่ได้กระทำโดยระบบคอมพิวเตอร์ ตลอดจนการรวบรวมพยานหลักฐานที่อยู่รูปข้อมูลอิเล็กทรอนิกส์
3. เพื่อเร่งให้เกิดความร่วมมือระหว่างประเทศที่รวดเร็วและบรรลุเป้าหมายของอนุสัญญา

---

[1] ไมโครซอฟท์ประเทศไทย, “อาชญากรรมทางคอมพิวเตอร์ประเภทต่างๆ,” [Online] แหล่งที่มา : www.microsoft.com/thailand/piracy/cybercrime.aspx [วันที่ 12 มกราคม 2551]

[2] “Council of Europe,” [Online] Available from : www.conventions.coe.int/Treaty/EN/cadreprincipal.htm [วันที่ 12 มกราคม 2551]

ในปัจจุบันอนุสัญญานี้มีรัฐลงนามในอนุสัญญาแล้ว 29 ประเทศ[3] และมีรัฐให้สัตยาบันในอนุสัญญาแล้ว 9 ประเทศ[4] ซึ่งอนุสัญญาได้มีผลใช้บังคับเมื่อ 1 กรกฎาคม 2004 หลังจากที่ประเทศลิธัวเนียซึ่งเป็นประเทศที่ 5 ได้ให้สัตยาบันแก่อนุสัญญาเมื่อ 18 มีนาคม 2004

โดยความผิดในการเข้าถึงคอมพิวเตอร์โดยมิชอบนั้นก็เป็นฐานความผิดหลักความผิดหนึ่งในอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์นี้ โดยได้กำหนดการกระทำที่เป็นความผิดไว้ว่า การเข้าถึงคอมพิวเตอร์โดยมิชอบ หมายถึง การเข้าถึงบางส่วนหรือทั้งหมดของระบบคอมพิวเตอร์โดยไม่มีสิทธิ โดยผ่านมาตรการป้องกันด้วยเจตนาที่จะได้มาซึ่งข้อมูลคอมพิวเตอร์หรือเจตนาไม่บริสุทธิ์อื่น หรือในการติดต่อกับระบบคอมพิวเตอร์ที่ได้เชื่อมต่อกับระบบคอมพิวเตอร์อื่น[5]

3.1.3 องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Cooperation and Development)[6]

---

[3] ประกอบด้วยประเทศในกลุ่มคณะมนตรีแห่งยุโรป 25 ประเทศ ได้แก่ Armenia, Austria, Belgium, Bulgaria, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Latvia, Luxembourg, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Ukraine and United Kingdom และประเทศนอกกลุ่มคณะมนตรีแห่งยุโรป 4 ประเทศ ได้แก่ Canada, Japan, South Africa and United States

[4] ประกอบด้วย Albania, Croatia, Cyprus, Estonia, Hungary, Lithuania, Romania, Slovenia and the former Yugoslav Republic of Macedonia

[5] CONVENTIONON CYBERCRIME: the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system [Online] Available from : www.conventions.coe.int/Treaty/EN/cadreprincipal.htm [วันที่ 12 มกราคม 2551]

[6] OECD Guidelines for the Security of Information Systems were adopted as a Recommendation of the OECD Council on 26 November 1992

OECD เป็นองค์กรระหว่างประเทศที่ริเริ่มพัฒนาการที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ ตั้งแต่ปี 1983 ด้วยการจัดตั้งคณะกรรมาธิการผู้เชี่ยวชาญ เพื่อหารือเกี่ยวกับปัญหาอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ ซึ่งต่อมาในปี 1986 คณะกรรมการดังกล่าวได้จัดทำข้อเสนอแนะแก่ประเทศสมาชิกในการบัญญัติกฎหมายภายในให้มีความสอดคล้องกันในฐานความผิดที่สำคัญ เช่น การรบกวนข้อมูลหรือโปรแกรมคอมพิวเตอร์เพื่อให้ได้มาซึ่งประโยชน์ในทางทรัพย์สิน การปลอมแปลงทางคอมพิวเตอร์ การขัดขวางการทำงานของคอมพิวเตอร์และระบบโทรคมนาคม การเข้าถึงหรือดักการสื่อสารของระบบคอมพิวเตอร์โดยมิชอบ

นอกจากองค์กรระหว่างประเทศต่างๆ ที่เล็งเห็นความสำคัญของการกระทำความผิดเกี่ยวกับการเข้าถึงโดยมิชอบแล้ว ประเทศต่างๆ โดยเฉพาะประเทศที่มีความก้าวหน้าทางเทคโนโลยีก็ตระหนักถึงความจำเป็นที่จะต้องมีกฎหมายเกี่ยวกับการกระทำผิดทางคอมพิวเตอร์ออกมาเช่นกัน โดยผู้เขียนจะขอกล่าวถึงกฎหมายเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจของประเทศสหรัฐอเมริกา ประเทศอังกฤษ และประเทศเยอรมัน ดังนี้

3.2 ความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ของต่างประเทศ

2.3.2.1 ประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกานับว่าเป็นประเทศที่มีความเจริญก้าวหน้าทางเทคโนโลยีมากที่สุดแห่งหนึ่งของโลก ดังนั้นอาชญากรรมเกี่ยวกับเทคโนโลยีต่างๆ จึงเกิดขึ้นเป็นจำนวนมาก เมื่อกฎหมายที่มีอยู่ไม่สามารถดำเนินคดีกับผู้กระทำผิดได้ ทำให้สหรัฐอเมริกาจำเป็นต้องจึงมีการบัญญัติกฎหมายที่ดำเนินการทางกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ขึ้น

กฎหมายสหรัฐอเมริกาที่ใช้ดำเนินคดีกับอาชญากรรมคอมพิวเตอร์นั้นมีอยู่หลายฉบับ คือ 18 USC §1029 Fraud and Related Activity in Connection with Access §1030 Fraud and Related Activity in Connection with Computers §1362 Communication Lines, Stations, or Systems §2511 Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited, §2701 Unlawful Access to Stored Communications §2702

Disclosure of Contents §2703 Requirements for Governmental Access, and No Electronic Theft Act available[7]

หากแต่กฎหมายที่เกี่ยวข้องโดยตรงและมักถูกอ้างอิงถึงเมื่อถูกถึงความผิดในการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ ได้แก่ The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CFAA) ที่มีการแก้ไขเพิ่มเติมกฎหมายในปี 1989 1990 1994 1996 2001 และปี 2002 มีแนวความคิดในการบัญญัติกฎหมายเพื่อใช้ดำเนินคดีกับการกระทำความผิดต่อคอมพิวเตอร์รูปแบบต่างๆ การที่สภาคองเกรสเห็นว่า การกระทำรูปแบบใหม่นี้มีลักษณะพิเศษที่แตกต่างไปจากความผิดรูปแบบเดิม เพราะเป็นการกระทำที่เกี่ยวข้องกับสิ่งที่ไม่มีรูปร่าง ทำให้การจะดำเนินคดีโดยอาศัยความผิดฐาน Theft และ Larceny ตามกฎหมายเดิมเป็นเรื่องที่ยากลำบากเพื่อแก้ปัญหาเรื่องนี้ก็ควรที่จะบัญญัติกฎหมายใหม่ขึ้นมามากกว่าการพยายามจะนำกฎหมายเก่ามาใช้ดำเนินคดีกับความผิดรูปแบบใหม่[8] ผู้เขียนจึงจะขอศึกษาความผิดในการเข้าถึงโดยปราศจากอำนาจในความผิดตาม The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 มาตรา 1030 เป็นหลัก ดังนี้

เนื่องจาก CFAA 18 U.S.C. มาตรา 1030 มีรายละเอียดความรับผิดในอาชญากรรมคอมพิวเตอร์เรื่องการเข้าถึงโดยปราศอำนาจเป็นหลัก แม้จะมีบางส่วนก็ไม่เกี่ยวข้องกับความผิดในการเข้าถึงโดยปราศจากอำนาจ แต่โดยหลักแล้วจะเป็นความผิดในการเข้าถึงโดยปราศจากอำนาจหรือเกินขอบอำนาจ ซึ่งหากพิจารณาจากองค์ประกอบความผิดทั้งหมดตามมาตรา 1030 (a) (1) – (7) แล้ว จะเห็นได้ว่า กฎหมายของสหรัฐอเมริกาใน CFAA 18 U.S.C. มาตรา 1030 ได้ใช้วิธีกำหนดหลักเกณฑ์ของความผิดโดยมุ่งถึงการกระทำที่เป็นการเข้าถึงคอมพิวเตอร์เป็นหลักพื้นฐานในการกำหนดว่าการกระทำใดเป็นการกระทำความผิด แล้วจึงแยกรายละเอียดภายในอีกครั้งหนึ่งว่าเป็นการเข้าถึงข้อมูลประเภทใดที่กฎหมายมุ่งคุ้มครองหรือ

---

[7] "The following countries have updated laws to prosecute cyber crime," [Online] Available from : www.mcconnellinternational.com/services/Updatedlaws.htm [วันที่ 12 มกราคม 2551]

[8] องอาจ เทียนหิรัญ, "อาชญากรรมคอมพิวเตอร์ : การกำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์," (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2546), หน้า 43.

เข้าถึงเพื่อที่จะไปกระทำความผิดอื่นใดต่อไป เช่น การเข้าถึงโดยปราศจากอำนาจและได้ไปซึ่งข้อมูลความมั่นคงของรัฐ หรือการเข้าโดยปราศจากอำนาจโดยตั้งใจที่จะฉ้อโกง ซึ่งความผิดในการเข้าถึงโดยปราศจากอำนาจนั้น ปรากฏใน มาตรา 1030 (a) (1) (2) (3) (4) (5)(ii)(iii) ส่วนความผิดในการส่งโปรแกรมมุ่งร้ายเพื่อสร้างความเสียหาย ตามมาตรา 1030 (a) (5)(i) ความผิดในการฉ้อโกง ค้าขายรหัสผ่านโดยผิดกฎหมาย ตาม1030 (a) (6) และความผิดในการข่มขู่จะทำลายคอมพิวเตอร์ที่ถูกป้องกัน ตามมาตรา 1030 (a) (7) นั้นไม่เกี่ยวข้องกันความผิดในการเข้าถึงโดยปราศจากอำนาจแต่อย่างใด จึงไม่ขอกล่าวถึงในวิทยานิพนธ์ฉบับนี้ โดยผู้เขียนจึงจะขอแยกองค์ประกอบความผิดเฉพาะส่วนที่เกี่ยวข้องกันการเข้าถึงโดยปราศจากอำนาจดังต่อไปนี้

1. **ความผิดฐานเข้าถึงโดยปราศจากอำนาจและได้ไปซึ่งข้อมูลความมั่นคงของรัฐ** มาตรา 1030 (a) (1)[9] บัญญัติไว้ว่า

---

[9](a) Whoever--(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(a) ผู้ใด

(1) โดยรู้ เข้าถึงคอมพิวเตอร์[10]โดยปราศจากอำนาจหรือเกินขอบอำนาจ[11] และด้วยวิธีการดังกล่าว ได้ไปซึ่งข้อมูลที่รัฐบาลสหรัฐอเมริกา มีคำสั่งของฝ่ายบริหารหรือกฎหมายลายลักษณ์อักษรกำหนดให้มีการคุ้มครองเพื่อป้องกันการเปิดเผยข้อมูลนั้นโดยปราศจากอำนาจเนื่องจากเหตุผลที่เกี่ยวกับความปลอดภัยของประเทศหรือเกี่ยวกับการต่างประเทศ หรือเป็นข้อมูลใดๆ ที่เป็นความลับตามความหมายในย่อหน้า y ของมาตรา 11 แห่ง Atomic Energy Act of 1954 ซึ่งเป็นเหตุผลอันเชื่อได้ว่าข้อมูลที่ได้รับมานั้นอาจถูกนำไปใช้เพื่อสร้างความเสียหายให้กับสหรัฐอเมริกา หรือเพื่อให้เกิดประโยชน์ต่อรัฐอื่น โดยเจตนาติดต่อสื่อสาร ส่ง รับส่งข้อมูล หรือพยายามติดต่อสื่อสาร ส่ง รับส่งข้อมูล หรือถูกติดต่อสื่อสาร ถูกส่ง ถูกรับส่งข้อมูลดังกล่าวไปยังบุคคลใดๆ ซึ่งไม่มีสิทธิได้รับข้อมูลนั้น หรือเจตนาเก็บข้อมูลนั้นไว้โดยไม่ยอมส่งข้อมูลดังกล่าวไปให้แก่เจ้าหน้าที่ของรัฐผู้มีสิทธิที่จะรับข้อมูลนั้น

---

[10] คอมพิวเตอร์ (computer) มีนิยามไว้ใน FCAA มาตรา 1030 (e) (1) ว่า คอมพิวเตอร์หมายถึง เครื่องอิเล็กทรอนิกส์ แม่เหล็ก แสง หรือไฟฟ้าอิเล็กตรอน หรือเครื่องที่มีกระบวนการคำนวณข้อมูลความเร็วสูง ที่แสดงถึงตรรกะ คณิตศาสตร์ หรือเก็บข้อมูล และรวมถึงเครื่องเก็บข้อมูลใดๆ หรือเครื่องติดต่อสื่อสาร ที่สัมพันธ์โดยตรงหรือปฏิบัติการร่วมกันกับเครื่องมือเหล่านี้ แต่ไม่หมายความรวมไปถึง เครื่องพิมพ์ดีด หรือเครื่องเรียงพิมพ์ เครื่องคำนวณที่พกพา หรือเครื่องมืออื่นที่มีลักษณะเดียวกัน (the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device)

[11] เกินขอบอำนาจ (exceeds authorized access) มีนิยามไว้ใน FCAA มาตรา 1030 (e) (5) หมายถึง การเข้าสู่คอมพิวเตอร์โดยมีอำนาจและใช้การเข้าถึงนั้นเอาไปหรือเปลี่ยนแปลงข้อมูลในคอมพิวเตอร์นั้นซึ่งผู้เข้าถึงไม่มีสิทธิเอาไปหรือเปลี่ยนแปลง (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)

จะต้องถูกลงโทษตามอนุมาตรา (c) ของมาตรานี้

ตามบทบัญญัติดังกล่าว อาจกล่าวได้ว่าความผิดตาม CFAA มาตรา 1030 (a) (1) นั้น เป็นความผิดฐานเข้าถึงโดยปราศจากอำนาจและได้ไปซึ่งข้อมูลความมั่นคงของรัฐ และแยกองค์ประกอบได้ ดังนี้[12]

1. ผู้ใด โดยรู้ เข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบอำนาจ
2. ได้ไปซึ่งข้อมูลที่รัฐบาลสหรัฐอเมริกา
3. มีเหตุผลอันเชื่อได้ว่าข้อมูลที่ได้รับมานั้นอาจถูกนำไปใช้เพื่อสร้างความเสียหายให้กับสหรัฐอเมริกา หรือเพื่อให้เกิดประโยชน์ต่อรัฐอื่น
4. โดยเจตนาติดต่อสื่อสาร ส่ง รับส่งข้อมูล (หรือพยายาม) หรือเจตนาเก็บข้อมูลนั้นไว้โดยไม่ยอมส่งข้อมูลดังกล่าวไปให้แก่เจ้าหน้าที่ของรัฐผู้มีสิทธิที่จะรับข้อมูลนั้น

ผู้กระทำความผิดตามมาตรานี้เป็นความผิดร้ายแรง โดยมีโทษปรับ หรือโทษจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(1)(A)[13] และในกรณีที่กระทำความผิดในมาตรา 1030 มาก่อนก็จะถูกลงโทษปรับ หรือโทษจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(1)(B)[14]

---

[12] United States Department of Justice, Prosecuting Computer Crimes : Computer Fraud and Abuse Act [Online] Available from : www.cybercrime.gov [วันที่ 1 กุมภาพันธ์ 2551]

[13] The punishment for an offense under subsection (a) or (b) of this section is--**(1)(A)** a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph

[14] The punishment for an offense under subsection (a) or (b) of this section is--**(1)((B)** a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs

2. ความผิดฐานเข้าไปโดยปราศจากอำนาจและเอาไปซึ่งความลับ มาตรา 1030 (a) (2) บัญญัติไว้ว่า

(a) ผู้ใด

(2)โดยเจตนาเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบอำนาจ และได้รับซึ่ง

(A) ข้อมูลทางการเงินของสถาบันการเงินหรือสถาบันที่ให้กู้ยืมที่ถูกนิยามไว้ในมาตรา 1602 (n) ของหมวด 15 หรือข้อมูลซึ่งเก็บไว้ในแฟ้มข้อมูลของสำนักงานข้อมูลของผู้บริโภค ซึ่งมีข้อความอย่างเดียวกันกับที่กำหนดไว้ใน The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) ข้อมูลจากหน่วยงานหรือตัวแทนใดๆ ของสหรัฐอเมริกา หรือ

(C) ข้อมูลจากคอมพิวเตอร์ที่ถูกป้องกันถ้าการกระทำนั้นเกี่ยวข้องกับการติดต่อสื่อสารระหว่างมลรัฐหรือการติดต่อสื่อสารระหว่างประเทศ[15]

จะต้องถูกลงโทษตามอนุมาตรา (c) ของมาตรานี้

ซึ่งความผิดฐานเข้าไปโดยปราศจากอำนาจและเอาไปซึ่งความลับ (มาตรา 1030 (a) (2)) อาจแยกองค์ประกอบได้ ดังนี้

---

after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph

[15] (a) Whoever--(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication

1. โดยเจตนาเข้าถึงคอมพิวเตอร์
2. โดยปราศจากอำนาจหรือเกินขอบอำนาจ
3. ได้ไปซึ่งข้อมูลจาก
    3.1 ข้อมูลทางการเงินจากสถาบันการเงินหรือสำนักงานข้อมูลของผู้บริโภค หรือ
    3.2 ข้อมูลที่รัฐบาลหรือข้อมูลจากหน่วยงานหรือตัวแทนใดๆ ของสหรัฐอเมริกา หรือ
    3.3 ข้อมูลจากคอมพิวเตอร์ที่ถูกป้องกันถ้าการกระทำนั้นเกี่ยวข้องกับการติดต่อสื่อสารระหว่างมลรัฐหรือการติดต่อสื่อสารระหว่างประเทศหรือเพื่อให้เกิดประโยชน์ต่อรัฐอื่น

ผู้กระทำความผิดตามมาตรานี้เป็นความผิดไม่ร้ายแรง โดยมีโทษปรับ หรือโทษจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(2)(A)[16] ถ้าหากเพียงได้รับไปซึ่งข้อมูลที่มีค่าน้อยกว่า 5,000 เหรียญสหรัฐ เป็นความผิดไม่ร้ายแรง ถ้าไม่กระทำความผิดอื่นอีก แต่การกระทำความผิดหรือพยายามกระทำความผิดตามมาตรานี้จะกลายเป็นความผิดร้ายแรง เมื่อ

(1) เป็นการกระทำเพื่อผลประโยชน์ทางการค้าหรือข้อมูลทางการเงินของสถาบันการเงินหรือสถาบันที่ให้กู้ยืม
(2) กระทำความผิดอาญาอื่นหรือละเมิดที่ฝ่าฝืนต่อรัฐธรรมนูญหรือกฎหมายมลรัฐ หรือ
(3) ไปซึ่งข้อมูลที่มีค่ามากกว่า 5,000 เหรียญสหรัฐ

ในกรณีดังกล่าวก็จะถูกลงโทษปรับ หรือโทษจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(2)(B)[17]

---

[16] The punishment for an offense under subsection (a) or (b) of this section is-- (2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph

[17] 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

3. **ความผิดฐานบุกรุกเข้าไปในคอมพิวเตอร์ของรัฐ** มาตรา 1030 (a) (3) บัญญัติไว้ว่า

(a) ผู้ใด

(3) โดยเจตนาเข้าถึงคอมพิวเตอร์ที่ไม่ได้มีไว้เพื่อการสาธารณะของหน่วยงานหรือตัวแทนของสหรัฐอเมริกาโดยปราศจากอำนาจ ซึ่งคอมพิวเตอร์ของหน่วยงานหรือตัวแทนนั้นมีไว้เพื่อการใช้งานสำหรับรัฐบาลสหรัฐอเมริกาโดยเฉพาะ หรือในกรณีที่คอมพิวเตอร์ไม่ได้ถูกใช้งานสำหรับรัฐบาลสหรัฐอเมริกาโดยเฉพาะแต่ถูกใช้งานโดยหรือสำหรับรัฐบาลสหรัฐอเมริกาและการกระทำดังกล่าวส่งผลกระทบต่อการใช้งานของรัฐบาลสหรัฐอเมริกาหรือการใช้งานสำหรับสหรัฐอเมริกา[18]

จะต้องถูกลงโทษตามอนุมาตรา (c) ของมาตรานี้

โดยความผิดฐานบุกรุกเข้าไปในคอมพิวเตอร์ของรัฐ (มาตรา 1030 (a) (3)) อาจแยกองค์ประกอบได้ ดังนี้

1. เข้าถึงโดยเจตนา
2. โดยปราศจากอำนาจ

---

both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000

[18] (a) Whoever--(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

3. คอมพิวเตอร์ที่ไม่ได้มีไว้เพื่อการสาธารณะของสหรัฐอเมริกาซึ่งใช้งานหรือถูกใช้งานโดยหรือสำหรับรัฐบาลสหรัฐอเมริกาโดยเฉพาะ

4. ส่งผลกระทบต่อการใช้คอมพิวเตอร์ของสหรัฐอเมริกา

ผู้กระทำความผิดตามมาตรานี้ มีโทษปรับ หรือโทษจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(2)(A) และในกรณีที่กระทำความผิดในมาตรา 1030 มาก่อนก็จะถูกลงโทษปรับ หรือโทษจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(2)(C)

4. **ความผิดฐานเข้าถึงคอมพิวเตอร์เพื่อฉ้อโกง** ตามมาตรา 1030 (a) (4) นั้น บัญญัติไว้ว่า

(a) ผู้ใด

(4) โดยรู้และตั้งใจฉ้อโกง เข้าถึงคอมพิวเตอร์ที่มีการป้องกัน[19]โดยไม่มีอำนาจหรือเกินขอบอำนาจ และกระทำการต่อไปโดยตั้งใจฉ้อโกงและได้รับไปซึ่งสิ่งที่มีค่าใดๆ เว้นแต่วัตถุ

---

[19] คอมพิวเตอร์ที่มีการป้องกัน (protected computer) มีนิยามไว้ใน FCAA มาตรา 1030 (e) (2) ว่า คอมพิวเตอร์ที่ (A) ใช้โดยเฉพาะในสถาบันการเงินหรือรัฐบาลของสหรัฐอเมริกา หรือในกรณีที่คอมพิวเตอร์ไม่ได้ใช้ในกรณีดังกล่าว ถูกใช้หรือสำหรับสถาบันการเงินหรือรัฐบาลของสหรัฐอเมริกา และมีผลเป็นความผิดในการใช้หรือสำหรับสถาบันการเงินหรือรัฐบาลของสหรัฐอเมริกา (B) ซึ่งถูกใช้ในการค้าพาณิชย์หรือติดต่อสื่อสารระหว่างมลรัฐหรือระหว่างประเทศ รวมถึงคอมพิวเตอร์ที่ตั้งอยู่นอกประเทศสหรัฐอเมริกาซึ่งถูกใช้จัดการในการค้าพาณิชย์หรือติดต่อสื่อสารระหว่างมลรัฐหรือระหว่างประเทศของสหรัฐอเมริกา ((2) the term "protected computer" means a computer--(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States)

ของการฉ้อโกงและสิ่งของที่ได้มา รวมเฉพาะการใช้คอมพิวเตอร์และมูลค่าของการใช้ดังกล่าวนั้นไม่เกิน 5,000 เหรียญสหรัฐในช่วงเวลาหนึ่งปี[20]

จะต้องถูกลงโทษตามอนุมาตรา (c) ของมาตรานี้

โดยความผิดฐานเข้าถึงคอมพิวเตอร์เพื่อฉ้อโกง (มาตรา 1030 (a) (4)) อาจแยกองค์ประกอบได้ ดังนี้

1. เข้าถึงโดยปราศจากอำนาจหรือเกินขอบอำนาจซึ่งคอมพิวเตอร์ที่มีการป้องกันโดยรู้
2. ตั้งใจที่จะฉ้อโกง
3. เข้าถึงต่อไปเพื่อตั้งใจจะฉ้อโกง
4. ได้รับบางสิ่งที่มีมูลค่า รวมถึงการใช้ ถ้ามีมูลค่าเกิน 5,000 เหรียญดอลลาร์สหรัฐ

ผู้กระทำความผิดตามมาตรานี้ มีโทษปรับ หรือโทษจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ และในกรณีที่กระทำความผิดในมาตรา 1030 มาก่อนก็จะถูกลงโทษปรับ หรือโทษจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(3)[21]

5.**ความผิดฐานเข้าถึงและทำให้เกิดความเสียหาย** ตามมาตรา 1030 (a) (5) (A) (ii) และ มาตรา 1030 (a) (5) (A) (iii)) บัญญัติไว้ว่า

---

[20] Whoever--(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period

[21] The punishment for an offense under subsection (a) or (b) of this section is-- (3) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph

(a) ผู้ใด

(5)

(A)

(i) โดยรู้ ทำให้เกิดการส่งโปรแกรม ข้อมูล รหัส หรือคำสั่ง และการกระทำดังกล่าวเจตนาทำให้เกิดความเสียหายต่อคอมพิวเตอร์ที่ได้รับการป้องกันโดยปราศจากอำนาจ

(ii) เจตนาเข้าถึงคอมพิวเตอร์ที่ได้รับการป้องกันโดยปราศจากอำนาจ และจากการกระทำดังกล่าวทำให้เกิดความเสียหายโดยประมาทโดยรู้ตัว[22] (Reckless) หรือ

(iii) เจตนาเข้าถึงคอมพิวเตอร์ที่ได้รับการป้องกันโดยปราศจากอำนาจ และจากการกระทำดังกล่าวทำให้เกิดความเสียหาย

(B) จากการกระทำดังกล่าวในข้อ (i) (ii) หรือ (iii) ของย่อหน้า (A) ทำให้เกิด (หรือในกรณีที่เป็นการพยายามกระทำความผิด ถ้าความผิดนั้นได้กระทำสำเร็จจนเป็นเหตุให้เกิด)

(i) ความเสียหายต่อบุคคลหนึ่งหรือมากกว่าในช่วงเวลาหนึ่งปี (และสำหรับจุดประสงค์ในการสอบสวน ดำเนินคดี หรือกระบวนการพิจารณาอื่นโดยรัฐ ทำให้เกิดความเสียหายที่เกี่ยวข้องกับการกระทำดังกล่าวสำหรับคอมพิวเตอร์ที่ถูกป้องกันหนึ่งเครื่องหรือมากกว่า) เป็นเงินรวมกันไม่น้อยกว่า 5,000 เหรียญสหรัฐ

---

[22] ประมาทโดยรู้ตัว (Recklessness) เป็นสภาวะทางจิตอย่างหนึ่งที่ผู้กระทำไม่เพียงแต่ขาดความระมัดระวังเท่านั้น แต่ได้กระทำไปโดยเฉยเมยไม่นำพาต่อเหตุการณ์ที่จะเกิดขึ้น กล่าวคือได้กระทำโดยรู้สึกอยู่แล้วว่าเป็นการเสี่ยงที่จะเกิดภัย แต่ยังขืนทำลง บางครั้งจึงมีผู้เรียกลักษณะของสภาวะแห่งจิตเช่นนี้ว่า ประมาทโดยจงใจ (advertent negligence) คือจงใจทำแต่ไม่แน่ว่าจะเกิดผล บางทีก็เรียกว่าเป็น willfull negligence ซึ่งเรื่องนี้ศาลเคยวินิจฉัยไว้ในคดี R.V.Bateman (1925) ว่า ประมาทประเภทนี้ต้องถึงขนาดที่ลูกขุนเห็นว่าจะเพียงแต่ให้ใช้ค่าเสียหายกันยังไม่พอ เพราะเป็นความไม่นำพาต่อความปลอดภัยของผู้อื่นอันควรต้องรับผิดในทางอาญา

(ii) การแก้ไขเปลี่ยนแปลงหรือการทำให้เกิดความเสียหายต่อผลทดสอบทางการแพทย์ คำวินิจฉัยทางการแพทย์ การรักษาพยาบาลหรืออนามัยของบุคคลหนึ่งหรือมากกว่านั้น

(iii) การทำให้ผู้ใดได้รับบาดเจ็บทางร่างกาย

(iv) การข่มขู่ว่าจะทำให้เกิดอันตรายต่อสุขภาพและอนามัยของสาธารณะ หรือ

(v) ความเสียหายซึ่งส่งผลกระทบต่อระบบคอมพิวเตอร์ซึ่งถูกใช้โดยหรือสำหรับหน่วยงานของรัฐในการบริหารงานยุติธรรม การทหาร หรือความมั่นคงของชาติ[23]

จะต้องถูกลงโทษตามอนุมาตรา (c) ของมาตรานี้

---

[23] (5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

ความผิดฐานเข้าถึงและทำให้เกิดความเสียหาย ตามมาตรา 1030 (a) (5) (A) (ii) และ มาตรา 1030 (a) (5) (A) (iii) นั้น องค์ประกอบเกือบทั้งหมดไม่แตกต่างกัน โดยทั้ง (ii) และ (iii) นั้นมีองค์ประกอบแตกต่างกันในเพียงขั้นของเจตนา ผู้เขียนจึงขอแยกองค์ประกอบรวมได้ ดังนี้

1. เจตนาเข้าถึงคอมพิวเตอร์ที่ได้รับการป้องกันโดยปราศจากอำนาจ
2. ทำให้เกิดความเสียหาย (1030 (a) (5) (A) (iii)) หรือ ประมาทโดยรู้ตัวเป็นเหตุให้เกิดความ เสียหาย (1030 (a) (5) (A) (ii))
3. ทำให้เกิด
    3.1 เสียหายไม่น้อยกว่า 5,000 เหรียญสหรัฐ ภายในหนึ่งปี หรือ
    3.2 แก้ไขเปลี่ยนแปลงต่อผลทางการแพทย์ หรือ
    3.3 ได้รับบาดเจ็บทางร่างกาย
    3.4 ข่มขู่ที่จะทำให้เกิดอันตรายต่อสุขภาพและอนามัยของสาธารณะ หรือ
    3.5 ความเสียหายซึ่งส่งผลกระทบต่อระบบคอมพิวเตอร์ซึ่งถูกใช้โดยหรือสำหรับหน่วยงานของรัฐในการบริหารงานยุติธรรม การทหาร หรือความมั่นคงของชาติ

ผู้กระทำความผิดตามมาตรา1030 (a) (5) (A) (ii) มีโทษปรับ หรือโทษจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (a)(4)(B)[24] และในกรณีที่กระทำความผิดในมาตรา 1030 มาก่อนก็จะถูกลงโทษปรับ หรือโทษจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(4)(C) และผู้กระทำความผิดตามมาตรา1030 (a) (5) (A) (iii) มีโทษปรับหรือโทษจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(2)(A)[25] และในกรณีที่

---

[24] The punishment for an offense under subsection (a) or (b) of this section is—(4)(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection

[25] The punishment for an offense under subsection (a) or (b) of this section is-- (2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after

กระทำความผิดในมาตรา 1030 มาก่อนก็จะถูกลงโทษปรับ หรือโทษจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ตามมาตรา 1030 (c)(3)(B)[26]

จะเห็นได้ว่าบทบัญญัติของกฎหมายของประเทศสหรัฐอเมริกาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมีรายละเอียดเป็นจำนวนมากตามลักษณะของการออกกฎหมายของประเทศคอมมอนลอว์ ประกอบกับจุดมุ่งหมายในการออกกฎหมายเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ในเริ่มแรกนั้นไม่มีจุดประสงค์จะคุ้มครองระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยทั่วไปแต่อย่างใด แต่มีจุดประสงค์เพื่อที่จะคุ้มครองคอมพิวเตอร์ของรัฐบาลหรือหน่วยงานของรัฐบาลรวมถึงสถาบันการเงินเท่านั้น ไม่ได้ครอบคลุมไปถึงคอมพิวเตอร์ของเอกชน แต่ในภายหลังได้มีการขยายขอบเขตความคุ้มครองไปถึงเอกชนด้วย

เมื่อพิจารณาบทบัญญัติของประเทศสหรัฐอเมริกาแล้ว จะเห็นได้ว่าบทบัญญัติของ CFAA 18 U.S.C. มาตรา 1030 มีรายละเอียดมากซึ่งยากที่จะทำความเข้าใจว่ากฎหมายมีขอบเขตเพียงใด ดังนั้นเพื่อที่จะสามารถเข้าใจได้โดยง่าย จึงอาจทำเป็นตารางเพื่อแยกพิจารณาได้ดังนี้

CFAA 18 U.S.C. มาตรา 1030 อาจมองในภาพรวมได้ ดังนี้[27]

(a)	การกระทำที่เป็นความผิดตามกฎหมาย
(1)	เข้าถึงโดยปราศจากอำนาจหรือเกินขอบอำนาจ และเอาไปซึ่งข้อมูลที่เป็นความลับ

---

a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph

[26] The punishment for an offense under subsection (a) or (b) of this section is—(3)(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph

[27] James T. Tsai, “The Misery of Mitra : Considering Criminal Punishment for Computer Crime,” [Online] Available from : http://law.bepress.com/expresso/eps/853 [วันที่ 20 มกราคม 2551]

(2)	เข้าถึงข้อมูลของสถาบันการเงิน ตัวแทนรัฐบาล หรือการติดต่อสื่อสารระหว่างมลรัฐหรือระหว่างประเทศ โดยปราศจากอำนาจหรือเกินขอบอำนาจ
(3)	เข้าถึงคอมพิวเตอร์ของรัฐบาล
(4)	เข้าถึงโดยปราศจากอำนาจหรือเกินขอบอำนาจเพื่อจะทำการฉ้อโกง
(5)	(i) ส่งโปรแกรมมุ่งร้ายเพื่อสร้างความเสียหาย (ii) เข้าถึงโดยเจตนาหรือประมาทโดยรู้ตัวทำให้เกิดความเสียหาย (iii) เข้าถึงโดยเจตนาและก่อให้เกิดความเสียหาย
(6)	การฉ้อโกง ค้าขายโดยผิดกฎหมาย
(7)	การข่มขู่
(b)	การพยายามกระทำความผิดตาม (a)
(c)	การลงโทษ

นอกจากนี้ การลงโทษอาจจะแยกออกได้ ดังนี้[28]

(c)	การลงโทษ (รวมทั้งความผิดสำเร็จและพยายาม)
(1)	ความผิดตาม (a) (1)
(A)	ปรับหรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ในการกระทำผิดครั้งแรก
(B)	ปรับหรือจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ ในกรณีที่ทำความผิดตามมาตรานี้ซ้ำ
(2)	(a) (2), (a) (3), (a) (5) (A) (iii) หรือ (a) (6)
(A)	ปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ ในการกระทำผิดครั้งแรก
(B)	กรณีความผิดตาม (a) (2) ปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ สำหรับความผิดตาม (i) การกระทำผิดเพื่อผลประโยชน์ด้านการค้าหรือการเงิน (ii) เพื่อกระทำความผิดอาญาอื่นหรือทำละเมิด (iii) ถ้าข้อมูลนั้นมีมูลค่าเกิน 5.000 ดอลลาร์สหรัฐ
(C)	กรณีตาม (a) (2), (a) (3) หรือ (a) (6) ปรับหรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ในกรณีที่ทำความผิดตามมาตรานี้ซ้ำ
(3)	(a) (4), (a) (7), (a) (5) (A) (iii)

[28] เรื่องเดียวกัน,

(A)	กรณีความผิดตาม (a) (4), (a) (7) ปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ ในการกระทำผิดครั้งแรก
(B)	ปรับหรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ ในกรณีที่ทำความผิดตามมาตรานี้ซ้ำ
(4)	(a) (5) (A) (i), (a) (5) (A) (ii) (ยกเว้นกรณีที่เข้ากรณีย่อหน้า (5))
(A)	(a) (5) (A) (i) ปรับหรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ
(B)	(a) (5) (A) (ii) ปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ
(C)	ปรับหรือจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ ในกรณีที่ทำความผิดตามมาตรานี้ซ้ำ
(5)	(a) (5) (A) (i)
(A)	โดยรู้หรือประมาทโดยรู้ตัวเป็นเหตุให้เกิดอันตรายแก่กาย ปรับหรือจำคุกไม่เกิน 20 ปี หรือทั้งจำทั้งปรับ
(B)	โดยรู้หรือประมาทโดยรู้ตัวเป็นเหตุให้บุคคลถึงแก่ความตาย ปรับหรือจำคุกตลอดชีวิต หรือทั้งจำทั้งปรับ

เมื่อพิจารณาจากตารางการแยกลักษณะของแต่ละอนุมาตราในมาตรา 1030 และบทลงโทษ แล้วจะเห็นได้ว่า โดยหลักแล้ว การกระทำความผิดตามมาตราดังกล่าวเป็นเรื่องการเข้าถึงโดยปราศจากอำนาจหรือเกินขอบอำนาจและมีการแยกลักษณะการกระทำผิดไว้ในหลายกรณี อาจสรุปรวมทั้งความผิดและโทษของบทบัญญัติตาม มาตรา 1030 ได้ดังนี้

ฐานความผิดและบทกำหนดโทษ

ฐานความผิด	มาตรา	บทลงโทษอย่างสูง (กรณีจำคุก)
เอาไปซึ่งข้อมูลเกี่ยวกับความมั่นคงของประเทศสหรัฐอเมริกา	(a) (1)	10 ปี (*20 ปี)
เอาไปซึ่งข้อมูลที่เป็นความลับ	(a) (2)	1 ปี หรือ 5 ปี
บุกรุกเข้าไปในคอมพิวเตอร์ของรัฐ	(a) (3)	1 ปี (*10 ปี)
เข้าถึงคอมพิวเตอร์เพื่อฉ้อโกงหรือเอาสิ่งที่มีราคา	(a) (4)	5 ปี (*10 ปี)

ส่งโปรแกรมมุ่งร้ายโดยรู้	(a) (5) (A) (i)	10 ปี (*20 ปี หรือตลอดชีวิต)
เข้าถึงโดยเจตนาหรือประมาทโดยรู้ตัวทำให้เกิดความเสียหาย	(a) (5) (A) (ii)	5 ปี (*20 ปี)
เข้าถึงโดยเจตนาและก่อให้เกิดความเสียหาย	(a) (5) (A) (iii)	1 ปี (*10 ปี)
การซื้อขายรหัสผ่าน	(a) (6)	1 ปี (*10 ปี)
ข่มขู่ที่จะทำอันตรายคอมพิวเตอร์	(a) (7)	5 ปี (*10 ปี)

* โทษจำคุกสูงสุดสำหรับกรณีการกระทำผิดตามมาตรานี้ซ้ำอีก

จากตัวบทและการแยกลักษณะของอนุมาตราดังกล่าวข้างต้น ผู้เขียนจะสรุปว่าการกระทำความผิดเนื่องจากการเข้าถึงโดยปราศจากอำนาจหรือเกินขอบอำนาจที่เป็นองค์ประกอบความผิดในของมาตรา 1030 ในอนุมาตราต่างๆ มีดังนี้

การเข้าถึงโดยปราศจากอำนาจที่เป็นองค์ประกอบความผิดในมาตรา 1030 สรุปได้ดังนี้[29]

มาตรา 1030	โดยปราศจากอำนาจ	เกินขอบอำนาจ	ไม่มีองค์ประกอบดังกล่าว
(a) (1) เอาไปซึ่งข้อมูลเกี่ยวกับความมั่นคงของประเทศสหรัฐอเมริกา	/	/	
(a) (2) เอาไปซึ่งข้อมูลที่เป็นความลับ	/	/	
(a) (3) บุกรุกเข้าไปในคอมพิวเตอร์ของรัฐ	/		
(a) (4) เข้าถึงคอมพิวเตอร์เพื่อฉ้อโกงหรือเอาสิ่งที่มีราคา	/	/	
(a) (5) (A) (i) ส่งโปรแกรมมุ่งร้ายโดยรู้			/
(a) (5) (A) (ii) เข้าถึงโดยเจตนาหรือประมาทโดยรู้ตัว	/		

[29] United States Department of Justice, "Prosecuting Computer Crimes : Computer Fraud and Abuse Act" [Online]

ทำให้เกิดความเสียหาย			
(a) (5) (A) (iii) เข้าถึงโดยเจตนาและก่อให้เกิดความเสียหาย	/		
(a) (6) การซื้อขายรหัสผ่าน			/
(a) (7) ข่มขู่ที่จะทำอันตรายคอมพิวเตอร์			/

ตามองค์ประกอบข้างต้นจะเห็นได้ว่า ในประเทศสหรัฐอเมริกาตาม CFAA มาตรา 1030 มีการกำหนดความผิดในการเข้าถึงโดยปราศจากอำนาจไว้มีความหลากหลาย โดยผู้เขียนมีข้อสังเกต ดังนี้

จากบทบัญญัติของกฎหมาย CFAA มาตรา 1030 อาจจะสรุปได้ว่า

1. การเข้าถึงโดยปราศจากอำนาจที่จะเป็นความผิดตาม CFAA มาตรา 1030 สามารถเกิดขึ้นได้ไม่ต้องคำนึงถึงว่าจะเป็นคอมพิวเตอร์ที่มีการป้องกันหรือไม่ โดยจะเห็นได้ว่าหากเป็นสิ่งสำคัญที่กฎหมายมุ่งคุ้มครองเป็นหลักโดยเฉพาะข้อมูลของรัฐหรือสถาบันการเงินแม้ไม่เป็นคอมพิวเตอร์ที่มีการป้องกันถ้าเข้าไปโดยปราศจากอำนาจก็เป็นความผิด ดังปรากฏอยู่ในมาตรา 1030 (a) (1) (2) (3) และในขณะเดียวกันสำหรับการเข้าถึงคอมพิวเตอร์ที่มีการป้องกันก็เป็นความผิด ตาม มาตรา 1030 (a) (4) มาตรา 1030 (a) (5) (A) (ii) และมาตรา 1030 (a) (5) (A) (iii) ด้วยเช่นกัน

แต่อย่างไรก็ตามคำว่าคอมพิวเตอร์ที่มีการป้องกันในความหมายของประเทศสหรัฐอเมริกานั้นมีความแตกต่างจากคำว่าระบบคอมพิวเตอร์ที่มีการป้องกันการเข้าถึงโดยเฉพาะของไทย เนื่องจากคำว่าคอมพิวเตอร์ที่มีการป้องกันหมายถึงคอมพิวเตอร์ที่ (1) ใช้โดยเฉพาะในสถาบันการเงินหรือรัฐบาลของสหรัฐอเมริกา หรือในกรณีที่คอมพิวเตอร์ไม่ได้ใช้ในกรณีดังกล่าวถูกใช้หรือสำหรับสถาบันการเงินหรือรัฐบาลของสหรัฐอเมริกา และมีผลเป็นความผิดในการใช้หรือสำหรับสถาบันการเงินหรือรัฐบาลของสหรัฐอเมริกา (2) ซึ่งถูกใช้ในการค้าพาณิชย์หรือติดต่อสื่อสารระหว่างมลรัฐหรือระหว่างประเทศ รวมถึงคอมพิวเตอร์ที่ตั้งอยู่นอกประเทศสหรัฐอเมริกาซึ่งถูกใช้จัดการในการค้าพาณิชย์หรือติดต่อสื่อสารระหว่างมลรัฐหรือระหว่างประเทศของสหรัฐอเมริกา ไม่ได้หมายความถึงระบบคอมพิวเตอร์ที่มีระบบป้องกันการเข้าถึงแต่อย่างใด

2. การเข้าถึงโดยปราศจากอำนาจโดยปกติแล้วไม่เป็นความผิดทางอาญา โดยเฉพาะเมื่อพิจารณาจาก CFAA มาตรา 1030 จะต้องมีองค์ประกอบอื่นนอกเหนือจากการ

เข้าไปโดยปราศจากอำนาจด้วยจึงจะเป็นความผิด เช่น ตามอนุมาตรา (a) (1) เป็นการเข้าไปโดยปราศจากอำนาจเพื่อเอาไปซึ่งข้อมูลเกี่ยวกับความมั่นคงของประเทศสหรัฐอเมริกา หรือแม้ในอนุมาตรา (a) (3) ที่เป็นการบุกรุกเข้าไปในคอมพิวเตอร์ของรัฐแม้จะไม่มีองค์ประกอบอื่นหากแต่การกระทำดังกล่าวก็ต้องส่งผลกระทบต่อสหรัฐอเมริกาจึงจะเป็นความผิดตามกฎหมายนี้

3. การคุ้มครองการเข้าถึงโดยปราศจากอำนาจของประเทศสหรัฐอเมริกาตาม CFAA มาตรา 1030 นั้นไม่มีลักษณะเป็นการคุ้มครองโดยทั่วไป หากแต่มีรายละเอียดเฉพาะเจาะจงว่าเป็นการคุ้มครองเพื่อจุดประสงค์ใด เช่น คอมพิวเตอร์หรือข้อมูลของรัฐ สถาบันการเงิน

4. โดยหลักแล้ว CFAA มาตรา 1030 จะคุ้มครองคอมพิวเตอร์หรือข้อมูลของรัฐเป็นหลัก เนื่องจากเริ่มแรก CFAA มาตรา 1030 บัญญัติขึ้นเพื่อคุ้มครองรัฐ แต่ต่อมาได้มีการขยายขอบเขตไปยังคอมพิวเตอร์ของเอกชนในการแก้ไขเพิ่มเติมกฎหมายในภายหลัง

5. จากบทบัญญัติของมาตรา 1030 (g) แม้กฎหมาย FCAA นี้จะเป็นกฎหมายอาญาเกี่ยวกับการกระทำผิดทางด้านคอมพิวเตอร์ แต่จากการแก้ไขกฎหมายเพิ่มเติมสหรัฐอเมริกาได้เพิ่มเติมหลักเกณฑ์ทางกฎหมายโดยเปิดช่องให้ผู้เสียหายสามารถฟ้องร้องทางแพ่งได้ด้วย

6. นอกเหนือจากความผิดที่เกี่ยวข้องกับการเข้าถึงคอมพิวเตอร์โดยตรงแล้ว ยังมีความผิดที่เกี่ยวข้องคือ ความผิดในการซื้อขายรหัสผ่านเพื่อฉ้อโกง ซึ่งแม้ไม่ใช่ความผิดโดยตรงหากแต่ก็เป็นความผิดที่สนับสนุนการกระทำผิดในการเข้าถึงโดยปราศจากอำนาจ

7. การให้คำนิยามทางกฎหมายนั้น CFAA มาตรา 1030 (e) ได้มีการให้คำนิยามคำว่า คอมพิวเตอร์ คอมพิวเตอร์ที่ถูกป้องกัน การเข้าถึงเกินขอบอำนาจ แต่ไม่มีคำนิยามว่าการเข้าถึงโดยปราศจากอำนาจหมายถึงอะไร

การพยายามกระทำความผิด

การพยายามกระทำความผิดตาม CFAA มาตรา 1030 นั้นเป็นความผิดโดยกำหนดไว้ให้เป็นความผิดตาม CFAA มาตรา 1030 (b) ว่า ผู้ใดพยายามกระทำความผิดตามอนุมาตรา (a) ของมาตรานี้จะต้องถูกลงโทษ ดังนั้นแม้เป็นการพยายามกระทำความผิดก็ต้องรับโทษด้วยเช่นกัน

การกำหนดโทษ

ในการกำหนดโทษของผู้กระทำผิดตาม CFAA มาตรา 1030 (a) และ มาตรา 1030 (b) นั้น ได้กำหนดไว้ใน CFAA มาตรา 1030 (c) โดยมีความหนักเบาของโทษแตกต่างกัน โดยโทษต่ำสุดคือจำคุกไม่เกิน 1 ปี เช่นในมาตรา 1030 (a) (2) หรือ มาตรา 1030 (a) (3) และโทษสูงสุดคือจำคุกตลอดชีวิต (กรณีที่ทำให้ผู้อื่นถึงแก่ความตาย)

ในส่วนของการเพิ่มโทษให้ผู้กระทำผิดรับโทษหนักขึ้นนี้ได้มีการแก้ไขจากบทบัญญัติเดิม เนื่องจากเดิมกฎหมายเขียนว่าต้องกระทำผิดในอนุมาตราเดียวกันจึงจะเพิ่มโทษที่จะลงได้ ดังนั้นหากทำผิดต่างอนุมาตราก็ไม่ต้องรับโทษที่เพิ่มขึ้นตามกฎหมาย แต่ในกฎหมายที่แก้ไขใหม่กำหนดถ้อยคำให้ครอบคลุมขึ้นว่า ในกรณีที่เป็นผู้กระทำผิดซ้ำซากโดยเคยกระทำผิดใน CFAA มาตรา 1030 มาก่อนแล้ว ก็ต้องรับโทษที่เพิ่มขึ้นตามกฎหมายบัญญัติ ดังนั้น ผู้กระทำผิดที่เคยกระทำผิดตามมาตรา 1030 มาแล้วและมากระทำผิดอีก แม้จะไม่ได้อยู่ในอนุมาตราเดียวกันก็ถือว่าเป็นผู้กระทำผิดซ้ำและต้องรับโทษเพิ่มขึ้นตามที่กำหนดไว้ในกฎหมายตาม CFAA มาตรา 1030 (c)

นอกจากนี้สำหรับความผิดฐานพยายามกระทำผิดตามมาตรา 1030 (a) ใน มาตรา 1030 (c) ได้กำหนดว่าผู้พยายามกระทำผิดตามมาตรา 1030 (a) นั้นต้องรับโทษเท่ากับความผิดสำเร็จ โดยได้กำหนดไว้ในกฎหมายโดยตรง

แนวความคิดเกี่ยวกับความรับผิดทางกฎหมายในการเข้าถึงโดยปราศจากอำนาจของประเทศสหรัฐอเมริกา

เมื่อพิจารณาถึงการออกกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศสหรัฐอเมริกาแล้ว ทั้งรัฐบาลกลางและมลรัฐต่างๆ ต่างออกกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์เกี่ยวกับการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ (Unauthorized access) เป็นของตนทุกรัฐ แม้กฎหมายของรัฐบาลกลางและกฎหมายของมลรัฐไม่เหมือนกันทั้งหมด หากแต่ทั้งหมดมีจุดร่วมกันในการกระทำความผิดที่เริ่มจาก “การเข้าถึงโดยปราศจากอำนาจ” และในบางกรณีรวมถึง “การเข้าถึงเกินขอบอำนาจ” ด้วย โดยเกือบทั้งหมดกฎหมายจะเริ่มที่การห้ามการเข้าถึงโดยปราศจากอำนาจหรือเกินขอบอำนาจ และจึงสร้างฐานความผิดที่หลากหลายขึ้นโดยเพิ่มเติมหลักเกณฑ์ตามที่กฎหมายต้องการ

ดังนั้นการที่จะเข้าใจถึงบทบัญญัติที่เกี่ยวกับความผิดในการเข้าถึงโดยปราศจากอำนาจของประเทศสหรัฐอเมริกาได้ คงต้องเริ่มที่ความหมายของคำว่า “เข้าถึง” คอมพิวเตอร์และภายใต้สถานการณ์ใดที่การเข้าถึงนั้นเป็นการเข้าถึง “โดยปราศจากอำนาจ” โดยมีขอบเขต

เพียงใดที่กฎหมายต้องการคุ้มครองอย่างแท้จริง แม้แต่ศาลในประเทศสหรัฐอเมริกาก็มีความไม่ลงรอยกันในการตีความครอบคลุมถึงความหมายดังกล่าว เนื่องจากทั้งคำว่า “เข้าถึง” และ “โดยปราศจากอำนาจ” สามารถที่จะให้ความหมายที่แคบและกว้างได้แล้วแต่การพิจารณา

โดยตัวอย่างในคดีเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจในอดีตนั้นมีเพียงเล็กน้อย มีเพียงไม่กี่คดีที่มีการตีความคำว่า “เข้าถึง” และมีคดีไม่มากนักที่มีการตีความคำว่า “โดยปราศจากอำนาจ” แต่อย่างไรก็ตามก็เป็นการสะท้อนแนวคิดเกี่ยวกับการตีความดังกล่าว โดยมีคำพิพากษาเพียงเล็กน้อยที่ตีความความหมายของคำว่าเข้าถึงคอมพิวเตอร์หรือการเข้าถึงโดยปราศจากอำนาจไว้ สิ่งที่คล้ายคลึงกับการตีความคำว่า “เข้าถึง” เกิดขึ้นในคดีของศาลสูงแคนซัสในปี 1996 ในคดี State v. Allen โดย Allen ได้ใช้คอมพิวเตอร์ของเขาในการทำซ้ำเพื่อทำให้คอมพิวเตอร์ของบริษัท Southwestern Bell Telephone ที่ควบคุมการเปิด-ปิดการโทรศัพท์ทางไกลทำให้ผู้ใช้โทรศัพท์ทางไกลฟรี โดย Allen ต่อสู้ว่าไม่มีหลักฐานว่าตนได้เข้าไปยังคอมพิวเตอร์ของบริษัท Bell จริงๆ ศาลเห็นว่าการตีความคำว่า “เข้าถึง” อย่างกว้างขวางตามที่กฎหมายบัญญัติ[30]จะทำให้การกระทำทางกายภาพที่ไม่ได้รับอนุญาตทั้งหมดเป็นความผิดทางอาญา ซึ่งไม่ถูกต้องและเห็นว่าควรใช้ความหมายพื้นฐานตามปกติ

ดังนั้นความหมายของคำว่าเข้าถึงจึงความเป็นความหมายคล้ายคลึงกับความหมายทางกายภาพโดยหมายถึงการใส่ชื่อผู้ใช้และรหัสผ่านที่ถูกต้องและทำให้ผู้ใช้ได้เข้าไปใน (inside) เครื่องคอมพิวเตอร์อย่างแท้จริง และเมื่อขาดพยานหลักฐานว่า Allen ได้เข้าไปในเครื่องคอมพิวเตอร์อย่างแท้จริงเพื่อหาข้อมูลข้างใน ดังนั้นเขาจึงไม่ได้เข้าถึงคอมพิวเตอร์ของบริษัท Bell

ศาลของรัฐบาลกลางได้ตัดสินคล้ายคลึงกันในคดี Moulton v. VC3 ซึ่งเป็นคดีแพ่งระหว่างบริษัทรักษาความปลอดภัยของคอมพิวเตอร์ โดยคดีเกิดขึ้นในปี 1994 บริษัทแรกฟ้องบริษัทที่สองเมื่อลูกจ้างของบริษัทที่สองได้ทำ port scan[31] คอมพิวเตอร์ของบริษัทแรก โดย

---

[30] 21-3755. Computer crime; computer password disclosure; computer trespass. "Access" means to instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system or computer network.

[31] port scan คือ การทดสอบคอมพิวเตอร์เป้าหมาย โดย port คือประตูอิเล็กทรอนิกส์ชนิดหนึ่ง และ port ที่เปิดอยู่ก็เหมือนกับประตูที่เปิดอยู่และพร้อมที่จะรับข้อมูล

ศาลได้ตัดสินว่าการ scan port ของบริษัทที่สองไม่ใช่การเข้าถึงคอมพิวเตอร์ของบริษัทแรก เนื่องจากไม่มีการเข้าไป (inside) เกิดขึ้น

ขณะที่ทั้งคดีของ State v. Allen และคดี Moulton v. VC3 ได้มองว่าการเข้าถึงคอมพิวเตอร์มีขีดจำกัด โดยต้องมีการเข้าไปในคอมพิวเตอร์จึงจะถือว่าเป็นการเข้าถึง แต่ก็มีคดีที่ตัดสินแตกต่างออกไปโดยให้คำนิยามของคำว่า “เข้าถึง” ที่กว้างขวางกว่า

ในคดีของศาลสูงวอชิงตัน State v. Riley นั้น ข้อเท็จจริงของคดีคล้ายคลึงกับคดี State v. Allen โดย Riley ได้ใช้คอมพิวเตอร์ของเขาในการทำซ้ำเพื่อหมุนคอมพิวเตอร์ของบริษัท Northwest Telco และเดารหัสผ่านทำให้ผู้ใช้ใช้โทรศัพท์ทางไกลฟรี โดย Riley ได้ต่อสู้ว่าเขาไม่ได้เข้าไปในคอมพิวเตอร์ของบริษัทดังกล่าว แต่ศาลวอชิงตันได้อธิบายคำว่า “เข้าถึง” แตกต่างจากาศาลแคนซัสในคดี Allen โดยศาลวอชิงตันได้ถือเอาคำนิยามของคำว่า “เข้าถึง” อย่างกว้าง ซึ่งรวมถึงการสื่อสารกับคอมพิวเตอร์ด้วย และตัดสินว่าการกระทำของ Riley เป็นการเข้าถึงคอมพิวเตอร์แล้ว

คำนิยามของคำว่า “เข้าถึง” ได้ขยายกว้างขึ้นในคดีแพ่ง ระหว่าง America Online v. National Health Care Discount, Inc. (NHCD) ซึ่งเป็นคดีหนึ่งในจำนวนหลายคดีที่ฟ้องโดย AOL ต่อผู้ส่งสแปมเมล์[32] โดย AOL ฟ้อง NHCD (บริษัทขายสมุนไพรเพื่อสุขภาพ) ในการส่งแสปมเมล์โดยส่งไปยังผู้ใช้บัญชีของ AOL โดย AOL บอกว่า การส่งอีเมล์เป็นการฝ่าฝืนข้อกำหนดในการใช้บริการของ AOL ผู้ส่งแสปมเข้าถึงคอมพิวเตอร์ของ AOL เป็น

เมื่อมีการ scan แล้ว port ที่เปิดอยู่ก็จะส่งข้อความกลับมาว่าเปิดอยู่ ในขณะที่ port ที่ปิดจะส่งข้อความว่าผิดพลาด (error) ซึ่ง port ที่เปิดเป็นช่องทางให้สามารถบุกรุกได้

[32] สแปม (spam) คือชื่อเรียกของการส่งข้อความที่ผู้รับไม่ได้ร้องขอ ผ่านทางระบบอิเล็กทรอนิกส์ โดยส่วนมากจะทำให้เกิดความไม่พอใจต่อผู้รับข้อความ สแปมที่พบเห็นได้บ่อยได้แก่ การส่งสแปมผ่านทางอีเมล์ ในการโฆษณาชวนเชื่อ หรือโฆษณาขายของ โดยการส่งอีเมล์ประเภทหนึ่งที่เราไม่ต้องการ ซึ่งจะมาจากทั่วโลก โดยที่เราไม่รู้เลยว่า ผู้ที่ส่งมาให้นั้นเป็นใคร จุดประสงค์คือ ผู้ส่งส่วนใหญ่ต้องการที่จะโฆษณา สินค้าหรือบริการต่าง ๆ ของบริษัทของตนเอง ซึ่งเป็นประเภทหนึ่งของเมลขยะซึ่งนอกจากจะทำให้ผู้รับรำคาญใจและเสียเวลาในการกำจัดข้อความเหล่านี้แล้ว (วิกิพีเดีย สารานุกรมเสรี : http://th.wikipedia.org)

การเข้าถึงโดยไม่ได้รับอนุญาต ศาลบอกว่าแม้ CFAA จะไม่ได้นิยามคำว่าเข้าถึงไว้ แต่การกระทำดังกล่าวของ NHCD เป็นการเข้าถึงแล้วแม้ว่าผู้ใช้อาจจะยังไม่ได้เป็นการเข้าถึงก็ตาม

นอกจากนิยามของคำว่า “เข้าถึง” แล้ว ศาลในประเทศสหรัฐอเมริกายังต้องเผชิญกับปัญหาในการพยายามอธิบายคำว่า “โดยปราศจากอำนาจ” ซึ่งมีคดีที่ตีความความหมายคำว่า “โดยปราศจากอำนาจ” ดังนี้

คดี United States v. Morris ซึ่งรู้จักกันในคดีการส่งหนอนไวรัสอินเทอร์เน็ตโดยถูกจับในความผิดตาม 1030 (a)(5)(A) โดยตั้งใจเข้าไปในคอมพิวเตอร์ของรัฐโดยปราศจากอำนาจทำให้เกิดความเสียหาย ลูกขุนตัดสินลงโทษ Morris อุทธรณ์ว่าการเข้าถึงคอมพิวเตอร์ของเขาไม่ได้ปราศจากอำนาจ และเขามีสิทธิที่จะเข้าถึงคอมโดยอ้างว่าตนเองมีบัญชี ศาลไม่รับอุทธรณ์

ศาลให้มาตรฐานใหม่ของการเข้าถึงโดยปราศจากอำนาจ ศาลกล่าวว่า Morris เข้าถึงคอมพิวเตอร์โยไม่มีอำนาจเพราะเขาใช้จุดอ่อนในหลายๆ โปรแกรมเพื่อให้เข้าถึงคอมพิวเตอร์ของบุคคลอื่น แม้ว่าศาลจะไม่ได้ให้รายละเอียดในมาตรฐานนี้แต่อาจสรุปได้ว่า เมื่อผู้ใช้หาประโยชน์จากจุดอ่อนในโปรแกรมและใช้ทางที่ไม่ได้ตั้งใจให้เป็นทางเข้าถึงเป็นทางเข้าถึงคอมพิวเตอร์นั้น จึงเป็นการเข้าถึงโดยปราศจากอำนาจ

ส่วนในคดี Shurgard Storage Center Inc. v. Safeguard Self Storage, Inc., ก็ตัดสินเช่นเดียวกัน โดยตามคำฟ้อง จำเลยได้รับความลับทางธุรกิจและการค้าจากลูกจ้างของบริษัทโจทก์โดย Eric Leland ได้ส่งจดหมายอิเล็กโทรนิกส์เกี่ยวกับความลับทางการค้าของโจทก์ไปยังจำเลย โจทก์ฟ้องว่าจำเลยกระทำความผิดตามมาตรา 1030(a)(2)(C) บนทฤษฎีที่ว่า Leland ได้เข้าถึงคอมพิวเตอร์ของโจทก์โดยเจตนาและโดยปราศจากอำนาจหรือเกินขอบอำนาจและได้รับข้อมูลของโจทก์ไปโดยฝ่าฝืนต่อกฎหมาย จำเลยให้การปฏิเสธ

ศาลยอมรับทฤษฎีของโจทก์โดยศาลเห็นว่าลูกจ้างของโจทก์สูญเสียอำนาจและปราศจากอำนาจเมื่อเขาได้เข้าไปเอาและส่งข้อมูลให้กับจำเลยผ่านทางจดหมายอิเล็กโทรนิกส์

การกล่าวอ้างทฤษฎีนี้ค่อนข้างกว้าง โดยภายใต้ทฤษฎีนี้เมื่อไหร่ก็ตามที่ลูกจ้างใช้คอมพิวเตอร์อย่างเป็นปฏิปักษ์กับประโยชน์ของนายจ้าง ลูกจ้างไม่ได้อยู่ในฐานะตัวแทนของนายจ้างและการเข้าถึงคอมพิวเตอร์ของนายจ้างจึงเป็นความผิด ทำให้พฤติกรรมจะเป็นตัวกำหนดว่าเมื่อใดที่การเข้าถึงนั้นมีอำนาจหรือปราศจากอำนาจ

อย่างไรก็ตามศาลยอมรับความหมายของการเข้าถึงโดยปราศจากอำนาจของลูกจ้างในขอบเขตที่แคบกว่าในคดี United States v. Czubinski, โดยลูกจ้างส่งข้อมูลของนายจ้างไปยังเพื่อนหรือคู่แข่งทางการค้าของนายจ้าง ซึ่งการเข้าถึงนั้นปราศจากอำนาจโดยขึ้นอยู่กับกฎของที่ทำงานว่าลูกจ้างสามารถเข้าถึงข้อมูลได้เพียงเท่าที่เกี่ยวข้องกับงาน ดังนั้นศาลจึงมองว่าเป็นการเข้าถึงโดยปราศจากอำนาจ ซึ่งกรณีนี้นายจ้างมีสิทธิจำกัดสิทธิของลูกจ้างในการใช้คอมพิวเตอร์ของบริษัท ซึ่งนายจ้างอนุญาตให้เข้าถึงเพียงเพื่อการทำงานเท่านั้น

ศาล Georgia ใช้หลักเกณฑ์เดียวกันในคดี Fugarino v. State, โดยนาย Fugarino ถูกกล่าวหาว่าใช้คอมพิวเตอร์โดยรู้และไม่มีอำนาจและตั้งใจที่จะทำอันตรายต่อข้อมูล นาย Fugarino มีอาชีพเป็นโปรแกรมเมอร์ของบริษัทแล้วมีพฤติกรรมในที่ทำงานที่แปลกประหลาด เมื่อนาย Fugarino รู้ว่าลูกจ้างคนอื่นถูกไล่ออกจากบริษัทก็โมโหและกล่าวว่าจะไม่มีใครมาแทนตำแหน่งเค้าได้ จากนั้นนาย Fugarino ก็เริ่มลบฟังก์ชั่นการทำงานของโปรแกรมจากเครือข่ายคอมพิวเตอร์ของนายจ้าง และเมื่อนายจ้างเผชิญหน้ากับเขาให้ทำให้คอมพิวเตอร์สามารถใช้งานได้ดังเดิม แต่นาย Fugarino ปฏิเสธ

นาย Fugarino อุทธรณ์ว่าการกระทำของเขาไม่ใช่การกระทำที่ปราศจากอำนาจ ศาล Georgia ตัดสินว่านาย Fugarino กระทำไปโดนปราศจากอำนาจเพราะว่าเจ้าของบริษัทไม่ได้ให้อำนาจนาย Fugarino ในการลบโปรแกรมส่วนใดส่วนหนึ่งของบริษัทได้

จะเห็นได้ว่าแม้ว่านาย Fugarino จะเป็นโปรแกรมเมอร์ของบริษัทโดยปกติแล้วสามารถแก้ไขเปลี่ยนแปลงข้อมูลที่เกี่ยวข้องกับการทำงานของตนได้ แต่เมื่อการลบนั้นมีเจตนาร้ายต่อนายจ้าง นาย Fugarino จึงไม่มีอำนาจกระทำได้

ในคดีของ State v. Olson นั้นตรงกันข้ามโดยนาย Olson ได้ใช้ข้อมูลคอมพิวเตอร์ของตำรวจเข้าไปเพื่อหารายละเอียดเกี่ยวกับใบอนุญาตขับรถยนต์ของนักศึกษาหญิงคนหนึ่ง นาย Olson ถูกฟ้องว่าเข้าถึงคอมพิวเตอร์ของรัฐโดยปราศจากอำนาจ โดยนาย Olson ต่อสู้ว่าตนเองมีอำนาจในการเข้าถึงได้

ศาลเห็นว่าการเข้าถึงโดยเหตุผลส่วนตัวนั้นไม่ใช่การเข้าถึงโดยปราศจากอำนาจ เพราะเป็นเพียงเหตุผลส่วนตัวและไม่ได้หาประโยชน์จากกฎของสถานที่ทำงาน

จากคดีของนาย Olson และนาย Fugarino ทำให้เห็นได้ว่านายจ้างต้องเป็นผู้จำกัดการเข้าถึง ซึ่งในคดีของนาย Olson นั้นไม่เป็นความผิดเนื่องจากไม่มีระเบียบของที่ทำงานจำกัดไว้

ในคดีของ Briggs v. State ในรัฐ Marryland ในคดีนี้ผู้ดูแลระบบคอมพิวเตอร์ผู้ซึ่งมีอำนาจควบคุมจัดการ การใส่รหัสผ่านให้กับข้อมูลต่างๆที่สำคัญ เขาได้ใช้รหัสผ่านที่นายจ้างไม่รู้และในช่วงเวลาสั้นๆ ที่ก่อนเขาจะลาออก นาย Briggs ได้เปลี่ยนรหัสผ่านของไฟล์ โดยเปลี่ยนชื่อเป็น “ha ha he he” ทำให้นายจ้างไม่สามารถเข้าถึงข้อมูลที่เข้ารหัสไว้ได้ และเมื่อนายจ้างถามถึงรหัสผ่าน นาย Briggs ก็ได้อ้างว่าลืมไปแล้ว

นาย Briggs ถูกฟ้องว่าเข้าถึงคอมพิวเตอร์ของนายจ้างโดยปราศจากอำนาจ ศาลตัดสินว่านาย Briggs ไม่มีความผิดในการเข้าถึงโดยปราศจากอำนาจ เนื่องจากในฐานะผู้ดูแลระบบแล้วนาย Briggs มีอำนาจเข้าคอมพิวเตอร์ของนายจ้างแม้ว่าจะได้ทำในสิ่งที่ไม่มีกฎอนุญาตให้ทำ นาย Briggs ก็ไม่ได้ขาดอำนาจที่จะเข้าถึงคอมพิวเตอร์ของนายจ้าง

คดีนี้ตรงข้ามกับคดี Shurgard โดยคดีของนาย Briggs นั้นการพิจารณาว่าเป็นความผิดหรือไม่อยู่บนพื้นฐานของข้อกำหนดมากกว่าพฤติกรรมของผู้กระทำ เมื่อข้อเท็จจริงปรากฏว่านาย Briggs ไม่มีจุดประสงค์ในเรื่องผลประโยชน์ของนายจ้าง ทำให้การเข้าถึงของคอมพิวเตอร์ไม่เป็นการเข้าถึงโดยปราศจากอำนาจ

หากจะพิจารณาจากบทบัญญัติของกฎหมายแล้ว คงจะต้องพิจารณาว่า ศาลจะให้ขอบเขตคำว่าโดยปราศจากอำนาจอย่างไร โดยใช้หลักเกณฑ์การที่มีอำนาจเข้าถึงตามสิทธิของตนแล้ว หากใช้สิทธิของตนเป็นปฏิปักษ์กับเจ้าของข้อมูลหรือใช้เพื่อประโยชน์ส่วนตนไม่เกี่ยวกับงานที่ทำจะทำให้การเข้าถึงนั้นเป็นการเข้าถึงโดยปราศจากอำนาจหรือไม่ ซึ่งแนวความคิดเกี่ยวกับกรณีเหล่านี้อาจจะแยกมุมมองออกเป็นสองส่วนคือ มองในแง่พฤติกรรมหรือมองในแง่ข้อกำหนด หากมองในแง่พฤติกรรมแล้ว การกระทำที่เป็นปฏิปักษ์แก่เจ้าของย่อมเป็นการไม่ชอบการใดๆ ที่ทำลงย่อมไม่มีอำนาจกระทำได้ ผู้กระทำจึงมีความผิดในการเข้าถึงโดยมิชอบโดยเทียบเคียงกับคดี Shurgard Storage Center Inc. v. Safeguard Self Storage, Inc., และคดี United States v. Czubinski

แต่หากมองว่าลูกจ้างมีอำนาจในการเข้าถึงข้อมูลที่ตนมีสิทธิการเข้าถึงนั้นย่อมเป็นการเข้าถึงโดยชอบ แม้ลูกจ้างจะก่อให้เกิดผลร้ายต่อนายจ้างก็ไม่เป็นความผิดในการเข้าถึงแต่อย่างใด โดยเทียบเคียงกับคดี DPP v Bignell หรือคดี State v. Olson[33]

จะเห็นได้ว่าในการตีความคำว่า “เข้าถึง” และคำว่า “โดยปราศจากอำนาจ” ของศาลสหรัฐอเมริกานั้นมีทั้งการตีความทั้งอย่างกว้างและอย่างแคบแล้วแต่ศาลนั้นจะพิจารณาตามแต่มุมมองซึ่งมีความแตกต่างกันไป จึงเห็นได้ว่าแม้แต่ในประเทศสหรัฐอเมริกาเองก็มีการตีความที่หลากหลายไม่เป็นหลักเกณฑ์เดียวกันแม้จะมีการใช้กฎหมายเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจมาแล้วนับสิบปี แต่อย่างไรก็ตามก็กรณีคดีต่างๆ ที่เกิดขึ้นนั้นอาจนำไปเป็นตัวอย่างที่จะพิจารณาในประเทศไทยได้ต่อไป

2.3.2.2 ประเทศอังกฤษ

การไม่มีอำนาจในการเข้าสู่ระบบคอมพิวเตอร์นั้น ในประเทศอังกฤษได้พิจารณาเปรียบเทียบกับความผิดฐานบุกรุก (Trespass) และความผิดเกี่ยวกับทรัพย์สิน (Theft) ซึ่งในเรื่องของการเจาะระบบคอมพิวเตอร์ (Hacking) ถ้าพิจารณาตามหลักกฎหมายในเรื่องบุกรุกตามกฎหมายอังกฤษเดิมนั้นไม่เป็นความผิดทางอาญาเป็นเพียงแต่ความผิดทางแพ่งเท่านั้น แต่อังกฤษได้บัญญัติกฎหมายว่าการเข้าสู่ระบบประมวลผลโดยปราศจากอำนาจเป็นความผิดทางอาญา ไม่ว่าผู้เข้าสู่ระบบประมวลผลจะเป็นพวกแฮกเกอร์หรือไม่ก็ตาม ซึ่งอาจจะเป็นลูกจ้างที่ไม่มีอำนาจเข้าไป (Without Color of Right) หรือบุคคลภายนอกก็ตาม ดังนั้นในเรื่องการกำหนดให้เป็นความผิดของการปราศจากอำนาจในการเข้าสู่ระบบประมวลคอมพิวเตอร์ (Basic Hacking Offence) นั้นตามกฎหมายอังกฤษนั้นถือว่าเป็นสิ่งผิดปกติ (Anomaly) เพราะแม้แต่การบุกรุกที่เป็นการกระทำทางกายภาพโดยเข้าไปในบ้านของบุคคลไม่เป็นความผิดทางอาญา แต่

---

[33] Orin S. Kerr, “Cybercrime's Scope: Interpreting 'Access' and Authorization' in Computer Misuse Statutes,” Public Law and Legal Theory Research Paper Series Research Paper No. 65 [Online] Available from : http://www.law.nyu.edu/journals/lawreview/issues/vol78/no5/NYU502.pdf [วันที่ 7 มกราคม 2551]

การบุกรุกเข้าไปทางอิเล็กทรอนิกส์ในการเข้าสู่ระบบประมวลผลส่วนบุคคลเป็นความผิดทางอาญา[34]

โดยประเทศอังกฤษ ได้กำหนดความผิดฐานเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ (Unauthorized Access) ไว้ใน Computer Misuse Act 1990 มาตรา 1 และมาตรา 2 ซึ่งอาจความรับผิดออกเป็น 2 ส่วน ได้ดังนี้

1. **การเข้าถึงโดยปราศจากอำนาจซึ่งสิ่งที่อยู่ในคอมพิวเตอร์** (เช่น โปรแกรม หรือข้อมูล) ตาม Computer Misuse Act 1990 (CMA) มาตรา 1 ซึ่งถูกแก้ไขเพิ่มเติมโดย Police and Justice Act 2006 (แต่จะมีผลบังคับใช้ประมาณเดือนเมษายน 2008) ดังนี้

มาตรา 1[35]

---

[34] สุเนติ คงเทพ, "การไม่มีอำนาจเข้าสู่ระบบประมวลผล (Hacking)," บทบัณฑิตย์ เล่มที่ 55 ตอน 1 (มีนาคม 2542)

[35] (1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer or to enable any such access to be secured;

(b) the access he intends to secure or to enable to be secured is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable—

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

(1) บุคคลมีความผิด ถ้า

(a) ผู้นั้นได้ทำให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ โดยความจงใจที่จะผ่านสิ่งปกป้องคุ้มครองไม่ให้เข้าสู่ระบบได้ และได้ผ่านสิ่งปกป้องหรือสามารถทำการเข้าถึงใดๆ เช่นว่านั้นเข้าไปยังโปรแกรมใดๆ หรือข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ใดๆ

(b) การผ่านสิ่งปกป้องคุ้มครองหรืออาจถูกปกป้องคุ้มครองเข้าไปสู่ระบบด้วยความจงใจนั้นเป็นการกระทำโดยปราศจากอำนาจ และ

(c) ผู้นั้นได้รู้อยู่ในเวลาที่เขาได้กระทำการอันเป็นเหตุให้คอมพิวเตอร์แสดงผล หรือแสดงการทำงานอันปราศจากอำนาจนั้น

(2) ความจงใจของบุคคลที่เขาได้กระทำความผิดภายใต้มาตรานี้ ไม่จำเป็นต้องเป็นการกระทำที่เป็น

(a) โปรแกรมพิเศษหรือเฉพาะเจาะจงใดๆ หรือข้อมูล หรือ

(b) โปรแกรมหรือข้อมูลของสิ่งเฉพาะเจาะจงใดๆ หรือ

(c) โปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ใดๆ โดยเฉพาะ

(3) บุคคลจะมีความผิดภายใต้บทบัญญัตินี้ จะต้องระวางโทษ

(a) ในการพิจารณาคดีแบบรวบรัด (Summary Conviction) ในประเทศอังกฤษและเวลล์ จำคุกไม่เกิน 12 เดือน หรือปรับ หรือทั้งจำทั้งปรับ

(b) ในการพิจารณาคดีแบบรวบรัด (Summary Conviction) ในประเทศสก็อตแลนด์ จำคุกไม่เกิน 6 เดือน หรือปรับ หรือทั้งจำทั้งปรับ

(c) หากเป็นความผิดร้ายแรงและถูกลงโทษ จำคุกไม่เกิน 2 ปี หรือปรับ หรือทั้งจำทั้งปรับ

แนวการกำหนดความรับผิดในในการเข้าถึงโดยปราศจากอำนาจ[36] ตามมาตรา 1

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

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both

[36] "Computer Misuse Act 1990" [Online] Available from : www.cr-international.com/2008_UK_CPS_Draft_Guiding_Principles_Regarding_Hacking_Tools.pdf [วันที่ 2 มกราคม 2551]

โดยพื้นฐานของมาตรานี้คือการพยายามหรือเข้าถึงคอมพิวเตอร์หรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์ โดยทำให้คอมพิวเตอร์ทำงานด้วยตั้งใจที่จะเข้าถึง โดยการพยายามเข้าถึงระบบการทำงานของคอมพิวเตอร์โดยปราศจากอำนาจนั้นผิดกฎหมายไม่ว่าจะตั้งใจทำอันตรายหรือไม่ก็ตาม ซึ่งแฮกเกอร์ต้องตระหนักว่าการพยายามเข้าถึงคือการเข้าถึงโดยปราศจากอำนาจไม่ว่าจะเป็นการใช้ชื่อหรือ ID และรหัสผ่าน โดยไม่มีอำนาจเข้าถึงคอมพิวเตอร์นั้นหรือพิมพ์หรือส่งข้อมูลนั้นไปทางอีเมล์หรือกระดานสนทนาออนไลน์หรือโดยทางอื่น และถึงแม้ว่าการเข้าถึงในตอนแรกจะมีอำนาจ แต่ต่อมาใช้สิทธิเกินกว่าส่วนที่ตนเองมีอำนาจเข้าถึงก็เป็นความผิดเช่นกัน[37]

มาตรานี้ไม่เพียงแต่เอาผิดเฉพาะแฮกเกอร์เท่านั้น แต่รวมถึงลูกจ้างที่เข้าถึงเกินขอบอำนาจและเข้าถึงส่วนที่เกินอำนาจหน้าที่ในการทำงานของตน ในคดีของ R v Bow Street Magistrates Court and Allison (AP) Ex parte Government of the United States of America (Allison) [2002]2 AC 216, เมื่อศาลตัดสินว่า ลูกจ้างมีความผิดในการเข้าถึงโดยปราศจากอำนาจ ตามมาตรา 1 CMA เพราะลูกจ้างรู้ว่าตนเองไม่มีอำนาจในการเข้าถึง และศาลวางหลักเกณฑ์ว่าลูกจ้างจะมีความผิดในการเข้าถึงต่อเมื่อนายจ้างได้กำหนดอำนาจของลูกจ้างอย่างชัดเจนในการเข้าถึงโปรแกรมหรือข้อมูล

โดยการดำเนินคดีตาม CMA ที่รวมถึงลูกจ้างนั้น ต้องพิจารณาว่าลูกจ้างเข้าถึงอย่างระมัดระวังตามสัญญาจ้างและบริบทข้างเคียง เช่น สัญญาปากเปล่าที่ให้ไว้ต่อหน้าคนอื่นหรือไม่ เพื่อที่จะตัดสินว่านายจ้างได้จำกัดการเข้าถึงของลูกจ้างไว้อย่างชัดเจน ซึ่งโดยปกติแล้วจะใช้เป็นพยานหลักฐานแสดงว่าการเข้าถึงนั้นปราศจากอำนาจหรือไม่

แต่ในขณะที่คดี DPP v Bignell [1998] 1 Cr App R8 ก่อนหน้านี้ ตำรวจสองนายใช้อำนาจเรียกข้อมูลจากสำนักงานตำรวจแห่งชาติ (the police national computer) จากผู้ปฏิบัติเพื่อจุดประสงค์ในทางสาธารณะเท่านั้น แต่นายตำรวจนั้นทำเพื่อจุดประสงค์ส่วนตัว ศาลตัดสินว่าการกระทำของตำรวจทั้งสองไม่เป็นความผิด เขามีอำนาจในการเข้าถึงข้อมูลนั้น[38]

---

[37] “Computer Misuse Act 1990” [Online] Available from : http://en.wikipedia.org/wiki/Computer_Misuse_Act_1990 [วันที่ 12 กุมภาพันธ์ 2551]

[38] Computer Misuse Act 1990 [Online] Available from : www.cr-international.com/2008_UK_CPS_Draft_Guiding_Principles_Regarding_Hacking_Tools.pdf

นอกจากนี้ยังมีคดีลักษณะคล้ายคดี DPP v Bignell แต่ตัดสินต่างกัน คือ R v Bennett อดีตผู้กำกับการตำรวจใช้คอมพิวเตอร์ของสำนักงานตำรวจแห่งชาติติดตามแฟนของอดีตภรรยา โดยจำเลยให้การรับสารภาพและถูกตัดสินว่ามีความผิดและปรับ 150 ปอนด์

2. **การเข้าถึงโดยปราศจากอำนาจ โดยเจตนาที่จะกระทำหรือให้ความสะดวกแก่การกระทำความผิดอื่น** ตาม Computer Misuse Act 1990 (CMA) มาตรา 2

มาตรา 2 เป็นมาตราที่ใช้บังคับกับกรณีที่เป็นความผิดที่ซับซ้อนขึ้น (Ulterior Hacking Offence) โดยมาตรา 2 บัญญัติว่า[39]

---

[39] 2(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent—

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences—

(a) for which the sentence is fixed by law; or

(b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the [1980 c. 43.] Magistrates' Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5) A person guilty of an offence under this section shall be liable—

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

(1) บุคคลที่มีความผิดภายใต้บทบัญญัตินี้ ถ้าหากว่าเขาได้กระทำผิดตามมาตรา 1 ด้วยเจตนา (มาตรา 1 บัญญัติว่าการไม่มีอำนาจในการเข้าสู่ระบบเป็นความผิด)

(a) ได้กระทำผิดในสิ่งที่มาตรานี้บังคับให้ หรือ

(b) ให้ความสะดวกในการกระทำผิด (ไม่ว่าโดยตนเองหรือโดยบุคคลใดๆ) และความผิดที่เขาจงใจในการกระทำผิด หรือให้ความสะดวกดังกล่าวต่อไปในมาตรานี้ให้ถือว่าเป็นผู้กระทำผิดเช่นเดียวกับผู้กระทำผิดที่ตนช่วย

(2) มาตรานี้ใช้กับความผิด

(a) ใช้กับความผิดที่ถูกกำหนดไว้ในกฎหมาย หรือ

(b) ใช้กับบุคคลผู้มีอายุ 21 ปี หรือกว่านี้

(3) เพื่อวัตถุประสงค์ของมาตรานี้ไม่ว่าการกระทำความผิดของผู้กระทำผิดที่อยู่ห่างไกล (Remote hacker) จะได้กระทำลงในโอกาสที่ไม่มีอำนาจในการเข้าสู่ระบบนั้นหรือไม่ หรือโดยอาศัยโอกาสอื่นใดก็ตาม

(4) บุคคลอาจจะมีความผิดตามมาตรานี้ถึงแม้ว่าจะมีข้อเท็จจริงว่าการกระทำความผิดของผู้กระทำความผิดที่อยู่ห่างไกลจะไม่ได้กระทำลงก็ตาม

(5) บุคคลผู้กระทำผิดตามมาตรานี้ต้องรับผิด

(a) จะพิจารณาคดีแบบรวบรัด และถูกลงโทษจำคุกไม่เกิน 6 เดือน หรือปรับ หรือทั้งจำทั้งปรับ

(b) หากเป็นความผิดร้ายแรงและถูกลงโทษ ไม่เกิน 5 ปี หรือปรับ หรือทั้งจำทั้งปรับ

แนวการกำหนดความรับผิดในในการเข้าถึงโดยปราศจากอำนาจ ตามมาตรา 2

กรณีของมาตรา 2 นั้น ใช้ในกรณีความผิดที่ใช้ใน Crown Court หรือจะใช้ในศาล Magistrate ก็ได้ ซึ่งขึ้นอยู่กับความร้ายแรงของความผิด ซึ่งมาตรา 2 ใช้ในความผิดประเภทที่เป็นความผิดร้ายแรง หรือที่เป็นการกระทำความผิดโดยจงใจ หรือให้ความสะดวกแก่ผู้กระทำผิดในการก่อให้เกิดการกระทำความผิดร้ายแรงขึ้น สำหรับความผิดที่เรียกว่า Further

---

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

Offence เป็นความผิดประเภทที่ไม่จำเป็นจะต้องพิสูจน์ถึงเจตนาของผู้กระทำผิด (Hacker) ว่าได้มีเจตนากระทำผิดเกิดขึ้นจริงหรือไม่

ความผิดตามมาตรา 1 เป็นกรณีที่ใช้กับการที่ไม่อาจพิสูจน์เจตนาในอนาคตได้ ซึ่งจะมีโทษเบากว่า แต่หากพิสูจน์เจตนาในอนาคตได้ให้ใช้มาตรา 2 ซึ่งมาตรา 2 นั้น เป็นมาตราที่มีบทลงโทษผู้กระทำผิดในอนาคต ซึ่งเป็นหลักเกณฑ์ที่ทำการเทียบเคียงมาจากการพยายามกระทำความผิดใน Criminal Attempt Act 1981 มาตรา 1 (2) เช่น แดงได้ข้อมูลมาว่าขาวเป็นชู้กับส้ม แดงต้องการหมิ่นประมาทขาวกับส้ม โดยแดงบอกเหลืองว่า ขาวเป็นชู้กับส้ม เหลืองได้ทราบข้อมูลนี้แล้ว ต่อมาเหลืองนำไปบอกแสด ถือว่าเหลืองผิดหมิ่นประมาทด้วย หรืออีกกรณีหนึ่ง เหลืองกลับนำข้อมูลที่ได้มานี้ไปข่มขู่ให้ยื่นให้ซึ่งทรัพย์สินถ้าไม่ได้จะประกาศว่าขาวเป็นชู้กับส้มทางหนังสือพิมพ์ เหลืองผิด Black Mail แต่การที่เหลืองได้ข้อมูลเรื่องขาวมีชู้กับส้มมาจากแดงนั้นไม่ผิดทางอาญา แม้ว่าเหลืองตั้งใจจะนำข้อมูลนี้ไป Black Mail ขาว แต่ยังไม่ได้แสดงการกระทำอะไรลงไปเพียงแต่คิดอยู่ในใจ เหลืองก็ยังไม่ผิดทางอาญาเช่นเดียวกัน แม้แต่พยายามจะกระทำผิดก็ตาม แต่กรณีตามมาตรา 2 (4) ตามบทบัญญัติข้างต้นนั้นเป็นเรื่องไม่ปกติ คือ เพียงแต่เหลืองได้ข้อมูลมาและมีความตั้งใจจะ Black Mail ขาวนั้น เหลืองมีความผิดทางอาญาตามมาตรา 2 (4) แล้ว ซึ่งกรณีนี้เป็นกรณีที่กฎหมายของอังกฤษมีความระมัดระวังอย่างที่สุด คือ แม้ได้ข้อมูลมาโดยตั้งใจจะแฮก แต่ยังไม่ได้ทำการแฮกเข้าไป ก็เป็นความผิดตามมาตรา 2 (4)

ความผิดฐานการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจนี้เป็นบทบัญญัติพื้นฐานที่ใช้กับการเข้าถึงโดยปราศจากอำนาจที่ไม่สลับซับซ้อน โดยแยกการกระทำทางกายภาพต่อคอมพิวเตอร์โดยตรง และการตรวจสอบข้อมูลอย่างละเอียด (the scrutiny of data) โดยไม่มีการโต้ตอบใด ๆ กับคอมพิวเตอร์เลย ทำให้ความผิดฐานนี้ไม่รวมถึงการอ่านเอกสารที่เป็นความลับที่อยู่ภายนอกคอมพิวเตอร์ (Confidential computer output) การอ่านข้อมูลที่ปรากฏบนจอภาพด้วย

ในการบัญญัติความผิดฐานการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจนี้ไม่ได้กำหนดว่าคอมพิวเตอร์นั้นจะต้องมีมาตรการรักษาความปลอดภัยของเครื่องหรือไม่ หากเป็นการเข้าถึงคอมพิวเตอร์สำเร็จก็เป็นความผิดฐานนี้ โดยผู้กระทำไม่จำเป็นต้องผ่านมาตรการรักษาความปลอดภัยก็เป็นความผิด

แนวคิดเกี่ยวกับความรับผิดทางกฎหมายเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจในประเทศอังกฤษ

โดยหลักแล้วการพิจารณาถึงความรับผิดทางอาญาจะพิจารณาทั้งในส่วนที่เป็นภาวะวิสัย (objective) และอัตวิสัย (subjective) โดยถือหลักว่า การกระทำใดจะเป็นผิดทางอาญาได้ จะต้องประกอบด้วยการกระทำที่ละเมิดต่อกฎหมาย หรือการกระทำที่แสดงออกภายนอกนั้นผิดกฎหมาย (actus reus)[40] และจะต้องมีส่วนของจิตใจที่จะถูกตำหนิได้ ซึ่งการพิจารณานี้เป็นไปตามหลักที่ว่า Actus non facit reum nisi mens sit rea (The act does not constitute guilt unless the mind be guilty) ซึ่งหมายความว่า การกระทำไม่ก่อให้เกิดเป็นความผิด เว้นแต่จะพิสูจน์ได้ว่าบุคคลนั้นมีเจตนากระทำความผิด เพราะฉะนั้นการพิจารณาความรับผิดของบุคคลจึงเริ่มพิจารณาจากส่วน actus reus ก่อน เมื่อได้ความว่าส่วนการกระทำภายนอกนั้นเป็นการผิดกฎหมายแล้ว จึงไปพิจารณาส่วนภายใน (mental element) ซึ่งส่วนภายในที่เป็นสภาวะทางจิตใจนี้อาจจะเป็นเรื่องของเจตนาในการกระทำผิด (Intention) การประมาทโดยรู้ตัว (Reckless) ประมาท (Negligence) หรือความพลั้งเผลอของจิตใจที่ไม่อาจตำหนิได้ (Blameless inadvertent)[41]

ในการพิจารณาบทบัญญัติของกฎหมายนั้น สิ่งที่จะต้องพิจารณาเริ่มแรกก่อนที่จะพิจารณาถึงความรับผิด คือ อะไรคือคอมพิวเตอร์ ซึ่ง CMA ไม่ได้ให้คำนิยามของคำว่าคอมพิวเตอร์ไว้เนื่องจากเกรงว่าคำนิยามจะล้าสมัยเพราะเทคโนโลยีที่พัฒนาไปอย่างรวดเร็ว แต่อย่างไรก็ตาม ศาลของประเทศอังกฤษได้ยอมรับความหมายของคอมพิวเตอร์ที่เป็นปัจจุบัน ในคดี DPP v McKeown, DPP v Jones ศาลได้ให้คำนิยามของคอมพิวเตอร์ว่า “เครื่องมือสำหรับเก็บ ดำเนินการ และกู้คืนข้อมูล[42]

---

[40] actus คือ act ซึ่งหมายถึงการกระทำ ส่วน reus คือ wrong หมายถึงความผิดซึ่งอาจจะกล่าวได้ว่า actus reus คือการกระทำในสิ่งที่ผิดกฎหมายหรือสิ่งที่กฎหมายห้าม

[41] J.C.Smith and Brian Hogan, Criminal Law, 4ed. (London, Butterworths, 1978) p.47.

[42] “Computer Misuse Act 1990” [Online] Available from : www.cr-international.com/2008_UK_CPS_Draft_Guiding_Principles_Regarding_Hacking_Tools.pdf

และ Computer Misuse Act 1990 (CMA) มาตรา 17[43] ได้ตีความความหมายของคำว่า “เข้าถึงโดยปราศจากอำนาจ” ว่า การเข้าถึงโดยปราศจากอำนาจ คือ การเข้าถึงของบุคคลในโปรแกรมหรือข้อมูลใดๆ ที่อยู่ในคอมพิวเตอร์นั้นโดยเขาไม่มีสิทธิที่จะเข้าถึงโปรแกรมหรือข้อมูลนั้น หรือ เขาไม่ได้รับอนุญาตให้เข้าถึงโปรแกรมหรือข้อมูลนั้น

ส่วนคำว่า “คอมพิวเตอร์ใดๆ” (any computer) ใน มาตรา 1(1)(a) CMA ไม่ได้จำกัดว่าผู้กระทำความผิดต้องใช้คอมพิวเตอร์เครื่องหนึ่งเข้าถึงคอมพิวเตอร์เครื่องอื่นโดยปราศจากอำนาจ แต่ความผิดฐานนี้คือการทำให้คอมพิวเตอร์ทำงานโดยตั้งใจที่จะเข้าถึงโปรแกรมหรือข้อมูลใดๆ โดยปราศจากอำนาจที่อยู่ในคอมพิวเตอร์เครื่องนั้น

โดยความผิดตามมาตรา 1 เป็นกรณีที่ใช้กับการที่ไม่อาจพิสูจน์เจตนาในอนาคตได้ ซึ่งจะมีโทษเบากว่า ซึ่งเพียงแต่เข้าถึงเท่านั้นก็เป็นความผิดแล้ว เช่น คดี R v Daniel Cuthbert[44] นาย Cuthbert ที่ปรึกษาความปลอดภัยด้านไอทีบริจาคเงิน 30 ปอนด์ ให้กับเวปไซต์ที่ก่อตั้งขึ้นเพื่อเป็นกองทุนให้ความช่วยเหลือผู้เคราะห์ร้ายในเหตุการณ์สึนามิ ได้เจาะเข้าไปในระบบรักษาความปลอดภัยของเวปไซต์ดังกล่าว โดยอ้างว่าต้องการเพียงทดสอบระบบรักษาความปลอดภัยหลังจากที่ตนได้บริจาคเงินไปแล้วเท่านั้น โดยนาย Cuthbert มีความผิดในการเข้าไปโดยมิชอบ ตาม Computer Misuse Act 1990 มาตรา 1 และถูกลงโทษปรับ 400 ปอนด์ โดยในการพิจารณานั้นไม่ปรากฏว่า นาย Cuthbert มีความตั้งใจที่จะฉ้อโกงหรือหาเงินจากการเจาะระบบแต่อย่างใด

แต่หากพิสูจน์เจตนาในอนาคตได้ก็จะมีความผิดตามมาตรา 2 เมื่อพิจารณาถึงหลักเกณฑ์ความรับผิดทางกฎหมายแล้ว ความผิดฐานการเข้าถึงคอมพิวเตอร์โดยปราศจาก

---

[43] (5) Access of any kind by any person to any program or data held in a computer is unauthorised if—

(a) he is not himself entitled to control access of the kind in question to the program or data; and

(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

[44] BBC news, “Tsunami web hacker found guilty,” [Online] Available from : http://news.bbc.co.uk/2/hi/uk_news/england/london/4317008.stm [วันที่ 2 มกราคม 2551]

อำนาจของประเทศอังกฤษอาจพิจารณาองค์ประกอบภายใน (Mens rea) ได้โดยแยกพิจารณาเป็น 2 ประการ คือ

1. ผู้กระทำมีเจตนาที่จะเข้าถึงโปรแกรมคอมพิวเตอร์ หรือข้อมูลใด ๆ ที่อยู่ในคอมพิวเตอร์ใด ๆ คำว่า “ใด ๆ” (any) ในมาตรา 1 นี้ เป็นข้อความที่ขยายเจตนา อันแสดงให้เห็นชัดเจนยิ่งขึ้นว่า เจตนานั้นไม่จำเป็นต้องมีความสัมพันธ์กับคอมพิวเตอร์ที่ผู้กระทำผิดใช้กระทำการดังกล่าวในเวลานั้น และไม่จำเป็นต้องเป็นเจตนาโดยตรงที่เป็นการมุ่งต่อโปรแกรมเฉพาะเจาะจงใด ๆ หรือข้อมูลใด ๆ หรือโปรแกรมหรือข้อมูลชนิดใดชนิดหนึ่งโดยเฉพาะ สรุปคือในความผิดฐานนี้แม้ว่าผู้กระทำจะยังไม่มีโปรแกรมหรือข้อมูลที่แน่นอนที่จะเข้าถึงโดยเฉพาะก็เป็นความผิด ดังนั้นผู้กระทำที่เข้าถึงคอมพิวเตอร์แม้ยังไม่มีความคิดชัดเจนว่าจะทำอย่างไรต่อไปนั้น แต่เกิดความคิดที่จะกระทำต่อโปรแกรมหรือข้อมูลในภายหลังจากการเข้าถึงแล้วก็เป็นความผิดไปด้วย

2. เจตนาภายใน คือผู้กระทำความผิดจะต้องรู้ในขณะที่กระทำให้คอมพิวเตอร์แสดงผลหรือแสดงการกระทำงานใดๆ ว่าปราศจากอำนาจแต่ได้เข้าถึงโปรแกรมหรือข้อมูลด้วยความจงใจ กล่าวโดยสรุปคือว่า ในการฟ้องร้องผู้กระทำความผิด “ฐานเข้าถึงโดยปราศจากอำนาจ” โจทก์จะต้องพิสูจน์ให้ศาลเห็นถึงสาระสำคัญ 2 ประการคือ ประการที่หนึ่งจำเลยมีเจตนาเข้าสู่ระบบและประการที่สอง จำเลยได้รู้ในขณะที่เขากระทำให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆว่าเขาได้เข้าไปสู่ระบบด้วยความจงใจโดยปราศจากอำนาจ ซึ่งการพิสูจน์ทั้งสองประการที่เป็นเรื่องของจิตใจของผู้กระทำนั้นถือเป็นหลักในการที่จะลงโทษผู้นั้น[45]

ในความผิดตาม Computer Misuse Act 1990 ที่เกี่ยวข้องกับการเข้าถึงโดยมิชอบด้วยกฎหมาย นั้น มีตัวอย่างคดีต่างๆ ดังนี้[46]

R v Michelle Begley [Coventry Magistrates Court]

---

[45] พรทิพย์ ตัณฑวนันท์, “ อาชญากรรมเกี่ยวกับข้อมูลอิเล็กทรอนิกส์,” (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยธรรมศาสตร์ ,2548), หน้า 71-72.

[46] Michael J L Turner , “Computer Misuse Act 1990 casesm,” [Online] Available from : www.computerevidence.co.uk/Cases/CMA.htm [วันที่ 2 มกราคม 2551]

Computer Misuse Act 1990, s 1 Unauthorized access - Harassment - Misuse of police national computer

WPC ใช้คอมพิวเตอร์ของสำนักงานตำรวจแห่งชาติเพื่อที่จะตามหาผู้หญิงที่ทำธุรกิจด้วยและเพื่อนชายของเธอโดยเข้าถึงบันทึกเกี่ยวกับสิทธิเลือกตั้งและทะเบียนรถยนต์ จำเลยถูกตัดสินว่ามีความผิดและลงโทษจำคุก 3 ปี

R v Bow Street Magistrates Court and Allison ex parte Government of USA[47]

[House of Lords 05/08/1999 The Times 7 September 1999; [1999] 4 All E R 1; [1999] 3 WLR 620; [1999] Masons CLR 380 [1998] 3 WLR 1156; [1998] Masons CLR 234; The Times 2 June 1998. [1999] C&L Oct/Nov, 21]

Computer Misuse Act 1990, ss 1, 2, 15, 17(5) Unauthorized access - Authority - Meaning of "control access" in s 17(5) - Extradition – Conspiracy

ลูกจ้างคนหนึ่งของบริษัทอเมริกันเอ็กเพรสได้เข้าถึงโดยมิชอบ ขณะที่ผู้ร่วมกระทำผิดใช้บัตรปลอมในเอทีเอ็มที่ลอนดอน และได้เงินไปเป็นจำนวนหนึ่งล้านดอลลาร์สหรัฐ โดยศาลตัดสินว่า การเข้าถึงโดยปราศจากอำนาจ หมายรวมถึง การใช้คอมพิวเตอร์เพื่อการได้รับข้อมูลในการเข้าถึงข้อมูลโดยปราศจากอำนาจ และคำว่า “Hacking” หมายถึงการเข้าถึงโดยปราศจากอำนาจทุกรูปแบบ ไม่ว่าจะเป็นบุคคลภายในหรือบุคคลภายนอก

R v Malcolm Farquharson

[Croydon Magistrates Court 09/12/1993 Computer Weekly 13 January 1994]

Computer Misuse Act 1990, ss 1, 2 Unauthorized access - Authorization

---

[47]United Kingdom Parliament, “R v Bow Street Magistrates Court and Allison ex parte Government of USA,” [Online] Available from : www.parliament.the-stationery-office.co.uk:80/pa/ld199899/ldjudgmt/jd990805/bow.htm [วันที่ 2 มกราคม 2551]

ศาลตัดสินว่าการใช้โทรศัพท์เพื่อบอกผู้ร่วมกระทำผิดอีกคนหนึ่งให้เข้าถึงข้อมูล ทำให้จำเลยเป็นผู้ร่วมกระทำผิดในฐานเจาะระบบ

ประเทศเยอรมัน

ประเทศเยอรมันมีกฎหมายที่กำหนดโทษทางอาญาเกี่ยวกับการเจาะระบบคอมพิวเตอร์โดยกำหนดไว้ในประมวลกฎหมายอาญาของเยอรมัน ซึ่งแตกต่างจากประเทศทั่วไปที่มักกำหนดความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์ไว้เป็นพระราชบัญญัติต่างหากแยกออกมาจากประมวลกฎหมายอาญาโดยทั่วไป โดยประเทศต่างๆ โดยมากมองว่ากฎหมายอาญาเกี่ยวกับคอมพิวเตอร์เป็นเรื่องที่แตกต่างจากกฎหมายอาญาเดิมค่อนข้างมากจึงควรแยกออกมาจากประมวลกฎหมายอาญาที่มีมานาน

เดิมกฎหมายของประเทศเยอรมันไม่ถือว่าการเจาะผ่านสิ่งปกป้องคุ้มครองเข้าไปเพียงอย่างเดียวเป็นความผิดทางอาญา เพราะนักกฎหมายชาวเยอรมันมีความเห็นว่าการเจาะผ่านระบบคอมพิวเตอร์เข้าไปเป็นการเข้าไปดูเฉยๆ เหมือนกับการที่เรามองดูข้อความในกระดาษที่คนอื่นเขียนเอาไว้บนโต๊ะ จึงไม่มีเหตุผลเพียงพอที่จะเป็นความผิดทางอาญา ซึ่งอาจสืบเนื่องมาจากแนวความคิดทางกฎหมายอาญาของเยอรมันที่มุ่งจะให้เกิดความสมดุลระหว่างสิทธิเสรีภาพของประชาชนและความสงบเรียบร้อยของสังคม กล่าวคือ หากมีบทกฎหมายลงโทษทางอาญามากเกินขอบเขต ก็จะก่อให้เกิดความผิดอาญาจนเฟ้อ (Over-Criminalisation) อันเป็นการล่วงละเมิดต่อสิทธิเสรีภาพของบุคคลได้ แต่อย่างไรก็ตามหลังจากที่กลุ่มสหภาพยุโรปได้มีการจัดตั้งกรรมาธิการผู้เชี่ยวชาญด้านอาชญากรรมทางคอมพิวเตอร์ขึ้นในปี 1985 เพื่อกำหนดแนวทางในการบัญญัติกฎหมายให้ครอบคลุมถึงลักษณะการกระทำที่สมควรบัญญัติเป็นความผิดและกำหนดแนวทางในการบัญญัติกฎหมายเกี่ยวกับการเข้าถึงโดยมิชอบว่าการเข้าถึงโดยมิชอบเพียงอย่างเดียวก็เป็นความผิดอาญาได้ ไม่จำเป็นต้องกระทำการใดๆ เพิ่มขึ้นอีก ประเทศเยอรมันในฐานะประเทศสมาชิกของกลุ่มสหภาพยุโรปก็ได้มีการปรับเปลี่ยนกฎหมายตามแนวทางดังกล่าว และได้ประกาศใช้เมื่อวันที่ 11 กรกฎาคม 2550

ก่อนที่จะกล่าวถึงกฎหมายเกี่ยวกับการเจาะระบบในประเทศเยอรมัน ผู้เขียนขอเริ่มที่กฎหมายเดิมก่อนที่จะมีการแก้ไขเปลี่ยนแปลงก่อน เนื่องจากการที่จะทำความเข้าใจกฎหมายใหม่ได้นั้นอาจจะต้องเริ่มที่กฎหมายที่ถูกยกเลิกไปก่อนเพื่อเข้าใจถึงแนวคิดเดิมและปัญหาที่เกิดจนต้องมีการแก้ไขกฎหมายขึ้น โดยมาตรา 202 a เดิม ซึ่งเป็นกฎหมายเกี่ยวกับการจารกรรมข้อมูลบัญญัติไว้ ดังนี้

มาตรา 202a (เดิม) StGB การจารกรรมข้อมูล (Ausspähen von Daten)[48]

"ผู้ใดกระทำการใด ๆ โดยไม่มีอำนาจ เพื่อให้ได้มาซึ่งข้อมูล ที่มิได้มีไว้สำหรับตน และเป็นข้อมูลที่มีมาตรการรักษาความปลอดภัยโดยเฉพาะสำหรับป้องกันมิให้มีการเข้าถึงข้อมูลนั้นได้ ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือมีโทษปรับ

ข้อมูล ตามบทบัญญัติในวรรคแรก หมายเฉพาะ ข้อมูลที่มีการบันทึก หรือส่งผ่านให้กันโดยวิธีการทางอิเล็กทรอนิกส์ ด้วยแม่เหล็กไฟฟ้า หรือวิธีการใด ๆ ที่ไม่สามารถมองเห็นได้ด้วยตาเปล่า"

อาจกล่าวได้ว่ามาตรา 202a เดิมนี้เป็นฐานความผิดแรกในฐานะมาตรการสำคัญที่ประเทศเยอรมันบัญญัติขึ้นเพื่อรับมือกับอาชญากรรมคอมพิวเตอร์ตั้งแต่ประมาณปี 1985-1987 มาแล้ว ซึ่งเป็นช่วงที่ระบบฐานข้อมูลต่าง ๆ กำลังเพิ่มความสำคัญและถูกพัฒนาขึ้นจำนวนมาก พร้อม ๆ กับอาชญากรรมที่เกี่ยวกับเครือข่ายข้อมูล (Datennetzkriminalität) ก็เพิ่มจำนวนขึ้นเช่นกัน การกระทำความผิดโดยความผิดในลักษณะนี้ก็คือการเข้าถึงคอมพิวเตอร์เพื่อลักเอาไปซึ่งข้อมูลคอมพิวเตอร์ของผู้เสียหาย อย่างไรก็ตาม ในวงการกฎหมายเยอรมัน แท้จริงแล้วความผิดฐานนี้ ก็คือ ความผิดฐาน "เจาะระบบ" (Hacken or Hacking) ฐานหนึ่งด้วยนั่นเอง

ทั้งนี้เพราะโดยตัวองค์ประกอบความผิด จะเกิดความผิดฐานนี้ขึ้นได้ ประกอบไปด้วยสองกรณี ด้วยกันคือ ผู้กระทำต้องเข้าไปในระบบคอมพิวเตอร์ โดยไม่มีอำนาจ (unbefugt) ก่อน แล้วจึงทำจารกรรม หรือลักเอากลุ่มข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์ที่ต้องการ ด้วยการทำซ้ำออกไป หรือมิเช่นนั้นก็ต้องมี "การดัก" รับข้อมูลที่อยู่ในขั้นตอนการ "รับ-ส่ง" โดยอาจไม่ต้องเข้าสู่ระบบคอมพิวเตอร์

---

[48] Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shell be punished with imprisonment for not more than three years or a fine.

Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner

เนื่องจากเดิมผู้บัญญัติกฎหมายเยอรมันมีแนวคิดว่า ไม่ควรมีการลงโทษ หรือกำหนดให้ “การเจาะระบบ” ที่ผู้กระทำมุ่งหมายเพียงเพื่อเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นอย่างเดียว โดยไม่ต้องการทำ อันตรายต่อข้อมูลเป็นความผิด (แตกต่างจากกฎหมายของอีกหลาย ๆ ประเทศ รวมทั้งแนวทางที่กำหนดไว้ในอนุสัญญา Cybercrime ด้วย) ดังนั้นการเจาะระบบจะเป็นความผิดตามกฎหมายเยอรมันได้จึงต้องมีการกระทำต่อข้อมูลด้วย

อย่างไรก็ตาม เป็นที่น่าสังเกตว่า ตามกฎหมายเยอรมันแล้ว ความผิดฐานนี้ กลับไม่ได้บรรจุอยู่ในหมวด “ความผิดต่อทรัพย์” (ลักทรัพย์) ตามที่เคยมีการถกเถียงถึงประเด็นการลักทรัพย์ในวงวิชาการ กฎหมายเมืองไทย แต่กลับบรรจุอยู่ในความผิดที่ก่อให้เกิดความเสียหายต่อ “ความลับ หรือชีวิตความเป็นส่วนตัว” ในประมวลกฎหมายอาญาแทน

แสดงให้เห็นว่า เดิมประเทศเยอรมันมองว่า การ Hack ที่จะถือเป็นความผิด และเป็นการละเมิดสิทธิส่วนตัวได้ ก็ต่อเมื่อผู้กระทำนั้นได้กระทำการถึงขนาดนำข้อมูลไปด้วยเท่านั้น แค่เพียงเจาะระบบเข้าไปเฉย ๆ ยังไม่อาจถือเป็นการทำลาย “ความลับ” หรือ “ชีวิต” ส่วนบุคคลแต่อย่างใด[49] แต่อย่างไรก็ตามประเทศเยอรมันเป็นสมาชิกของสหภาพยุโรปและปัญหาในการนำตัวผู้กระทำผิดมาลงโทษ ต่อมาประเทศเยอรมันจึงได้มีการปรับเปลี่ยนแก้ไขกฎหมายให้สอดคล้องกับข้อตกลงเกี่ยวกับอาชญากรรมคอมพิวเตอร์ของสหภาพยุโรป โดยได้มีการแก้ไขกฎหมายดังนี้

มาตรา 202a (ใหม่) StGB การเจาะระบบ[50]

“ผู้ใดกระทำการใด ๆ โดยไม่มีอำนาจเข้าถึงข้อมูลที่มิได้มีไว้สำหรับตน และเป็นข้อมูลที่มีมาตรการรักษาความปลอดภัยโดยเฉพาะสำหรับป้องกันมิให้มีการเข้าถึงข้อมูลนั้นได้ ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือมีโทษปรับ”

---

[49] สาวตรี สุขศรี, “ความผิดเกี่ยวกับคอมพิวเตอร์ และอินเตอร์เน็ทตามประมวลกฎหมายอาญาเยอรมัน,” [Online] แหล่งที่มา : www.biolawcom.de [วันที่ 27 พฤศจิกายน 2550]

[50] Whoever, without authorization, provides access for himself or another to data, that was not intended to come to his attention and was specially protected against unauthorized access, shell be punished with imprisonment for not more than three years or a fine.

อาจแยกองค์ประกอบได้ ดังนี้

1. ผู้ใดกระทำการใด ๆ โดยไม่มีอำนาจ
2. เข้าถึงข้อมูลที่มิได้มีไว้สำหรับตน
3. และเป็นข้อมูลที่มีมาตรการรักษาความปลอดภัยโดยเฉพาะสำหรับป้องกันมิให้มีการเข้าถึง

จากการแยกองค์ประกอบและเทียบกับบทบัญญัติเดิม จะเห็นได้ว่ามาตรา 202a ที่แก้ไขใหม่นี้แก้ไขบทบัญญัติจากคำว่า “ได้มาซึ่งข้อมูล” เป็น “เข้าถึงซึ่งข้อมูล” เท่านั้น หากแต่ทำให้หลักเกณฑ์ความรับผิดในความผิดเกี่ยวกับการเจาะระบบเปลี่ยนแปลงไป โดยแต่เดิมองค์ประกอบความผิด ประกอบไปด้วยสองขั้นตอน คือ เข้าไปในระบบคอมพิวเตอร์ โดยไม่มีอำนาจก่อน แล้วจึงทำจารกรรมหรือลักเอากลุ่มข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์ที่ต้องการด้วยการทำซ้ำออกไป แต่ด้วยบทบัญญัติที่แก้ไขใหม่นี้ทำให้ขั้นตอนที่สองคือการจารกรรมหรือลักเอาข้อมูลไปไม่เป็นองค์ประกอบความผิดอีกต่อไป เมื่อพิจารณาจากตัวบทที่แก้ไขใหม่แล้วทำให้เห็นได้ว่าเพียงแค่เข้าไปโดยปราศจากอำนาจก็เป็นความผิดตามกฎหมายแล้ว

การพยายามกระทำความผิด

การพยายามกระทำความผิดตามกฎหมายเยอรมันนั้นมีความแตกต่างจากกฎหมายไทยตรงที่กฎหมายไทยได้กำหนดการพยายามกระทำความผิดไว้ในหลักทั่วไปดังนั้นจึงสามารถที่จะนำหลักในเรื่องการพยายามกระทำความผิดไปใช้ได้กับทุกฐานความผิด ดังนั้นการพยายามกระทำความผิดจึงเป็นความผิดทางอาญาโดยไม่ต้องกำหนดฐานความผิดเกี่ยวกับการพยายามกระทำความผิดขึ้นในความผิดฐานต่างๆ แต่อย่างใด แต่ในประเทศเยอรมันนั้นการพยายามกระทำความผิดอย่างใดอย่างหนึ่งไม่ถือว่าเป็นความผิดทันทีโดยถือว่าหากกฎหมายต้องการลงโทษฐานพยายามกระทำความผิดกฎหมายต้องบัญญัติไว้ในฐานความผิดนั้น ๆ ด้วย หากไม่ได้กำหนดไว้ไม่ถือว่าเป็นความผิดทางอาญา และไม่สามารถลงโทษฐานพยายามกระทำความผิดฐานนั้นๆ ได้ ดังนั้นจากบทบัญญัติในมาตรา 202a จึงเห็นได้ว่าตามกฎหมายเยอรมันแล้วการพยายามกระทำการเจาะระบบคอมพิวเตอร์ไม่เป็นความผิด

ตัวอย่างคดีของประเทศเยอรมัน

เนื่องจากกฎหมายว่าด้วยการเจาะระบบของประเทศเยอรมันเพิ่งประกาศใช้ไม่นาน จึงยังไม่มีตัวอย่างคดีที่เกิดขึ้นตามกฎหมายใหม่ แต่ตามทบัญญัติเดิมมีตัวอย่างคดีที่เกี่ยวข้องคือ คดี Tristan (จาก Sonoda Wistra 1988, 167/168) Hacker ชาวเยอรมัน

จำนวน 20 คน ประสบความสำเร็จในการทะลุทะลวงผ่านระบบป้องกันข้อมูล โดยกระทำการผ่านเครือข่ายของประเทศญี่ปุ่น โดยทะลุทะลวงเข้าไปในสถาบันวิจัยพลังงาน (High Energy Physics Research Institute) ได้สำเร็จ ต่อมาพวก Hacker ได้ทะลุทะลวงเข้าไปในระบบประมวลผล (EDP) โดยได้เข้าไปใน Data Banks ของประเทศสหรัฐอเมริกาโดยเฉพาะอย่างยิ่งได้ทะลุทะลวงเข้าไปในเครื่องเมนเฟรมของ Lawrene Berkley ซึ่งเป็นเครื่องที่ทำหน้าที่เป็นประตูผ่านเข้าสู่ระบบเครื่องคอมพิวเตอร์ต่างๆ ของทหาร รวมทั้งของรัฐอื่นๆ ด้วย และหลังจากนั้นพวก Hacker ได้ขายความรู้ต่างๆ ที่ได้จากการทะลุทะลวงระบบ Network และวิธีการเชื่อมต่อ Network เข้าด้วยกัน รวมทั้งวิธีการผ่านเข้าไปในเส้นทางที่ได้ทำการ Lock outs เอาไว้ ซึ่งพวก Hacker ได้ทำการขายความรู้นี้ให้กับหน่วยสืบราชการลับ KGB โดยขายผ่านทางเจ้าหน้าที่ทูตทางการค้าในเบอร์ลินตะวันออก และในวันที่ 15 กุมภาพันธ์ 1990 ศาล Celle Higher Regional Court ได้พิพากษาว่าพวก Hacker ได้กระทำผิดฐานเป็นตัวแทนให้ชาวต่างชาติใช้บริการ Intelligence Service ตามมาตรา 99 แห่งประมวลกฎหมายอาญาเยอรมัน (STGB) ศาลพิพากษาลงโทษจำคุกผู้กระทำผิดหลายคนด้วยกัน โดยลงโทษจำคุกไม่เกิน 2 ปี[51]

[51] ฉัทปณัย รัตนพันธ์, “อาชญากรรมทางคอมพิวเตอร์ : ศึกษาการกำหนดฐานความผิดและการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์,” (สารนิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยธรรมศาสตร์, 2547), หน้า 17-18.

บทที่ 4

การกำหนดความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ประเทศไทยตระหนักถึงความจำเป็นในการกำหนดความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์มาเป็นเวลานานแล้วโดยได้เริ่มยกร่างตั้งแต่ปี พ.ศ. 2544 แต่ด้วยเหตุที่กฎหมายเกี่ยวกับคอมพิวเตอร์เป็นกฎหมายที่มีลักษณะแตกต่างจากกฎหมายทั่วไปที่นักกฎหมายคุ้นเคย เนื่องจากกฎหมายนี้เกี่ยวกับกับเทคโนโลยีซึ่งเป็นเรื่องใหม่ที่ต้องทำความเข้าใจเป็นอย่างมาก อีกทั้งด้วยเทคโนโลยีที่เปลี่ยนแปลงอย่างไม่หยุดยั้งทำให้การร่างกฎหมายจำเป็นต้องปรับปรุงให้เหมาะสมกับความก้าวหน้าของเทคโนโลยี ทำให้กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ใช้ระยะเวลานานโดยผ่านการปรับปรุงและเปลี่ยนแปลงหลายต่อหลายครั้ง แม้กระทั่งชื่อของกฎหมายก็ถูกเปลี่ยนจากร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์เป็นพระราชบัญญัติว่าด้วยกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เนื่องจากผู้ร่างกฎหมายเห็นว่าเนื้อหาในการกำหนดฐานความผิดนั้นไม่ได้มีแต่อาชญากรรมคอมพิวเตอร์โดยแท้เท่านั้น หากแต่มีการกระทำความผิดอื่นทางคอมพิวเตอร์หากแต่ไม่ใช่อาชญากรรมคอมพิวเตอร์โดยแท้แต่อย่างใดหากแต่ใช้คอมพิวเตอร์ในการกระทำผิดเท่านั้น เช่น การหมิ่นประมาททางอินเทอร์เน็ต การฉ้อโกงทางอินเทอร์เน็ต จึงได้มีการเปลี่ยนชื่อกฎหมายเป็นพระราชบัญญัติว่าด้วยกระทำความผิดเกี่ยวกับคอมพิวเตอร์

นอกจากชื่อกฎหมายที่ถูกเปลี่ยนแปลงก่อนประกาศใช้เป็นกฎหมายแล้ว ในส่วนของฐานความผิดก็เช่นเดียวกัน ได้มีการปรับปรุงตามความผิดใหม่ๆ ที่เกิดขึ้นเนื่องจากเทคโนโลยีที่เปลี่ยนแปลง โดยผู้เขียนจะขอยกตัวอย่างการปรับเปลี่ยนองค์ประกอบความผิดบางส่วนในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ ที่เกี่ยวข้องกับวิทยานิพนธ์นี้เท่านั้น ซึ่งได้มีการปรับเปลี่ยนมาหลายครั้ง จนในที่สุดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ผ่านการเห็นชอบจากสภานิติบัญญัติและลงพระปรมาภิไธย เมื่อวันที่ 10 มิถุนายน พ.ศ. 2550 และการประกาศลงในราชกิจจานุเบกษา เมื่อ 18 มิถุนายน พ.ศ. 2550 โดยมีผลใช้บังคับตั้งแต่ 18 กรกฎาคม พ.ศ. 2550

โดยหลักการของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในส่วนที่เกี่ยวกับความรับผิดในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้น ได้

กำหนดความผิดเกี่ยวกับการรักษาความลับ ความครบถ้วนและการทำงานของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ไว้ว่า การกำหนดความผิดฐานเข้าถึงโดยมิชอบหรือโดยไม่มีอำนาจ ซึ่งการเข้าถึงนี้หมายความถึงกรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์และกรณีผู้กระทำผิดดำเนินการด้วยวิธีการใดวิธีการหนึ่งเพื่อให้ได้รหัสผ่านมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นโดยตนเองนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั้นเอง และหมายรวมถึงกรณีที่บุคคลนั้นอยู่ห่างโดยตนเองและสามารถเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนเองต้องการด้วย โดยอาจเป็นการเข้าถึงฮาร์ดแวร์หรือส่วนประกอบต่างๆของคอมพิวเตอร์หรือข้อมูลที่ถูกบันทึกในระบบคอมพิวเตอร์ ซึ่งมาตรานี้ได้กำหนดให้การเข้าถึงโดยมิชอบเป็นความผิดแม้ผู้กระทำจะมิได้มีมูลเหตุจูงใจเพื่อให้เกิดความเสียหายใดๆ ทั้งนี้ เพราะการกระทำดังกล่าวสามารถก่อให้เกิดความผิดฐานอื่นๆ ตามมาได้โดยง่าย

การกำหนดให้การเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์เป็นความผิดโดยปรากฏอยู่ในมาตรา 5 มาตรา 6 และมาตรา 7 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ดังนี้

มาตรา 5 เป็นบทบัญญัติว่าด้วยการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ โดยบัญญัติว่า “ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ”

มาตรา 6 เป็นบทบัญญัติว่าด้วยการล่วงรู้มาตรการการป้องกันแล้วนำไปเผยแพร่โดยมิชอบ โดยบัญญัติว่า “ผู้ใดล่วงรู้มาตรการการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ”

มาตรา 7 เป็นบทบัญญัติว่าด้วยการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ โดยบัญญัติว่า “ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ”

เพื่อให้เกิดความเข้าใจในบทบัญญัติกฎหมายดังกล่าว ผู้เขียนจะแยกอธิบายถึงการกำหนดฐานความผิดในเรื่องการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5) การล่วงรู้มาตรการป้องกันแล้วนำไปเผยแพร่โดยมิชอบ (มาตรา 6) และความผิดในการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7) เพื่อเป็นพื้นฐานในการพิจารณาและปรับใช้กฎหมายต่อไป ดังนี้

4.1 การกำหนดฐานความผิด

ก่อนที่จะเริ่มพิจารณาฐานความผิดในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้น สิ่งที่จะต้องพิจารณาเป็นสิ่งแรกคือความจำเป็นในการกำหนดฐานความผิดในคดีอาญา โดยปัญหาที่มีการถกเถียงกันเมื่อมีการบัญญัติกฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ขึ้นคือ การเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์มีความร้ายแรงและมีผลกระทบทางสังคมจนต้องกำหนดเป็นความผิดทางอาญาหรือไม่ เนื่องจากกฎหมายอาญาเป็นกฎหมายที่มีบทลงโทษที่รุนแรงเกี่ยวพันกับสิทธิเสรีภาพ การเคลื่อนไหวตลอดไปถึงชีวิตของบุคคล การที่จะกำหนดกฎหมายอาญาขึ้นจึงต้องมีการพิจารณาอย่างรอบคอบเพื่อไม่ให้กระทบกับสิทธิของบุคคลเกินสมควรจนกลายเป็นกฎหมายอาญาเฟ้อ

ความผิดในการเข้าถึงโดยมิชอบนั้นเป็นการกระทำความผิดเกี่ยวกับการรักษาความลับ ความครบถ้วน และการทำงานของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ จึงถือเป็นการกระทำที่คุกคามหรือเป็นอันตรายต่อความปลอดภัย (Security) ของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ เมื่อระบบไม่มีความปลอดภัยก็จะส่งผลกระทบต่อความครบถ้วน การรักษาความลับ และความพร้อมหรือเสถียรภาพในการใช้งานของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์[1] ซึ่งเป็นฐานความผิดพื้นฐานในการกระทำผิดเกี่ยวกับคอมพิวเตอร์นั่นเอง ในส่วนความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้น นานาประเทศและนักกฎหมายโดยทั่วไปต่างเห็นพ้องต้องกันว่าการกระทำดังกล่าวก่อให้เกิดความเสียหายต่อบุคคล

---

[1] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, “แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์,” [Online] แหล่งที่มา : www.etcommission.go.th/books/Cyber_crime.pdf [วันที่ 21 กรกฎาคม 2550]

โดยส่วนรวมและต่อสังคมและอาจส่งผลกระทบในวงกว้างทั้งในแง่สังคม เศรษฐกิจ หรือแม้กระทั่งการเมือง การกระทำความผิดดังกล่าวจึงควรกำหนดเป็นความผิดอาญา

แต่ประเด็นที่มีความแตกต่างและเป็นที่ถกเถียงกันคือ การเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ในระดับใดที่ควรเป็นความผิดทางอาญาและต้องถูกลงโทษ โดยประเด็นที่จำเป็นต้องพิจารณาเกี่ยวกับการกระทำความผิดฐานนี้คือ เพียงแค่มีการเข้าถึงโดยไม่ได้รับอนุญาตจะถือว่าเป็นการก่ออาชญากรรมได้หรือไม่ หรือผู้กระทำผิดต้องมีมูลเหตุจูงใจที่จะกระทำให้เกิดความเสียหายด้วย เช่น บุคคลซึ่งมิได้มีมูลเหตุจูงใจดังกล่าวแต่ต้องการทดลองวิชาจึงเข้าไปในระบบข้อมูลของบุคคลอื่นโดยมิได้มีมูลเหตุจูงใจที่จะก่อให้เกิดความเสียหาย กรณีดังกล่าวควรกำหนดให้ต้องรับผิดและมีบทลงโทษหรือไม่ และกรณีที่มีการเข้าถึงแม้โดยไม่มีมูลเหตุจูงใจที่จะก่อให้เกิดความเสียหาย เช่น การเข้าไปในระบบคอมพิวเตอร์ของโรงพยาบาลและทำให้เกิดการเปลี่ยนแปลงคำสั่งการรักษาพยาบาล การผ่าตัด หรือการจ่ายยาให้ผู้ป่วยผิดพลาดไปจากที่กำหนดไว้เดิม อันเป็นอันตรายอย่างยิ่งต่อผู้ป่วย กรณีดังกล่าวนี้จะกำหนดขอบเขตในการพิจารณาว่าเป็นความผิดหรือไม่[2]

ซึ่งในการกำหนดฐานความผิดดังกล่าวมีความแตกต่างกันไปในแต่ละประเทศ โดยในประเทศที่กำหนดให้เป็นความผิดทันทีเมื่อการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ ได้แก่ อังกฤษ มาเลเซีย สิงคโปร์ อิสราเอล ฝรั่งเศส ส่วนในบางประเทศได้กำหนดให้ผู้กระทำต้องรับโทษหนักขึ้นหากการเข้าถึงดังกล่าวได้ก่อให้เกิดความเสียหายหรือเป็นการกระทำผิดโดยมีเจตนาเพื่อกระทำความผิดอื่นต่อไป อาทิ ออสเตรเลีย ฝรั่งเศส อิตาลี นอร์เวย์ สิงคโปร์

ประเทศที่กำหนดให้การเข้าถึงโดยมิชอบเป็นความผิดต่อเมื่อได้ละเมิดระบบการรักษาความมั่นคงเพื่อความปลอดภัยของระบบคอมพิวเตอร์ได้แก่ ประเทศเยอรมัน อิตาลี ออสเตรเลีย เนเธอร์แลนด์ สวิตเซอร์แลนด์ ในขณะเดียวกัน ก็มีบางประเทศที่กำหนดให้ผู้กระทำต้องรับผิดหนักขึ้นหากการเข้าถึงดังกล่าวเป็นการละเมิดระบบการรักษาความมั่นคง เช่น โปรตุเกส

---

[2]เรื่องเดียวกัน,

จากตัวอย่างกฎหมายต่างประเทศที่ยกมาจะเห็นได้ว่า แนวทางการบัญญัติความผิดฐานเข้าถึงโดยมิชอบมีอยู่ด้วยกัน 3 แนวทาง[3] กล่าวคือ

แนวทางที่ 1 กำหนดให้เป็นความผิดทันทีเมื่อมีการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบ

แนวทางที่ 2 กำหนดให้เป็นความผิดเฉพาะแต่กรณีได้ละเมิดหรือฝ่าฝืนระบบการรักษาความมั่นคงหรือปลอดภัยเท่านั้น

แนวทางที่ 3 กำหนดให้ผู้กระทำต้องรับผิดหนักขึ้นหากการเข้าถึงดังกล่าวเป็นการละเมิดระบบรักษาความมั่นคงหรือปลอดภัย

สำหรับในประเทศไทย พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดให้การเข้าถึงเป็นความผิดในตัวเอง (mala inse) กล่าวคือ แม้ว่าผู้กระทำจะมิได้มีมูลเหตุจูงใจเพื่อก่อให้เกิดความเสียหาย หรือการกระทำดังกล่าวจะยังมิได้ก่อให้เกิดความเสียหายก็ตาม ทั้งนี้ เพราะเห็นว่าการกระทำดังกล่าวนั้นสามารถก่อให้เกิดการกระทำผิดฐานอื่นหรือฐานที่ใกล้เคียงค่อนข้างง่ายและอาจก่อให้เกิดความเสียหายร้ายแรง ทั้งการพิสูจน์มูลเหตุจูงใจทำได้ค่อนข้างยาก

นอกจากนี้เพื่อไม่ให้ฐานความผิดเกี่ยวกับการเข้าถึงดังกล่าวมีความกว้างขวางมากเกินไป พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงกำหนดให้การเข้าถึงที่จะเป็นความผิดทางอาญานั้น ต้องเป็นความผิดในกรณีที่ได้ละเมิดหรือฝ่าฝืนระบบการรักษาความมั่นคงหรือปลอดภัยที่มีการป้องกันโดยเฉพาะเท่านั้น โดยเห็นว่าการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ผู้ที่เป็นเจ้าของไม่ได้มีการป้องกันโดยเฉพาะนั้นแสดงว่าเจ้าของไม่ได้หวงห้ามหรือไม่มีเจตนาที่จะป้องกันไว้โดยเฉพาะ จึงไม่น่าจะเป็นความผิดอาญา ซึ่งเมื่อกล่าวถึงเหตุที่ต้องกำหนดฐานความผิดขึ้นแล้ว สิ่งที่ต้องพิจารณาต่อไปคือ การกำหนดองค์ประกอบความผิดในความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ว่ามีองค์ประกอบเช่นใด โดยจะเริ่มจากองค์ประกอบภายนอกก่อน ดังนี้

---

[3] เรื่องเดียวกัน,

4.2 องค์ประกอบภายนอกของการกระทำความผิด

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดฐานความผิดในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ไว้ใน 3 มาตรา คือการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5) การล่วงรู้มาตรการป้องกันแล้วนำไปเผยแพร่โดยมิชอบ (มาตรา 6) และความผิดในการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7) ดังที่ได้กล่าวมาแล้ว โดยความผิดในการเข้าถึงโดยมิชอบตามมาตรา 5 และมาตรา 7 นั้นเป็นบทบัญญัติของกฎหมายที่กำหนดความผิดในเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ไว้โดยตรงว่าการกระทำเช่นใดเป็นความผิดทางอาญา

การที่ผู้ร่างกฎหมายบัญญัติให้ความผิดฐานการเข้าถึงระบบคอมพิวเตอร์และการเข้าถึงข้อมูลคอมพิวเตอร์แยกออกจากกันเป็น 2 มาตรา นั้น เนื่องจากเห็นว่าความผิดฐานเข้าถึงข้อมูลโดยมิชอบ ข้อมูลนั้นต้องเป็นข้อมูลที่เก็บหรือส่งด้วยวิธีการทางอิเล็กทรอนิกส์ ซึ่งมิได้หมายถึงระบบคอมพิวเตอร์เพราะไม่สามารถเก็บหรือส่งได้ ผู้ร่างเห็นว่าหากบัญญัติไว้เป็นมาตราเดียวกันอาจทำให้เกิดความสับสน จึงได้บัญญัติความผิดฐานเข้าถึงระบบคอมพิวเตอร์และความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ไว้แยกจากกัน และเห็นว่าการการกระทำความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ตามมาตรา 7 นั้น จะต้องมีการเข้าถึงระบบคอมพิวเตอร์เสียก่อนจึงจะสามารถเข้าถึงข้อมูลได้ แต่ก็มีบางกรณีที่การกระทำความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ไม่จำต้องกระทำผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบก่อนเสมอไป ตัวอย่างเช่น การนำข้อมูลที่บรรจุไว้ในแผ่นดิสเกตต์ของผู้อื่นที่ได้มีการใช้วิธีการป้องกันการเข้าถึงโดยเฉพาะไว้ เช่น การตั้งรหัสผ่านป้องกันการเข้าถึงไฟล์ข้อมูล แล้วจึงนำแผ่นดิสเกตต์ดังกล่าวไปเปิดอ่านในระบบคอมพิวเตอร์ของตนเอง[4]

ส่วนความผิดอีกฐานหนึ่งที่เกี่ยวข้องกับความผิดในการเข้าถึงโดยมิชอบคือความผิดในการล่วงรู้มาตรการป้องกันการเข้าถึงแล้วนำไปเปิดเผย (มาตรา 6) ซึ่งแม้จะไม่ได้กำหนดความผิดในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ไว้โดยตรง หากแต่ก็เป็นมาตราที่เกี่ยวพันกัน โดยกล่าวถึงการล่วงรู้มาตรการป้องกันการเข้าถึงและนำไปเปิดเผย

---

[4] เรื่องเดียวกัน,

หากพิจารณาจากมาตราที่กล่าวถึงข้างต้นแล้ว จะเห็นได้ว่าความผิดในการเข้าถึงโดยมิชอบตามมาตรา 5 และมาตรา 7 เป็นมาตราหลักในความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ ดังนั้นผู้เขียนจึงจะพิจารณาถึงองค์ประกอบภายนอกในความผิดในการเข้าถึงระบบคอมพิวเตอร์ในมาตรา 5 และความผิดในฐานความผิดในการเข้าถึงข้อมูลคอมพิวเตอร์ในมาตรา 7 ก่อน จึงจะไปพิจารณาองค์ประกอบความผิดเกี่ยวกับการล่วงรู้มาตรการป้องกันการเข้าถึงแล้วนำไปเปิดเผยในมาตรา 6 ต่อไป

โดยผู้เขียนจะขอพิจารณาองค์ประกอบภายนอกของการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบก่อน ดังนี้

4.2.1 การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5)

มาตรา 5 บัญญัติว่า “ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ”

เมื่อพิจารณาจากบทบัญญัติข้างต้น อาจแยกองค์ประกอบได้ดังนี้

1. ผู้ใด
2. เข้าถึงโดยมิชอบ
3. ระบบคอมพิวเตอร์
4. ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน

โดยองค์ประกอบของบัญญัติดังที่ได้กล่าวมานั้น อาจแยกพิจารณาตามได้ดังนี้

1. ผู้ใด

คำว่า “ผู้ใด” เป็นคำกว้างๆ หมายถึงใครก็ได้ ซึ่งในกฎหมายอาญานั้นโดยปกติย่อมหมายถึงบุคคลธรรมดา ดังนั้นคำว่า “ผู้ใด” ในมาตรานี้จึงหมายถึงบุคคลทั่วไปไม่ว่าจะเป็นเพศใดก็ตามก็สามารถกระทำผิดตามมาตรานี้ได้ ส่วนในกรณีที่เป็นนิติบุคคลนั้นจะเห็นได้ว่านิติบุคคลโดยทั่วไปไม่สามารถกระทำผิดทางอาญาได้ คำว่า “ผู้ใด” จึงไม่ได้หมายถึงนิติบุคคลด้วยแต่อย่างใด ดังนั้นองค์ประกอบในส่วนนี้จึงเป็นความหมายตามปกติที่ปรากฏในประมวลกฎหมายอาญา

อย่างไรก็ตาม ในเรื่องอาชญากรรมทางคอมพิวเตอร์นั้น ผู้กระทำความผิดอาจไม่ได้กระทำด้วยตนเอง หากแต่ใช้โปรแกรมที่เรียกว่า “บอทเน็ต โดยในวงการนักวางระบบรักษาความปลอดภัยระบบบนเครือข่ายอินเทอร์เน็ตเรียกกันติดปากว่าพวก “บอท” (Bot) หรือ “โรบอท” (Robot) หรือ “บอทเน็ต” (Botnet) โดยบอทเน็ต คือ กลุ่มคอมพิวเตอร์จำนวนมากที่แฮกเกอร์สามารถควบคุมจากทางไกลและเป็นที่นิยมมากในหมู่อาชญากรไฮเทคเพราะสามารถใช้ประโยชน์ได้มาก คอมพิวเตอร์ที่โดนแฮคเกอร์ยึดระบบ นิยมเรียกว่า ทาส (slave) หรือ บอท (bot) ซึ่งนำไปใช้ส่งอีเมล์ สแปม (spam) หรือ อีเมล์หลอกให้ผู้ใช้เปิดเผยข้อมูลส่วนตัวได้เป็นอย่างดี (phishing e-mails) และยังเป็นเครือข่ายเพาะหรือแพร่กระจายเชื้อไวรัสคอมพิวเตอร์ หรือนำไปใช้เป็นระบบเก็บข้อมูลผิดกกหมายนานาชนิด นักก่อกวน (spammers) นักต้มตุ๋นบนอินเทอร์เน็ตมักเช่าบอทเน็ตเพื่อดำเนินกิจกรรมผิดกฎหมายต่างๆ ภัยคุกคามประเภทบอทนั้นรุนแรงมากในต่างประเทศถึงขั้นมีการใช้เจ้าบอทดังกล่าวเป็นเครื่องมือในการขู่กรรโชกเงิน ซึ่งสถานการณ์ของการทำลายล้างดังกล่าวต่างเรียกกันว่า “Botnet Return” แนวคิดบนวิธีการของบอทเน็ตนั้น กล่าวง่ายๆ ก็คือ การยืมมือคนในเครือข่ายอินเทอร์เน็ตระดมส่งอีเมล์ไปทำลายแบนด์วิดธ์ของเป้าหมายจนไม่สามารถทำการติดต่อสื่อสารได้ ซึ่งคนในเครือข่ายดังกล่าวจำนวนนับล้านคนจะถูกใช้เป็นเครื่องมือโดยที่เจ้าตัวไม่รู้ตัว เพราะว่าคนเหล่านั้นติดเชื้อร้ายที่เรียกว่าบอทเข้าให้แล้ว[5]

ดังนั้นหากเครื่องคอมพิวเตอร์ถูกบอทเน็ตโจมตีหรือพยายามเจาะเข้ามาในระบบคอมพิวเตอร์ สิ่งที่จะต้องพิจารณาคือผู้ใดคือผู้กระทำความผิด ซึ่งในประเด็นนี้อาจไม่เป็นการยากที่จะวิเคราะห์เนื่องจากเครื่องคอมพิวเตอร์ที่ถูกเข้าควมคุม (บอทเน็ต) และเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นนั้นก็เปรียบเสมือนการที่คนร้ายจับมือบุคคลหนึ่งเขกศีรษะของอีกบุคคลหนึ่ง จึงถือได้ว่าบุคคลที่ถูกจับมือนั้นไม่มีการกระทำเป็นของตนเอง หากแต่เป็นเพียงเครื่องมือของคนร้ายเท่านั้น จึงไม่มีความผิดและถือว่าผู้ที่กระทำความผิดคือคนที่จับมือคนอื่นไปทำร้ายอีกคนหนึ่งเท่านั้น เช่นเดียวกันผู้ที่ถือว่าเป็นผู้กระทำความผิดในการใช้บอทเน็ตในการโจมตีคือแฮกเกอร์ที่ทำการควบคุมหรือชักใยบอทเน็ตต่างๆ อยู่เบื้องหลังนั้นเอง

2. เข้าถึงโดยมิชอบ

---

[5] กษมา กองสมัคร, “ตามรอยอาชญากรรมไฮเทค (4191),” IT-Digest ปีที่ 4 ฉบับที่ 19 (1 ตุลาคม 2550) [Online] แหล่งที่มา : www.nectec.or.th [27 ตุลาคม 2550]

การเข้าถึงโดยมิชอบนั้นอาจแยกองค์ประกอบย่อยออกเป็น 2 ส่วน คือ “เข้าถึง” และ “โดยมิชอบ” เพื่อที่จะเข้าใจได้ง่ายผู้เขียนจะขอแยกพิจารณาคำว่า “เข้าถึง” และ “โดยมิชอบ” ก่อนว่าแต่ละส่วนมีความหมายว่าอย่างไร โดยจะเริ่มที่คำว่า เข้าถึง ดังนี้

การให้ความหมายของคำว่าการเข้าถึงคอมพิวเตอร์นั้น โดยทั่วไปแล้วอาจแยกพิจารณาจากลักษณะของการเข้าถึงอาจแยกออกได้เป็น 2 กรณี คือ การเข้าถึงในความหมายอย่างแคบ คือการเข้าไปโดยเทียบเคียงกับลักษณะของการบุกรุกที่เกิดขึ้นในโลกทางกายภาพ กล่าวคือมีการเข้าไป (inside) ในคอมพิวเตอร์ เช่น การเข้าไปในระบบจดหมายอิเล็กทรอนิกส์โดยใช้รหัสของผู้อื่น กล่าวคือได้มีการล่วงล้ำเข้าไปอย่างแท้จริงโดยเทียบกับการบุกรุกที่มีการเข้าถึงสถานที่นั้น แต่การเข้าถึงคอมพิวเตอร์ในความหมายอย่างกว้างนั้นมีแนวคิดที่อ้างอิงกับการทำงานของคอมพิวเตอร์เป็นหลักโดยไม่ได้เน้นเทียบเคียงกับพฤติกรรมการบุกรุกในความเป็นจริง โดยมุ่งเน้นที่ไปการทำงานของคอมพิวเตอร์ที่เกิดขึ้นโดยเห็นว่าการเข้าถึงนั้นคือการทำให้คอมพิวเตอร์ทำงาน หากทำให้คอมพิวเตอร์มีการตอบสนอง (response) กับคำสั่งที่ได้มีการสั่ง (input)

การให้ความหมายของคำว่าเข้าถึงอย่างกว้างหรืออย่างแคบนั้นเป็นสิ่งที่ศาลจะต้องพิจารณาความเหมาะสมในการตีความ โดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ได้ให้คำนิยามของคำว่าเข้าถึงไว้เนื่องจากที่ประชุมคณะกรรมการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เห็นว่า ไม่ต้องมีการเพิ่มเติมคำนิยาม “การเข้าถึง” เพราะเป็นถ้อยคำที่มีนัยในตัวและศาลจะเป็นผู้ตีความอยู่แล้ว[6]

การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ อาจเกิดได้หลายกรณี ซึ่งอาจแยกประเภทของการเข้าถึงออกเป็น 2 ประเภทใหญ่ๆ คือ การเข้าถึงทั้งในระดับกายภาพ เช่นกรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์ และผู้กระทำผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั้นเอง และหมายความรวมถึงการเข้าถึงระบบคอมพิวเตอร์แม้ตัวบุคคลที่

---

[6] “สรุปสาระสำคัญการประชุมคณะกรรมาธิการวิสามัญ ครั้งที่ 5/2549,” [Online] แหล่งที่มา : http://wiki.nectec.or.th/nectecpedia [27 ตุลาคม 2550]

เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์ แต่สามารถเจาะระบบเข้าไปในระบบคอมพิวเตอร์ที่ตนต้องการได้ไม่ว่าผู้เจาะระบบจะอยู่ที่ไหนก็ตาม

นอกจากนั้นยังหมายถึงการเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้ ดังนั้นจึงอาจหมายถึง การเข้าถึงฮาร์ดแวร์ หรือส่วนประกอบต่างๆ ของคอมพิวเตอร์[7]

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะเห็นได้ว่าคำว่าโดยมิชอบเป็นส่วนขยายของคำว่า “เข้าถึง” ว่าอย่างไรจึงจะเป็นความผิด ซึ่งพระราชบัญญัตินี้ก็ได้ใช้คำว่า “เข้าถึงโดยมิชอบ” จึงจะเป็นความผิดตามกฎหมาย คำว่า “โดยมิชอบ” นี้ เป็นถ้อยคำที่มีความได้หลายนัย แล้วแต่ผู้ตีความว่าจะตีความถึงคำว่า “เข้าถึงโดยมิชอบ” เช่นใด โดยอาจหมายถึงไม่ชอบด้วยกฎหมาย (illegal) โดยปราศจากอำนาจ (unauthorized) หรือ ไม่เหมาะสม (improper) ก็ได้ ซึ่งตามพระราชบัญญัตินี้มีผู้ให้ความหมายไว้ว่า “การเข้าถึงโดยมิชอบ” ซึ่งถือว่าเป็นความผิดฐานนี้จะต้องเป็นการเข้าถึงโดยปราศจากสิทธิโดยชอบธรรม (without right) จึงอาจแปลความได้ว่าหากผู้ทำการเข้าถึงนั้นเป็นบุคคลที่มีสิทธิเข้าถึงไม่ว่าด้วยถือสิทธิตามกฎหมายหรือได้รับอนุญาตจากเจ้าของระบบ ตัวอย่างเช่น การเข้าถึงเพื่อดูแลระบบของผู้ดูแลเว็บ (webmaster) ก็ถือว่าเข้าถึงโดยชอบ แต่อย่างไรก็ตามหากผู้ได้รับอนุญาตให้ทำการเข้าถึงนั้นได้เข้าถึงระบบเกินกว่าที่ตนได้รับอนุญาต ในกรณีนี้บุคคลดังกล่าวก็ย่อมต้องรับผิดเช่นเดียวกัน[8]

3. ระบบคอมพิวเตอร์

ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้มีการกำหนดคำนิยามของคำว่าระบบคอมพิวเตอร์ไว้ว่า

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

---

[7] นายพรเพชร วิชิตชลชัย, “คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550,” หน้า 8-9. [Online] แหล่งที่มา : www.doa.go.th/human/other_50/com02_50.pdf [วันที่ 21 กันยายน 2550]

[8] เรื่องเดียวกัน, หน้า 9.

ดังนั้น “ระบบคอมพิวเตอร์” จึงได้แก่ ฮาร์ดแวร์และซอฟต์แวร์ที่พัฒนาขึ้นเพื่อประมวลผลข้อมูลดิจิทัล (digital data) อันประกอบด้วย เครื่องคอมพิวเตอร์ และอุปกรณ์รอบข้าง (peripheral) ต่างๆในการรับเข้าหรือป้อนข้อมูล (input) นำออกหรือแสดงผลข้อมูล (output) และบันทึกหรือเก็บข้อมูล (store and record) ดังนั้น ระบบคอมพิวเตอร์จึงอาจเป็นอุปกรณ์เพียงเครื่องเดียวหรือหลายเครื่องอันมีลักษณะเป็นชุดเชื่อมต่อกัน ทั้งนี้ โดยอาจเชื่อมต่อกันผ่านระบบเครือข่ายและมีลักษณะการทำงานโดยอัตโนมัติตามโปรแกรมที่กำหนดไว้และไม่มีการแทรกแซงโดยตรงจากมนุษย์ โดยมีการทำงานประมวลผลข้อมูลโดยอัตโนมัติแล้ว ดังนั้นเครื่องคอมพิวเตอร์ เช่น โน๊ตบุ๊คที่ซื้อมายังไม่ถือว่าเป็น “ระบบคอมพิวเตอร์” จนกว่าจะได้มีการทำงานผ่านระบบเครือข่ายหรือโดยซอฟต์แวร์ ส่วนโปรแกรมคอมพิวเตอร์จะหมายถึงชุดคำสั่งที่ทำหน้าที่สั่งการให้คอมพิวเตอร์ทำงาน

4. มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน

องค์ประกอบในส่วนนี้อาจแยกย่อยออกไปได้อีกเป็น

4.1 มาตรการป้องกันการเข้าถึงโดยเฉพาะ และ

4.2 มาตรการนั้นมิได้มีไว้สำหรับตน

โดยระบบคอมพิวเตอร์ใดที่เป็นระบบที่มีวิธีการป้องกันการเข้าถึงโดยเฉพาะนั้น ผู้ร่างกฎหมายเห็นว่าเป็นข้อเท็จจริงที่จะต้องนำสืบเป็นเรื่องๆ ไป ส่วนเหตุผลที่บัญญัติองค์ประกอบความผิดนี้ก็เพราะมีระบบคอมพิวเตอร์จำนวนมากที่เจ้าของไม่ได้หวงแหนการที่บุคคลใดจะเข้าถึง[9] เมื่อมิได้หวงแหนแล้วกฎหมายจึงสันนิษฐานว่าระบบคอมพิวเตอร์นั้นไม่เป็นความลับ เจ้าของระบบไม่ขัดขวางหากจะมีผู้หนึ่งผู้ใดเข้าถึงระบบคอมพิวเตอร์ของตน

องค์ประกอบในส่วนนี้ผู้เขียนจะขอพิจารณาจากองค์ประกอบในส่วน “มาตรการป้องกันการเข้าถึงโดยเฉพาะ” ก่อนว่าลักษณะอย่างไรจึงจะถือว่าเป็นระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีวิธีการป้องกันการเข้าถึงโดยเฉพาะ เนื่องจากมีความหมายกว้างมาก เช่น คอมพิวเตอร์ส่วนบุคคลเครื่องหนึ่งไม่มีระบบรักษาความปลอดภัยของข้อมูลอยู่ในเครื่องเลย และก็ไม่ได้กำหนดรหัสผ่านสำหรับการเปิดดูข้อมูลตั้งอยู่ในบ้าน ในกรณีเช่นนี้จะถือว่า

---

[9] เรื่องเดียวกัน, หน้า 9.

ข้อมูลคอมพิวเตอร์มีวิธีการป้องกันการเข้าถึงโดยเฉพาะหรือไม่ หากมีคนเข้าไปเปิดดูข้อมูลจะมีความผิดหรือไม่ ซึ่งในกรณีนี้ตามบทบัญญัติของกฎหมายแล้วน่าจะพิจารณาได้ว่ามาตรการป้องกันการเข้าถึงโดยเฉพาะนั้นต้องเป็นมาตรการป้องกันในแง่ของระบบคอมพิวเตอร์นั้นเอง หากเป็นเครื่องคอมพิวเตอร์ที่ไม่มีระบบป้องกันในระบบของตนหากแต่มีการป้องกันทางกายภาพ เช่น มีการเข้าสิ่งกีดขวางไปตั้งไว้ไม่ให้เข้าถึงเครื่องคอมพิวเตอร์ หรือเก็บไว้ในห้องที่ปิดไว้ ไม่ถือว่าเป็นมาตรการป้องกันการเข้าถึงโดยเฉพาะแต่อย่างใด เนื่องจากไม่ใช่วิธีการทางด้านคอมพิวเตอร์ จึงไม่ถือว่าเป็นการเข้าถึงโดยมิชอบ เช่นเดียวกับกรณีที่มีการเก็บแผ่นดิสเกตต์หรือแฮนดี้ไดร์ฟที่ไม่มีการตั้งรหัสผ่านสำหรับการเข้าถึงข้อมูลไว้ในลิ้นชักแล้วใส่กุญแจไว้ ในกรณีเช่นนี้ไม่น่าจะถือว่าเป็นวิธีการป้องกันการเข้าถึงโดยเฉพาะเช่นกัน ดังนั้นวิธีป้องกันการเข้าถึงโดยเฉพาะจึงหมายถึงการป้องกันประเภท รหัสผ่าน การแสกนนิ้ว รวมถึงไฟล์วอร์

ส่วนองค์ประกอบในแง่ “มาตรการนั้นมิได้มีไว้สำหรับตน” หมายถึง การป้องกันนั้นหากผู้ที่เข้าถึงมีอำนาจที่จะเข้าไปได้ ผู้นั้นก็ไม่มีความผิด เช่นลูกจ้างสามารถเข้าถึงข้อมูลของบริษัทนายจ้างได้เนื่องจากมีอำนาจหน้าที่ปฏิบัติงานในส่วนนั้น หรือกรณีเข้าไปโดยมีอำนาจ เช่น webmaster เข้าไปดูแลระบบภายใต้อำนาจที่ตนมีอยู่ก็ไม่ถือว่ามีการกระทำผิด

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในส่วนที่เกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์โดยมิชอบนั้น เมื่อพิจารณาถึงองค์ประกอบความผิดแล้ว จะเห็นได้ว่ากฎหมายมุ่งคุ้มครองระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีการป้องกันไว้โดยเฉพาะเท่านั้น หากข้อมูลดังกล่าวไม่มีการป้องกันไว้แล้ว กฎหมายถือว่าการเข้าถึงดังกล่าวไม่มีความผิด เนื่องจากเมื่อเจ้าของไม่ป้องกันแสดงว่าเจ้าของไม่หวงห้าม แม้จะระบบหรือข้อมูลที่เป็นความลับก็ไม่เป็นความผิดแต่อย่างใด

ความผิดในการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7)

มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

เมื่อพิจารณาจากบทบัญญัติข้างต้น อาจแยกองค์ประกอบได้ดังนี้

1. ผู้ใด
2. เข้าถึงโดยมิชอบ

3. ข้อมูลคอมพิวเตอร์
4. ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน

ซึ่งอาจแยกพิจารณาตามองค์ประกอบความผิดได้ดังนี้

เนื่องจากองค์ประกอบภายนอกของการกระทำผิดในความผิดฐานเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่ปรากฏในมาตรา 5 และมาตรา 7 นั้นมีองค์ประกอบแทบจะเหมือนกันทุกประการ โดยมีความแตกต่างกันเพียงแค่ในมาตรา 5 นั้นเป็นเรื่องของระบบคอมพิวเตอร์ แต่ในมาตรา 7 เป็นเรื่องของข้อมูลคอมพิวเตอร์ เท่านั้น ดังนั้นองค์ประกอบในส่วนอื่นของความผิดในการเข้าถึงข้อมูลโดยมิชอบ (มาตรา 7) จึงจะขออธิบายโดยสรุปเนื่องจากไม่แตกต่างจากความผิดในการเข้าถึงระบบโดยมิชอบ (มาตรา 5) แต่อย่างใด

1. **ผู้ใด**

คำว่า ผู้ใด ในมาตรานี้ก็ไม่แตกต่างจากที่ได้กล่าวถึงมาแล้วในความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5) ว่าเป็นถ้อยคำทั่วไปและเมื่อกฎหมายใช้คำว่า ผู้ใด ย่อมหมายถึงบุคคลใดก็ได้ ไม่จำกัดทั้งเพศหรืออายุ หากสามารถมีการกระทำที่ครบองค์ประกอบความผิดแล้ว ย่อมถูกลงโทษตามกฎหมาย แต่อย่างไรก็ตาม ด้วยลักษณะของความผิดเกี่ยวกับการเข้าระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์แล้ว ผู้ที่จะกระทำผิดได้ต้องมีความรู้ความสามารถในการใช้คอมพิวเตอร์ในระดับหนึ่งและมีความสนใจในเรื่องเทคโนโลยี ดังนั้นจึงมักพบว่าผู้กระทำผิดมักจะเป็นบุคคลในวัยรุ่นหรือวัยทำงานเป็นส่วนใหญ่

2. **เข้าถึงโดยมิชอบ**

คำว่า “เข้าถึงโดยมิชอบ” นี้ ก็มีความหมายเดียวกับถ้อยคำในความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5) คือการเข้าถึงโดยปราศจากสิทธิอันชอบธรรม เพียงแต่การเข้าถึงในมาตรานี้เปลี่ยนจากการเข้าถึงระบบคอมพิวเตอร์เป็นการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ โดยความผิดในการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบอาจครอบคลุมไปถึงความผิดในการใช้คอมพิวเตอร์โดยมิชอบ และความผิดในการโจรกรรมหลักฐานการยืนยันตัวตนของบุคคลอื่น (Identity Theft) ด้วย แม้จะไม่ใช่ความผิดโดยตรงก็ตาม เนื่องจากการโจรกรรมหลักฐานการยืนยันตัวตนของบุคคลอื่นนั้น มักมีการเข้าไปในข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบและการกระทำการเพื่อให้ได้มาซึ่งข้อมูลของผู้อื่นโดยฉ้อฉล เพื่อที่จะให้ได้มาซึ่ง

ผลประโยชน์ทางการเงิน สิ่งของหรือบริการต่างๆ ทั้งนี้ ข้อมูลส่วนตัวของบุคคลอื่นที่นำไปใช้โดยฉ้อฉลและปราศจากการได้รับอนุญาตนี้ อาจเป็นการนำเอารายละเอียดของ ชื่อ นามสกุล วันเดือนปีเกิด หมายเลขบัตรประจำตัวประชาชน หมายเลขบัตรเครดิต หรือรายละเอียดเกี่ยวกับเลขบัญชีในธนาคาร อย่างไรก็ดีข้อมูลเหล่านี้อาจไม่ได้นำไปใช้เพื่อผลประโยชน์ทางการเงิน สิ่งของหรือบริการต่างๆโดยตรง แต่อาจนำไปใช้เพื่อให้ได้มาซึ่งเอกสารที่ทางราชการออกให้เพื่อนำเอกสารเหล่านี้ไปใช้โดยฉ้อฉลต่อไป เช่น การนำข้อมูลเหล่านั้นไปขอบัตรประชาชน ใบอนุญาตขับรถ หรือแม้กระทั่งการทำหนังสือเดินทางและขอวีซ่า ออกไปยังประเทศอื่นๆแต่อย่างไรก็ตามบทบัญญัติมุ่งหมายที่จะลงโทษเฉพาะการเข้าถึงโดยมิชอบเท่านั้นไม่ได้ลงโทษการโจรกรรมแต่อย่างใด[10]

3. ข้อมูลคอมพิวเตอร์

องค์ประกอบในส่วนนี้เป็นองค์ประกอบส่วนเดียวที่แตกต่างจากมาตรา 5 โดยในมาตรา 5 นั้น กฎหมายมุ่งที่จะคุ้มครองระบบคอมพิวเตอร์ ในขณะที่มาตรา 7 นั้นสิ่งที่กฎหมายมุ่งคุ้มครองคือข้อมูลคอมพิวเตอร์ โดยข้อมูลคอมพิวเตอร์ที่กล่าวถึงนี้ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ให้คำนิยามไว้ในมาตรา 3 ว่า

ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

ซึ่งจากความหมายดังกล่าว ข้อมูลคอมพิวเตอร์ แบ่งได้เป็น 2 ประเภท คือ

1. ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์

---

[10] สราวุธ เบญจกุล, “E-crime” อาชญากรรมทางอิเล็กทรอนิกส์ มหันตภัยในโลกยุคใหม่ [Online],” แหล่งที่มา : www.etcommission.go.th/e-crime.html [วันที่ 10 มกราคม 2551]

2. ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์[11]

อนึ่ง คำว่า “ข้อมูลอิเล็กทรอนิกส์” ตามกฎหมายฉบับนี้ไม่ได้จำกัดอยู่เฉพาะข้อมูลอิเล็กทรอนิกส์ที่ใช้ในการติดต่อสื่อสารเท่านั้น แต่มุ่งประสงค์ให้ครอบคลุมถึงข้อมูลหรือบันทึกที่สร้างขึ้นโดยคอมพิวเตอร์ แม้จะไม่ได้ใช้เป็นสื่อในการสื่อสารกับบุคคลอื่นก็ตาม และวิธีการทางอิเล็กทรอนิกส์ในที่นี้ให้รวมถึงพัฒนาการทางเทคโนโลยีในลักษณะอื่นที่คล้ายคลึงกันในอนาคต [12]

ความหมาย “ข้อมูลคอมพิวเตอร์” หมายถึงข้อมูลทุกอย่างที่อยู่ในระบบคอมพิวเตอร์ รวมทั้งชุดคำสั่งด้วยหากอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ นอกจากนั้นยังให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

ความจริงแล้ว “ข้อมูลอิเล็กทรอนิกส์” ย่อมอยู่ในความหมายของข้อมูลคอมพิวเตอร์อยู่แล้ว แต่เพื่อให้ครอบคลุมถึงข้อมูลประเภทอื่นๆ ที่อาจสร้างด้วยวิธีการทางอิเล็กทรอนิกส์อื่นๆ ในอนาคตที่ไม่ใช่เทคโนโลยีคอมพิวเตอร์ก็ได้ อย่างไรก็ตาม

“ข้อมูลอิเล็กทรอนิกส์” ตามที่บัญญัติไว้ในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ได้ให้ความหมายคำว่า “ข้อมูลอิเล็กทรอนิกส์” ไว้ว่า “ข้อความที่ได้สร้าง ส่ง เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือ โทรสาร ดังนั้น ความหมายจึงกว้างรวมออกไปถึงโทรเลข โทรพิมพ์ โทรสาร อย่างไรก็ตามองค์ประกอบความผิดตามพระราชบัญญัตินี้ส่วนใหญ่จะเชื่อมโยงองค์ประกอบความผิด “ข้อมูลคอมพิวเตอร์” กับ “ระบบคอมพิวเตอร์” เข้า

---

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

[12] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, “คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544,” หน้า 16. [Online] แหล่งที่มา : www.etcommission.go.th/books/et_des_2544.html [วันที่ 20 สิงหาคม 2550]

ด้วยกัน ดังนั้นกรณีของโทรเลข โทรพิมพ์ หรือโทรสารหากเป็นความผิดที่ต้องเชื่อมโยงกับระบบคอมพิวเตอร์ เช่นการดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์โดยมิชอบตามมาตรา ๘ นั้น จะต้องเป็นกรณีที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ เป็นต้น ดังนั้นการดักรับโทรเลข โทรพิมพ์หรือโทรสารที่ไม่ได้ส่งในระบบคอมพิวเตอร์ย่อมไม่เป็นความผิดตามมาตราดังกล่าว เป็นต้น

โดยเมื่อพิจารณาต่อไปถึงชนิดของข้อมูลคอมพิวเตอร์ที่จะได้รับความคุ้มครองต้องเป็นข้อมูลคอมพิวเตอร์ที่มิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ดังนั้นข้อเท็จจริงจึงควรเป็นว่าข้อมูลคอมพิวเตอร์นี้ควรเป็นข้อมูลที่ประสงค์จะส่งให้รับรู้เฉพาะบุคคลที่ต้องการเท่านั้นโดยไม่จำเพาะเจาะจงว่าต้องเป็นข้อมูลลับหรือไม่ และต้องไม่ได้เป็นข้อมูลที่ต้องการให้บุคคลอื่นหรือประชาชนทั่วไปล่วงรู้หรือนำข้อมูลนั้นไปใช้ประโยชน์ โดยไม่ได้รับอนุญาตจากทั้งผู้ส่งและผู้รับ เนื่องจากมาตรา 8 มีวัตถุประสงค์เพื่อให้ความคุ้มครองสิทธิความเป็นส่วนตัวแก่ผู้ใช้ระบบคอมพิวเตอร์ ไม่ให้บุคคลอื่นเข้ามาล่วงรู้ถึงข้อมูลตนโดยมิชอบ

ดังนั้น จะเห็นได้ว่าในการก่ออาชญากรรมทางคอมพิวเตอร์นั้นการกระทำความผิดโดยการคุกคามหรือก่อความเสียหายให้เกิดขึ้นคงจะไม่ใช่แต่เพียงกับข้อมูลอิเล็กทรอนิกส์ในความหมายตามพระราชบัญญัติดังกล่าวเท่านั้นเพราะการกระทำความผิดทางคอมพิวเตอร์นั้นอาจเป็นการกระทำต่อ“ข้อมูล” ซึ่งไม่ได้สื่อความหมายถึงเรื่องราวต่างๆ ทำนองเดียวกับ“ข้อความ” แต่อย่างใด ตัวอย่างของ“ข้อมูล” เช่นข้อมูลซึ่งเป็นรหัสผ่านหรือลายมือชื่ออิเล็กทรอนิกส์เป็นต้นกระนั้นก็ตามแม้ “ข้อมูล” จะมีลักษณะหลากหลายแล้วแต่การสร้างและวัตถุประสงค์ในการใช้งาน แต่ “ข้อมูล” ที่กล่าวถึงนี้ต้องมีลักษณะสำคัญประการหนึ่ง คือ ต้องเป็น“ข้อมูลดิจิทัล” (digital) เท่านั้น

นอกจากนี้ แม้ว่าข้อมูลคอมพิวเตอร์จะเป็นสิ่งที่ได้รับการรับรองและคุ้มครองตามกฎหมายอาญาโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งเพิ่งมีการบังคับใช้ หากแต่ข้อมูลคอมพิวเตอร์ก็ไม่ใช่เรื่องใหม่ที่ไม่เคยปรากฏหรือให้ความหมายโดยศาลมาก่อน ในส่วนของความหมายของข้อมูลคอมพิวเตอร์ที่ปรากฏอยู่ในคำพิพากษาศาลฎีกานั้น ศาลฎีกาได้ให้ความหมายของคำว่าข้อมูลไว้ในฎีกาที่ 5161/2547[13] และกล่าวว่า

---

[13] คำพิพากษาฎีกาที่ 5161/2547 ข้อมูล ตามพจนานุกรมให้ความหมายว่า ข้อเท็จจริง หรือ สิ่งที่ถือหรือยอมรับว่าเป็นข้อเท็จจริง สำหรับใช้เป็นหลักอนุมานหาความจริง

ข้อมูลคอมพิวเตอร์ไม่ใช่ทรัพย์ การคัดลอกข้อมูลจึงไม่ใช่การลักทรัพย์ แต่อย่างไรก็ตามไม่ใช่ว่าศาลฎีกาจะไม่คุ้มครองการกระทำที่ทำต่อข้อมูลคอมพิวเตอร์แต่อย่างใด ผู้ที่ทำให้ข้อมูลคอมพิวเตอร์เสียหายก็ต้องชดใช้ค่าเสียหายเช่นกัน ดังที่ปรากฏอยู่ในฎีกาที่ 518/2545[14]

4. ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน

ข้อมูลคอมพิวเตอร์ใดที่เป็นระบบที่มีวิธีการป้องกันการเข้าถึงโดยเฉพาะนั้น ผู้ร่างกฎหมายเห็นว่าเป็นข้อเท็จจริงที่จะต้องนำสืบเป็นเรื่องๆ ไปเช่นเดียวกับมาตรการป้องกันระบบคอมพิวเตอร์ เมื่อมิได้หวงแหนแล้วกฎหมายจึงสันนิษฐานว่าข้อมูลคอมพิวเตอร์นั้นไม่เป็นความลับ เจ้าของข้อมูลไม่ขัดขวางหากจะมีผู้หนึ่งผู้ใดเข้าถึงข้อมูลคอมพิวเตอร์ของตน

ซึ่งการป้องกันโดยทั่วไปที่มีใช้อยู่ในปัจจุบันนั้น คือ ในส่วนของระบบคอมพิวเตอร์ จะมีวิธีการป้องกัน โดยแบ่งเป็น การป้องกันโดยรหัสผ่าน การป้องกันโดยการ์ด การป้องกันโดยกุญแจ หรือ การป้องกันโดยระบบไบโอเมตริกซ์ (เช่น การแสกนนิ้ว หรือม่านตา) ส่วนการป้องกันข้อมูลคอมพิวเตอร์นั้นปัจจุบันมีการป้องกันโดยรหัสผ่าน

หรือการคำนวณ ส่วนข้อเท็จจริง หมายความว่า ข้อความแห่งเหตุการณ์ที่เป็นมาหรือที่เป็นอยู่จริง ข้อความหรือเหตุการณ์ที่จะต้องวินิจฉัยว่าเท็จหรือจริง ดังนั้นข้อมูลจึงไม่นับเป็นวัตถุมีรูปร่าง สำหรับตัวอักษร ภาพ แผนผัง และตราสารเป็นเพียงสัญลักษณ์ที่ถ่ายทอดความหมายของข้อมูลออกจากแผ่นบันทึกข้อมูล โดยอาศัยเครื่องคอมพิวเตอร์ มิใช่รูปร่างของข้อมูล เมื่อประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 137 บัญญัติว่า ทรัพย์ หมายความว่า วัตถุมีรูปร่าง ข้อมูลในแผ่นบันทึกข้อมูลจึงไม่ถือเป็นทรัพย์ การที่จำเลยนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลจากแผ่นบันทึกข้อมูลของโจทก์ร่วม จึงไม่เป็นความผิดฐานลักทรัพย์

[14] คำพิพากษาฎีกาที่ 518/2545 เมื่อเครื่องคอมพิวเตอร์ได้รับความเสียหายต้องป้อนถ่ายข้อมูลใหม่แม้ผู้ป้อนถ่ายข้อมูลที่ถูกกลบเข้าเครื่องคอมพิวเตอร์ที่ขนย้ายจะเป็นพนักงานประจำของจำเลย แต่การกระทำดังกล่าวเนื่องจากผลการกระทำของโจทก์ที่ทำให้จำเลยเสียหายเป็นแรงงานของพนักงานนั้นไป จำเลยจึงเรียกให้โจทก์ชำระค่าเสียหายส่วนนี้ตามสัญญาจ้างขนย้ายเครื่องใช้สำนักงานระหว่างโจทก์จำเลยได้

ส่วนการป้องกันทางด้านระบบเครือข่ายนั้น โดยปกติเครื่องคอมพิวเตอร์จะมีระบบป้องกันที่เรียกว่า firewall[15] ซึ่งหากแปลตามศัพท์จะหมายถึง กำแพงไฟ ซึ่งทางด้านคอมพิวเตอร์แล้วหมายถึงการป้องกันการบุกรุกโดยการสร้างกำแพง โดย Firewall เป็นเครื่องมือที่ใช้สำหรับป้องกันระบบ Network (เครือข่าย) จากการสื่อสารทั่วไปที่ถูกบุกรุกจากผู้ที่ไม่มีสิทธิ เป็นเรื่องเกี่ยวกับการรักษาความปลอดภัยในระบบ Network หรือระบบเครือข่าย การป้องกันโดยใช้ระบบ Firewall นี้จะเป็นการกำหนดกฎเกณฑ์ในการควบคุมการเข้าออก หรือการควบคุมการรับส่งข้อมูล ในระบบเครือข่าย ดังนั้นการเปิด Firewall จึงมาตรการป้องกันทางเครือข่ายอย่างหนึ่ง Firewall เป็นอุปกรณ์ที่ทำหน้าที่รักษาความปลอดภัยของระบบเครือข่ายครับ จะติดตั้งไว้ที่ปากทางออกที่เชื่อมต่อกับอินเทอร์เน็ต Firewall[16] จะทำหน้าที่ตรวจสอบข้อมูลที่วิ่งผ่านเข้าออกเครือข่ายว่าเป็นข้อมูลได้รับอนุญาตหรือไม่ และคอยตรวจสอบว่ามีใครพยายามเจาะระบบหรือไม่[17] โดยหน้าที่สำคัญของ Firewall นั้นได้แก่

1. ป้องกันไม่ให้เครื่องคอมพิวเตอร์ภายนอกเครือข่ายเรียกดูข้อมูลภายในหน่วยงาน
2. กำหนดว่าเครื่องคอมพิวเตอร์เครื่องใดสามารถรับส่งข้อมูลกับเครื่องคอมพิวเตอร์เครื่องอื่นที่อยู่นอกเครือข่ายได้
3. ตรวจสอบไวรัสไม่ให้ผ่านเข้ามาในระบบ
4. ตรวจสอบการบุกรุกระบบเครือข่าย
5. กำหนดช่วงเวลาการใช้งานเครือข่าย

---

[15]Firewall เครื่องมือป้องกันการบุกรุก, [Online] แหล่งที่มา : www.it-guides.com/lesson/network8.html [วันที่ 15 มกราคม 2551]

[16] Firewall จะมีสองแบบคือแบบที่เป็นซอฟต์แวร์และแบบที่ฮาร์ดแวร์ แบบที่เป็นซอฟต์แวร์นั้นบริษัทจะขายเฉพาะซอฟต์แวร์เราจะต้องเอามาติดตั้งบนเครื่องคอมพิวเตอร์เองหรือเราจะให้บริษัทเขาติดตั้งมาให้เลยก็ได้ ส่วน Firewall ที่เป็นฮาร์ดแวร์นั้นจะเป็นกล่องสำเร็จรูปมาเลยเรียบร้อยพร้อมติดตั้งใช้งานได้ทันที

[17] ปิยะ สมบุญสำราญ, “แนวการจัดการระบบรักษาความปลอดภัยสำหรับ E-Business (ตอนที่ 16),” [Online] แหล่งที่มา : http://se-ed.net/internet/Article%5CE-Business%5CE-Biz16.htm [วันที่ 15 มกราคม 2551]

ดังนั้นการเปิด Firewall จึงเป็นการป้องกันการเข้าถึง ซึ่งในกรณีที่มีการปิด Firewall แล้วอาจถึงได้ว่าเจ้าของเครื่องคอมพิวเตอร์นั้น ไม่มีจุดประสงค์จะป้องกันการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ของตนแต่อย่างใด ดังนั้นการเข้าถึงจึงไม่เป็นความผิด

ส่วนองค์ประกอบในแง่ "มาตรการนั้นมิได้มีไว้สำหรับตน" หมายถึง การป้องกันนั้นหากผู้ที่เข้าถึงมีอำนาจที่จะเข้าไปได้ผู้นั้นก็ไม่มีความผิด เช่นลูกจ้างสามารถเข้าถึงข้อมูลของบริษัทนายจ้างได้เนื่องจากมีอำนาจหน้าที่ปฏิบัติงานในส่วนนั้น

ความผิดในการล่วงรู้มาตรการการป้องกันโดยมิชอบและนำไปเปิดเผย (มาตรา 6)

มาตรา 6 ได้กำหนดหลักเกณฑ์ความรับผิดทางอาญาในการล่วงรู้มาตรการป้องกันโดยมิชอบและนำไปเปิดเผยว่า "ผู้ใดล่วงรู้มาตรการการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ"

องค์ประกอบความผิดมาตรา 6 นี้ อาจแยกได้เป็น

1. **ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ**

หมายความว่าระบบคอมพิวเตอร์นั้นมีมาตรการการเข้าถึง เช่น มีการลงทะเบียน username และ password หรือมีวิธีการอื่นใดที่จัดขึ้นเป็นการเฉพาะ การที่จะเป็นความผิดตามมาตรานี้ต้องเป็นเรื่องที่ผู้กระทำล่วงรู้ ซึ่งการล่วงรู้นั้นจะต้องได้มาโดยชอบหรือไม่ชอบไม่สำคัญ[18]

2. **นำไปเปิดเผยโดยมิชอบ**

---

[18] นายพรเพชร วิชิตชลชัย, "คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550," หน้า 10.

หมายความว่า เพียงแต่นำมาตรการนั้นเปิดเผยแก่ผู้หนึ่งผู้ใดหรือหลายคนก็เข้าองค์ประกอบความผิดแล้ว เมื่อเปิดเผยแล้วผู้ใดจะทราบหรือนำไปใช้หรือไม่ ไม่สำคัญ[19]

3. ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

เป็นองค์ประกอบความผิดอีกประการหนึ่งที่ต้องพิจารณาด้วยว่าเป็นการเปิดเผยนั้นอยู่ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือไม่ หากเป็นเรื่องที่ไม่น่าจะทำให้ผู้ใดเสียหายก็ไม่มีความผิด ซึ่งองค์ประกอบนี้เหมือนกับองค์ประกอบในความผิดฐานปลอมแปลงเอกสาร ซึ่งการที่จะพิจารณาว่าน่าจะเกิดความเสียหายแก่บุคคลอื่นหรือไม่เป็นหน้าที่ของศาลที่จะต้องพิจารณา และไม่จำเป็นที่จะต้องเกิดความเสียหายก่อนเพียงแค่แน่จะเกิดความเสียหายก็เพียงพอแล้ว

4.3 องค์ประกอบภายในของการกระทำผิด

การกระทำที่ต้องรับโทษตามกฎหมายอาญานั้น นอกจากจะต้องครบองค์ประกอบภายนอก ยังจะต้องพิจารณาถึงองค์ประกอบภายในด้วยเช่นกัน การกระทำที่ปรากฏออกมาอย่างเดียวกันแต่ผู้กระทำอาจมีความรับผิดแตกต่างกันออกไปขึ้นอยู่กับเจตนาของผู้กระทำความผิดเอง พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ก็เป็นกฎหมายอาญาอย่างหนึ่ง จึงจำต้องพิจารณาถึงองค์ประกอบภายในในการพิจารณาการกระทำความผิดในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ด้วยเช่นกัน โดยองค์ประกอบภายในนั้น ตามกฎหมายแยกได้เป็นการกระทำโดยเจตนา และประมาท ตามประมวลกฎหมายอาญา มาตรา 59 โดยผู้เขียนจะขอเริ่มพิจารณาจากเจตนาก่อน ดังนี้

4.3.1 การกระทำโดยเจตนา

ประมวลกฎหมายอาญา มาตรา 59 บัญญัติว่า บุคคลจะต้องรับผิดในทางอาญาก็ต่อเมื่อได้กระทำโดยเจตนา เว้นแต่จะได้กระทำโดยประมาท ในกรณีที่กฎหมายบัญญัติให้ต้องรับผิดเมื่อได้กระทำโดยประมาท หรือเว้นแต่ในกรณีที่กฎหมายบัญญัติไว้โดยแจ้งชัดให้ต้องรับผิดแม้ได้กระทำโดยไม่มีเจตนา

---

[19] เรื่องเดียวกัน,

กระทำโดยเจตนา ได้แก่ กระทำโดยรู้สำนึกในการที่กระทำและในขณะเดียวกันผู้กระทำ ประสงค์ต่อผลหรือย่อมเล็งเห็นผลของการกระทำนั้น

ถ้าผู้กระทำมิได้รู้ข้อเท็จจริงอันเป็นองค์ประกอบของความผิดจะถือว่าผู้กระทำประสงค์ต่อผล หรือย่อมเล็งเห็นผลของการกระทำนั้นมิได้

กระทำโดยประมาท ได้แก่ กระทำความผิดมิใช่โดยเจตนาแต่กระทำโดยปราศจากความระมัดระวังซึ่งบุคคลในภาวะเช่นนั้น จักต้องมีตามวิสัยและพฤติการณ์และผู้กระทำอาจใช้ความระมัดระวัง เช่นว่านั้นได้แต่หาได้ใช้ให้เพียงพอไม่

การกระทำ ให้หมายความรวมถึง การให้เกิดผลอันหนึ่งอันใดขึ้นโดยงดเว้นการที่จักต้องกระทำ เพื่อป้องกันผลนั้นด้วย

เมื่อพิจารณาจากประมวลกฎหมายอาญา มาตรา 59 แล้ว จะเห็นได้ว่าโดยหลักแล้วองค์ประกอบภายในของความผิดอาญาแต่ละมาตรา คือ เจตนา ดังนั้นบุคคลที่กระทำความผิดจะต้องรับโทษต่อเมื่อได้กระทำโดยเจตนา อย่างไรก็ตาม สำหรับความผิดบางมาตราองค์ประกอบภายใน คือ ประมาท ซึ่งถือว่าเป็นข้อยกเว้น นอกจากนั้นในความผิดบางประเภทไม่ต้องการองค์ประกอบภายในเลย กล่าว แม้ผู้กระทำจะไม่เจตนาและไม่ประมาท ผู้กระทำก็ต้องรับผิด แต่กรณีจะต้องรับผิดเนื่องจากการกระทำโดยประมาทนั้นต้องเป็นกรณีที่กฎหมายบัญญัติไว้โดยชัดแจ้งว่าแม้จะกระทำโดยประมาทก็ต้องรับผิด รวมถึงในกรณีที่ไม่เจตนาและไม่ประมาทก็เช่นกัน ต้องมีกฎหมายบัญญัติไว้ว่าแม้ไม่เจตนาและไม่ประมาทก็ต้องรับผิด มิฉะนั้นหากไม่มีเจตนาที่จะกระทำการฝ่าฝืนกฎหมายแล้ว ก็ถือว่าไม่มีเจตนากระทำความผิด

เมื่อพิจารณาถึงบทบัญญัติเกี่ยวกับเจตนาในกฎหมายอาญาแล้ว และพิจารณาดูความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะเห็นได้ว่าความผิดในการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ และการล่วงรู้มาตรการป้องกันแล้วนำไปเปิดเผยโดยมิชอบนั้นเป็นการบัญญัติกฎหมายโดยทั่วไป ไม่มีถ้อยคำใดเป็นพิเศษ จึงต้องถือตามหลักกฎหมายอาญาตามมาตรา 59 ว่า ผู้กระทำจะมีความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5) หรือมีความผิดฐานล่วงรู้มาตรการป้องกันแล้วนำไปเผยแพร่โดยมิชอบ (มาตรา 6) หรือมีความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7) นั้น ต้องเป็นการกระทำโดยเจตนาเท่านั้น

โดยคำว่า เจตนา ในมาตรา 59 นั้น คำว่า เจตนาไม่ได้ระบุว่าต้องเป็นเจตนาชั่วร้าย (mens rea or vicious will) ซึ่งเป็นพื้นฐานของเจตนาในกฎหมายอาญาเลย[20] ดังนั้น เจตนาตามมาตรา 59 นี้ เป็นเพียงเจตนากระทำความผิด (criminal intention) ตามที่กฎหมายบัญญัติซึ่งเป็นความไม่ดีอยู่ในตัวอยู่แล้ว เพราะกฎหมายมีไว้เพื่อเป็นระเบียบของชุมชน และต้องแยกออกจากเรื่องของมูลเหตุชักจูงใจ (motive, mobile) อันเป็นความสำนึกส่วนตัว โดยทั่วไปไม่มีผลในทางกฎหมาย เช่น จำเลยรับจ้างสีข้าวโดยคิดค่าจ้างเพียงเล็กน้อย เพื่อให้ชาวบ้านมีข้าวสารกิน ไม่เป็นข้อแก้ตัวให้พ้นความผิดตามพระราชบัญญัติค้าข้าวที่ต้องขออนุญาตก่อน[21] ดังนั้นในความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์โดยมิชอบก็เช่นเดียวกัน ตามบทบัญญัติของกฎหมายแล้วก็ต้องพิจารณาเพียงว่าการกระทำความผิดดังกล่าวมีเจตนาที่จะเข้าถึงโดยมิชอบหรือไม่เท่านั้น ไม่จำเป็นต้องพิจารณาถึงมูลเหตุชักจูงแต่อย่างใด ถึงแม้ผู้ที่เข้าถึงจะไม่มีเจตนาร้ายที่จะแก้ไขเปลี่ยนแปลงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยอ้างว่าเข้าไปดูอย่างเดียวก็ไม่เป็นข้อแก้ตัวให้พ้นจากความผิดในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ได้

4.3.2 ประมาท

ตามประมวลกฎหมายอาญา มาตรา 59 บัญญัติว่า กระทำโดยประมาท ได้แก่ กระทำความผิดมิใช่โดยเจตนาแต่กระทำโดยปราศจากความระมัดระวังซึ่งบุคคลในภาวะเช่นนั้นจักต้องมีตามวิสัยและพฤติการณ์และผู้กระทำอาจใช้ความระมัดระวัง เช่นว่านั้นได้แต่หาได้ใช้ให้เพียงพอไม่ ซึ่งตามหลักประมวลกฎหมายอาญาแล้ว การกระทำใดที่ไม่มีกฎหมายกำหนดให้ต้องรับผิดในการกระทำโดยประมาท แม้ผู้กระทำผิดกระทำครบองค์ประกอบภายนอกแล้วหากแต่เป็นการกระทำโดยประมาท ผู้กระทำก็ไม่ต้องรับผิด เพราะไม่มีกฎหมายบัญญัติให้เป็นความผิดแต่อย่างใด ในเรื่องความรับผิดในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ก็เช่นกัน เมื่อบทบัญญัติทางกฎหมายไม่ได้กำหนดให้การกระทำโดยประมาทในการเข้าถึงระบบคอมพิวเตอร์

---

[20] Miller, Criminal Law, p. 744 อ้างถึงใน ทวีเกียรติ มีนะกนิษฐ, กฎหมายอาญา หลักและปัญหา (กรุงเทพมหานคร : สำนักพิมพ์นิติธรรม, 2545), หน้า 97.

[21] คำพิพากษาฎีกาที่ 245/2512 อ้างถึงใน ทวีเกียรติ มีนะกนิษฐ, กฎหมายอาญา หลักและปัญหา (กรุงเทพมหานคร : สำนักพิมพ์นิติธรรม, 2545),หน้า 97.

และข้อมูลคอมพิวเตอร์เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่อย่างใด ดังนั้นการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์โดยประมาทจึงไม่เป็นความผิด

4.4 ความผิดสำเร็จ พยายาม ตระเตรียม

เมื่อมีการกระทำความผิดอาญาเกี่ยวกับการการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์เกิดขึ้น อาจพิจารณาขั้นตอนของการกระทำย้อนหลังไปได้ดังนี้

1. แดงคิดที่จะเจาะระบบคอมพิวเตอร์ของดำ
2. แดงตกลงใจที่จะเจาะระบบคอมพิวเตอร์ของดำ
3. แตงตระเตรียมกระทำการเจาะระบบคอมพิวเตอร์ของดำ
4. แดงลงมือเจาะระบบคอมพิวเตอร์ของดำ
5. การกระทำของแดงเป็นผลสำเร็จ แตงสามารถเข้าถึงระบบคอมพิวเตอร์ของดำได้

จะเห็นได้ว่าจากขั้นตอนการกระทำทั้งหมดของแดง กฎหมายไม่เอาโทษแดงในการที่แดงคิดและตกลงในที่จะกระทำความผิดตามข้อ 1 และข้อ 2 เพราะเป็นเรื่องที่อยู่ภายในจิตใจของบุคคลผู้นั้นเอง แม้ผู้นั้นจะมีจิตใจชั่วร้าย แต่หากยังไม่มีการกระทำใดๆ ออกมาแล้ว กฎหมายก็ยังไม่ลงโทษ ส่วนในการตระเตรียมกระทำความผิดตามข้อ 3 นั้นถือได้ว่าเป็นการแสดงออกซึ่งการกระทำแล้ว แต่โดยหลักกฎหมายก็ยังไม่ลงโทษเว้นแต่จะมีกฎหมายกำหนดให้การตระเตรียมนั้นเป็นความผิด เช่น การตระเตรียมเพื่อวางเพลิงเผาทรัพย์ เป็นต้น ดังนั้นโดยปกติแล้วกฎหมายจะลงโทษการกระทำที่เข้าขั้น “ลงมือ” เป็นต้นไป เหตุผลก็คือ การกระทำก่อนถึงขั้น “ลงมือ” ซึ่งเรียกกันว่า “ตระเตรียม” นั้น “ยังไม่เป็นการแสดงออกที่น่าเชื่อถือได้อย่างเพียงพอถึงจิตใจที่จะเป็นอาชญากรอย่างแน่นอน”[22] ดังนั้นตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ก็เช่นเดียวกันเมื่อกฎหมายไม่ได้กำหนดให้การตระเตรียมในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์เป็นความผิด ดังนั้นการตระเตรียมดังกล่าวจึงไม่เป็นความผิดทางอาญา

---

[22] Andenaes, The General Part of the Criminal Law of Norway, p. 288 อ้างถึงใน เกียรติขจร วัจนะสวัสดิ์, คำอธิบายกฎหมายอาญา ภาค 1 ฉบับพิมพ์ครั้งที่ 9 (กรุงเทพมหานคร : จิรรัชการพิมพ์, 2549) หน้า 522.

กฎหมายจะลงโทษผู้กระทำผิดก็ต่อเมื่อการกระทำนั้นเลยขั้นตระเตรียมเข้าขั้นลงมือกระทำความผิดแล้ว ซึ่งถือว่าเป็นการพยายามกระทำความผิด ซึ่งการพยายามกระทำความผิดนี้ ปรากฏอยู่ในประมวลกฎหมายอาญา มาตรา 80 และมาตรา 81

โดยในประมวลกฎหมายอาญา มาตรา 80 วรรคแรก บัญญัติว่า “ผู้ใดลงมือกระทำความผิดแต่กระทำไปไม่ตลอด หรือกระทำไปตลอดแล้ว แต่การกระทำนั้นไม่บรรลุผล ผู้นั้นพยายามกระทำความผิด”

กรณีที่จะถือว่าเป็นการพยายามกระทำความผิดได้ จะต้องประกอบด้วยหลักเกณฑ์ 3 ประการ ดังนี้

1. ผู้กระทำจะต้องมีเจตนากระทำความผิด และ
2. ผู้กระทำจะต้องกระทำการเพื่อให้บรรลุตามเจตนาอันเป็นการกระทำที่เลยขั้นตระเตรียม กล่าวคือถึงขั้นลงมือกระทำความผิดแล้ว
3. ผู้กระทำกระทำไปไม่ตลอด หรือกระทำไปตลอดแล้วแต่การกระทำนั้นไม่บรรลุผล

ในประมวลกฎหมายอาญา มาตรา 81 วรรคหนึ่ง บัญญัติว่า “ผู้ใดกระทำการโดยมุ่งต่อผลซึ่งกฎหมายบัญญัติเป็นความผิดแต่การกระทำนั้นไม่สามารถจะบรรลุผลได้อย่างแน่แท้ เพราะเหตุปัจจัยซึ่งใช้ในการกระทำ หรือเหตุแห่งวัตถุที่มุ่งหมายกระทำต่อ ให้ถือว่าผู้นั้นพยายามกระทำความผิด แต่ให้ลงโทษไม่เกินกึ่งหนึ่งที่กฎหมายกำหนดไว้สำหรับความผิดนั้น”

หลักในมาตรา 81 นี้ เรียกกันทั่วไปว่า “การพยายามกระทำความผิดซึ่งเป็นไปไม่ได้อย่างแน่แท้” ซึ่งมีหลักเกณฑ์ดังนี้

1. ผู้กระทำจะต้องมีเจตนากระทำความผิด และ
2. ผู้กระทำจะต้องกระทำการเพื่อให้บรรลุผลตามเจตนาอันเป็นการกระทำที่เลยขั้นตระเตรียม กล่าวคือถึงขั้นลงมือกระทำความผิดแล้ว และ
3. ผู้กระทำกระทำไปไม่ตลอด หรือกระทำไปตลอดแล้วแต่การกระทำนั้นไม่บรรลุผล
4. การกระทำนั้นไม่สามารถจะบรรลุผลได้อย่างแน่แท้ เพราะเหตุปัจจัยซึ่งใช้ในการกระทำหรือเหตุแห่งวัตถุที่มุ่งหมายกระทำต่อ

เมื่อพิจารณาจากประมวลกฎหมายอาญาเกี่ยวกับการพยายามกระทำความผิดแล้ว สิ่งที่จะต้องพิจารณาคือความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นจะมีความผิดฐานพยายามกระทำความผิดดังกล่าวได้หรือไม่ เนื่องจากแม้การพยายามกระทำความผิดตามกฎหมายไทยจะมีลักษณะเป็นบททั่วไปที่สามารถนำไปปรับใช้ได้กับทุกฐานความผิดทางอาญา แต่ก็มีในบางฐานความผิดที่โดยลักษณะการกระทำความนั้นไม่สามารถมีความผิดฐานพยายามได้[23] เช่น

1) การกระทำความผิดฐานละเว้น ตามม.374

2) การกระทำโดยประมาทฐานต่างๆ เช่น ม.205 ม.225 ม.239 ม.291 ม.300 ม.311 ม.390

3) ความผิดที่ไม่ต้องการผล เช่น ม.154 ม.156 ม.157 162(3) ม.168 ม.169 ม.170 ม.171 ม.216 ม.374 เป็นต้น นอกจากหลักดังกล่าวข้างต้นแล้ว ถ้าหากว่าความผิดใดที่ต้องการผล ความผิดนั้นๆย่อมมีพยายามกระทำความผิด นั่นเอง และเมื่อการกระทำโดยงดเว้น เป็นการกระทำที่ต้องการผล จึงมีการพยายามกระทำความผิดได้

4) ความผิดเป็นตัวการ ก็ดี ความผิดเป็นผู้ใช้ก็ดี หรือ ความผิดเป็นผู้สนับสนุนก็ดี ก็จะไม่มีการพยายามกระทำผิดเช่นกัน

5) ความผิดฐานทำร้ายร่างกายได้รับอันตรายสาหัส ตามม.297 ก็เป็นอีกฐานความผิดหนึ่งที่ไม่มีพยายามกระทำผิด

6) ความผิดฐานฆ่าคนตายโดยไม่เจตนา ตามม.290 ก็ไม่มีพยายามกระทำความผิดเช่นกัน

7) ความผิดฐานชุลมุนต่อสู้ ตามม.294 กับม.299 ก็ไม่มีการพยายามกระทำความผิดด้วยเช่นเดียวกัน

---

[23] แหล่งที่มา : www.thaijustice.com/webboard.asp?sub=0&id=598428 [วันที่ 15 มกราคม 2551]

8) ความผิดที่มีองค์ประกอบว่า " น่าจะเสียหาย หรือ อาจเสียหาย " ไม่มีการพยายามกระทำความผิดเช่นเดียวกัน เช่น ม.137 ม.172 ม.188 ม.220 - ม. 221 ม.225 - ม.231 ม.233 - ม.234 ม.236 - ม237 ม.264 ม.267 - ม.269 ม. 307 ม.322 ม.323 เป็นต้น

ดังนั้นสิ่งที่ต้องนำมาพิจารณาในความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์โดยมิชอบ คือ ความผิดดังกล่าวต้องการผลหรือไม่ เพราะหากการกระทำผิดดังกล่าวไม่ต้องการผลแล้วก็ไม่สามารถมีการพยายามกระทำความผิดได้ ซึ่งหากพิจารณาจากตัวบทของมาตรา 5 และมาตรา 7 แล้ว จะเห็นได้ว่า การเข้าถึงนั้นเป็นความผิดที่ต้องการผลกล่าวคือต้องมีการเข้าถึงเกิดขึ้น ดังนั้นจึงเป็นความผิดสำเร็จ ดังนั้นจึงมีความผิดฐานพยายามเข้าถึงโดยมิชอบได้

4.5 ตัวการ ผู้ใช้ ผู้สนับสนุน

ในกรณีที่มีผู้เกี่ยวข้องในการกระทำความผิดตั้งแต่ 2 คนขึ้นไป โดยการที่มีผู้เกี่ยวข้องในการกระทำความผิดตั้งแต่ 2 คนขึ้นไปนี้ ผู้เกี่ยวข้องจะต้องมีความรับผิดมากน้อยเพียงใด ก็ขึ้นอยู่กับการกระทำของตน ประมวลกฎหมายอาญาได้บัญญัติเกี่ยวกับเรื่องนี้ไว้ในมาตรา 83, 84, 85 และ 86 ซึ่งพอสรุปได้ดังนี้

1. ผู้ที่ได้ร่วมกระทำความผิดด้วยกัน เรียกว่า ตัวการ
2. ผู้ที่ก่อให้ผู้อื่นกระทำความผิด เรียกว่า ผู้ใช้
3. ผู้ที่ช่วยเหลือให้ความสะดวกในการที่ผู้อื่นกระทำความผิด เรียกว่า ผู้สนับสนุน

ซึ่งในความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้น ผู้ที่เกี่ยวข้องอาจเป็นได้ทั้งตัวการ ผู้ใช้ หรือผู้สนับสนุนในการกระทำผิดฐานเข้าถึงโดยมิชอบ

4.6 เหตุเพิ่มโทษ

ในการกระทำความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์โดยมิชอบนั้น เป็นความผิดพื้นฐานที่สามารถนำไปสู่การประกอบความผิดอื่นๆ ซึ่งก่อให้เกิดความเสียหายเป็นอย่างมาก เช่น การจารกรรมข้อมูล การก่อกวนรวมไปถึงการก่อวินาศกรรม การเปลี่ยนแปลงข้อมูล จะเห็นได้ว่าแม้ว่าการกระทำดังกล่าวเหมือนจะไม่น่า

ก่อให้เกิดความเสียหายได้เป็นจำนวนมาก หากแต่ผลกระทบนั้นอาจเสียหายมากกว่าที่คาดคิด การกระทำดังกล่าวอาจก่อให้เกิดอันตรายถึงชีวิตได้ เช่น การเปลี่ยนแปลงรายการยาที่ให้แก่ผู้ป่วยอาจทำให้ผู้ป่วยเสียชีวิตได้ แต่อย่างไรก็ตามเนื่องจากบทบัญญัติของกฎหมายว่าการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดหลักเกณฑ์เกี่ยวกับความผิดได้เป็นการทั่วไป ไม่มีบทหนักหรือบทเพิ่มโทษ ดังนั้นแม้จะทำให้เกิดความเสียหายมากมายเพียงใดก็ไม่สามารถที่จะเพิ่มโทษได้ เช่น การบุกรุกเข้าไปในระบบคอมพิวเตอร์ของบุคคลทั่วไปเพื่อแอบอ่านจดหมายส่วนตัว การบุกรุกเข้าไปในระบบคอมพิวเตอร์ของบริษัทเอกชนเพื่อแอบดูข้อมูลทางการค้า หรือจะบุกรุกเข้าไปในระบบคอมพิวเตอร์ของทางการทหาร ก็ไม่มีความแตกต่างกันแต่อย่างใด หากแต่อาจสามารถเพิ่มโทษได้ตามประมวลกฎหมายอาญามาตรา 92[24] ซึ่งอาจเพิ่มโทษได้หนึ่งในสามหากผู้กระทำผิดกระทำผิดอีกภายในระยะเวลาที่ต้องรับโทษอยู่ หรือภายในเวลาห้าปีนับแต่วันพ้นโทษ ซึ่งเป็นบทเพิ่มโทษทั่วไป แต่ไม่สามารถนำมาตรา 93 มาเพิ่มโทษได้เนื่องจากไม่ใช่โทษในอนุมาตราที่กำหนดไว้ในมาตรา 93[25] ของประมวลกฎหมายอาญาแต่อย่างใด

---

[24] ประมวลกฎหมายอาญามาตรา 92 บัญญัติว่า “ผู้ใดต้องคำพิพากษาถึงที่สุดให้ลงโทษจำคุกถ้าและได้ กระทำความผิดใดๆ อีก ในระหว่างที่ยังจะต้องรับโทษอยู่ก็ดี ภายในเวลาห้าปีนับแต่วันพ้นโทษก็ดี หากศาลจะพิพากษาลงโทษครั้งหลัง ถึงจำคุกก็ให้เพิ่มโทษที่จะลงแก่ผู้นั้นหนึ่งในสามของโทษ ที่ศาลกำหนด สำหรับความผิดครั้งหลัง”

[25] ประมวลกฎหมายอาญามาตรา 93 บัญญัติว่า “ผู้ใดต้องคำพิพากษาถึงที่สุดให้ลงโทษจำคุก ถ้าและ ได้กระทำความผิดอย่างหนึ่งอย่างใดที่จำแนกไว้ในอนุมาตรา ต่อไปนี้ ซ้ำในอนุมาตราเดียวกันอีกในระหว่างที่ยังจะต้องรับโทษอยู่ก็ดี ภายในเวลาสามปีนับแต่วันพ้นโทษก็ดี ถ้าความผิดครั้งแรกเป็นความผิด ซึ่งศาลพิพากษาลงโทษจำคุกไม่น้อยกว่าหกเดือน หากศาลจะพิพากษาลงโทษครั้งหลังถึงจำคุกก็ให้เพิ่มโทษที่จะลง

บทที่ 5

วิเคราะห์ปัญหาเกี่ยวกับความรับผิดทางอาญาในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ก่อนที่จะมีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่มีการบัญญัติความผิดเกี่ยวกับการเข้าถึงโดยมิชอบนั้น การกระทำความผิดเกี่ยวกับการเข้าถึงโดยมิชอบในคอมพิวเตอร์ไม่สามารถที่จะนำตัวผู้กระทำมาลงโทษได้ เนื่องจากไม่มีกฎหมายบัญญัติว่าการกระทำดังกล่าวเป็นความผิด และกฎหมายอาญาที่มีอยู่ในขณะนั้นก็ไม่สามารถนำมาปรับใช้ได้ โดยเราไม่อาจกล่าวว่าการเข้าถึงโดยมิชอบเป็นความผิดฐานบุกรุกได้ และการขโมยข้อมูลคอมพิวเตอร์ก็ไม่เป็นความผิดฐานลักทรัพย์แต่อย่างใด[1] จึงต้องมีการบัญญัติกฎหมายใหม่ขึ้นมารองรับการกระทำความผิดดังกล่าวขึ้น

ความรับผิดทางอาญาในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น เป็นกฎหมายใหม่ที่เพิ่งผ่านการประกาศในราชกิจจานุเบกษามีผลบังคับใช้เป็นกฎหมาย จึงยังเป็นกฎหมายใหม่ที่ยังไม่มีคดีขึ้นสู่ศาลเนื่องจากกระทำความผิดในกรณีดังกล่าว นอกจากนี้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ยังเป็นกฎหมายที่เกี่ยวข้องกับเทคโนโลยีและ

---

[1]คำพิพากษาฎีกาที่ 5161/2547 ข้อมูล ตามพจนานุกรมให้ความหมายว่า ข้อเท็จจริง หรือ สิ่งที่ถือหรือยอมรับว่าเป็นข้อเท็จจริง สำหรับใช้เป็นหลักอนุมานหาความจริงหรือการคำนวณ ส่วนข้อเท็จจริง หมายความว่า ข้อความแห่งเหตุการณ์ที่เป็นมาหรือที่เป็นอยู่จริง ข้อความหรือเหตุการณ์ที่จะต้องวินิจฉัยว่าเท็จหรือจริง ดังนั้นข้อมูลจึงไม่นับเป็นวัตถุมีรูปร่าง สำหรับตัวอักษร ภาพ แผนผัง และตราสารเป็นเพียงสัญลักษณ์ที่ถ่ายทอดความหมายของข้อมูลออกจากแผ่นบันทึกข้อมูลโดยอาศัยเครื่องคอมพิวเตอร์ มิใช่รูปร่างของข้อมูล เมื่อประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 137 บัญญัติว่า ทรัพย์ หมายความว่า วัตถุมีรูปร่าง ข้อมูลในแผ่นบันทึกข้อมูลจึงไม่ถือเป็นทรัพย์ การที่จำเลยนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลจากแผ่นบันทึกข้อมูลของโจทก์ร่วม จึงไม่เป็นความผิดฐานลักทรัพย์

ศาสตร์ทางคอมพิวเตอร์ซึ่งมีความยุ่งยากซับซ้อนแต่ขณะเดียวกันก็เป็นที่นิยมใช้กันอยู่ทั่วไป เนื่องจากความสะดวกสบายในการใช้คอมพิวเตอร์ในด้านต่างๆ ดังนั้น กฎหมายนี้จึงมีผลกระทบต่อบุคคลเป็นวงกว้างโดยเฉพาะกลุ่มที่ใช้คอมพิวเตอร์อยู่เป็นประจำ โดยคนกลุ่มหนึ่งอาจไม่พอใจที่จะมีกฎเกณฑ์มาบังคับหลังจากที่คิดว่าในระบบคอมพิวเตอร์หรือระบบเครือข่ายเป็นที่ที่มีสิทธิเสรีภาพ ไม่มีการจำกัดด้วยกฎเกณฑ์มาก่อน จึงอาจต้องใช้เวลาในการปรับตัว แต่ขณะเดียวกันคนอีกกลุ่มหนึ่งอาจจะพอใจที่มีการออกกฎระเบียบออกมาควบคุมโลกเสมือนที่นับวันมีแต่จะขยายตัวมากยิ่งขึ้นและก่อให้เกิดการละเมิดสิทธิต่างๆ กันอยู่บ่อยครั้ง

อย่างไรก็ตาม เนื่องจากความผิดที่บัญญัติขึ้นในพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นเรื่องใหม่ในสังคมไทย ทั้งในสิ่งที่กฎหมายมุ่งคุ้มครอง พฤติกรรมและวิธีการกระทำความผิด ตลอดจนการตีความเพื่อบังคับใช้กฎหมายก็เป็นสิ่งที่แตกต่างไปจากประมวลกฎหมายอาญาแทบทั้งสิ้น จึงอาจทำให้พระราชบัญญัติดังกล่าวมีปัญหาที่จะต้องได้รับการพิจารณาอีกมาก โดยหลังจากที่ผู้เขียนเองได้ศึกษาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในเรื่องการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์แล้ว ดังที่ได้แยกแยะและอธิบายองค์ประกอบในความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5) ความผิดในการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7) และความผิดในการล่วงรู้มาตรการป้องกันแล้วนำไปเผยแพร่โดยมิชอบ (มาตรา 6) ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในบทที่ผ่านมาแล้ว ผู้เขียนได้เห็นถึงสิ่งที่เป็นปัญหาเกี่ยวกับความรับผิดทางอาญาในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์โดยมิชอบ โดยอาจแยกพิจารณาได้ดังนี้

5.1 ปัญหาในการบัญญัติกฎหมายเกี่ยวกับการเข้าถึงโดยมิชอบ

5.1.1 การกำหนดฐานความผิดตามกฎหมาย

ในการกำหนดฐานความผิดตามกฎหมายนั้น จะเห็นได้ว่าประเทศไทยได้ใช้รูปแบบของการกำหนดฐานความผิดโดยกำหนดว่าการเข้าถึงที่จะเป็นความผิดทางอาญานั้นต้องประกอบด้วยองค์ประกอบ 3 ส่วน คือ 1. การเข้าถึง 2. การเข้าถึงนั้นต้องเป็นการเข้าถึงโดยมิชอบ และ 3. คอมพิวเตอร์ที่ถูกเข้าถึงนั้นต้องมีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นไม่ได้มีไว้สำหรับตน

จะเห็นได้ว่าองค์ประกอบของการกระทำความผิดในการเข้าถึงนั้นมีมากกว่าองค์ประกอบความรับผิดในการเข้าถึงของประเทศสหรัฐอเมริกา และประเทศอังกฤษที่กำหนดเพียงว่าถ้าเป็นการเข้าถึงโดยปราศจากอำนาจแล้ว การเข้าถึงนั้นย่อมเป็นความผิดในทันทีโดยไม่ต้องพิจารณาว่าต้องมีมาตรการป้องกันหรือไม่ แม้ไม่มีมาตรการป้องกันก็ตาม หากการเข้าถึงโดยปราศจากอำนาจก็เป็นความผิด ในขณะที่ประเทศไทยกำหนดว่าการเข้าถึงโดยมิชอบจะเป็นความผิดได้ต่อเมื่อมีการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีการป้องกันเท่านั้น หากไม่มีการป้องกันแล้ว การกระทำนั้นย่อมไม่เป็นความผิด

แม้ว่าโดยปกติแล้ว การบัญญัติให้การเข้าถึงโดยปราศจากอำนาจจะทำให้หลายฝ่ายกังวลว่าเป็นการใช้กฎหมายอาญาเฟ้อหรือมีขอบเขตที่กว้างเกินสมควร แต่การกำหนดองค์ประกอบความผิดเกี่ยวกับการล่วงล้ำมาตรการป้องกัน (infringing security measures) นั้น ในหลายประเทศ[2]พบว่าเป็นการก่อให้เกิดปัญหาในการลงโทษผู้กระทำความผิดตามมา โดยการใช้ถ้อยคำดังกล่าวส่งเสริมให้ประชาชนใช้ระบบรักษาความปลอดภัยของคอมพิวเตอร์มากขึ้น ในขณะที่รัฐเพิกเฉยที่จะดำเนินคดีกับผู้กระทำความผิด เพราะหากผู้กระทำความผิดได้เข้าไปในคอมพิวเตอร์ที่ไม่ได้ติดตั้งมาตรการป้องกันแล้ว กฎหมายไม่สามารถลงโทษผู้กระทำได้

การกำหนดองค์ประกอบความผิดดังกล่าวนั้นมีผู้ให้ความเห็นว่า[3]การกำหนดให้การล่วงล้ำมาตรการป้องกันเป็นองค์ประกอบความผิดด้วยนั้นไม่เหมาะสม เนื่องจากจะทำให้มีปัญหาในการตีความว่าอะไรคือมาตรการป้องกันการเข้าถึงโดยเฉพาะแล้ว ยังเป็นการผลักภาระทางอ้อมให้ประชาชนต้องเป็นผู้ดูแลรักษาคอมพิวเตอร์ของตนเอง ซึ่งสำหรับประชาชนทั่วไปที่ไม่ได้เป็นผู้ที่มีความรู้ทางด้านกฎหมายคอมพิวเตอร์และคิดว่าตนเองไม่ได้มีสิ่งที่เป็นความลับอยู่ในคอมพิวเตอร์แล้ว ย่อมไม่ได้ทำการป้องกันและไม่อาจทราบได้ว่ากฎหมายจะไม่คุ้มครองตนเองหากว่าไม่มีมาตรการป้องกันการเข้าถึง

---

[2] Judge Stein Schjqlberg and Amanda M. Hubbard, “Background paper harmonizing national and legal approaches on cyber,” [Online] Available from : www.itu.int [วันที่ 7 มกราคม 2551]

[3] Ibid.,

ผู้เขียนเองก็เห็นด้วยกับแนวคิดดังกล่าว เนื่องจากการกำหนดให้มาตรการป้องกันเป็นองค์ประกอบความผิดในเรื่องการเข้าถึงโดยมิชอบอาจจะก่อให้เกิดปัญหาได้ว่า แม้เจ้าของคอมพิวเตอร์จะคิดว่าตนเองไม่มีสิ่งที่เป็นความลับหรือมีค่าทางเศรษฐกิจอยู่ในคอมพิวเตอร์ของตน แต่ก็ไม่ได้หมายความว่าจะยินยอมให้ผู้อื่นเข้ามาใช้หรือดูข้อมูลในคอมพิวเตอร์ของตนเองได้ ซึ่งอาจเปรียบได้กับการออกจากบ้านโดยไม่ได้ใส่กุญแจบ้าน ซึ่งแม้จะเป็นความประมาทของเจ้าของบ้านที่ไม่ดูแลทรัพย์สินของตนให้ดี แต่ไม่ได้หมายความว่าผู้บุกรุกเข้าไปนั้นจะไม่มีความผิดตามกฎหมายแต่อย่างใด เพราะกฎหมายย่อมต้องให้ความคุ้มครองและลงโทษผู้กระทำผิดอย่างเหมาะสม โดยในกรณีเช่นนี้ การบัญญัติกฎหมายอาจทำได้โดยกำหนดองค์ประกอบความรับผิดของกฎหมายเพิ่มขึ้น โดยอาจกำหนดว่าต้องมีเจตนาที่จะได้ไปซึ่งข้อมูลคอมพิวเตอร์หรือมีเจตนาไม่สุจริต หรือเกี่ยวกับระบบคอมพิวเตอร์ที่เกี่ยวข้องกับระบบคอมพิวเตอร์อื่นแทนการกำหนดองค์ประกอบเรื่องมาตรการป้องกัน[4]

5.1.2 **การกำหนดเหตุเพิ่มโทษ**

ดังที่กล่าวมาแล้วในบทที่ 4 ว่า การกระทำความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์โดยมิชอบนั้น เป็นความผิดพื้นฐานที่สามารถนำไปสู่การประกอบความผิดอื่นๆ ซึ่งก่อให้เกิดความเสียหายเป็นอย่างมาก แต่บทบัญญัติของกฎหมายในเรื่องการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดหลักเกณฑ์เกี่ยวกับความผิดไว้เป็นการทั่วไปและบทลงโทษไม่สูงนักโดยไม่มีบทหนักหรือบทเพิ่มโทษ ดังนั้นแม้จะทำให้เกิดความเสียหายมากมายเพียงใดก็ไม่สามารถที่จะเพิ่มโทษได้ ทำให้การบุกรุกเข้าไปในระบบคอมพิวเตอร์ของบุคคลทั่วไปเพื่อแอบอ่านจดหมายส่วนตัว การบุกรุกเข้าไปในระบบคอมพิวเตอร์ของบริษัทเอกชนเพื่อแอบดูข้อมูลทางการค้า หรือการบุกรุกเข้าไปในระบบคอมพิวเตอร์ของทางการทหาร ไม่มีความแตกต่างกันแต่อย่างใด

การกำหนดโทษดังกล่าวจึงแตกต่างกับความรับผิดในการเข้าถึงโดยปราศจากอำนาจในต่างประเทศ เช่น ประเทศสหรัฐอเมริกาได้มีการแบ่งแยกความรับผิดในการเข้าถึงโดยปราศจากอำนาจตามประเภทและความสำคัญของข้อมูล และกำหนดโทษแตกต่างกันไปตาม

---

[4] Ibid.,

ความสำคัญของข้อมูลที่มุ่งคุ้มครอง เป็นการเน้นถึงความสำคัญของข้อมูลบางประเภทที่กฎหมายมุ่งที่จะคุ้มครองมากกว่าข้อมูลประเภทอื่น และในประเทศอังกฤษเองก็มีการกำหนดให้การเข้าถึงโดยมีเจตนาที่จะกระทำความผิดอื่นนั้น ผู้กระทำต้องรับโทษหนักขึ้น เนื่องจากเห็นว่าการเข้าถึงเพียงอย่างเดียวกับการเข้าถึงโดยมีเจตนาร้ายมีความร้ายแรงต่างกัน

ขณะที่ความผิดฐานอื่นในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีหลักเกณฑ์การเพิ่มโทษที่ปรากฏอยู่ตามมาตรา 12 ในกรณีที่ก่อให้เกิดความเสียหายแก่ประชาชนหรือต่อความมั่นคงปลอดภัยของประเทศความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ แต่ในความผิดเกี่ยวกับการเข้าถึงโดยมิชอบกลับไม่มีการกำหนดโทษสูงขึ้นในกรณีที่กระทำต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีความสำคัญ ซึ่งหากเทียบเคียงกับประเทศสหรัฐอเมริกาแล้วจะเห็นได้ว่ามีการกำหนดให้รับโทษหนักขึ้นหากการเข้าถึงนั้นเป็นการเข้าถึงข้อมูลที่มีความสำคัญต่อประเทศหรือข้อมูลทางการเงิน

ผู้เขียนเองก็เห็นด้วยกับแนวความคิดดังกล่าว เนื่องจากข้อมูลคอมพิวเตอร์ที่ถูกเข้าถึงนั้นอาจมีความแตกต่างกันในระดับความสำคัญของข้อมูลนั้น เช่นข้อมูลทางการทหารย่อมมีความสำคัญมากกว่าข้อมูลส่วนบุคคลทั่วไป และการเข้าถึงควรมีบทกำหนดโทษที่หนักกว่าการเข้าถึงข้อมูลโดยทั่วไป จึงควรมีการจัดความสำคัญของข้อมูลที่เข้าถึงตามความสำคัญที่เห็นสมควรเพื่อที่จะมีการลงโทษที่เหมาะสมกับการกระทำความผิดได้ดีกว่าที่จะกำหนดเป็นพื้นฐานทั่วไป และเพื่อแบ่งแยกผู้กระทำความผิดที่เป็นเพียงเด็กที่คึกคะนองออกจากผู้กระทำความผิดที่ประสงค์ร้ายอย่างแท้จริง

5.1.3 **ความผิดต่อส่วนตัวหรือความผิดต่อแผ่นดิน**

ปัญหาอีกกรณีหนึ่งที่อาจเป็นที่ถกเถียงกันว่าบทบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับการเข้าถึงโดยมิชอบนั้นควรเป็นความผิดอันยอมความได้หรือไม่ เนื่องจากเห็นว่าความผิดในการเข้าถึงโดยมิชอบเป็นความผิดที่ไม่ร้ายแรง ซึ่งข้อดีของการกำหนดให้การเข้าถึงโดยมิชอบเป็นความผิดอันยอมความได้คือ จะทำให้การกระทำความผิดนั้นสามารถยอมความกันได้และสามารถถอนฟ้องได้โดยการตกลงกันระหว่างคู่ความ

แต่อย่างไรก็ตามก็มีผู้ให้ความเห็นว่า หากกำหนดให้เป็นความผิดอันยอมความได้แล้วอาจมีปัญหาในการระบุตัวผู้เสียหาย และหากไม่เป็นความผิดอันยอมความได้แล้วเพียงแค่กล่าวโทษพนักงานสอบสวนก็สามารถดำเนินคดีต่อได้[5]

จะเห็นได้ว่าทั้งสองแนวทางต่างมีข้อดีและข้อเสียแตกต่างกัน โดยการทำให้เป็นความผิดอันยอมความได้นั้นจะเป็นผลดีในแง่กฎหมายสารบัญญัติที่เปิดช่องให้สามารถตกลงยอมความกันได้และมีผลดีต่อการกระทำผิดในบางลักษณะ เช่น การทำผิดของบิดามารดาต่อบุตรหรือคนใกล้ชิด ทำให้ตกลงยอมความกันได้โดยไม่ต้องนำคดีขึ้นสู่ศาล ซึ่งหากเป็นความผิดที่ยอมความไม่ได้อาจจะทำให้ไม่สามารถหยุดการดำเนินคดีได้ หากแต่การกำหนดให้เป็นความผิดอาญาแผ่นดินนั้นย่อมมีผลดีต่อการสืบสวนสอบสวน เนื่องจากความผิดอันยอมความได้นั้นต้องมีผู้เสียหายร้องทุกข์ พนักงานสอบสวนไม่สามารถที่จะเริ่มคดีเองได้ นอกจากนี้กว่าผู้เสียหายจะรู้ตัวผู้กระทำผิดอาจใช้ระยะเวลานาน

ในกรณีปัญหานี้หากสอบถามบุคคลทั่วไปแล้วมักจะมีความเห็นโน้มเอียงไปทางในแง่กฎหมายสารบัญญัติที่เห็นว่าควรยอมความกันได้ เนื่องจากเห็นว่าเป็นความผิดที่สามารถตกลงกันได้ และในบางกรณีผู้กระทำเป็นเพียงเด็กหรือวัยรุ่นซึ่งทำด้วยความคึกคะนองเท่านั้น ซึ่งในกรณีนี้ผู้เขียนเห็นด้วยกับแนวคิดที่ควรกำหนดให้เป็นความผิดอันยอมความได้ แม้จะมีปัญหาในการสืบสวนสอบสวนแต่ผู้เขียนเห็นว่าจะเป็นผลดีมากกว่าหากสามารถตกลงยอมความกันได้ในกรณีที่ไม่ได้ก่อให้เกิดความเสียหายใดๆ ขึ้น

แม้ผู้เขียนจะได้ทำการวิเคราะห์ถึงบทบัญญัติของกฎหมายที่กำหนดหลักเกณฑ์และวิธีการในการกำหนดหลักเกณฑ์ในการลงโทษแล้วและมีความเห็นไม่สอดคล้องกับกฎหมายที่ออกมาบังคับใช้ในบางส่วน หากแต่เมื่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ประกาศใช้แล้ว เพื่อให้เกิดความเข้าใจในปัญหาที่สำคัญอีกส่วนหนึ่งคือ การใช้และตีความกฎหมายว่าด้วยการเข้าถึงโดยมิชอบ ผู้เขียนก็จะขอวิเคราะห์ปัญหาในการตีความกฎหมาย ดังนี้

5.2 ปัญหาข้อกฎหมาย

---

[5] “สรุปสาระสำคัญการประชุมคณะกรรมาธิการวิสามัญ ครั้งที่ 6/2550,” [Online] แหล่งที่มา : http://wiki.nectec.or.th/nectecpedia/index.php [วันที่ 17 มกราคม 2551]

ความผิดในการเข้าถึงโดยมิชอบเป็นความผิดใหม่ที่นักกฎหมายไทยไม่คุ้นเคย เนื่องจากเป็นฐานความผิดที่ถูกกำหนดขึ้นใหม่ซึ่งมีแนวคิดแตกต่างไปจากกฎหมายอาญาเดิมแทบทั้งสิ้นไม่ว่าจะเป็นวิธีการกระทำผิด สิ่งที่กฎหมายมุ่งคุ้มครอง ตลอดจนการดำเนินคดีทางกฎหมาย ความรู้ความเข้าใจในตัวบทกฎหมายจึงมีน้อยเนื่องจากมีศัพท์ใหม่ที่ไม่เคยมีในกฎหมายและยังมีความหมายที่ไม่ชัดเจนในตัวเองที่กลายเป็นองค์ประกอบในบทบัญญัติที่เป็นกฎหมายอาญา ทำให้มีปัญหาที่อาจพบได้ดังต่อไปนี้

5.2.1 **คำนิยามระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ทางกฎหมาย**

ดังที่ได้กล่าวมาแล้วในบทที่ 2 ถึงนิยามของคำว่า “ระบบคอมพิวเตอร์” และคำว่า “ข้อมูลคอมพิวเตอร์” ว่ามีความแตกต่างจากความหมายทางเทคนิคโดยทั่วไปของศาสตร์ทางด้านคอมพิวเตอร์ โดยผู้เขียนจะขอเริ่มพิจารณาจากคำว่า “ระบบคอมพิวเตอร์” ก่อน โดยจะขอนำคำว่า “คอมพิวเตอร์” ในศาสตร์ทางด้านคอมพิวเตอร์มาเปรียบเทียบกับคำว่า “ระบบคอมพิวเตอร์” ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เนื่องจากคำว่า “ระบบคอมพิวเตอร์” ในแง่ของศาสตร์ทางคอมพิวเตอร์แล้วจะมีความหมายแตกต่างโดยเน้นถึงจุดประสงค์ในการใช้งานคอมพิวเตอร์มากกว่าจะเป็นการให้คำนิยามหรืออธิบายลักษณะแต่อย่างใด[6]

คำว่าคอมพิวเตอร์นั้น ในปัจจุบันได้มีการขยายความไปอย่างกว้างขวาง เนื่องจากอุปกรณ์อิเล็กทรอนิกส์หลายอย่างมีคุณสมบัติเหมือนกับคอมพิวเตอร์จนในทางด้านเทคนิคแล้วอุปกรณ์ดังกล่าวจึงเป็นคอมพิวเตอร์แม้ว่าจะไม่ได้ถูกเรียกว่าคอมพิวเตอร์ก็ตาม หากมีคุณสมบัติครบถ้วนดังต่อไปนี้ก็ถือเป็นคอมพิวเตอร์ในแง่ศาสตร์ทางด้านคอมพิวเตอร์ คือ

1. การรับข้อมูลเข้า (Input) คือ การนำข้อมูลเข้าซึ่งสามารถผ่านทางอุปกรณ์ชนิดต่างๆ แล้วแต่ชนิดของข้อมูลที่จะป้อนเข้าไป

2. มีการประมวลผลข้อมูล (Process) โดยเมื่อนำข้อมูลเข้ามาแล้ว มีการดำเนินการกับข้อมูลตามคำสั่งที่ได้รับมาเพื่อให้ได้ผลลัพธ์ตามที่ต้องการ

---

[6] สัมภาษณ์ ธงชัย โรจน์กังสดาล, เลขานุการภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 30 มกราคม 2551

3. มีชุดคำสั่ง (software) ที่สั่งให้เกิดการทำงานตามที่ได้กำหนดไว้ในชุดคำสั่งนั้น โดยสามารถใส่ชุดคำสั่งใหม่ลงไปได้ด้วย

4. มีหน่วยความจำ (memory) คือ มีแหล่งเก็บข้อมูลที่นำเข้ามา

5. มีการแสดงผลลัพธ์ (Output) เป็นการนำผลลัพธ์จากการประมวลผลมาแสดงให้ทราบทางอุปกรณ์ที่กำหนดไว้ โดยทั่วไปจะแสดงผ่านทางจอภาพ หรือเรียกกันโดยทั่วไปว่า "จอมอนิเตอร์" (Monitor)

ดังนั้นอุปกรณ์อิเล็กทรอนิกส์ เช่น ไอโฟน โทรศัพท์มือถือรุ่นใหม่ที่มีระบบปฏิบัติการ เครื่องเล่นเกม จึงถือเป็นคอมพิวเตอร์ในความหมายนี้

แต่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้นิยามเพียงแค่คำว่า “ระบบคอมพิวเตอร์” โดยไม่มีการนิยามคำว่า “คอมพิวเตอร์” ไว้แต่อย่างใด โดยได้นิยามคำว่า “ระบบคอมพิวเตอร์” ไว้ว่า

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ”

ซึ่งอาจแยกองค์ประกอบของความหมายดังกล่าว ได้ดังนี้

1. เป็นอุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน ซึ่งคือ อุปกรณ์ต่างๆของคอมพิวเตอร์ที่เชื่อมเข้าด้วยกัน เช่น จอภาพ คีย์บอร์ด เม้าท์ หรือเคสซีพียู

2. มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลอัตโนมัติ คือการกำหนดชุดคำสั่งให้คอมพิวเตอร์ทำงานเช่น ระบบปฏิบัติการวินโดว์ หรือระบบปฏิบัติการลีนุ๊ก หรือระบบปฏิบัติการแม็ค

ซึ่งจากนิยามดังกล่าว สิ่งที่จะเกิดขึ้นเมื่อมีการบังคับใช้กฎหมายคือ การตีความว่าอะไรคือความหมายของคอมพิวเตอร์ โดยจะเห็นได้ว่าคำว่าคอมพิวเตอร์นั้นมีทั้งความหมายที่แคบคือหมายถึงคอมพิวเตอร์ที่รู้จักกันทั่วไปและเรียกว่าคอมพิวเตอร์ เช่น คอมพิวเตอร์ส่วนบุคคลหรือโน๊คบุ๊ค และคอมพิวเตอร์ในความหมายทางด้านศาสตร์ทางคอมพิวเตอร์ที่มีความหมายกว้าง

รวมไปถึงอุปกรณ์อิเล็กทรอนิกส์อื่นๆ ที่มีคุณสมบัติของคอมพิวเตอร์ด้วย เช่น เครื่องเล่นเกม ไอโฟน เป็นต้น นอกจากนี้ยังมียังมีผู้ให้ความหมายของคำว่า “คอมพิวเตอร์”[7] ในแง่ที่กว้างขวางขึ้นไปอีก โดยรวมไปถึงอุปกรณ์อิเล็กทรอนิกส์อื่นๆ ที่มีการนำเข้า ประมวลผล ส่งออก และมีชุดคำสั่งอยู่โดยไม่จำเป็นต้องสามารถใส่ชุดคำสั่งใหม่ไปได้ก็เป็นคอมพิวเตอร์ ซึ่งจะทำให้คำว่าคอมพิวเตอร์นั้นรวมตลอดไปถึงอุปกรณ์อื่น เช่น เครื่องเล่น MP3 เครื่องรับส่งโทรสาร ด้วย

หากพิจารณาจากความหมายนี้แล้ว คอมพิวเตอร์ในความหมายตามปกติที่คนทั่วไปเข้าใจเป็นคอมพิวเตอร์ในความหมายที่แคบ หากแต่มีอุปกรณ์อิเล็กทรอนิกส์หลายประเภทที่มีคุณสมบัติเหมือนคอมพิวเตอร์และในทางศาสตร์ของคอมพิวเตอร์แล้วถือว่ามีคุณสมบัติของคอมพิวเตอร์อย่างครบถ้วน เช่น ไอโฟน ปาล์ม และอาจมีผู้นิยามคำว่า “คอมพิวเตอร์” อย่างกว้างขวางจนรวมไปถึงอุปกรณ์อื่นที่มีชุดคำสั่งด้วย เช่น เครื่องเล่น Mp3

ดังนั้นปัญหาที่อาจเกิดขึ้นคือตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้ความหมายของคำว่าคอมพิวเตอร์ไว้อย่างไร หากมองว่าคอมพิวเตอร์คือคอมพิวเตอร์ในความหมายอย่างแคบที่คนทั่วไปรู้จักกัน อาจทำให้เกิดปัญหาว่าอุปกรณ์อิเล็กทรอนิกส์อื่นที่ไม่ถูกเรียกว่าคอมพิวเตอร์จะไม่ใช่คอมพิวเตอร์ในฐานะองค์ประกอบหนึ่งของความหมายของคำว่าระบบคอมพิวเตอร์ตามกฎหมายนี้ และอาจมองว่าคำว่า ระบบคอมพิวเตอร์ในความหมายตามกฎหมายเป็นความหมายของคำว่าคอมพิวเตอร์ตามปกติไม่ใช่ความหมายของคอมพิวเตอร์ทางเทคนิคได้ เนื่องจากตามคำนิยามได้กำหนดว่าระบบคอมพิวเตอร์เป็นอุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ ซึ่งหากจะให้หมายความรวมถึงคอมพิวเตอร์ในแง่เทคนิคด้วยแล้วต้องไม่มีคำว่า (อุปกรณ์หรือชุดอุปกรณ์) ของคอมพิวเตอร์ เพราะจะเป็นนิยามซ้อนนิยามขึ้น ซึ่งเป็นไปไม่ได้ที่จะนิยามคำว่าคอมพิวเตอร์โดยมีคำว่าคอมพิวเตอร์อยู่ในนิยามนั้น

ดังนั้น จึงมีผู้เห็นว่า[8]ความหมายของคอมพิวเตอร์ในนิยามตามกฎหมายจึงหมายถึงคอมพิวเตอร์ที่รู้กันอยู่ทั่วไป เช่น คอมพิวเตอร์ส่วนบุคคล ดังนั้นนิยามตามกฎหมายดังกล่าวจึงไม่ครอบคลุมไปถึงอุปกรณ์อิเล็กทรอนิกส์อื่นที่มีคุณสมบัติเหมือนคอมพิวเตอร์ เช่น

---

[7] สัมภาษณ์ ดร.สันติธร บุญเจือ, คณบดี คณะเทคโนโลยีสารสนเทศและการสื่อสาร วิทยาลัยการศึกษาทางไกลอินเทอร์เน็ต มหาวิทยาลัยอัสสัมชัญ ,วันที่ 24 ธันวาคม 2550

[8] สัมภาษณ์ ธงชัย โรจน์กังสดาล, 30 มกราคม 2551

ไอโฟน หรือโทรศัพท์มือถือรุ่นใหม่ที่มีระบบปฏิบัติการ เนื่องจากอุปกรณ์เหล่านี้ไม่ใช่ระบบคอมพิวเตอร์ตามนิยามของพระราชบัญญัตินี้

ในขณะเดียวกนกฎหมายของต่างประเทศ เช่น ในประเทศสหรัฐอเมริกามีกฎหมายที่ใช้ดำเนินคดีกับอาชญากรรมคอมพิวเตอร์ที่เกี่ยวข้องโดยตรง ได้แก่ The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CFAA) และให้นิยามคำว่าคอมพิวเตอร์ไว้ใน FCAA มาตรา 1030 (e) (1) ว่า คอมพิวเตอร์หมายถึง เครื่องอิเล็กทรอนิกส์ แม่เหล็ก แสง หรือไฟฟ้าอิเล็กตรอน หรือเครื่องที่มีกระบวนการคำนวณข้อมูลความเร็วสูง ที่แสดงถึงตรรกะ คณิตศาสตร์ หรือเก็บข้อมูล และรวมถึงเครื่องเก็บข้อมูลใดๆ หรือเครื่องติดต่อสื่อสาร ที่สัมพันธ์โดยตรงหรือปฏิบัติการร่วมกันกับเครื่องมือเหล่านี้ แต่ไม่หมายความรวมไปถึง เครื่องพิมพ์ดีด หรือเครื่องเรียงพิมพ์ เครื่องคำนวณที่พกพา หรือเครื่องมืออื่นที่มีลักษณะเดียวกัน

โดยหากเทียบกับคำนิยามของระบบคอมพิวเตอร์ที่ปรากฏอยู่ในอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสหภาพยุโรปแล้ว จะเห็นได้ว่า อนุสัญญาดังกล่าวได้ให้คำนิยามของระบบคอมพิวเตอร์[9] ว่า ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมต่อกันหรือเกี่ยวข้องกันตัวหนึ่งหรือมากกว่านั้น โดยได้มีการกำหนดชุดคำสั่งให้ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

นอกจากนี้ ได้มีการให้คำอธิบายว่า[10] ระบบคอมพิวเตอร์ภายใต้อนุสัญญานี้ คืออุปกรณ์ที่ประกอบด้วย hardware และ software ที่ถูกพัฒนาโดยกระบวนการประมวลผล

---

[9] “computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data [Online] Available from : http://conventions.coe.int [วันที่ 7 ธันวาคม 2550]

[10] “Council of Europe's Explanatory Report on the Convention,” [Online] Available from : http://conventions.coe.int/Treaty/en/Reports/Html/185.htm [วันที่ 8 ธันวาคม 2550]

ข้อมูลดิจิตอลอัตโนมัติ ซึ่งอาจรวมถึง input output และที่เก็บข้อมูล อุปกรณ์นั้นอาจมีเครื่องเดียวหรือเชื่อมต่อกันเป็นเครือข่ายกับอุปกรณ์อื่นที่คล้ายกัน

ในขณะที่ประเทศสหรัฐอเมริกามีคำนิยามคำว่าคอมพิวเตอร์ แต่ประเทศไทยไม่ได้คำนิยามไว้ แต่ได้ให้คำนิยามคำว่าระบบคอมพิวเตอร์เหมือนกับที่ปรากฏอยู่ในอนุสัญญาของสหภาพยุโรปแทน ดังที่จะเห็นได้จากการเทียบระหว่างคำนิยามของคำว่า “ระบบคอมพิวเตอร์” ของประเทศไทยและในอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสหภาพยุโรปแล้ว จะเห็นได้ว่าแทบไม่มีความแตกต่างกัน หากแต่จุดที่แตกต่างกันคือคำนิยามระบบคอมพิวเตอร์ของประเทศไทยได้เพิ่มคำว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ ซึ่งอาจทำให้เกิดการแปลความไปได้ว่าต้องเป็นอุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์เท่านั้น

โดยการตีความว่าอะไรคือคอมพิวเตอร์ในความหมายของกฎหมายก็อาจจะกลายเป็นประเด็นที่ถูกหยิบยกขึ้นมากล่าวอ้างได้ในอนาคตว่าอุปกรณ์ใดเป็นคอมพิวเตอร์ เมื่อคอมพิวเตอร์มีความหมายได้หลากหลายตามผู้ให้คำนิยาม จึงอาจทำให้มีผู้มองว่าคำว่าคอมพิวเตอร์ที่ปรากฏในความหมายของระบบคอมพิวเตอร์คือคอมพิวเตอร์ที่รู้จักกันในชีวิตประจำวัน เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล หรือโน๊ตบุ๊ค ซึ่งอุปกรณ์จำพวกไอโฟน ปาล์ม หรือมือถือที่มีระบบปฏิบัติการจึงไม่ใช่คอมพิวเตอร์ที่บุคคลทั่วไปเข้าใจ ดังนั้นหากไม่ใช่สิ่งที่เรียกว่าคอมพิวเตอร์แล้วก็อาจจะไม่ใช่อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ในนิยามของกฎหมาย ส่วนคำนิยามของคำว่าคอมพิวเตอร์ของสหรัฐอเมริกาก็มีการให้คำนิยามไว้อย่างกว้างครอบคลุมอุปกรณ์อิเล็กทรอนิกส์ต่างๆ ซึ่งมีความกว้างขวางพิจารณารวมถึงอุปกรณ์อิเล็กทรอนิกส์และอื่นๆ

แม้ในนิยามของระบบคอมพิวเตอร์ตามกฎหมายจะมีการตีความได้ทั้งสองนัยคือ อาจจะรวมถึงอุปกรณ์ที่ทำงานเหมือนคอมพิวเตอร์ เช่น ไอโฟน ปาล์ม หรือมือถือที่มีระบบปฏิบัติการหรือไม่ก็ได้ ในขณะเดียวกันหากให้ความหมายของคำว่าคอมพิวเตอร์กว้างขวางมาก อาจทำให้คำว่าคอมพิวเตอร์รวมตลอดไปถึงอุปกรณ์ไอพอด เครื่องเล่น MP3 หรือแม้แต่โทรสารได้ ดังนั้นการนิยามคำว่าคอมพิวเตอร์ให้ชัดเจนอาจจะเป็นการเหมาะสมกว่าเพราะการไม่นิยามความหมายของคำว่าคอมพิวเตอร์อาจก่อให้เกิดปัญหาตามมาว่าหากมีการกระทำผิดในการเข้าถึงโดยมิชอบในอุปกรณ์ดังกล่าวจะเป็นความผิดในการเข้าถึงระบบคอมพิวเตอร์หรือไม่ เนื่องจากนิยามความหมายของกฎหมายอาจถูกตีความเกินเลยไปถึงอุปกรณ์อิเล็กทรอนิกส์อื่นที่ไม่ใช่อุปกรณ์ที่กฎหมายมุ่งคุ้มครอง หรือตีความว่าไม่ครอบคลุมไปถึงอุปกรณ์อิเล็กทรอนิกส์อื่นที่

ไม่ใช่คอมพิวเตอร์ที่บุคคลทั่วไปในสังคมรู้ก็ได้ ในขณะเดียวกันปัจจุบันนี้อุปกรณ์ต่างๆ เหล่านี้ก็มีประสิทธิภาพคล้ายคอมพิวเตอร์โดยทั่วไปและมีบทบาทในชีวิตประจำวันมากยิ่งขึ้น รวมถึงมีระบบป้องกันไม่แตกต่างจากคอมพิวเตอร์เลย เช่น อาจมีการเข้ารหัส หรือแม้แต่การแสกนนิ้ว เพื่อพิสูจน์ว่าเป็นเจ้าของอุปกรณ์นั้นที่จะสามารถใช้งานอุปกรณ์นั้นได้เพื่อป้องกันไม่ให้ผู้อื่นเข้ามาใช้เครื่องของตน เช่น กรณีไอโฟนก็ยังมีการบุกรุกได้โดยมีการส่งโทรจันทางไอโฟนเกิดขึ้นแล้ว[11] ซึ่งสิ่งเหล่านี้จะเกิดมากขึ้นตามความนิยมในการใช้อุปกรณ์เหล่านี้

ดังนั้น หากพิจารณาถึงความเป็นไปได้และความเจริญก้าวหน้าของเทคโนโลยีในอนาคตแล้ว จะเห็นได้ว่าการกำหนดขอบเขตนิยามของกฎหมายให้มีความหมายถึงคอมพิวเตอร์โดยทั่วไป อาจไม่ครอบคลุมไปถึงอุปกรณ์อิเล็กทรอนิกส์อื่นที่มีคุณสมบัติของคอมพิวเตอร์แล้ว การบังคับใช้กฎหมายก็จะขาดประสิทธิภาพและมีขอบเขตที่แคบ ไม่สามารถนำตัวผู้กระทำผิดมาลงโทษได้ โดยผู้เขียนเห็นว่า นิยามของคำว่า “ระบบคอมพิวเตอร์” นั้น ควรจะมีการตัดคำว่า “ของคอมพิวเตอร์” ออกเพื่อให้เป็นถ้อยคำที่ไม่จำกัดความหมายของระบบคอมพิวเตอร์ให้ยึดติดอยู่กับคำว่าคอมพิวเตอร์ในความหมายทั่วไป หากแต่จะเปิดโอกาสให้ตีความครอบคลุมไปถึงเทคโนโลยีที่เกิดขึ้นใหม่ที่มีชื่อเรียกอย่างอื่นหากแต่มีคุณสมบัติเหมือนกับเครื่องคอมพิวเตอร์โดยทั่วไปได้และไม่ก่อให้เกิดการตีความโดยไม่จำเป็น หรืออาจจะกำหนดคำนิยามของคำว่า “คอมพิวเตอร์” ขึ้น เพื่อให้เกิดความชัดเจนว่าคอมพิวเตอร์คืออะไรและสามารถนำไปพิจารณาถึงนิยามของคำว่า “ระบบคอมพิวเตอร์” ได้

นอกเหนือจากปัญหาในเรื่องนิยามของระบบคอมพิวเตอร์ดังที่ได้กล่าวมาแล้ว ปัญหาสำคัญคือ การพิเคราะห์องค์ประกอบความผิดในการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบว่าเป็นอย่างไร โดยองค์ประกอบความผิดในการเข้าถึงโดยมิชอบนั้นประกอบด้วยการเข้าถึงโดยมิชอบ และมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้น

---

[11] “โทรจันตัวแรกบน iPhone,” [Online] แหล่งที่มา : www.blognone.com/node/6697 [วันที่ 13 มกราคม 2551]

มิได้มีไว้สำหรับตน ซึ่งในองค์ประกอบที่กล่าวมาทั้งสองส่วนที่กล่าวมาต่างมีปัญหาในการกำหนดขอบเขตและพฤติกรรมของผู้กระทำ เนื่องจากเป็นเรื่องใหม่และเป็นถ้อยคำค่อนข้างใหม่ในกฎหมาย จึงจำเป็นต้องการให้ความหมายของคำดังกล่าวให้ชัดเจนในระดับหนึ่ง โดยผู้เขียนจะขอเริ่มพิจารณาจากคำว่า “เข้าถึง” ดังนี้

5.2.2 **การเข้าถึง**

คำว่าเข้าถึง (access) เป็นคำใหม่ในกฎหมายอาญาซึ่งมีผู้นำไปเทียบกับคำว่าบุกรุกตามประมวลกฎหมายอาญา แม้โดยจุดประสงค์พื้นฐานของการบุกรุกและการเข้าถึงจะไม่แตกต่างกันคือเข้าไปในที่ที่ตนไม่มีสิทธิหรือได้รับอนุญาต หากแต่มีความแตกต่างกันมากในการจำกัดขอบเขตในการกระทำนั้นหรือให้คำอธิบายในการกระทำดังกล่าวว่าเป็นการบุกรุกหรือเป็นการเข้าถึงหรือไม่ เนื่องจากการบุกรุกตามปกติเป็นการเข้าไปในความหมายทางกายภาพเป็นการกระทำต่ออสังหาริมทรัพย์[12] ดังนั้นจึงอาจจะไม่เป็นปัญหามากนักที่จะพิจารณาว่าการกระทำใดเป็นการบุกรุกเนื่องจากสามารถมองเห็นได้ด้วยทางสายตา ทุกคนรู้ว่าการกั้นรั้ว ก่อกำแพง หรือการปักป้ายห้าม เป็นความหมายว่าห้ามเข้าตามบริบทของสังคม โดยทั่วไปการบุกรุกจึงมีสภาพที่เห็นได้ชัดเจน แต่คำว่าเข้าถึงนั้นเป็นสิ่งที่แตกต่างกันออกไป โดยปกติแล้วการเข้าถึงในแง่ของคอมพิวเตอร์ไม่ใช่การเข้าถึงโดยทางกายภาพเหมือนการบุกรุกโดยทั่วไป การเข้าไปดูข้อมูลในคอมพิวเตอร์จึงไม่ใช่การบุกรุกตามประมวลกฎหมายอาญา[13] การเข้าถึงจึงไม่ใช่สิ่งที่สามารถมองเห็นได้ด้วยสายตาและขอบเขตทางกายภาพ จึงยากที่จะให้คำจำกัดความและจำกัดขอบเขตของการกระทำได้

หากพิจารณาจากศาสตร์ทางด้านคอมพิวเตอร์แล้ว คำว่า access หมายถึง เข้าถึง บอกตำแหน่ง การอ่านหน่วยความจำ และทำให้พร้อมที่จะนำมาใช้งาน คำว่า access ใช้กับการเข้าสู่แผ่นดิสก์ แฟ้มข้อมูล ระเบียนและเครือข่ายต่างๆ โดยการเข้าถึงนั้นมีได้หลายระดับ[14] คือ

---

[12] รองศาสตราจารย์ ดร. ทวีเกียรติ มีนะกนิษฐ, คำอธิบายกฎหมายอาญา ภาคความผิดและลหุโทษ, พิมพ์ครั้งที่ 2 (กรุงเทพฯ : วิญญูชน, 2548), หน้า 215 - 223.

[13] เรื่องเดียวกัน,

[14] สัมภาษณ์ ธงชัย โรจน์กังสดาล, 30 มกราคม 2551

1. การเข้าถึงอุปกรณ์หรือชุดอุปกรณ์ (hardware) ซึ่งหมายถึง การแตะต้องสัมผัสอุปกรณ์เหล่านั้น ซึ่งแม้เพียงส่วนใดส่วนหนึ่งก็ได้ เช่น การเปิดเครื่องคอมพิวเตอร์ หรือการแตะต้องคีย์บอร์ด

2. การเข้าถึงระบบปฏิบัติการ คือ การเข้าถึงระบบปฏิบัติการของคอมพิวเตอร์ เช่น ระบบปฏิบัติการวินโดว์ โดยการทำให้เครื่องคอมพิวเตอร์เรียกให้ระบบวินโดว์ทำงาน

3. การเข้าถึงในระดับโปรแกรมหรือข้อมูล คือ การเข้าถึงโปรแกรมหรือข้อมูลต่างๆ ที่อยู่ในเครื่องคอมพิวเตอร์ เช่นโปรแกรม word ข้อมูลรูปภาพ และรวมถึงการมองเห็นโปรแกรมหรือข้อมูลด้วย

หากจะกล่าวให้กว้างแล้ว การเข้าถึงในความหมายของศาสตร์ทางคอมพิวเตอร์ดังกล่าวอาจเริ่มตั้งแต่การกดปุ่มเปิดเครื่องคอมพิวเตอร์หรือสัมผัสอุปกรณ์ก็ว่าได้ และการเข้าถึงนั้นไม่จำกัดวิธีการที่จะกระทำ การเข้าถึงทางกายภาพอาจจะต้องเริ่มตั้งแต่การเข้าถึงอุปกรณ์ หากแต่การเข้าถึงโดยผ่านระบบเครือข่ายทางไกลก็อาจจะเริ่มที่การเข้าถึงระบบปฏิบัติการก่อนโดยไม่จำเป็นต้องเข้าถึงอุปกรณ์แต่อย่างใด ดังนั้นในแง่ Software หรือข้อมูลแล้ว แม้แต่การมองเห็นก็อาจอยู่ในความหมายของการเข้าถึงได้ การเข้าถึงจึงมีขอบเขตที่กว้างขวางเป็นอย่างมาก

เมื่อความหมายของการเข้าถึงในแง่คอมพิวเตอร์โดยทั่วไปมีความหมายที่กว้างและครอบคลุมการกระทำต่อคอมพิวเตอร์แทบทั้งหมด ดังนั้นสิ่งที่สำคัญคือในแง่มุมของกฎหมายแล้วพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ควรที่จะมีขอบเขตของคำว่าเข้าถึงอย่างไร เนื่องจากคำว่าเข้าถึงนั้นเป็นองค์ประกอบสำคัญในความผิดทางอาญาฐานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ โดยการที่พระราชบัญญัติดังกล่าวไม่ได้ให้คำนิยามของคำว่าเข้าถึงไว้จึงมีความจำเป็นที่จะต้องพิจารณาว่าการเข้าถึงมีความหมายว่าอย่างไร เพื่อที่จะสามารถเข้าใจความหมายและขอบเขตของการกระทำได้ถูกต้อง

ทางด้านกฎหมายก็ได้มีผู้ให้ความหมายของคำว่าเข้าถึง (access) ไว้กว้างๆ ว่า[15] การเข้าถึงเป็นการเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้ ดังนั้น จึงอาจหมายถึง การเข้าถึงฮาร์ดแวร์ หรือส่วนประกอบต่างๆของคอมพิวเตอร์ หรือข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง เช่น ข้อมูลจราจร เป็นต้น

นอกจากนี้ "การเข้าถึง" ยังสามารถหมายถึงการเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต อันเป็นการเชื่อมโยงระหว่างเครือข่ายหลายๆเครือข่ายเข้าด้วยกัน และยังหมายถึง การเข้าถึงโดยผ่านระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบ LAN (Local Area Network) อันเป็นเครือข่ายที่เชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้ๆ กันเข้าด้วยกัน

หากแต่เมื่อพิจารณาอย่างแท้จริงแล้ว จะเห็นได้ว่าเป็นคำอธิบายที่กว้างและเป็นนามธรรมจนไม่รู้จะตีกรอบหรือขอบเขตของคำว่าเข้าถึงได้อย่างไร การสัมผัสคีย์บอร์ด หน้าจอ หรือขยับเมาท์เป็นการเข้าถึงหรือไม่ในเมื่อคีย์บอร์ด หน้าจอ หรือเมาท์ของเครื่องคอมพิวเตอร์ก็เป็นอุปกรณ์ของคอมพิวเตอร์อย่างหนึ่ง และหน้าจอที่แสดงผลออกมาก็เป็นการแสดงข้อมูลคอมพิวเตอร์รูปแบบหนึ่งที่ผู้มองอาจจะสามารถเข้าใจได้

หากจะพิจารณาว่าการกระทำใดเป็นการเข้าถึงแล้ว อาจจะพิจารณาเปรียบเทียบได้ 2 แนวทาง[16] คือการเข้าถึงในความหมายอย่างแคบโดยอาศัยการเทียบเคียงกับพฤติการณ์ที่เกิดขึ้นในชีวิตจริงในโลกทางกายภาพ และการเข้าถึงในความหมายอย่างกว้างโดยพิจารณาจากการทำงานของคอมพิวเตอร์เป็นหลัก ซึ่งการเข้าถึงในความหมายอย่างแคบนี้อาจเปรียบเทียบ

---

[15]กฎหมายอาชญากรรมทางคอมพิวเตอร์ [Online] แหล่งที่มา : www.lawyerthai.com/articles/it/031.php [วันที่ 10 สิงหาคม 2550]

[16] Orin S. Kerr, Cybercrime's Scope: Interpreting 'Access' and Authorization' in Computer Misuse Statutes, Public Law and Legal Theory Research Paper Series Research Paper No. 65 [Online] Available from : http://www.law.nyu.edu/journals/lawreview/issues/vol78/no5/NYU502.pdf [วันที่ 7 มกราคม 2551]

ระหว่างการใช้คอมพิวเตอร์กับการเข้าไปในที่ดินหรือสถานที่ เช่น อาจมองได้ว่าผู้ใช้พยายามใช้เครือข่ายคอมพิวเตอร์ที่มีการป้องกันโดยรหัสผ่าน และพบกับหน้าจอมีการให้เรียกให้ใส่ชื่อผู้ใช้และรหัสผ่านเพื่อดำเนินการต่อไป ซึ่งอาจกล่าวได้ว่าหน้าจอนั้นคล้ายคลึงกับกุญแจของประตูหน้าบ้าน และการใส่ชื่อผู้ใช้และรหัสผ่านคือการใช้กุญแจเปิดกุญแจ ซึ่งผู้ใช้ที่มีชื่อผู้ใช้และรหัสผ่านถูกต้องก็สามารถเข้าไปในคอมพิวเตอร์ได้ แต่ถ้าใส่ชื่อผู้ใช้และรหัสผ่านผิดจะถูกปฏิเสธไม่ให้เข้า

การเปรียบเทียบโดยการเทียบเคียงดังกล่าวนั้น แม้ในบางกรณีอาจจะสามารถมองเห็นได้ชัดว่าเป็นการเข้าถึงแล้วหรือไม่ เช่น การเข้าถึงโดยอาศัยชื่อและรหัสผ่านของผู้อื่นเพื่อที่จะเข้าไปดูข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์ หากแต่ในบางกรณีแล้วการเทียบเคียงอาจจะไม่ทำให้เห็นภาพชัดเจน เช่น อาจจะกล่าวได้ว่าการเข้าไปในเวปไซต์สาธารณะ ก็เหมือนกับเราเข้าไปในร้านค้าเพื่อร้านค้าในโลกแห่งความเป็นจริงหรือไม่ ซึ่งคำตอบที่ถูกต้องนั้นไม่ชัดเจน การเยี่ยมชมเวปไซต์ที่สามารถเห็นได้ เท่ากับเห็นประตูร้านจากถนนสาธารณะ มากกว่าได้เข้าไปในร้านจริงๆ ซึ่งถ้าหากมองว่าเป็นการเห็นร้านจากถนนอาจจะทำให้ไม่เป็นการเข้าถึงได้ แต่การเทียบเคียงความคิดระหว่างโลกทางกายภาพกับโลกเสมือนจริงให้ทางแก้ปัญหาของคอมพิวเตอร์ทางหนึ่งเพื่อที่จะเข้าใจความหมายของความหมายของคำว่าเข้าถึงคอมพิวเตอร์[17]

อย่างไรก็ตามการเทียบเคียงในโลกเสมือนกับโลกแห่งความเป็นจริงไม่ใช่วิธีการเดียวที่จะเข้าใจคำว่า “เข้าถึง” การพิจารณาเพื่อความเข้าใจในอีกรูปแบบหนึ่งคือ การทำความเข้าใจคำว่า “เข้าถึง” นั้นอาจจะเริ่มจากการคิดว่าคอมพิวเตอร์คือเครื่องจักรแบบง่ายที่ติดต่อกับเครื่องอื่นโดยส่งและรับข้อมูล เช่น เมื่อผู้ใช้เยี่ยมชมเวปไซต์ คอมพิวเตอร์ของผู้ใช้จะส่งคำขอไปยังคอมพิวเตอร์ซึ่งเป็นที่ตั้งเวปไซต์เพื่อขอให้ส่งไฟล์คอมพิวเตอร์กลับมา เมื่อไฟล์ถูกส่งกลับมายังผู้ใช้ ผู้ใช้คอมพิวเตอร์จัดเรียงไฟล์และแสดงในรูปของเวปไซต์ ถ้ามองตรงไปยังวิธีที่คอมพิวเตอร์ทำงานก็อาจสามารถอธิบายการเข้าถึงได้ โดยมองจากการที่ผู้ใช้ส่งการติดต่อซึ่งมีการเข้าถึงทางกายภาพในคอมพิวเตอร์นั้น เช่น ผู้ใช้เข้าถึงคอมพิวเตอร์เมื่อเค้าส่งคำสั่งไปยังคอมพิวเตอร์นั้นเพื่อสั่งให้คอมพิวเตอร์ทำงานและคอมพิวเตอร์ตอบสนองกลับมายังผู้ใช้ ในแง่นี้จึงเป็นการเข้าถึงคอมพิวเตอร์แล้ว[18]

---

[17] Ibid.,

[18] Ibid.,

เมื่อพิจารณาแล้วจะเห็นได้ว่าพื้นฐานของคำว่า “เข้าถึง” หากมุ่งไปที่การทำงานของคอมพิวเตอร์จะสามารถอธิบายขอบเขตของการเข้าถึงได้เป็นระบบมากกว่าและกว้างขวางกว่าการใช้วิธีการเทียบเคียงกับโลกทางกายภาพ ซึ่งอาจจะทำให้เกิดปัญหาว่าเมื่อใดเป็นการเข้าถึงต้องมีการเข้าไปในคอมพิวเตอร์จริงหรือไม่จึงจะเป็นการเข้าถึงตามความหมายดังกล่าวเนื่องจากมาตรฐานในโลกความจริงและโลกเสมือนให้ผลลัพธ์ที่แตกต่างกัน เช่น กรณีผู้ใช้หวังจะเข้าไปในคอมพิวเตอร์ที่มีรหัสผ่าน และส่งคำร้องไปยังคอมพิวเตอร์ขอให้ส่งหน้าเวปไซต์กลับทันทีที่ผู้ใช้ใส่ชื่อผู้ใช้และรหัสผ่าน คอมพิวเตอร์ทำงานส่งหน้าเวปไซต์กลับมายังผู้ใช้นี้ยังไม่ใช่การเข้าถึงคอมพิวเตอร์จากภาพที่เห็นเสมือนจริง แต่คล้ายกับการเดินไปยังประตูที่ใส่กุญแจแต่ยังไม่พยายามไขกุญแจนั้น[19]

ดังนั้นจากแนวคิดดังกล่าวผู้เขียนเห็นด้วยว่า การสัมผัสคอมพิวเตอร์นั้นจะเป็นการเข้าถึงซึ่งระบบคอมพิวเตอร์ได้ต่อเมื่อเป็นการสัมผัสที่มีผลเป็นการป้อนคำสั่งทำให้คอมพิวเตอร์ทำงานโดยมีลักษณะเป็นการเข้าควบคุมหรือสื่อสาร เช่น การพิมพ์หรือกดปุ่มใดๆ หรือการขยับเมาส์ที่ทำให้คอมพิวเตอร์ตอบสนอง เพราะการสัมผัสที่ไม่ทำให้คอมพิวเตอร์ตอบสนองต่อคำสั่งนั้น เช่น การสัมผัสคีย์บอร์ดแต่ไม่ได้กดปุ่มหรือสั่งคำสั่งใดๆ รวมถึงการสัมผัสหน้าจอหรือตัวเครื่อง ไม่ถือว่าเป็นการเข้าถึงระบบคอมพิวเตอร์ เนื่องจากไม่มีการพยายามทำให้คอมพิวเตอร์ตอบสนองต่อการกระทำนั้นนอกจากนี้ยังเป็นการกำหนดขอบเขตที่กว้างจนเกินไปหากจะวางกรอบว่าเพียงแค่สัมผัสถูกคอมพิวเตอร์ก็เป็นการเข้าถึงแล้ว

แม้ผู้เขียนจะเห็นว่าการกำหนดว่าการสัมผัสคอมพิวเตอร์ที่จะเป็นการเข้าถึงนั้นต้องเป็นการสัมผัสที่เป็นการป้อนคำสั่งให้คอมพิวเตอร์ทำงานก็ตามก็ยังเป็นขอบเขตที่กว้างอยู่ แต่อย่างไรก็ตามการเข้าถึงดังกล่าวจะเป็นความผิดทางอาญาตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ต้องเป็นการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบที่มีการมาตรการป้องกันโดยเฉพาะ ซึ่งการกดหรือพิมพ์คีย์บอร์ดหรือการขยับเมาส์ของเครื่องคอมพิวเตอร์ไม่ได้เป็นการเข้าถึงโดยมิชอบซึ่งคอมพิวเตอร์ที่มีการ

---

[19] Ibid.,

ป้องกันไว้แต่อย่างใด ถือได้ว่าเจ้าของเครื่องคอมพิวเตอร์ไม่ได้มีเจตนาที่จะป้องกันผู้อื่นในการสัมผัสคีย์บอร์ด หรือเมาส์ของเครื่องคอมพิวเตอร์นั้น

ดังนั้น ตราบใดที่การกระทำนั้นไม่มีลักษณะเป็นกระทำโดยมิชอบเพื่อฝ่าระบบป้องกัน และในกรณีของการมองเห็นข้อมูลบนหน้าจอของเครื่องคอมพิวเตอร์ก็เช่นกัน หากเป็นข้อมูลที่ไม่ได้มีการป้องกันไว้แล้วก็ไม่เป็นความผิด ความหมายของคำว่าเข้าถึงจึงความหมายที่กว้างหากแต่จะถูกจำกัดด้วยองค์ประกอบอื่นของความผิดในฐานนั้น เช่น ต้องเป็นการเข้าถึงโดยมิชอบ หรือเป็นการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ ซึ่งจะช่วยจำกัดขอบเขตของความรับผิดทางอาญาให้อยู่ในขอบเขตที่เหมาะสมได้ในระดับหนึ่ง

การนิยามการเข้าถึงดังกล่าวแม้จะกว้าง หากแต่ผู้เขียนเห็นว่าเป็นสิ่งที่ดีกว่าการให้นิยามคำว่าเข้าถึงในทางที่แคบซึ่งอาจทำให้เกิดปัญหาในการตีความได้ เนื่องจากผู้ใช้แต่ละคนจะมีการปฏิสัมพันธ์กับคอมพิวเตอร์อย่างหลากหลายทางด้วยเหตุผลที่แตกต่างกัน จึงเป็นการยากที่จะพยายามกำหนดพฤติกรรมทุกอย่างของผู้ใช้และกำหนดว่าการกระทำใดเป็นการเข้าถึงหรือไม่ ผู้ใช้คอมพิวเตอร์ตามปกติอาจจะเข้าเครือข่ายคอมพิวเตอร์โดยการใช้รหัสผ่าน เปิดไฟล์บน Server เปิดเวปไซต์ หรือส่งจดหมายอิเล็กทรอนิกส์

ยิ่งไปกว่านั้น การใช้งานของผู้ใช้คอมพิวเตอร์เปลี่ยนแปลงตลอดเวลาตามเทคโนโลยีที่เปลี่ยนแปลงไป เช่น เวปไซต์ที่ให้บริการจดหมายอิเล็กทรอนิกส์ เช่น Hotmail หรือ Yahoo ที่อาจมีปัญหาในการตีความ เมื่อลูกค้าของ Hotmail หรือ Yahoo เข้าไปใน Sever Hotmail หรือ Yahoo เพื่อที่จะส่งหรือรับจดหมายอิเล็กทรอนิกส์ แต่ในเวลาเดียวกันแล้วการกระทำดังกล่าวคือการท่องเวปไซต์ (เนื่องจากโปรแกรมของจดหมายอิเล็กทรอนิกส์อยู่บนเวปไซต์) การเรียกดูข้อมูลที่เก็บไว้ (โดยดูจดหมายอิเล็กทรอนิกส์ที่เข้ามา) และการส่งไฟล์ออก (โดยการส่งจดหมายอิเล็กทรอนิกส์) ถ้าการกระทำใดการกระทำหนึ่งไม่ใช่การเข้าถึงแล้ว ศาลที่ต้องตัดสินคดีอาจจะไม่สามารถตอบคำถามได้ว่าเพราะเหตุใดการกระทำนั้นจึงเป็นการเข้าถึงหรือไม่ใช่การเข้าถึง[20]

---

[20] Ibid.,

โดยการตีความในแง่นี้อาจเห็นได้จาก คดี State v. Allen ของประเทศสหรัฐอเมริกา (ดังที่ได้กล่าวมาแล้วในบทที่ 3) ที่มองว่าการทำซ้ำโดยการควบคุมการเปิด-ปิดการโทรศัพท์ทางไกลทำให้ผู้ใช้โทรศัพท์ทางไกลฟรีและเดารหัสผ่านเพื่อเข้าไปใช้ได้นั้น เมื่อศาลตีความคำว่า “เข้าถึง” คล้ายคลึงกับความหมายทางกายภาพโดยหมายถึงการใส่ชื่อผู้ใช้และรหัสผ่านที่ถูกต้องและทำให้ผู้ใช้ได้เข้าไปใน (inside) เครื่องคอมพิวเตอร์อย่างแท้จริง และเมื่อขาดพยานหลักฐานว่า Allen ได้เข้าไปในเครื่องคอมพิวเตอร์อย่างแท้จริงเพื่อหาข้อมูลข้างใน ดังนั้นเขาจึงไม่ได้เข้าถึงคอมพิวเตอร์ของบริษัท Bell

การตีความดังกล่าวนั้น จะทำให้คำว่าเข้าถึงมีความหมายที่แคบและทำให้ผู้กระทำผิดหลบเลี่ยงกฎหมายโดยกล่าวอ้างว่าตนเองไม่ได้เข้าถึงคอมพิวเตอร์แต่อย่างใด และด้วยเทคโนโลยีใหม่ๆ ที่ทำให้ผู้กระทำสามารถกระทำความผิดโดยการเทคนิคทางด้านคอมพิวเตอร์ที่ซับซ้อนขึ้นและต้องมีการตีความว่าการกระทำใดเป็นการเข้าถึง เช่นที่ปรากฏอยู่ในคดี Moulton v. VC3 ศาลได้ตัดสินว่าการ scan port ไม่ใช่การเข้าถึงคอมพิวเตอร์ เนื่องจากการกระทำดังกล่าวไม่มีการเข้าถึงคอมพิวเตอร์แต่อย่างใด ทั้งที่การกระทำดังกล่าวเป็นการกระทำที่อาจนำไปสู่การ hack คอมพิวเตอร์ได้ เนื่องจากเป็นการค้นหาช่องว่างในเครื่องคอมพิวเตอร์ของบุคคลอื่นโดยอาจมีจุดมุ่งหมายที่จะบุกรุกเข้าไป

ดังนั้นจะเห็นได้ว่า การตีความอย่างแคบทำให้ผู้ที่ประสงค์ร้ายอาจกล่าวอ้างได้ว่าตนเองไม่ได้เข้าถึงคอมพิวเตอร์แต่อย่างใด ซึ่งตามกฎหมายไทยแล้ว หากการเข้าถึงไม่เป็นความผิดแล้ว การกระทำอย่างอื่นที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ได้กำหนดให้เป็นความผิด เช่น การจารกรรมข้อมูลคอมพิวเตอร์ ก็จะไม่เป็นความผิดด้วย เนื่องจากไม่มีการกำหนดให้เป็นความผิดที่แยกจากการเข้าถึงโดยมิชอบแต่อย่างใด โดยมองว่าการเข้าถึงข้อมูลคอมพิวเตอร์คือการจารกรรมข้อมูลนั่นเอง ซึ่งในหลายกรณีอาจทำให้ผู้กระทำความผิดสามารถหลุดลอดจากการลงโทษทางกฎหมายได้เนื่องไม่มีการเข้าถึงโดยมิชอบเกิดขึ้น

ผู้เขียนจึงเห็นด้วยว่าการเข้าถึงควรที่จะตีความในความหมายอย่างกว้าง ดังที่ปรากฏอยู่ในคดี State v. Riley (ดังที่ได้กล่าวมาแล้วในบทที่ 3) ที่มีข้อเท็จจริงของคดีคล้ายคลึงกับคดี State v. Allen แต่ศาลวอชิงตันตัดสินว่าการกระทำของ Riley ที่ทำซ้ำโดยควบคุมการเปิด-ปิดการโทรศัพท์ทางไกลทำให้ผู้ใช้โทรศัพท์ทางไกลฟรีและเดารหัสผ่านเพื่อเข้าไปใช้ได้นั้นเป็นการเข้าถึงคอมพิวเตอร์แล้ว ซึ่งเป็นการแปลความคำว่าเข้าถึงอย่างกว้างเพื่อให้ครอบคลุมพฤติกรรมที่

อาจเกิดขึ้นได้ และการแปลความอย่างกว้างจะทำให้แนวคิดเกี่ยวกับเรื่อง scan port นั้นถือเป็นการเข้าถึงแล้วเพราะได้มีการติดต่อสื่อสารกับคอมพิวเตอร์ การกระทำดังกล่าวจึงเป็นการเข้าถึง (access) เช่นกัน

จากแนวความคิดในการตีความคำว่า "เข้าถึง" อย่างกว้างนี้ ผู้เขียนจะขอยกตัวอย่างลักษณะการเข้าถึงที่เป็นความผิดทางอาญาตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้นพิจารณาเปรียบเทียบ โดยเริ่มจากการเข้าถึงทางด้านกายภาพก่อนเนื่องจากการเข้าถึงทางด้านกายภาพนั้นเป็นการเข้าถึงที่ง่ายที่สุดหากว่าผู้เข้าถึงรู้ถึงชื่อผู้ใช้และรหัสโดยไม่จำเป็นต้องมีความรู้ทางด้านคอมพิวเตอร์ก็สามารถเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นได้โดยมิชอบ โดยวิเคราะห์ว่าการกระทำใดถือว่าเป็นการเข้าถึงทางกายภาพ ซึ่งปัญหาที่อาจพบจากการพิจารณาคำว่าเข้าถึงในกรณีนี้คือ ปัญหาที่ว่าการเข้าถึงมีขอบเขตเพียงใด การแตะต้องคอมพิวเตอร์เพียงอย่างเดียวถือว่าเป็นการเข้าถึงแล้วหรือไม่ ระดับใดจึงจะถือว่าเป็นการเข้าถึงระบบคอมพิวเตอร์ที่เป็นความผิดตามกฎหมาย

หากจะเปรียบเทียบขั้นตอนการเข้าถึง อาจจะเริ่มจากสถานการณ์ดังนี้ 1. การที่เอเดินไปที่โต๊ะคอมพิวเตอร์ของบี 2. เอนั่งลงที่โต๊ะคอมพิวเตอร์ของบี 3. เอแตะคีย์บอร์ดและเมาส์ของบี 4. เอเห็นภาพหน้าจอคอมพิวเตอร์ของบีที่มีการป้องกันโดยการกรอกรหัสผ่าน 5. เอกรอกชื่อและรหัสผ่านของบี 6. เอกดปุ่ม enter และเข้าสู่ระบบคอมพิวเตอร์ของบีผ่านรหัสผ่านของบี เมื่อแยกขั้นตอนออกมาแล้วจะเห็นได้ว่าขั้นตอนที่เอแตะคีย์บอร์ดและเมาส์ของบีทำให้คอมพิวเตอร์ของบีตอบสนอง อาจเรียกว่าเป็นการเข้าถึงคอมพิวเตอร์ของบีแล้วแต่การกระทำนั้นไม่เป็นความผิดเนื่องจากไม่มีการป้องกันใดๆ ไว้ โดยขั้นตอนที่ถือว่าเป็นการเข้าถึงที่เป็นความผิดตามกฎหมายคือขั้นตอนที่กด enter เนื่องจากเป็นการเข้าถึงโดยผ่านระบบป้องกันของคอมพิวเตอร์และทำให้คอมพิวเตอร์ประมวลผลเข้าไปสู่ระบบคอมพิวเตอร์ภายในแล้ว การกระทำดังกล่าวจึงเป็นความผิดอาญา

ส่วนการเข้าถึงโดยผ่านระบบเครือข่ายนั้นเป็นการเข้าถึงที่ห่างโดยระยะทางหรืออาจกล่าวได้ว่าเป็นการเข้าถึงที่ไม่สัมผัสกับระบบคอมพิวเตอร์เครื่องนั้นโดยตรง โดยไม่จำเป็นต้องพิจารณาว่าห่างกันเพียงใด หากไม่ใช่เจตนาที่จะเข้าถึงระบบคอมพิวเตอร์เครื่องนั้นแล้ว แม้ห่างกันไม่กี่เซนติเมตรก็ถือว่าเป็นการเข้าถึงโดยผ่านระบบเครือข่ายไม่ใช่ทางกายภาพ เช่น การที่แฮกเกอร์ทำการ scan port ก็ถือเป็นการเข้าถึงคอมพิวเตอร์แล้ว หรือการใช้โปรแกรมคอมพิวเตอร์ประเภทสปายแวร์ (Spyware) หรือไวรัส (Virus) ไม่ว่าจะผ่านไปทางอินเทอร์เน็ต (Internet) ระบบ LAN

(Local Area Network) หรือการติดต่อสื่อสารแบบไร้สาย (Wireless Communication) และเข้าไปในระบบคอมพิวเตอร์ของผู้นั้นผ่านช่องโหว่ของระบบดังกล่าว ถือเป็นการเข้าถึงโดยผ่านระบบเครือข่าย โดยการเข้าไปโดยใช้โปรแกรมมุ่งร้ายประเภทสปายแวร์หรือไวรัสนั้นมีผู้ให้ข้อสังเกตว่าจะถือว่ามีการเข้าถึงเมื่อใด เช่น เอส่งไวรัสมาให้บีผ่านทางจดหมายอิเล็กทรอนิกส์ เมื่อจดหมายอิเล็กทรอนิกส์เข้าไปอยู่ในความครอบครองของบีแล้วจะถือว่าเป็นการเข้าถึงหรือไม่ หรือบีต้องเปิดจดหมายนั้นแล้วทำให้โปรแกรมมุ่งร้ายนั้นติดตั้งตัวเองในคอมพิวเตอร์ของบีก่อน[21]

โดยผู้เขียนเห็นว่าแม้ว่าการที่เอส่งจดหมายอิเล็กทรอนิกส์ที่มีไวรัสให้บีจะเป็นการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของบีแล้ว แต่โดยสภาพแล้วระบบอีเมล์นั้นเป็นระบบเปิดไม่มีการป้องกันดังนั้นการเข้าถึงในกรณีนี้ยังไม่เป็นความผิดอาญา แต่ประเด็นที่น่าสนใจคือ[22]หากบีผู้รับกดดูเอกสารที่แนบไวรัสส่งมา ทำให้ไวรัสติดตั้งตนเองในระบบคอมพิวเตอร์ของบีแล้วโดยผ่านการป้องกันของคอมพิวเตอร์ของบีเข้ามาและแพร่กระจายไปยังรายชื่อที่บีมีอยู่ในรายการจดหมายอิเล็กทรอนิกส์ การที่บีกดให้ไวรัสทำงานนี้เป็นการทำให้เอเข้าสู่คอมพิวเตอร์ของบีอีกครั้งหนึ่งหรือบีผู้รับเป็นผู้ทำให้เกิดการเข้าถึงขึ้น หรือแท้จริงแล้วไม่มีการเข้าถึงครั้งที่ 2 แต่อย่างใด

ในที่สุดแล้วการพิจารณาประเด็นนี้ คำตอบอาจจะอยู่ที่ว่าเรามองการเข้าถึงในฐานะผลที่เกิดขึ้นหรือในฐานะการกระทำ ถ้ามองว่าการเข้าถึงเป็นผลแล้ว เอก็อาจจะเป็นผู้ก่อให้เกิดการเข้าถึงโดยมิชอบขึ้นโดยเอเป็นผู้ส่งไวรัสมาตั้งแต่แรกและมุ่งหมายให้คอมพิวเตอร์ของบีติดไวรัสที่ตนส่งมาและในที่สุดคอมพิวเตอร์ของบีก็ติดไวรัสสมความตั้งใจของเอ แต่ถ้ามองว่าการเข้าถึงโดยมิชอบนั้นเป็นการกระทำ บีผู้รับก็เป็นเหตุให้เกิดการเข้าถึงโดยมิชอบขึ้นไม่ใช่เอผู้ส่งไวรัส[23]

ในกรณีนี้ผู้เขียนเห็นว่าการส่งไวรัสผ่านจดหมายอิเล็กทรอนิกส์ที่ผู้รับยังไม่ได้เปิดออกและทำให้โปรแกรมทำงานแล้วก็เปรียบเสมือนการส่งจดหมายไว้ในตู้จดหมายเท่านั้นแม้จะอยู่

---

[21] Ibid.,

[22] Ibid.,

[23] Ibid.,

ในการครอบครองของบีก็ไม่ปรากฏว่ามีการหวงห้ามหรือป้องกันการส่งมาแต่อย่างใด การกระทำดังกล่าวจึงไม่เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และผู้เขียนก็เห็นด้วยกับความเห็นแรกที่ว่าการที่เอส่งไวรัสมายังคอมพิวเตอร์ของบีนั้นทันทีที่คอมพิวเตอร์ของบีติดไวรัสของเอ เอย่อมเป็นผู้กระทำผิดสำเร็จแล้วเนื่องจากเอไม่ต้องทำอะไรเพิ่มเติมอีกนอกจากรอให้บีกดรับเพื่อให้คอมพิวเตอร์ของบีติดไวรัส เอจึงมีความผิดในการเข้าถึงโดยมิชอบแล้ว แต่อย่างไรก็ตามในกรณีนี้เจ้าพนักงานที่มีอำนาจในการดำเนินคดีอาจจะหลีกเลี่ยงปัญหาการตีความโดยฟ้องร้องการกระทำความผิดในลักษณะนี้ในความผิดเกี่ยวกับไวรัสโดยตรง แต่อย่างไรก็ตามหากมีการฟ้องร้องในประเด็นนี้เกิดขึ้นก็เป็นประเด็นที่น่าสนใจว่าศาลจะตีความเช่นใด[24]

นอกจากนี้องค์ประกอบของคำว่าเข้าถึงนั้น ไม่ใช่เป็นการเข้าถึงโดยทั่วไป หากแต่ตามพระราชบัญญัติดังกล่าวได้กำหนดว่าการเข้าถึงที่จะเป็นความผิดทางกฎหมายได้นั้นต้องเป็นการเข้าถึงโดยมิชอบ ซึ่งการเข้าถึงโดยมิชอบ ประกอบด้วยคำว่า “เข้าถึง” และคำว่า “โดยมิชอบ” ซึ่งผู้เขียนได้กล่าวถึงคำว่าเข้าถึงแล้ว ดังนั้นสิ่งที่ผู้เขียนจะทำการพิจารณาต่อมาคือคำว่า “โดยมิชอบ” ว่าคำว่า “โดยมิชอบ” นั้นมีความหมายและขอบเขตเพียงใด ซึ่งต้องมีการทำความเข้าใจในความหมายของคำว่า การเข้าถึง “โดยมิชอบ” ดังนี้

5.2.2 โดยมิชอบ

คำว่า ”โดยมิชอบ” ที่ปรากฏอยู่ในประมวลกฎหมายอาญานั้น หากจะพิจารณาจากความหมายจากพจนานุกรมฉบับราชบัณฑิตยสถาน[25]แล้ว คำว่า “มิ” หมายถึง ไม่ (คำปฏิเสธความหมายของคำที่อยู่ถัดไป) เฉย ส่วนคำว่า “ชอบ” หมายถึง พอใจ ถูกต้อง เหมาะ ถูกใจ ถูกกัน มีสิทธิ ดังนั้นคำว่า “มิชอบ” จึงหมายถึง ไม่พอใจ ไม่ถูกต้อง ไม่เหมาะ ไม่ถูกใจ ไม่ถูกกัน ไม่มีสิทธิ ซึ่งจะเห็นได้ว่ามีความหมายค่อนข้างกว้างและครอบคลุมการกระทำที่ไม่เหมาะสมหรือไม่สมควรในความหมายโดยทั่วไป

คำว่า ”โดยมิชอบ” ในประมวลกฎหมายอาญาจะปรากฏอยู่ในฐานความผิดเกี่ยวกับเจ้าพนักงาน เช่น มาตรา 157 ตามประมวลกฎหมายอาญา บัญญัติว่า “ผู้ใดเป็นเจ้า

---

[24] Ibid.,

[25] พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2525

พนักงาน ปฏิบัติหรือละเว้นการปฏิบัติหน้าที่โดยมิชอบ เพื่อให้เกิดความเสียหายแก่ผู้หนึ่งผู้ใด หรือปฏิบัติ หรือละเว้นการปฏิบัติหน้าที่โดยทุจริตต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี หรือปรับตั้งแต่สองพันบาทถึงสองหมื่นบาท หรือทั้งจำทั้งปรับ"

โดยคำว่า "โดยมิชอบ" ในมาตรานี้ หมายความถึงโดยมิชอบด้วยหน้าที่ ซึ่งเจ้าพนักงานมีอยู่ตามกฎหมาย กฎ ข้อบังคับ คำสั่งของคณะรัฐมนตรี คำสั่งผู้บังคับบัญชา หรือระเบียบแบบแผนของทางราชการ ซึ่งออกได้โดยชอบด้วยกฎหมาย[26]

นอกจากในความผิดเกี่ยวกับเจ้าพนักงานแล้ว คำว่า "โดยมิชอบ" ก็เป็นองค์ประกอบความผิดที่พบอยู่ในประมวลกฎหมายอาญาที่เกี่ยวกับบัตรอิเล็กทรอนิกส์ในมาตรา 269/5 และมาตรา 269/6 ด้วยเช่นกัน โดยในเรื่องความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ มาตรา 269/5 บัญญัติว่า "ผู้ใดใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุก ไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาทหรือทั้งจำทั้งปรับ"

มาตรา 269/6 บัญญัติว่า "ผู้ใดมีไว้เพื่อนำออกใช้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบตามมาตรา 269/5 ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่น หรือประชาชนต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท หรือทั้งจำทั้งปรับ"

จะเห็นได้ว่าคำว่า "โดยมิชอบ" ที่มีใช้อยู่ในบทบัญญัติที่แตกต่างกันย่อมมีความหมายตามบริบทของบทบัญญัตินั้น ดังนั้นคำว่า "โดยมิชอบ" จึงเป็นคำที่มีลักษณะเป็นกลางแล้วแต่ผู้ใช้กฎหมายจะเป็นผู้ตีความให้เหมาะสมว่า "โดยมิชอบ" นั้นจะหมายถึงลักษณะการกระทำเช่นใด ซึ่งอาจแยกแยะประเภทการกำหนดหลักเกณฑ์ในการแปลความหมายของคำว่า "โดยมิชอบ" ได้ใน 3 ลักษณะใหญ่ๆ คือ ไม่ชอบด้วยกฎหมาย (illegal) โดยปราศจากอำนาจ (unauthorized) และ ไม่เหมาะสม ไม่ถูกต้อง (improper)

หากคำว่า "โดยมิชอบ" หมายถึง โดยมิชอบด้วยกฎหมาย (illegal) แล้ว ย่อมหมายความว่าการกระทำนั้นจะเป็นความผิดเมื่อเป็นการฝ่าฝืนข้อห้ามหรือข้อบังคับที่มีกฎหมาย

---

[26] ศาสตราจารย์ ดร. หยุด แสงอุทัย, กฎหมายอาญา ภาค 2-3 ฉบับพิมพ์ครั้งที่ 9 (กรุงเทพฯ : สำนักพิมพ์มหาวิทยาธรรมศาสตร์, 2542), หน้า 66.

ห้ามมิให้กระทำไว้ หรือไม่มีอำนาจหน้าที่ตามกฎหมายให้กระทำได้[27] ซึ่งหากแปลความของคำว่า “โดยมิชอบ” หมายถึงโดยมิชอบด้วยกฎหมายแล้ว ก็จะเป็นการแปลความหมายที่ค่อนข้างแคบ เนื่องจากจะหมายความว่าหากการเข้าถึงนั้นไม่มีกฎหมายห้าม หรือเข้าถึงโดยชอบด้วยกฎหมายแล้ว การเข้าถึงนั้นก็ย่อมไม่เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในเรื่องการเข้าถึงโดยมิชอบแต่อย่างใด

การตีความเช่นนี้จะทำให้การกระทำหลายอย่างไม่สามารถลงโทษได้เนื่องจากกฎหมายไม่ได้บัญญัติว่าการกระทำนั้นเป็นความผิด เช่น กรณีที่ไม่มีกำหนดห้ามแต่ผิดข้อสัญญาหรือข้อตกลงก็จะไม่เป็นความผิดเนื่องจากการกระทำนั้นเพียงแต่ผิดข้อสัญญาเท่านั้นไม่ได้ผิดกฎหมาย หรือกรณีที่ไม่มีอำนาจให้กระทำแต่การกระทำนั้นไม่ถึงขนาดไม่ชอบด้วยกฎหมาย การกระทำนั้นจะไม่เป็นความผิด โดยเฉพาะอย่างยิ่งกรณีที่มีอำนาจกระทำได้ตามอำนาจหน้าที่หากแต่การกระทำนั้นเป็นไปเพื่อประโยชน์ส่วนตัวก็ไม่เป็นความผิดเช่นเดียวกัน เนื่องจากผู้กระทำมีอำนาจกระทำได้จึงไม่เป็นการไม่ชอบด้วยกฎหมายแต่อย่างใด

แต่ถ้าจะแปลความหมายของคำว่า “โดยมิชอบ” ว่าหมายถึงโดยปราศจากอำนาจ (unauthorized) แล้ว จะมีความหมายกว้างกว่าที่จะแปลความหมายว่าโดยมิชอบด้วยกฎหมาย โดยคำว่าโดยปราศจากอำนาจนั้นหมายถึง การทำโดยไม่มีอำนาจ หรือทำโดยไม่มีอำนาจอย่างชัดแจ้งหรือโดยปริยาย[28] และการตีความคำว่าโดยมิชอบว่าหมายถึงโดยปราศอำนาจนี้ก็จะเหมือนกับความผิดในการเข้าถึงโดยปราศจากอำนาจในกฎหมายต่างประเทศ โดยในประเทศสหรัฐอเมริกา อังกฤษ[29] หรือเยอรมัน ก็ใช้ความหมายนี้ในการกำหนดว่าการเข้าถึงจะเป็นความผิดก็ต่อเมื่อเป็นการเข้าถึงโดยปราศจากอำนาจ ซึ่งจากการพิจารณาความหมายของคำ

---

[27] illegal (adj.) Forbidden by law; unlawful (not authorized by law), (Black’s law dictionary; seventh edition)

[28]Unauthorized (adj.) Done without authorized, made without actual, implied, or apperent authority (Black’s law dictionary; seventh edition)

[29] “การเข้าถึงโดยปราศจากอำนาจ” คือ การเข้าถึงของบุคคลในโปรแกรมหรือข้อมูลใดๆ ที่อยู่ในคอมพิวเตอร์นั้นโดยเขาไม่มีสิทธิที่จะเข้าถึงโปรแกรมหรือข้อมูลนั้น หรือ เขาไม่ได้รับอนุญาตให้เข้าถึงโปรแกรมหรือข้อมูลนั้น (Computer Misuse Act 1990 (CMA) มาตรา 17)

ว่า “โดยปราศจากอำนาจ” ที่ปรากฏอยู่ในกฎหมายต่างประเทศนั้น มีผู้สรุปได้ว่าการเข้าถึงโดยปราศจากอำนาจ อาจเทียบเคียงได้กับการเข้าถึงโดยไม่ได้รับอนุญาตนั่นเอง[30] โดยอาจเกิดจากกฎเกณฑ์หรือสัญญาก็ได้

อย่างไรก็ตามการให้ความหมายว่าการเข้าถึงโดยมิชอบหมายถึงการเข้าถึงโดยปราศจากอำนาจก็ไม่สามารถครอบคลุมกระทำที่เป็นความผิดได้ทั้งหมด และยังมีปัญหาที่เกิดการโต้เถียงกันหลายกรณี เช่น คำว่าโดยปราศจากอำนาจนั้นครอบคลุมเพียงใดนอกจากอำนาจตามกฎหมายแล้วจะรวมตลอดถึงข้อสัญญาต่างๆ ด้วยหรือไม่ โดยศาลสหรัฐอเมริกาเห็นว่าการเข้าถึงโดยปราศจากอำนาจนั้นรวมทั้งอำนาจตามกฎหมายและอำนาจตามสัญญาด้วย หากแต่มีผู้ไม่เห็นด้วยกับแนวทางการตีความดังกล่าวและเห็นว่าการเข้าถึงโดยปราศจากอำนาจนั้นควรใช้ในกรณีที่เป็นการฝ่าฝืนข้อกฎหมายหรือระเบียบข้อกำหนดเท่านั้น ไม่ควรตีความรวมตลอดไปถึงข้อสัญญาด้วย[31] นอกจากนี้ การเข้าถึงบางลักษณะที่เป็นการเข้าถึงโดยมีอำนาจ หากแต่เข้าไปทำสิ่งที่ไม่ถูกต้องกับระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ เช่น การเข้าไปโดยมีอำนาจแต่เข้าไปขโมยข้อมูล จะถือว่าเป็นการเข้าถึงโดยปราศอำนาจหรือไม่ ซึ่งแม้แต่ในต่างประเทศเองประเด็นปัญหานี้ก็ยังเป็นที่ถกเถียงกันว่าการกระทำนั้นเป็นความผิดหรือไม่เนื่องจากผู้กระทำมีอำนาจที่จะกระทำได้ตามสิทธิที่ตนมี และคำพิพากษาของศาลก็ไม่เป็นไปในทางเดียวกัน

การที่แนวทางในการตัดสินคดีของศาลไม่เป็นแนวทางเดียวกันนั้นก่อให้เกิดความไม่แน่นอนว่าการกระทำเช่นใดจึงจะเป็นความผิดหรือไม่เป็นความผิดตามกฎหมาย เช่น ในประเทศอังกฤษ ในคดีที่มีการใช้อำนาจตามตำแหน่งหน้าที่เข้าถึงข้อมูลโดยมีวัตถุประสงค์ส่วนตัว พฤติกรรมเช่นนี้จะถือว่าเป็นการเข้าถึงโดยปราศจากอำนาจหรือไม่ ซึ่งศาลในประเทศอังกฤษเองก็มีคำตัดสินที่ไม่เป็นแนวเดียวกันโดยคดีของ R v Bow Street Magistrates Court and Allison ศาลตัดสินว่า ลูกจ้างมีความผิดในการเข้าถึงโดยปราศจากอำนาจ ตามมาตรา 1 CMA เพราะลูกจ้างรู้ว่าตนเองไม่มีอำนาจในการเข้าถึง

---

[30] Orin S. Kerr, “Cybercrime's Scope: Interpreting 'Access' and Authorization' in Computer Misuse Statutes,” [Online]

[31] Ibid.,

แต่ในคดี DPP v Bignell [1998] ที่ตำรวจสองนายใช้อำนาจเรียกข้อมูลจากคอมพิวเตอร์สำนักงานตำรวจแห่งชาติ (the police national computer) จากผู้ปฏิบัติที่มีจุดประสงค์เพื่อใช้ในทางสาธารณะเท่านั้น แต่นายตำรวจนั้นกระทำไปเพื่อจุดประสงค์ส่วนตัว ศาลตัดสินว่าการกระทำของตำรวจทั้งสองไม่เป็นความผิด เนื่องจากตำรวจทั้งสองนายมีอำนาจในการเข้าถึงข้อมูลนั้น

การตัดสินที่มีความขัดแย้งกันอยู่ในลักษณะนี้ก็ปรากฏอยู่ในศาลของมลรัฐและศาลรัฐบาลกลางของสหรัฐอเมริกา เช่นคดี Shurgard Storage Center Inc. v. Safeguard Self Storage, Inc., และคดี United States v. Czubinski, (ดังที่ได้กล่าวมาแล้วในบทที่ 3) ตัดสินว่าการที่ลูกจ้างส่งข้อมูลของนายจ้างไปยังเพื่อนหรือคู่แข่งทางการค้าของนายจ้าง เป็นการเข้าถึงนั้นปราศจากอำนาจโดยกรณีนี้นายจ้างมีสิทธิจำกัดสิทธิของลูกจ้างในการใช้คอมพิวเตอร์ของบริษัทซึ่งนายจ้างอนุญาตให้เข้าถึงเพียงเพื่อการทำงานเท่านั้น

แต่ในคดีของ State v. Olson นั้นตรงกันข้ามกับคดีข้างต้น โดยข้อเท็จจริงที่ว่านาย Olson ได้ใช้ข้อมูลคอมพิวเตอร์ของตำรวจเข้าไปเพื่อหารายละเอียดเกี่ยวกับใบอนุญาตขับรถยนต์ของนักศึกษาหญิงคนหนึ่งนั้น ศาลเห็นว่าการเข้าถึงโดยเหตุผลส่วนตัวนั้นไม่ใช่การเข้าถึงโดยปราศจากอำนาจ เพราะเป็นเพียงเหตุผลส่วนตัวและไม่ได้หาประโยชน์จากกฎของสถานที่ทำงาน เช่นเดียวกับคดีของ Briggs v. State ที่ศาลตัดสินว่านาย Briggs ไม่มีความผิดในการเข้าถึงโดยปราศจากอำนาจ เนื่องจากในฐานะผู้ดูแลระบบแล้วนาย Briggs มีอำนาจเข้าคอมพิวเตอร์ของนายจ้างแม้ว่าจะได้ทำในสิ่งที่ไม่มีกฎอนุญาตให้ทำ

ในกรณีดังที่กล่าวมานี้ หากศาลไทยแปลความหมายว่าการเข้าถึงโดยมิชอบหมายถึงการเข้าถึงโดยปราศจากอำนาจแล้ว ศาลไทยก็อาจจะต้องเผชิญกับปัญหาเช่นเดียวกับศาลในต่างประเทศว่า หากลูกจ้างหรือผู้ปฏิบัติงานในหน่วยงานต่างๆ กระทำการในอำนาจหน้าที่ของตนแต่การกระทำนั้นขัดต่อประโยชน์ของนายจ้างหรือหน่วยงานของตน เช่น แอบคัดลอกข้อมูลของนายจ้างที่อยู่ในความดูแลของตนไปให้ผู้อื่น หรือใช้อำนาจหรือหน้าที่ที่ตนมีเข้าถึงข้อมูลเพื่อนำไปใช้ประโยชน์ส่วนตัว จะเป็นความผิดฐานเข้าถึงโดยมิชอบหรือไม่

โดยแนวความคิดเกี่ยวกับกรณีเหล่านี้เกิดข้อถกเถียงกันในต่างประเทศเนื่องจากการแยกออกเป็นสองมุมมอง คือ[32] มองในแง่พฤติกรรมและมองในแง่ข้อกำหนด หากมองในแง่พฤติกรรมแล้ว การกระทำที่เป็นปฏิปักษ์แก่เจ้าของย่อมเป็นการไม่ชอบ การใดๆ ที่ทำลงย่อมไม่มีอำนาจกระทำได้ ผู้กระทำจึงมีความผิดในการเข้าถึงโดยมิชอบโดยเทียบเคียงกับคดี Shurgard Storage Center Inc. v. Safeguard Self Storage, Inc., และคดี United States v. Czubinski (ดังที่ได้กล่าวมาแล้วในบทที่ 3)

แต่หากมองในแง่ข้อกำหนดแล้ว ลูกจ้างมีอำนาจในการเข้าถึงข้อมูลที่ตนมีสิทธิการเข้าถึงนั้นย่อมเป็นการเข้าถึงโดยชอบ แม้ลูกจ้างจะก่อให้เกิดผลร้ายต่อนายจ้างก็ไม่เป็นความผิดในการเข้าถึงแต่อย่างใด โดยเทียบเคียงกับคดี DPP v Bignell หรือคดี State v. Olson ดังที่ได้กล่าวมาแล้วในบทที่ 3 เช่นกัน[33]

หากศาลไทยมีแนวคิดในการเข้าถึงว่าหากการเข้าถึงโดยมิชอบคือการเข้าถึงโดยปราศจากอำนาจแล้ว การเข้าถึงนั้นก็ไม่เป็นความผิดในการเข้าถึงโดยมิชอบ เนื่องจากเป็นผู้มีอำนาจที่จะเข้าถึงได้ทำให้การเข้าถึงนั้นไม่เกี่ยวข้องกับการกระทำความผิดอื่นที่ตามมาแต่อย่างใด โดยมองเปรียบเทียบกับความผิดฐานบุกรุกซึ่งหากเข้ามาโดยชอบแล้ว แม้จะกระทำความผิดอื่นก็ไม่เป็นความผิดฐานบุกรุกอีก ซึ่งจะทำให้มีปัญหาในการนำตัวผู้กระทำความผิดมาลงโทษเนื่องจากในความผิดบางประเภท เช่น การขโมยข้อมูล ไม่เป็นการกำหนดเป็นฐานความผิดที่แยกออกไปจากการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ ทำให้หากเกิดการกระทำความผิดขึ้นก็จะไม่มีกฎหมายที่จะลงโทษได้ เนื่องจากกาเข้าถึงนั้นชอบแล้ว

นอกจากการแปลความหมายคำว่า “โดยมิชอบ” ว่า หมายถึง ไม่ชอบด้วยกฎหมายหรือโดยปราศจากอำนาจแล้ว เราอาจจะสามารถแปลความคำว่าโดยมิชอบได้อีกทางหนึ่งที่มีความหมายครอบคลุมกว่าการแปลความในสองกรณีข้างต้นโดยอาศัยคำพิพากษาศาลฎีกาเป็นเกณฑ์ในการกำหนดหลักเกณฑ์ในการตีความ ซึ่งคำว่า “โดยมิชอบ” อาจตีความตามแนวคำพิพากษาของศาลฎีกาที่เคยพิจารณาคำว่า “โดยมิชอบ” ไว้ และเห็นได้ว่ามีความหมายค่อนข้างกว้างทั้งทางแพ่งและทางอาญา ตามแต่ละคดีที่ศาลเห็นสมควร เช่น ศาลฎีกาเคย

---

[32] Ibid.,

[33] Ibid.,

ตีความคำว่า “โดยมิชอบ” ไว้ว่า หมายถึง ปราศจากสิทธิโดยชอบ[34] ไม่ระมัดระวังตามหน้าที่[35] ไม่ซื่อสัตย์สุจริต[36] ประพฤติตนไม่สมควร[37] ทุจริตต่อหน้าที่ [38] ฝ่าฝืนต่อกฎระเบียบและคำสั่งของผู้บังคับบัญชา[39] กระทำลงโดยไม่คำนึงถึงความเสียหายใดๆ[40] ไม่ขวนขวายดำเนินการตามหน้าที่และระเบียบข้อบังคับ[41] เบียดบังเวลาและทรัพย์สินของผู้อื่นเพื่อแสวงหาประโยชน์ส่วนตัว[42] ฝ่าฝืนระเบียบแบบแผนหรือระเบียบปฏิบัติ[43] มีเจตนาทุจริต[44] ใช้ประโยชน์ส่วนตัว[45] ทำให้ผู้อื่นได้รับประโยชน์โดยไม่ควร[46] ละเว้นไม่ตรวจสอบความถูกต้องแท้จริง[47] ฝ่าฝืนคำสั่ง[48] ละเลยไม่ปฏิบัติหน้าที่[49] กระทำการนอกหน้าที่[50] ทำโดยปราศจากอำนาจ[51] ขู่เข็ญใช้อำนาจครอบงำผิดคลองธรรม[52] กระทำลงทั้งที่เล็งเห็นผลความเสียหายที่จะเกิดขึ้น[53] ฝ่าฝืนระเบียบ[54] ใช้ดุลพินิจตาม

---

[34] คำพิพากษาฎีกาที่ 23/2540

[35] คำพิพากษาฎีกาที่ 109/2532

[36] คำพิพากษาฎีกาที่ 186-188/2477

[37] คำพิพากษาฎีกาที่ 944/2496

[38] คำพิพากษาฎีกาที่ 1161/2538

[39] คำพิพากษาฎีกาที่ 2125/2530

[40] คำพิพากษาฎีกาที่ 2503/2530

[41] คำพิพากษาฎีกาที่ 2577/2534

[42] คำพิพากษาฎีกาที่ 2621/2538

[43] คำพิพากษาฎีกาที่ 2811/2516

[44] คำพิพากษาฎีกาที่ 2830/2524

[45] คำพิพากษาฎีกาที่ 3333/2545

[46] คำพิพากษาฎีกาที่ 3162/2529

[47] คำพิพากษาฎีกาที่ 3295/2543

[48] คำพิพากษาฎีกาที่ 3296/2530

[49]คำพิพากษาฎีกาที่ 3346/2541

[50] คำพิพากษาฎีกาที่ 3738/2533

[51] คำพิพากษาฎีกาที่ 3803/2540

[52] คำพิพากษาฎีกาที่ 3805/2526

[53] คำพิพากษาฎีกาที่ 4076/2534

อำเภอใจหรือโดยปราศจากเหตุผล[55] การเลือกปฏิบัติ[56] ใช้ประโยชน์จากทรัพย์สินของผู้อื่นโดยผู้นั้นไม่ยินยอม[57]

จะเห็นได้ว่าศาลฎีกาตีความหรือให้ความหมายของคำว่าโดยมิชอบไว้อย่างหลากหลายไม่ใช่เพียงแค่ไม่ชอบด้วยกฎหมายหรือโดยปราศจากอำนาจเท่านั้น และในบางครั้งแม้การกระทำบางอย่างจะผิดระเบียบหรือไม่ชอบด้วยกฎหมายโดยตรง หากแต่ศาลก็ใช้ดุลพินิจพิจารณาว่าการกระทำนั้นไม่เป็นความผิด เช่น คำพิพากษาฎีกาที่ 437/2515[58] คำพิพากษาฎีกาที่ 786/2532[59] ซึ่งเป็นการตีความอย่างยืดหยุ่นเพื่อความเป็นธรรม

ดังนั้นหากจะสรุปความหมายของคำว่าโดยมิชอบที่ศาลฎีกาใช้เป็นแนวทางในการพิจารณาพิพากษาคดีแล้ว อาจจะกล่าวกว้างๆ ได้ว่า คำว่าโดยมิชอบนี้หมายถึง ไม่เหมาะสมหรือไม่ถูกต้อง (Improper)[60] โดยเปิดโอกาสให้ศาลได้ใช้ดุลพินิจกำหนดกฎเกณฑ์ว่าการกระทำใดเป็นการกระทำโดยมิชอบโดยพิจารณาเป็นกรณีๆ ไป เพื่อให้เกิดความเป็นธรรมในแต่ละคดี ซึ่งผู้เขียนเองก็มีความเห็นว่า คำว่า “โดยมิชอบ” ในความผิดฐานเข้าถึงโดยมิชอบนี้ควรจะมีความหมายที่กว้าง ซึ่งนอกเหนือจากจะทำให้เจ้าหน้าที่ที่ทำการสืบสวนสอบสวนสามารถทำงานได้อย่างคล่องตัวแล้ว ยังเป็นการเปิดโอกาสให้ศาลใช้ดุลพินิจในการกำหนดกฎเกณฑ์ในการลงโทษผู้กระทำความผิดได้อย่างยืดหยุ่นและปรับเปลี่ยนไปได้ตามสถานการณ์เมื่อต้องเผชิญหน้ากับเทคโนโลยีที่เปลี่ยนแปลงและผู้กระทำผิดที่หลากหลายตามลักษณะการกระทำความผิดที่อาจเกิดขึ้นได้ในอนาคต

---

[54] คำพิพากษาฎีกาที่ 4751/2541

[55] คำพิพากษาฎีกาที่ 7663/2543

[56] คำพิพากษาฎีกาที่ 7728-7731/2544

[57] คำพิพากษาฎีกาที่ 9523/2544

[58] คำพิพากษาฎีกาที่ 437/2515

[59] คำพิพากษาฎีกาที่ 786/2532

[60] Improper (adj.) 1. Incorrect; unsuitable or irregular. 2. Fraudulent or otherwise wrongful (Black’s law dictionary; seventh edition)

นอกจากนี้ แม้ว่าการเข้าถึงโดยมิชอบจะเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หากแต่การเข้าถึงข้อมูลโดยไม่มีอำนาจกระทำโดยทุจริต หรือกระทำการที่ไม่ชอบเพื่อหาประโยชน์ส่วนตัวโดยอาศัยคอมพิวเตอร์หรือแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ก็ไม่ใช่เรื่องใหม่ที่ไม่เคยปรากฏหรือให้ความหมายโดยศาลมาก่อน หากแต่เคยมีคำพิพากษาศาลฎีกาตัดสินว่าการกระทำดังกล่าวเป็นความผิดมาแล้วแม้ว่าจะไม่ใช่การตัดสินฐานเข้าถึงโดยมิชอบก็ตามเนื่องจากในขณะนั้นพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์บังคับใช้ ซึ่งหากเกิดขึ้นในปัจจุบันที่พระราชบัญญัติบังคับใช้แล้วการกระทำดังกล่าวอาจกล่าวได้ว่าเป็นการเข้าถึงโดยมิชอบด้วย เช่น พนักงานไม่ป้อนข้อมูลเข้าคอมพิวเตอร์เพื่อยักยอกทรัพย์[61] ผู้ควบคุมเครื่องคอมพิวเตอร์แก้ไขโปรแกรมในการตรวจข้อสอบ[62] พนักงานลงรายการฝากถอนเงินอันเป็นเท็จในเครื่องคอมพิวเตอร์[63] แก้ไขจำนวนเงินในเครื่องคอมพิวเตอร์ของธนาคารเพื่อยักยอกเงิน[64]

กรณีการเข้าถึงโดยมิชอบนั้น เมื่อพิจารณาจากตัวบทแล้วอาจมีสังเกตได้ว่าคำว่า “โดยมิชอบ” นั้น เป็นองค์ประกอบภายนอกของการกระทำความผิดหรือเป็นเจตนาพิเศษที่นอกเหนือจากเจตนาธรรมดา ซึ่งเจตนาพิเศษคือ “มูลเหตุจูงใจ” ในการกระทำนั้นๆ ซึ่งหากกฎหมายต้องการให้การกระทำความผิดนั้นต้องมีเจตนาพิเศษก็จะกำหนดไว้โดยเฉพาะ โดยสังเกตได้จากคำว่า “เพื่อ” เช่น ความผิดตามมาตรา 157 มีเจตนาพิเศษอยู่ 2 ส่วน ส่วนหนึ่งคือ “เพื่อให้เกิดความเสียหายแก่ผู้หนึ่งผู้ใด” อีกส่วนหนึ่งคือคำว่า “โดยทุจริต” โดยทุจริตนี้ก็เป็นเจตนาพิเศษ ซึ่งนิยามของคำว่าโดยทุจริต ก็คือ เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น โดยเจตนาพิเศษนั้น เนื่องจากกฎหมายใช้คำว่า “เพื่อ” ผู้กระทำจึงต้องมีเจตนาโดยตรงมุ่งต่อการนั้นเท่านั้น จึงจะถือว่าผู้กระทำมีเจตนาพิเศษ[65] ซึ่งคำว่าโดยมิ

---

[61] คำพิพากษาฎีกาที่ 153/2545

[62] คำพิพากษาฎีกาที่ 263/2543

[63] คำพิพากษาฎีกาที่ 7264/2542

[64] คำพิพากษาฎีกาที่ 496/2542

[65] ดร. เกียรติขจร วัจนะสวัสดิ์, คำบรรยายกฎหมายอาญา มาตรา 59-106 สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา ภาคหนึ่ง สมัยที่ 59 ปีการศึกษา 2549 เล่ม 7 หน้า 33.

ชอบไม่ได้มีความหมายในลักษณะที่เป็นเจตนามุ่งต่อการนั้นเหมือนคำว่าโดยทุจริตจึงไม่ใช่เจตนาพิเศษ ดังนั้นเมื่อไม่ใช่เจตนาพิเศษแล้วคำว่าโดยมิชอบที่ปรากฏอยู่ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงเป็นถ้อยคำที่ขยายคำว่า “เข้าถึง” เป็นองค์ประกอบภายนอกอย่างหนึ่งในความผิดฐานเข้าถึงโดยมิชอบ ไม่ใช่องค์ประกอบภายในแต่อย่างใด

ปัญหาอีกอย่างหนึ่งสำหรับความรับผิดในการเข้าถึงโดยมิชอบนั้น คือ ความยินยอมของเจ้าของ เนื่องจากหากเจ้าของยินยอมให้เข้าถึงแล้ว การเข้าถึงนั้นจะชอบถึงเมื่อใด ความยินยอมมีขอบเขตเพียงใด ซึ่งหากเปรียบเทียบกับหลักเกณฑ์ในเรื่องการบุกรุกแล้วจะเห็นได้ว่าหากเจ้าของสถานที่ยินยอมให้เข้ามาแล้วก็จะไม่เป็นการบุกรุก แม้จะกระทำความผิดอื่นก็ไม่ใช่ความผิดฐานบุกรุกแต่อย่างใด และไม่ถือว่ามีการบุกรุกเพื่อกระทำความผิดนั้น เช่นการลักทรัพย์ในเคหสถาน หากเข้าไปโดยได้รับอนุญาตหรือเห็นได้โดยปริยายว่าเจ้าของสถานที่อนุญาตอยู่ในตัว แม้จะอนุญาตให้เข้าไปโดยเหตุผลอื่นไม่ใช่ให้เข้าไปลักทรัพย์ก็ไม่เป็นความผิดฐานบุกรุก และแม้จะลักทรัพย์ไปก็ไม่เป็นความผิดฐานลักทรัพย์ในเคหสถาน[66] เป็นเพียงลักทรัพย์ธรรมดา ความยินยอมจึงเป็นสิ่งสำคัญที่จะกำหนดว่าการกระทำนั้นเป็นการบุกรุกหรือไม่

หากเทียบกับการเข้าถึงแล้ว จะเห็นได้ว่ามีความไม่ชัดเจนเกิดขึ้นจากลักษณะการกระทำความผิดนั้น เนื่องจากการบุกรุกตามประมวลกฎหมายอาญาเป็นเรื่องทางกายภาพและเป็นการบุกรุกเกิดขึ้นได้เพียงขณะเข้าไปและทันทีที่สามารถเข้าไปได้การบุกรุกนั้นก็สิ้นสุดลง การอยู่ต่อมาเป็นเพียงผลของการบุกรุกเท่านั้น[67] โดยศาสตราจารย์จิตติ ติงศภัทิย์ ได้อธิบายเพิ่มเติมไว้ในหมายเหตุว่า ถ้าจะมีการเข้าไปออกมาแล้วเข้าไปใหม่อยู่ทุกๆ วัน ก็คงไม่ทำให้เป็นการเข้าไปที่เกิดขึ้นใหม่ได้ เพราะการเข้าๆ ออกๆ อยู่ทุกวันก็เป็นการเข้าไปตั้งแต่แรกนั่นเอง ไม่มีการเข้าไปที่เป็นคนละอันต่างหากจากกัน[68] การบุกรุกจึงเกิดขึ้นและสิ้นสุดลงทันทีที่การเข้าไปนั้น

---

[66] คำพิพากษาฎีกาที่ 1076/2526

[67] คำพิพากษาฎีกาที่ 2253/2531

[68] รองศาสตราจารย์ ดร. ทวีเกียรติ มีนะกนิษฐ, <u>คำอธิบายกฎหมายอาญา ภาคความผิดและลหุโทษ</u>, หน้า 215-223.

สำเร็จ หากแต่คำว่าเข้าถึงนั้นมีลักษณะที่แตกต่างกันออกไปเนื่องจากมีปัญหาว่าการเข้าถึงสิ้นสุดลงเมื่อใด

หากจะเทียบกับการบุกรุกแล้ว จะเห็นได้ว่าการบุกรุกคือการเข้าไป แต่คำว่าเข้าถึงนั้น โดยนัยยะแล้วย่อมมีความหมายแตกต่างจากคำว่าบุกรุกที่มีการเข้าไปเกิดขึ้น หากแต่การเข้าถึงโดยมิชอบนั้นมีการให้ความหมายแตกต่างกัน ซึ่งอาจจะมองได้ใน 2 แง่มุม คือ เห็นได้ว่าเมื่อการเข้าถึงนั้นชอบด้วยกฎหมายหรือมีอำนาจก็จะทำให้การกระทำต่อมาหลังจากการเข้าถึงแล้วนั้นย่อมไม่เป็นความผิดฐานเข้าถึงอีกเนื่องจากการเข้าถึงในตอนแรกชอบแล้วผู้เข้าถึงมีสิทธิที่จะกระทำได้ ความยินยอมย่อมทำให้การเข้าถึงนั้นชอบ เช่นเดียวกับการเข้าไปโดยชอบแล้วทะเลาะกันภายหลังก็ไม่เป็นบุกรุก[69] และแม้จะเข้าไปกระทำความผิดอื่นก็ไม่ผิดฐานบุกรุกอีกเนื่องจากการเข้าไปชอบแล้ว แม้จะกระทำความผิดอื่นก็ไม่ใช่ความผิดฐานบุกรุกแต่อย่างใด และไม่ถือว่ามีการบุกรุกเพื่อกระทำความผิดนั้น[70] ซึ่งการตีความดังกล่าวจะทำให้คำว่าเข้าถึงโดนมิชอบนั้นมีลักษณะที่ไม่แตกต่างจากการบุกรุกทางกายภาพแต่อย่างใด และความยินยอมในความผิดฐานเข้าถึงโดยมิชอบทำให้การเข้าถึงไม่เป็นความผิด[71] เพราะขาดองค์ประกอบภายนอกไม่ถือว่าเป็นการเข้าถึงโดยมิชอบ

โดยประเด็นที่น่าพิจารณาต่อมาก็คือการที่อนุญาตให้เข้าถึงโดยไม่ได้อนุญาตให้กระทำการที่ไม่ชอบใดๆ หากแต่ผู้เข้าถึงที่ได้รับอนุญาตนั้นได้ทำการที่เป็นปฏิปักษ์กับเจ้าของหรือเป็นผลร้ายกับเจ้าของนั้นถือว่าจะกลับกลายเป็นความผิดหรือไม่ ถ้าเทียบกับการบุกรุกแล้ว จะเห็นได้ว่าการอนุญาตให้เข้าไปเพียงส่วนใดส่วนหนึ่งของเคหสถาน จะถือว่าอนุญาตให้เข้าไปในส่วนอื่นด้วยไม่ได้ เช่น อนุญาตให้เข้าไปในห้องนั่งเล่นไม่ได้อนุญาตให้เข้าไปในห้องนอน[72] เข้าไปในห้องนอนโดยไม่ได้รับอนุญาตให้เข้าไป[73] แต่อย่างไรก็ตามการเข้าถึงนั้นไม่มีลักษณะทาง

---

[69] คำพิพากษาฎีกาที่ 2941/40

[70] คำพิพากษาฎีกาที่ 772/52534

[71] ดร. เกียรติขจร วัจนะสวัสดิ์, คำอธิบายกฎหมายอาญา ภาค 1, หน้า 414-420.

[72] คำพิพากษาฎีกาที่ 2407/2527

[73] คำพิพากษาฎีกาที่ 2329/2536

กายภาพเหมือนการบุกรุกเนื่องจากการบุกรุกที่เกินขอบเขตนั้นคือเกินขอบเขตพื้นที่ที่เจ้าของอนุญาตซึ่งมีอาณาเขตที่เห็นได้ เช่น อนุญาตให้เข้าห้องนั่งเล่น ย่อมไม่ได้หมายความว่าอนุญาตให้เข้าไปยังห้องนอน โดยระหว่างห้องนอนกับห้องนั่งเล่นมีขอบเขตที่ชัดเจนอยู่ หากแต่การเข้าถึงโดยมิชอบนั้นไม่จำเป็นต้องทำในพื้นที่ที่เกินขอบเขตของพื้นที่ที่ได้รับอนุญาตแต่อย่างใด อาจจะกระทำสิ่งที่เป็นผลร้ายต่อเจ้าของทั้งที่อยู่ในขอบเขตที่อนุญาตให้ใช้ก็ได้ และแม้แต่ในเรื่องการบุกรุกเองก็มีกรณีที่ว่า ร้านค้าแม้ใช้เป็นที่อยู่อาศัยแต่ขณะเกิดเหตุลักทรัพย์เป็นเวลากลางวัน ไม่เป็นลักทรัพย์ในเคหสถาน[74]

แต่อย่างไรก็ตามเนื่องจากคำว่า “เข้าถึง” นั้น มีความหมายที่แตกต่างจากคำว่า “บุกรุก” จึงอาจมองได้ในอีกแง่มุมหนึ่งว่าการเข้าถึงคอมพิวเตอร์นั้นหากการเข้าถึงยังคงมีอยู่ตลอดไปตราบใดที่ยังมีการสื่อสารกับคอมพิวเตอร์อยู่ ไม่ว่าจะได้รับอนุญาตโดยชอบหรือมีอำนาจตามกฎหมายแล้วก็ตาม ก็อาจเป็นการเข้าถึงโดยมิชอบได้ทันทีที่ผู้ที่เข้าถึงนั้นกระทำสิ่งที่ไม่ถูกต้องหรือไม่เหมาะสมขึ้น เช่น การขโมยข้อมูลในคอมพิวเตอร์ที่ตนได้รับอนุญาตให้เข้าถึงได้ เนื่องจากผู้ที่อนุญาตให้เข้าถึงนั้นไม่มีเจตนาให้ผู้ที่ได้รับอนุญาตกระทำสิ่งที่ตนไม่ต้องการเช่น ขโมยข้อมูล เป็นต้น ซึ่งการให้ความหมายดังกล่าวจะทำให้ฐานความผิดนั้นครอบคลุมไปถึงกรณีที่เข้าไปโดยได้รับอนุญาตแต่ไปทำความเสียหายหรือทำสิ่งที่ไม่เหมาะสมด้วย ซึ่งหากพิจารณาในแง่นี้แล้ว การเข้าถึงจะคงอยู่ตลอดและเมื่อทำสิ่งที่ไม่ชอบขึ้น เช่น ขโมยข้อมูล การเข้าถึงที่ชอบนั้นก็จะเป็นการเข้าถึงที่ไม่ชอบและเป็นความผิดทันที

5.2.3 ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์

ดังที่ได้กล่าวถึงนิยามของคำว่าระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แล้ว จะเห็นได้ว่าความหมายของคำว่าระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์มีความทับซ้อนกันอยู่ในส่วนที่เรียกว่าเป็นคำสั่ง หรือชุดคำสั่ง ที่มีปรากฏทั้งในนิยามของคำว่าระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ จึงทำให้เกิดข้อสังเกตขึ้นว่าการเข้าถึงระบบคอมพิวเตอร์นั้นเป็นไปไม่ได้ที่จะไม่เข้าถึงข้อมูลคอมพิวเตอร์ เนื่องจากระบบคอมพิวเตอร์นั้นจะทำงานได้ก็ต้องมีระบบปฏิบัติการ

---

[74] คำพิพากษาฎีกาที่ 2193/2534

ของคอมพิวเตอร์ เช่น วินโดว์ ลีนุ๊ก หรือแม็คอินทอช อยู่ มิฉะนั้นคอมพิวเตอร์ก็จะไม่สามารถจัดการข้อมูลได้ตามที่ต้องการ

ดังนั้นการเปิดเครื่องคอมพิวเตอร์คือการเปิดให้ระบบปฏิบัติการทำงานนั่นเอง ในขณะเดียวกันระบบปฏิบัติการที่กล่าวมานี้ก็คือคำสั่งหรือชุดคำสั่งอยู่ในนิยามทั้งคำว่าระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ ทันทีที่กรอกรหัสผ่านแล้วก็จะเข้าถึงทั้งระบบคอมพิวเตอร์และข้อมูลทางคอมพิวเตอร์อย่างไม่อาจแบ่งแยกได้ ผู้เขียนจึงไม่เห็นความจำเป็นที่จะต้องแยกการเข้าถึงระบบคอมพิวเตอร์ออกจากข้อมูลคอมพิวเตอร์แต่อย่างใด หากไม่ได้มีความมุ่งหมายที่จะคุ้มครองอุปกรณ์หรือชุดอุปกรณ์ทางกายภาพเพียงอย่างเดียว เนื่องจากไม่สมประโยชน์ในการมุ่งคุ้มครองตามกฎหมายที่เห็นว่าการเข้าถึงข้อมูลเป็นเรื่องร้ายแรงกว่าการเข้าถึงระบบเพียงอย่างเดียว กฎหมายจึงได้แยกการเข้าถึงระบบคอมพิวเตอร์และการเข้าถึงข้อมูลคอมพิวเตอร์ออกจากกัน หากแต่ถ้าพิจารณาจากคำนิยามแล้วจะกลายเป็นว่าผู้ที่เข้าถึงระบบคอมพิวเตอร์ก็ต้องรับโทษในการเข้าถึงข้อมูลคอมพิวเตอร์ด้วยอย่างหลีกเลี่ยงไม่ได้ และอาจเป็นกรรมเดียวผิดกฎหมายหลายบท และรับโทษไม่แตกต่างจากผู้ที่เข้าถึงข้อมูลคอมพิวเตอร์เพียงอย่างเดียว

โดยในกฎหมายของประเทศสหรัฐอเมริกาและประเทศอังกฤษก็ไม่ได้มีการแยกระบบคอมพิวเตอร์ออกจากข้อมูลคอมพิวเตอร์แต่อย่างใด หากแต่ทั้งสองประเทศดังกล่าวกำหนดไว้คล้ายคลึงกันว่าการเข้าถึงที่จะเป็นความผิดนั้นคือการเข้าถึงคอมพิวเตอร์เพื่อที่จะเข้าถึงข้อมูลคอมพิวเตอร์ที่อยู่ในคอมพิวเตอร์นั้น ในขณะที่ในประเทศเยอรมันเองก็ได้มีการแก้ไขกฎหมายและกำหนดให้การเข้าถึงข้อมูลโดยเป็นความผิดโดยไม่ได้กำหนดความผิดในการเข้าถึงระบบคอมพิวเตอร์ ซึ่งประเทศต่างๆ นั้นเล็งเห็นว่าสิ่งที่สำคัญที่ผู้ไม่ประสงค์ดีหรือ hacker ต้องการนั้นไม่ใช่ตัวระบบคอมพิวเตอร์ที่เป็น hardware หากแต่มุ่งประสงค์ที่จะเข้าถึงข้อมูล การเข้าถึงระบบคอมพิวเตอร์จึงไม่ใช่สาระสำคัญที่จะต้องออกเป็นกฎหมายอาญาเพื่อลงโทษผู้กระทำผิด และเนื่องจากตามคำนิยามของพระราชบัญญัตินี้ก็ได้นิยามคำว่าข้อมูลคอมพิวเตอร์ครอบคลุมไปถึงระบบปฏิบัติการที่เป็นคำสั่งหรือชุดคำสั่งแล้ว จึงสามารถที่จะเอาลงโทษผู้เข้าถึงระบบปฏิบัติการได้โดยไม่ต้องแยกเป็นฐานความผิดต่างหาก

5.2.4 มาตรการป้องกันการเข้าถึงโดยเฉพาะ

คำว่า “มาตรการป้องกันการเข้าถึงโดยเฉพาะ” นั้น เป็นถ้อยคำหนึ่งในกฎหมายที่ต้องมีการพิจารณาว่าอย่างไรจึงจะถือว่าเป็นมาตรการป้องกันการเข้าถึงโดยเฉพาะ จำเป็นต้องมี

วิธีการโดยเฉพาะเพื่อให้เห็นว่าเป็นการห้ามมิให้เข้าถึงหรือไม่ ซึ่งในประเทศสหรัฐอเมริกาและประเทศอังกฤษนั้นไม่มีองค์ประกอบในส่วนนี้ หากแต่ปรากฏอยู่ในกฎหมายเกี่ยวกับประเทศเยอรมันที่กำหนดว่าจะเป็นความผิดในการเข้าถึงข้อมูลได้ ข้อมูลนั้นต้องมีมาตรการรักษาความปลอดภัยโดยเฉพาะสำหรับป้องกันมิให้มีการเข้าถึงข้อมูลนั้นได้

ดังที่ได้กล่าวมาแล้วข้างต้นว่าองค์ประกอบในส่วนนี้อาจจะเป็นปัญหาในการบังคับใช้กฎหมายและการปฏิบัติหน้าที่โดยรัฐ แต่อย่างไรก็ตามเมื่อบทบัญญัติในการเข้าถึงโดยมิชอบได้กำหนดให้มาตรการป้องกันการเข้าถึงโดยเฉพาะเป็นองค์ประกอบหนึ่งของกฎหมายอาญาแล้ว ผู้เขียนก็จะขอแยกพิจารณาได้ ดังนี้

การเข้าถึงที่จะเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ต้องเป็นการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีการป้องกันไว้โดยเฉพาะ ซึ่งตามปกติแล้วก็คือกรณีที่การห้ามไม่ให้เข้าถึงโดยเจ้าของระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์นั้นได้กำหนดวิธีการที่จะตรวจสอบสิทธิของผู้ที่จะเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์นั้นไว้ เช่น รหัสผ่าน การ์ด กุญแจ หรือ ไบโอเมตริกซ์ (เช่น การแสกนนิ้ว หรือม่านตา) เมื่อผู้เข้าถึงมีสิทธิถูกต้องแล้วก็สามารถเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ถูกป้องกันไว้ได้ และตามพระราชบัญญัตินี้ก็เขียนรายละเอียดไว้ว่าการเข้าถึงนั้นต้องเป็นการเข้าถึงที่มีการป้องกันการเข้าถึงโดยเฉพาะ หากไม่มีการป้องกันก็ถือว่าไม่ประสงค์จะไม่ให้คนอื่นเข้าถึง ถ้าเข้าถึงก็ไม่เป็นความผิด

สิ่งที่จะต้องพิจารณาเป็นสิ่งแรกคือ อะไรคือมาตรการป้องกันการเข้าถึงโดยเฉพาะ หากเป็นการกำหนดให้ใส่ชื่อและรหัส การแสกนนิ้วหรือม่านตา รวมถึงการติดตั้งไฟล์วอร์ ก็อาจเรียกได้ว่าเป็นการป้องกันการเข้าถึงได้ หากแต่ถ้าเป็นกรณีเช่น เอเป็นเด็กอายุเพียง 17 ปี หากแต่ได้เข้าไปในเวปไซต์สำหรับผู้ใหญ่ โดยก่อนที่จะเข้าถึงเนื้อหาภายในนั้น หน้าเวปไซต์ได้มีข้อกำหนดในการใช้บริการโดยถามว่ามีอายุเกิน 18 ปี หรือไม่ โดยเอได้กดตกลงว่าตนเองอายุเกิน 18 ปี และสามารถเข้าไปในเวปไซต์ได้ ปัญหาที่ตามมาคือ การกำหนดและถามดังกล่าวนั้น

เป็นมาตรการป้องกันการเข้าถึงแล้วหรือไม่ เนื่องจากหากกดว่าอายุไม่ถึง 18 ปี ก็ไม่สามารถเข้าถึงข้อมูลได้ เป็นการห้ามมิให้เด็กอายุไม่ถึง 18 ปีเข้าไปใช้บริการของทางเวปไซต์[75]

ซึ่งในกรณีนี้หากนำไปเปรียบเทียบกับสภาพของความเป็นจริงแล้ว การกระทำนี้อาจเทียบเคียงได้ว่าการกำหนดกฎเกณฑ์ดังกล่าวก็เหมือนสถานบริการเขียนป้ายว่าเด็กอายุไม่เกิน 18 ปี ห้ามเข้า แต่หากเข้าไปผู้เข้าก็ไม่มีความผิดและลงโทษตามกฎหมาย[76] ดังนั้นผู้เขียนจึงมีความเห็นว่า กรณีดังกล่าวยังไม่เป็นการป้องกันการเข้าถึงโดยเฉพาะ เนื่องจากไม่มีการตรวจสอบและมีลักษณะบังคับอย่างแท้จริงว่าต้องเป็นผู้ที่มีอายุเกิน 18 ปี หากแต่เป็นเพียงการสอบถามให้ผู้ใช้ตระหนักถึงสถานภาพของตนเท่านั้น ไม่มีสภาพบังคับแต่อย่างใด

โดยกรณีเวปไซต์ที่มีการกำหนดกฎเกณฑ์เกี่ยวกับการป้องกันไว้นั้น มีความชัดเจนแล้วว่าเจ้าของไม่ต้องการที่จะให้เข้าถึงหากแต่ผู้เข้าถึงที่ไม่มีสิทธิ์เข้าถึงได้พยายามเข้าถึงโดยวิธีการต่างๆ ที่เจ้าของไม่ต้องการ ดังนั้นผู้ที่พยายามเข้าถึงจึงเป็นผู้กระทำกระทำความผิดตามกฎหมายที่เห็นได้ชัดเจนอยู่แล้ว แต่ในบางกรณี เช่น กรณีที่มีบุคคลอื่นทำการบล็อกเวปไซต์ของบุคคลอีกคนหนึ่งเพื่อไม่ให้บุคคลอื่นเข้าถึงเวปไซต์นั้นได้ เป็นการกระทำที่ไม่ถูกต้องเนื่องจากผู้กระทำไม่มีสิทธิที่จะทำการหวงห้ามไม่ให้ผู้ใดก็ตามเข้าถึงเวปไซต์ของบุคคลอื่นได้ หากมีผู้กระทำการดังกล่าวขึ้น และผู้อื่นที่ประสงค์จะเข้าถึงเวปไซต์นั้นได้กระทำการใดๆ เพื่อที่จะเข้าถึงเวปไซต์นั้น ผู้ที่เข้าถึงนั้นย่อมไม่มีความผิดตามกฎหมายเนื่องจากผู้ทำการป้องกันไม่มีอำนาจที่จะทำการป้องกันได้ เปรียบเสมือนการนำสิ่งกีดขวางไปล้อมไว้ในที่สาธารณะเพื่อไม่ให้บุคคลอื่นเข้าถึง ทั้งที่ผู้ทำการหวงห้ามไม่มีสิทธิแต่อย่างใด หากมีผู้ที่จะข้ามผ่านสิ่งกีดขวางเข้าไปในที่สาธารณะแล้วย่อมไม่มีความผิด ซึ่งเป็นหลักการเดียวกับการเข้าถึงเวปไซต์ที่ถูกป้องกันโดยผู้ไม่มีสิทธิ

แต่ประเด็นที่ผู้เขียนเห็นว่าจะเป็นปัญหาในการพิจารณาในเรื่องการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีระบบป้องกันการเข้าถึงโดยเฉพาะนั้น คือกรณีที่เจ้าหน้าที่

---

[75] Orin S. Kerr, "Cybercrime's Scope: Interpreting 'Access' and Authorization' in Computer Misuse Statutes," [Online]

[76] "คำอธิบายกฎหมายสถานบริการ," [Online] แหล่งที่มา : www.wangchaiya.com/data/stanborikarn.pdf [10 มกราคม 2551]

ที่มีอำนาจตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ทำการป้องกันไม่ให้ผู้ใช้บริการอินเทอร์เน็ตเข้าไปยังเวปไซต์ที่ไม่สมควร (การบล็อกเวปไซต์) ตามอำนาจที่มีอยู่ตามมาตรา 20 แห่งพระราชบัญญัตินี้ แล้วมีบุคคลทำการด้วยวิธีการใดๆ เพื่อเข้าไปสู่เวปไซต์ที่ทำการบล็อกไว้ได้ ซึ่งในกรณีนี้ผู้กระทำจะมีความผิดหรือไม่ โดยจะถือว่าการที่เจ้าหน้าที่ที่ทำการบล็อกเวปไซต์นั้นเป็นกรณีที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนหรือไม่ เนื่องจากมีความแตกต่างกันในผู้ทำการป้องกันและเจตนาในการป้องกัน โดยการป้องกันโดยทั่วไปนั้นหมายถึงเจ้าของระบบหรือเจ้าของข้อมูลนั้นเองไม่ประสงค์ให้บุคคลอื่นที่ไม่ได้รับอนุญาตให้เข้าไปในส่วนที่ตนหวงห้ามไว้ แต่กรณีที่เจ้าหน้าที่ที่อาศัยอำนาจตามกฎหมายทำการบล็อกเวปไซต์นั้นเป็นกรณีที่เจ้าของเวปไซต์ไม่ได้ห้ามการเข้าถึงแต่อย่างใด หากแต่เจ้าพนักงานของรัฐทำการบล็อกเวปไซต์ดังกล่าวเองตามบทบัญญัติของกฎหมาย

ผู้เขียนเห็นว่า กรณีการบล็อกเวปไซต์นั้น หากเป็นกรณีที่ทางเจ้าหน้าที่ขอความร่วมมือโดยขอให้ผู้ให้บริการจำกัดไม่ให้เข้าถึงเวปไซต์ที่ไม่เหมาะสมโดยไม่ได้ใช้อำนาจตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แล้ว ผู้เขียนเห็นว่าการเข้าถึงเวปไซต์เหล่านั้นโดยวิธีการอื่นๆ เพื่อหลบเลี่ยงการป้องกันการเข้าถึงไม่เป็นความผิดฐานเข้าถึงโดยมิชอบ เนื่องจากไม่มีอำนาจตามกฎหมายที่จะมาบังคับไม่ให้เข้าถึงได้ และการเข้าถึงข้อมูลต่างๆ ที่เจ้าของไม่หวงห้ามก็เป็นสิทธิเสรีภาพของประชาชนในการเข้าถึงเวปไซต์ดังกล่าว

แต่ในกรณีที่เจ้าหน้าที่ใช้อำนาจตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อทำการปิดกั้นไม่ให้เข้าถึงเวปไซต์นั้น ผู้เขียนมีความเห็นว่าการป้องกันการเข้าถึงนั้นแม้จะไม่ได้กระทำโดยเจ้าของเวปไซต์นั้นก็ตาม หากแต่เจ้าหน้าที่มีอำนาจตามกฎหมายที่จะกระทำได้ เปรียบเสมือนการเข้าไปในบ้านที่ถูกรัฐยึดหรือสถานที่เกิดเหตุที่ห้ามบุคคลภายนอกเข้าเพื่อการสืบสวนสอบสวนหรือดำเนินคดี จึงเป็นการกระทำที่มีกฎหมายรองรับ หากฝ่าฝืนแล้วย่อมเป็นความผิดตามกฎหมาย

ในกรณีที่มีการพยายามทะลุเวปไซต์ที่ถูกหวงห้ามนั้น โดยปกติแล้วผู้กระทำมักจะใช้ Proxy[77] เพื่อปลอมแปลงตนและเข้าไปในเวปไซต์ที่ถูกบล็อกได้ ซึ่งอาจมีผู้กล่าวอ้างว่า

---

[77] Proxy Server หมายถึงอุปกรณ์ในระบบเครือข่ายที่รับเอาการร้องขอใช้บริการ (request) จากเครื่องลูกข่าย ได้แก่ โปรแกรมเวป บราวเซอร์ หรือ โปรแกรม FTP Client แล้ว

ตนเองไม่ได้ทำการฝ่า (Break in) มาตรการป้องกันการเข้าถึงเข้าไปจึงไม่เป็นความผิด แต่อย่างไรก็ตามในกรณีนี้ผู้เขียนมีความเห็นว่า การใช้ Proxy เพื่ออ้อมหรือปลอมแปลงตนเองเพื่อที่จะสามารถเข้าเวปไซต์ที่ถูกบล็อกได้นั้น ก็เป็นความผิดฐานเข้าถึงโดยมิชอบแล้ว เนื่องจากการเข้าถึงนั้นไม่จำกัดวิธีการแต่อย่างใด ผู้ที่เข้าถึงจะกล่าวอ้างเพียงว่าตนเองไม่ได้ฝ่าระบบป้องกันเข้าไปไม่ได้

นอกจากนั้นแล้วปัญหาในเรื่องของการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบกฎหมายได้ระบุไว้ด้วยว่าจะต้องเป็นระบบคอมพิวเตอร์ที่มีการป้องกันการเข้าถึงไว้โดยเฉพาะ ดังนั้นถ้าในกรณีข้อเท็จจริงที่ผู้ใช้ได้ติดตั้ง username และ password ไว้ในเครื่องเลย ถ้ามีคนอื่นเข้ามาใช้ระบบนั้นจะถือว่าผิดตามมาตรานี้หรือไม่[78]

มีความเห็นออกเป็น 2 แนวคือ

1. เห็นว่าถ้าเป็นกรณีตั้ง username และ password ไว้หน้าจอแล้วรอให้คลิก ok และเข้าระบบนั้นไม่น่าจะเป็นความผิดตามมาตรา 5 เพราะมาตรา 5 ต้องการป้องกันผู้ที่ได้ตั้งมาตรการการเข้าถึงไว้ แต่ตามข้อเท็จจริงนี้ มาตรการการป้องกันนี้กลับทำให้ผู้อื่นเข้าถึงได้โดยง่าย และไม่น่าจะถือว่าเป็นมาตรการป้องกันการเข้าถึง

2. เห็นว่าถ้าได้มีการนำ username และ password ไปเก็บไว้ในไฟล์ใดไฟล์หนึ่ง คือมีการป้องกันระดับหนึ่ง ถ้าผู้ที่เข้าไปได้ระดับหนึ่งต้องการเข้าไปในชั้นความลับที่ลึกขึ้น และไปเจอไฟล์ที่เก็บ username และ password ของอีเมล์ Account เช่นนี้ ก็น่าจะถือได้ว่าเป็นความผิด

ส่งผ่านการร้องขอนั้นไปยังเซิร์ฟเวอร์ปลายทางในเครือข่ายอินเทอร์เน็ต ดังนั้น Proxy Server จึงเปรียบเสมือนตัวแทนของเครื่องลูกข่ายที่อยู่ภายในระบบและเป็นตัวกลางระหว่างเครือข่ายภายในกับเครือข่ายภายนอก โดยมีภาระหน้าที่ที่ถูกกำหนดให้รับผิดชอบแตกต่างกันออกไปตามความต้องการของผู้ออกแบบระบบ [Online] แหล่งที่มา : www.vvetalk.com [10 มกราคม 2551]

[78] เอกสารสรุปการสัมมนา “การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และการเตรียมความพร้อมกับกฎหมายใหม่” [Online] หน้า 52-53.

ซึ่งในกรณีดังกล่าวนั้นผู้เขียนเห็นด้วยกับความเห็นแรกที่เห็นว่าการตั้ง username และ password ไว้หน้าจอแล้วรอให้คลิก ok นั้นถือว่าไม่มีการป้องกันการเข้าถึงแต่อย่างใด เนื่องจากวัตถุประสงค์ของการตั้ง username และ password ก็ป้องกันไม่ให้ผู้อื่นรู้ เป็นการชี้ตัวบุคคลที่มีอำนาจเข้าถึง (identity) เมื่อตั้ง username และ password ทิ้งไว้ ทำให้ใครเข้ามาใช้ก็ได้ จึงถือว่าไม่มีการป้องกัน ส่วนในกรณีที่นำ username และ password ไปเก็บไว้ในไฟล์ใดไฟล์หนึ่งนั้น ถ้าผู้ที่เข้าไปได้ไปเจอไฟล์ดังกล่าว และนำไปใช้ ผู้เขียนก็เห็นว่าการกระนั้นเป็นความผิดเช่นกัน เนื่องจากได้มีการตั้ง username และ password ไว้แล้วและไม่ได้กรอกไว้โดยตรง หากนำไปใช้ถือว่าเป็นความผิดเนื่องจากมีการป้องกันไว้แล้ว

นอกจากนี้ กรณีของการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเขาถึงโดยเฉพาะนี้ กรณีที่อาจพบเห็นหรือมีโอกาสเกิดขึ้นได้โดยง่ายคือกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์นั้นได้มีการป้องกันไว้ แต่เมื่อมีการใส่ username และ password และทำงานไปพักหนึ่ง ก็อาจจะเดินออกไปทำธุระอย่างอื่นโดยเปิดเครื่องคอมพิวเตอร์ทิ้งไว้ แล้วมีบุคคลอื่นเข้ามาใช้เครื่องคอมพิวเตอร์นั้น ในกรณีเช่นนี้จะเป็นความผิดในการเข้าถึงหรือไม่ โดยผู้เขียนเห็นว่า กรณีเช่นนี้ไม่เป็นความผิดในการเข้าถึงโดยมิชอบ เนื่องจากไม่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะแต่อย่างใด การที่เจ้าของคอมพิวเตอร์ออกไปจากคอมพิวเตอร์ไม่ว่าด้วยสาเหตุใดๆ แล้วปล่อยให้เครื่องคอมพิวเตอร์ที่ปกติมีการป้องกันไว้โดยไม่ได้ทำการออกจากระบบก่อน เป็นการแสดงให้เห็นว่าผู้ใช้ไม่มีความประสงค์ที่จะป้องกันแล้ว แม้จะมีผู้ที่เข้ามาใช้หรือหาประโยชน์ ก็ไม่ทำให้การกระทำนั้นเป็นความผิดเนื่องจากไม่มีมาตรการป้องกันการเข้าถึงแล้ว

ในกรณีมาตรการป้องกันการเข้าถึงในระบบเครือข่ายโดยการใช้ไฟล์วอร์นั้น สิ่งที่จะเป็นปัญหาในการพิจารณาคือ จุดอ่อนของระบบป้องกันของไฟล์วอร์ที่มีใช้อยู่ในปัจจุบันนั่นเอง เนื่องจากในปัจจุบันระบบการป้องกันของไฟล์วอร์เป็นระบบการป้องกันในระดับโปรแกรม โดย firewall จะป้องกันระบบจากผู้บุกรุกภายนอก ซึ่งอธิบายการทำงานง่ายๆ โดย เมื่อต่อเชื่อมอินเทอร์เน็ต และเรียกข้อมูลไปยัง Website ที่ต้องการ Web server จะส่งข้อมูลมายังเครื่องคอมพิวเตอร์ในลักษณะของชุดข้อมูลขนาดเล็กหรือ packet ซึ่งก่อนที่ packet จะเข้าถึงคอมพิวเตอร์นั้น firewall จะทำหน้าที่เป็นคนเฝ้าประตู เพื่อตรวจสอบว่า packet ชุดใดที่จะอนุญาตให้เข้ามาสู่ระบบได้

ซึ่งลักษณะการป้องกันในลักษณะนี้คือการป้องกันในระดับโปรแกรมโดยอนุญาตหรือไม่อนุญาตให้โปรแกรมบางประเภทเข้ามายังคอมพิวเตอร์ได้นั่นเอง ซึ่งปัญหาที่พบได้โดยทั่วไปคือ การป้องกันดังกล่าวจะมีการเปิดช่องทางบางช่องทางให้โปรแกรมบางประเภทเข้าถึงได้ และไม่อนุญาตให้โปรแกรมบางประเภทเข้าถึง เปรียบเสมือนประตูเมืองที่มีหลายประตู บางประตูจะมีคนเฝ้า ขณะที่บางประตูไม่มีคนเฝ้าไว้ ปัญหาที่ผู้เขียนจะกล่าวถึงคือ กรณีการบุกรุกในช่องทางที่ไม่ยามเฝ้านั่นเอง โดยปัญหาที่อาจเป็นที่โต้เถียงกันคือในกรณีที่ผู้บุกรุกเข้าถึงระบบคอมพิวเตอร์โดยสามารถผ่านไฟล์วอร์เข้ามาในช่องทางที่ไฟล์วอร์อนุญาตนั้นเป็นการเข้าถึงที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะหรือไม่ เนื่องจากผู้บุกรุกไม่ได้เข้ามาโดยฝ่าระบบป้องกันของไฟล์วอร์เข้ามาโดยตรง หากแต่เข้ามาในช่องทางที่ไฟล์วอร์อาจจะอนุญาตให้โปรแกรมบางประเภทเข้ามาในระบบได้ เช่น website

ซึ่งในกรณีนี้ผู้เขียนเห็นว่าแม้จะเข้ามาในช่องทางที่เปิดช่องให้เข้ามาได้ หากแต่ช่องทางนั้นไม่ได้มีไว้สำหรับผู้ที่ประสงค์ร้าย เช่น ช่องทางนั้นอาจจะเปิดไว้เพื่อให้ข้อมูลเวปไซต์เข้าออกได้ การที่มีการปลอมแปลงข้อมูลให้เหมือนข้อมูลเวปไซต์เพื่อที่จะเข้าถึงคอมพิวเตอร์ก็เหมือนการเข้าถึงบ้านที่มีการใส่กุญแจหน้าบ้านแต่ลืมปิดประตูหลังบ้าน ซึ่งการบุกรุกเข้ามาย่อมเป็นความผิดแล้วโดยจะกล่าวอ้างว่าประตูหลังบ้านเปิดอยู่ไม่ได้ เช่นเดียวกันกรณีของไฟล์วอร์การแอบเข้ามาในช่องทางที่เปิดไว้จึงเป็นความผิดฐานเข้าถึงโดยมิชอบแล้ว เนื่องจากการเข้าถึงนั้นไม่จำกัดวิธีการแต่อย่างใด ผู้ที่เข้าถึงจะกล่าวอ้างเพียงว่าตนเองไม่ได้ฝ่าระบบป้องกันเข้าไปไม่ได้

นอกจากนี้การเข้าถึงโดยผ่านระบบเครือข่ายอาจทำได้โดยการเชื่อมต่อในลักษณะ P2P (Peer-to-Peer) ซึ่งเทคโนโลยีระบบเครือข่ายแบบ Peer-to-Peer ทำให้ผู้ใช้สามารถแลกเปลี่ยนข้อมูล บริการ และ ทรัพยากรอื่นๆ ในเครื่องคอมพิวเตอร์ที่อยู่บนเครือข่ายได้โดยตรง ทำให้ผู้ใช้อินเทอร์เน็ตค้นหาและแลกเปลี่ยนไฟล์ข้อมูลต่างๆ ระหว่างคอมพิวเตอร์ซึ่งกันและกันได้โดยไม่จำเป็นต้องมีคอมพิวเตอร์แม่ข่าย (Central Server) ซึ่งในกรณีดังกล่าวจะมีลักษณะที่เชื่อมต่อโดยตรงโดยเชื่อมเครื่องคอมพิวเตอร์เข้าด้วยกัน โดยเครื่องคอมพิวเตอร์ของผู้ใช้จะต้องอนุญาตให้คอมพิวเตอร์ที่จะแลกเปลี่ยนข้อมูลกันสามารถเข้าถึงเครื่องของตนได้ ซึ่งอาจทำให้เกิดปัญหาได้ว่า เครื่องคอมพิวเตอร์ของบุคคลอื่นที่เชื่อมต่อนั้นอาจจะไม่ประสงค์ดีโดยถือโอกาสที่ทำการเชื่อมต่อแลกเปลี่ยนเข้ามาทำการขโมยข้อมูล หรือใส่สปายแวร์หรือไวรัสเข้าเครื่องคอมพิวเตอร์อีกเครื่องหนึ่งที่เชื่อมต่อกันได้โดยง่าย

ซึ่งในกรณีเช่นนี้ จะวิเคราะห์ได้ต่อเมื่อมองว่าการเข้าถึงตามการตีความของกฎหมายมีความหมายว่าอย่างไร หากมองว่าการเข้าถึงนั้นสิ้นสุดลงทันทีที่เข้ามาได้ และความชอบธรรมเกิดขึ้นเมื่อได้รับอนุญาตให้เข้ามาแล้วก็อาจกล่าวได้ว่าผู้ที่กระทำการดังกล่าวไม่มีความผิดในการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบ เนื่องจากแม้เครื่องคอมพิวเตอร์นั้นจะมีไฟล์วอร์หรือระบบป้องกันอื่น หากแต่เจ้าของเครื่องคอมพิวเตอร์ผู้ใช้ได้ทำการอนุญาตให้บุคคลนั้นเข้าถึงเครื่องคอมพิวเตอร์ของตนเองได้ จึงไม่ถือว่าเข้ามาโดยไม่ชอบและมีระบบป้องกันโดยเฉพาะเนื่องจากได้รับอนุญาตให้เข้ามาแล้ว โดยเปรียบเทียบกับความผิดฐานบุกรุกตามประมวลกฎหมายอาญาแล้ว หากเจ้าของอนุญาตให้ผู้อื่นเข้ามาในบ้านของตน บุคคลนั้นก็ไม่มีความผิดฐานบุกรุกแต่อย่างใด ดังนั้นเมื่อไม่เป็นความผิดในการเข้าถึงโดยมิชอบแล้ว แม้บุคคลนั้นจะทำการขโมยข้อมูลที่ไม่มีการป้องกันไว้โดยเฉพาะไปก็ไม่เป็นความผิด ซึ่งในกรณีเช่นนี้อาจทำให้เกิดปัญหาในการนำเอาผิดผู้กระทำความผิดตามกฎหมายได้

ดังนั้นหากจะพิจารณาว่าการเข้าถึงนั้นเกิดขึ้นและมีอยู่ตลอดเวลาที่ติดต่อสื่อสารกับคอมพิวเตอร์แล้ว อาจจะได้รับคำตอบในอีกลักษณะหนึ่งที่ว่าการเข้าถึงนั้นยังคงอยู่และแม้จะได้รับอนุญาตให้เข้าถึงได้ แต่ก็ทำได้ในขอบเขตที่เจ้าของอนุญาตและเหมาะสมเท่านั้น ทันทีที่กระทำความผิดหรือกระทำสิ่งที่ไม่ถูกต้องและก่อให้เกิดความเสียหายแก่เจ้าของ ผู้นั้นก็จะเป็นผู้กระทำความผิดฐานเข้าถึงโดยมิชอบทันที

5.2.5 มาตรการนั้นมิได้มีไว้สำหรับตน

ในการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีการป้องกันการเข้าถึงโดยเฉพาะนั้น จะเป็นความผิดเมื่อมาตรการนั้นไม่ได้มีไว้สำหรับตนเท่านั้น หากว่าตนเองมีอำนาจหรือได้รับอนุญาตให้เข้าถึงได้แล้ว การกระทำนั้นย่อมไม่เป็นความผิดแม้ว่ามาตรการการป้องกันนั้นจะมิได้มีไว้สำหรับตนก็ตาม เช่น ในกรณีของบริษัทของนายจ้างได้ให้จดหมายอิเล็กทรอนิกส์ของบริษัทแก่พนักงานทุกคน แม้ว่าลูกจ้างจะมีชื่อเป็นเจ้าของจดหมายอิเล็กทรอนิกส์นั้นก็ตาม หากมีระเบียบกำหนดไว้แล้ว เจ้าของหรือนายจ้างผู้มีอำนาจย่อมมีสิทธิที่จะเข้าถึงจดหมายอิเล็กทรอนิกส์ของพนักงานได้ ตามระเบียบที่วางไว้

ซึ่งในกรณีนี้ในประเทศสหรัฐอเมริกาได้มีคดีขึ้นสู่ศาลว่า บริษัทนายจ้างได้มีระเบียบเกี่ยวกับการจำกัดการใช้คอมพิวเตอร์เฉพาะจุดประสงค์ทางธุรกิจเท่านั้น และห้ามใช้สำหรับจุดประสงค์อื่นที่ไม่เกี่ยวข้อง เช่น เรื่องลามก ลูกจ้างถูกไล่ออกเนื่องจากดูภาพโป๊เด็กโดย

ใช้คอมพิวเตอร์ของบริษัทที่บ้าน ฝ่ายลูกจ้างฟ้องโดยอ้างถึงสิทธิในข้อมูลส่วนบุคคลบนคอมพิวเตอร์ ศาลตัดสินว่าลูกจ้างได้สละสิทธิเมื่อลูกจ้างได้ยอมรับนโยบายของบริษัทซึ่งลูกจ้างไม่มีสิทธิใช้คอมพิวเตอร์ในทางส่วนตัว[79]

แต่กรณีจะเป็นอย่างไรหากว่าไม่มีระเบียบในที่ทำงานกำหนดให้นายจ้างสามารถเข้าดูจดหมายอิเล็กทรอนิกส์ของลูกจ้างได้ แต่นายจ้างได้ทำการเข้าถึงจดหมายอิเล็กทรอนิกส์ของลูกจ้างโดยที่ไม่มีกฎหรือระเบียบให้อำนาจไว้ การกระทำของนายจ้างจะเป็นความผิดในการเข้าถึงโดยมิชอบหรือไม่ เนื่องจากจดหมายอิเล็กทรอนิกส์นั้นแม้จะเป็นของทางบริษัทให้แก่ลูกจ้าง หากแต่ถ้าไม่มีข้อตกลงหรือกฎให้นายจ้างหรือผู้มีอำนาจเข้าถึงได้แล้ว หากนายจ้างเข้าถึงจะเป็นเช่นไร นายจ้างจะมีความผิดในการเข้าถึงหรือไม่

ซึ่งทางด้านบริษัทหรือนายจ้างอาจกล่าวอ้างว่าตนเองมีอำนาจที่จะเข้าไปในจดหมายอิเล็กทรอนิกส์ที่บริษัทให้แก่ลูกจ้างได้ เพื่อประโยชน์ในการควบคุมการดำเนินงานของบริษัทและเป็นการตรวจสอบพฤติกรรมของลูกจ้าง แต่ฝ่ายลูกจ้างอาจจะโต้แย้งว่าเมื่อไม่มีการกำหนดไว้ในระเบียบของบริษัท แม้จดหมายอิเล็กทรอนิกส์นั้นบริษัทจะให้ใช้แต่ก็เป็นของส่วนตัวที่นายจ้างไม่มีสิทธิล่วงล้ำเข้ามาโดยไม่มีอำนาจ โดยผู้เขียนเองเห็นด้วยกับความคิดที่ว่าหากไม่มีระเบียบให้อำนาจนายจ้างแล้ว จดหมายอิเล็กทรอนิกส์ของลูกจ้างย่อมเป็นสิทธิส่วนบุคคล การเข้าถึงโดยไม่มีเหตุสมควรที่จำเป็นที่เกี่ยวข้องกับบริษัทจึงเป็นการละเมิดและอาจเป็นการเข้าถึงโดยปราศจากอำนาจ

นอกเหนือจากองค์ประกอบความผิดในการเข้าถึงโดยมิชอบแล้ว องค์ประกอบความผิดในการล่วงรู้มาตรการป้องกันการเข้าถึงโดยเฉพาะแล้วนำไปเปิดเผยโดยมิชอบ ก็มีปัญหาที่ต้องพิจารณาด้วยเช่นกัน

5.2.6 การล่วงรู้มาตรการป้องกันแล้วนำไปเผยแพร่โดยมิชอบ

---

[79] Jeffrey Steinberger, “Your Right to Employee E-Mail,” [Online] Available from : www.entrepreneur.com [วันที่ 27 มกราคม 2551]

ตามมาตรา 6 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นบทบัญญัติว่าด้วยการล่วงรู้มาตรการการป้องกันแล้วนำไปเผยแพร่โดยมิชอบ โดยบัญญัติว่า "ผู้ใดล่วงรู้มาตรการการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ"

ผู้เขียนเห็นว่าจากบทบัญญัติตามมาตรานี้จะเห็นได้ว่าเป็นการล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์เท่านั้น หากเป็นกรณีที่ล่วงรู้มาตรการป้องกันการเข้าถึงข้อมูลคอมพิวเตอร์แล้วจะแม้นำไปเผยแพร่ก็ไม่เป็นความผิดตามกฎหมายแต่อย่างใด ซึ่งอาจจะก่อให้เกิดช่องว่างทางกฎหมายได้ว่า การล่วงรู้มาตรการป้องกันของระบบคอมพิวเตอร์เป็นความผิดแต่การล่วงรู้มาตรการป้องกันของข้อมูลคอมพิวเตอร์กลับไม่เป็นความผิดตามกฎหมาย ซึ่งจะทำให้เกิดการลักลั่นของจุดประสงค์ที่กฎหมายมุ่งคุ้มครอง เนื่องจากโดยแท้จริงแล้ว สิ่งที่เป็นที่ต้องการของบุคคลในการกระทำผิดเกี่ยวกับคอมพิวเตอร์คือข้อมูลคอมพิวเตอร์ ไม่ใช่ระบบคอมพิวเตอร์แต่อย่างใด

นอกจากกรณีการล่วงรู้มาตรการการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ และนำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นนั้น มีประเด็นที่ต้องพิจารณาคือ หากเป็นการสอนในมหาวิทยาลัย หรือผู้ที่แต่งหนังสือเกี่ยวกับการแฮก หรือกรณีที่ทำไปเพื่อการศึกษาวิจัยและนำไปเปิดเผยในแวดวงวิชาการแล้ว การกระทำนั้นเป็นความผิดหรือไม่ โดยมีคดีในต่างประเทศ คือ คดี Felten v. RIAA: Hacking SDMI and Talking About It[80] โดย Professor Edward Felten นักวิทยาศาสตร์ทางคอมพิวเตอร์แห่งมหาวิทยาลัย Princeton และทีมวิจัย ได้เข้าร่วมการประลองความสามารถในการเจาะระบบความปลอดภัยของกลุ่ม the Secure Digital Music Initiative (SDMI) โดยเป้าหมายของ SDMIนั้นเพื่อสร้างระบบความปลอดภัยให้กับเพลงดิจิตอล ไม่ให้มีการทำซ้ำ และทำ

---

[80] นพมาศ ประสิทธิ์มณฑล, "อาชญากรรมคอมพิวเตอร์ ตามกฎหมายสหรัฐอเมริกา," กฎหมายอิเล็กทรอนิกส์เพื่อการศึกษา [Online]
แหล่งที่มา : www.geocities.com/elaw007/Article/cybercrime270502.html [วันที่ 27 พฤศจิกายน 2550]

ให้ทาง SDMI รู้ถึงจุดอ่อนของระบบตนเองได้ดีขึ้น และสร้างระบบที่ดีกว่าเพื่อป้องกันการทำซ้ำเพลงดิจิตอล

ศาตราจารย์ Felten และคณะ ได้ประสบความสำเร็จในการเจาะระบบความปลอดภัยดังกล่าว และศาตราจารย์ต้องการที่จะเผยแพร่งานวิจัยในการเจาะระบบดังกล่าวในงานประชุมนานาชาติครั้งที่สี่ของคณะทำงานที่ปกปิดข้อมูล อย่างไรก็ตามแผนการเผยแพร่งานวิจัยเป็นอันระงับไป ด้วย กลุ่ม RIAA ได้ยื่นจดหมายคำเตือนทางกฎหมายว่า การเปิดเผยข้อมูลเกี่ยวกับการเจาะระบบของ SDMI อาจเป็นการกระทำอันละเมิดต่อกฎหมายแห่งรัฐ และ รวมถึง DMCA ด้วย แม้ว่า ศาตราจารย์ Felten มิได้เปิดเผยงานวิจัยในการประชุมครั้งแรก แต่ได้เปิดเผยรายงานดังกล่าวในงานประชุม USENIX Security Symposium ครั้งที่ 10

มิถุนายน 2001 องค์กร Electronic Frontier Foundation (EFF) ต้องการหาแนวทางในหาการบังคับใช้ DMCA อย่างชัดเจน จึงยื่นฟ้องต่อศาลนิวเจอร์ซี่ (ภายใต้ชื่อคดี Felten v. RIAA) โดยมีจำเลยประกอบด้วย RIAA, อัยการสูงสุด Ashcroft และรายชื่อผู้สร้างเทคโนโลยีป้องกันการเจาะระบบอีกบางส่วน

ตามคำฟ้องของ EFF นั้นร้องขอให้ศาล ตัดสินว่า การตีพิมพ์งานวิจัยของศาตราจารย์ Felten และคณะ มิได้เป็นการละเมิด DMCA เนื่องจากการกระทำของศาตราจารย์ได้รับการปกป้องภายใต้เสรีภาพในการแสดงความคิดเห็น ตามรัฐธรรมนูญของสหรัฐอเมริกา ที่รู้จักกันในนาม First Amendment Speech และนอกจากนี้ EFF ร้องขอให้ศาลออกคำสั่งห้ามมิให้จำเลยทำการพยายามห้าม หรือขัดขวางไม่ให้ศาตราจารย์เผยแพร่งานวิจัยดังกล่าวไม่ว่าจะในงานประชุม the Information Hiding Workshop หรือ ที่อื่น ๆ ด้วย

RIAA จำเลย ได้โต้แย้งว่า คดีไม่มูล ไม่มีความขัดแย้งระหว่างEFF กับจำเลย เรียกว่า คดีความยังไม่เกิด นอกจากนั้น จำเลยกล่าวว่า การร้องขอให้ศาลออกคำสั่งข้างต้นก่อนเกิดความเสียหาย เป็นการขอที่ไกลกว่าเหตุ ทั้งที่ไม่ปรากฏความขัดแย้งระหว่างคู่กรณี

วันที่ 28 พฤศจิกายน 2001 ศาลตัดสินว่าไม่ปรากฏว่าคดีมีมูล ยกฟ้องตามคำฟ้องแย้งของจำเลย

จะเห็นได้ว่าแม้จะมีการฟ้องร้องคดีต่อศาลในเรื่องการเปิดเผยดังกล่าว แต่เนื่องจากเป็นการฟ้องเพื่อต้องการหาบรรทัดฐานในการกระทำดังกล่าว ศาลจึงยกฟ้องเนื่องจากคดีไม่มีมูลซึ่งไม่มี

ข้อโต้แย้งเกิดขึ้น จากกรณีดังกล่าวแม้จะไม่มีคดีพิพาทเกิดขึ้นแต่ก็ทำให้เกิดประเด็นที่น่าศึกษาว่า หากกรณีดังกล่าวเกิดขึ้นในประเทศไทย ผู้กระทำจะมีความผิดฐานล่วงรู้มาตรการการป้องกันแล้วนำไปเผยแพร่โดยมิชอบหรือไม่

การกระทำเช่นนี้อาจพบได้ในอีกคดีหนึ่งคือ คดี US v. Skylarov: Cracking an Adobe eBook โดย ในวันที่ 17 กรกฎาคม 2001 นาย Dmitri Sklyarov นักศึกษาชาวรัสเซียถูกจับกุมโดย FBI ทางตอนเหนือของรัฐแคลิฟอร์เนีย ด้วยเหตุที่ Sklyarov ได้ร่วมงานสัมมนา DEFCON-9 ที่ลาสเวกัส ในการประชุมดังกล่าว Sklyarov เสนอรายงานเกี่ยวกับทฤษฎี และทางปฏิบัติของระบบความปลอดภัยของ eBooks การกระทำดังกล่าวถูกกล่าวหาว่า เป็นการละเมิด DMCA ซึ่งถ้านาย Sklyarov ถูกตัดสินว่าผิดจริงตามกฎหมายดังกล่าว อาจมีโทษจำคุกถึงห้าปีและถูกปรับอีก $500,000

อย่างไรก็ตาม การละเมิด DMCA ผู้กระทำการดังกล่าว อาจอ้างข้อป้องกันในกรณีของ การใช้อย่างยุติธรรม หรือ Fair Use ภายใต้ 17 USC 107 ซึ่งเป็นกรณีที่กฎหมายอนุญาตให้มีการใช้งานอันมีลิขสิทธิ์ โดยไม่เป็นการละเมิดสิทธิ์ของเจ้าของลิขสิทธิ์ภายใต้เงื่อนไข ที่กฎหมายได้กำหนดไว้ เช่น เพื่อการวิพากษ์วิจารณ์ การรายงาน การวิจัย และเพื่อการศึกษา

เมื่อพิจารณาจากบทบัญญัติของกฎหมายที่กำหนดให้ผู้ที่ล่วงรู้มาตรการการป้องกันและนำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นเป็นความผิด ดังนั้นประเด็นที่ต้องพิจารณาในกรณีนี้คือ การที่นำไปเผยแพร่ในงานหรือการประชุมทางวิชาการนั้นเป็นการเปิดเผยโดยมิชอบหรือไม่ หากเป็นการเปิดเผยโดยมิชอบแล้วจะถือว่าเป็นประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือไม่

หากพิจารณาจากบทบัญญัติของกฎหมายแล้ว จะเห็นได้ว่าแม้จะเป็นการประชุมทางวิชาการ และไม่มีเจตนาจะแสวงหาประโยชน์โดยส่วนตัว แต่เนื้อหาที่จะเปิดเผยนั้นหากเจ้าของไม่ได้อนุญาตให้เปิดเผยแล้วก็จะกล่าวอ้างว่าเป็นการเปิดเผยโดยชอบไม่ได้ และถือเป็นประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่น

แต่อย่างไรก็ตามมีผู้ให้ความเห็นว่า[81] กรณีการเปิดเผยในแวดวงวิชาการนั้น หากเห็นว่าจุดอ่อนของโปรแกรมนั้นจะส่งผลกระทบต่อประชาชนผู้ใช้โดยทั่วไป และได้แจ้งให้เจ้าของทราบแล้ว หากยังไม่กระทำการสิ่งใด ก็ควรที่จะเปิดเผยเพื่อประโยชน์แก่ประชาชนผู้ใช้โดยทั่วไป การกระทำนั้นไม่ควรที่จะเป็นความผิดทางอาญา

แต่ในกรณีที่เป็นการสอนในมหาวิทยาลัยนั้นก็เป็นไปเพื่อการศึกษาวิจัยโดยตรง และไม่มีลักษณะเฉพาะเจาะจงหรือมุ่งประสงค์ต่อบุคคลหนึ่งบุคคลใด ผู้เขียนจึงเห็นการกระทำนั้นไม่เป็นความผิดตามมาตรานี้

นอกจากปัญหาที่พิจารณาได้จากองค์ประกอบภายนอกในการกระทำผิดฐานเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบแล้ว อาจพบปัญหาจากองค์ประกอบภายในของการกระทำผิดได้ ดังนี้

5.3 องค์ประกอบภายในของการกระทำความผิด

การเข้าถึงโดยมิชอบนั้นเป็นองค์ประกอบความผิดภายนอกจึงไม่ใช่การกระทำความผิดโดยไม่รู้ผิดชอบตามประมวลกฎหมายอาญามาตรา 65 ที่มีหลักว่า การกระทำความผิดในขณะไม่สามารถรู้ผิดชอบ หรือไม่สามารถบังคับตนเองได้ เพราะมีจิตบกพร่อง โรคจิตหรือจิตฟั่นเฟือน ผู้นั้นไม่ต้องรับโทษสำหรับความผิดนั้น และการเข้าถึงโดยมิชอบที่จะเป็นความผิดตามกฎหมายนั้น นอกจากองค์ประกอบภายนอกของการกระทำผิดแล้ว สิ่งที่จะต้องพิจารณาประกอบคือ องค์ประกอบภายในของการกระทำความผิด คือ เจตนาในการกระทำความผิด

เมื่อพิจารณาจากประมวลกฎหมายอาญา มาตรา 59 แล้ว จะเห็นได้ว่าโดยหลักแล้วองค์ประกอบภายในของความผิดอาญาแต่ละมาตรา คือ เจตนา โดยเมื่อพิจารณาถึงบทบัญญัติเกี่ยวกับเจตนาในกฎหมายอาญาแล้ว และพิจารณาดูความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แล้วจะเห็นได้ว่าความผิดในการเข้าถึงโดยมิชอบและความผิดในการล่วงรู้มาตรการการป้องกันแล้วนำไปเผยแพร่โดยมิชอบนั้น เป็นการบัญญัติกฎหมายโดยทั่วไปไม่มีถ้อยคำใดเป็นพิเศษ จึงต้องถือตามหลักกฎหมายอาญาตามมาตรา 59 ว่า การที่จะเป็นการ

---

[81] สัมภาษณ์ ธงชัย โรจน์กังสดาล, 30 มกราคม 2551

กระทำความผิดตามมาตรา 5 มาตรา 6 และมาตรา 7 นั้น ต้องเป็นการกระทำโดยเจตนา และการพิสูจน์เจตนาในความรับผิดฐานเข้าถึงโดยมิชอบนั้น ไม่แตกต่างจากเจตนาในประมวลกฎหมายอาญาแต่อย่างใด

โดยเจตนาตามมาตรา 59 นี้ เป็นเพียงเจตนากระทำความผิด (criminal intention) ตามที่กฎหมายบัญญัติซึ่งเป็นความไม่ดีอยู่ในตัวอยู่แล้ว เพราะกฎหมายมีไว้เพื่อเป็นระเบียบของชุมชน และต้องแยกออกจากเรื่องของมูลเหตุชักจูงใจ (motive, mobile) อันเป็นความสำนึกส่วนตัวโดยทั่วไปไม่มีผลในทางกฎหมาย ดังนั้นในความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์โดยมิชอบก็เช่นเดียวกัน ก็ต้องพิจารณาเพียงว่าการกระทำความผิดดังกล่าวมีเจตนาที่จะเข้าถึงโดยมิชอบหรือไม่เท่านั้น ไม่จำเป็นต้องพิจารณาถึงมูลเหตุชักจูงแต่อย่างใด ถึงแม้ผู้ที่เข้าถึงจะไม่มีเจตนาร้ายที่จะแก้ไขเปลี่ยนแปลงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ โดยอ้างว่าเข้าไปดูอย่างเดียวก็ไม่เป็นข้อแก้ตัวให้พ้นจากความผิดในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ได้

แต่ปัญหาที่อาจต้องพิจารณาคือ การกระทำใดที่ถือว่าผู้กระทำมีเจตนาในการเข้าถึง เช่น ในกรณีที่นายแดงต้องการหาข้อมูลโดยใช้โปรแกรมค้นหาข้อมูลทางอินเทอร์เน็ตซึ่งจะเห็นได้ว่า ในบางครั้งโปรแกรมค้นหาข้อมูลดังกล่าวสามารถทำให้ผู้ค้นหาสามารถเข้าไปในข้อมูลบางประเภทที่โดยปกติแล้วไม่สามารถเข้าถึงได้ และนายแดงต้องการค้นหาข้อมูลนั้นโดยกดเข้าไปในข้อมูลที่โปรแกรมแสดงผลขึ้นที่หน้าจอคอมพิวเตอร์ หากนายแดงไม่มีเจตนาที่จะใช้โปรแกรมสืบค้นนั้นเข้าถึงข้อมูลที่มีการป้องกันไว้โดยเฉพาะและนายแดงเข้าไปยังเวปไซต์ดังกล่าวโดยไม่ทราบว่าเวปไซต์นั้นกำจัดไว้ว่าเฉพาะสมาชิกเท่านั้นที่สามารถเข้าถึงได้ การกระทำของนายแดงจะเป็นความผิดหรือไม่

ในกรณีนี้ผู้เขียนมีความเห็นว่า นายแดงไม่มีเจตนาในการกระทำความผิดเนื่องจากประมวลกฎหมายอาญา มาตรา 53 วรรคสาม บัญญัติว่า ถ้าผู้กระทำมิได้รู้ข้อเท็จจริงอันเป็นองค์ประกอบของความผิดจะถือว่าผู้กระทำประสงค์ต่อผล หรือย่อมเล็งเห็นผลของการกระทำนั้นมิได้ ในกรณีนี้นายแดงไม่รู้ข้อเท็จจริงว่าเวปไซต์นั้นมีระบบป้องกันและตนเองไม่มีอำนาจเข้าไปได้ ดังนั้นนายแดงจึงไม่มีเจตนากระทำความผิด แต่ถ้านายแดงเข้าไปโดยเจตนาหรือรู้ว่าเวปไซต์นั้นมีระบบป้องกันไว้และตนไม่มีอำนาจที่จะเข้าไป ก็เป็นเรื่องง่ายที่จะกล่าวว่านายแดงมีเจตนาที่จะเข้าถึงเวปไซต์นั้นโดยมิชอบ

นอกจากการตีความเรื่องเจตนาในความผิดฐานเข้าถึงโดยมิชอบแล้ว ปัญหาที่อาจเป็นประเด็นในการพิจารณาคือ เจตนาในการกระทำความผิด เนื่องจากฐานความผิดดังกล่าวกำหนดว่าเพียงแค่มีเจตนาเข้าถึงก็เป็นความผิดแล้วไม่จำเป็นต้องมีเจตนาพิเศษแต่อย่างใด ซึ่งในกรณีนี้อาจก่อให้เกิดการวิพากษ์วิจารณ์ได้ในเรื่องเกี่ยวกับผลการตัดสินที่ออกมาส่งสาธารณชน เช่น คดี R v Daniel Cuthbert[82] ที่นาย Cuthbert บริจาคเงิน 30 ปอนด์ ให้กับเวปไซต์ที่ก่อตั้งขึ้นเพื่อเป็นกองทุนให้ความช่วยเหลือผู้เคราะห์ร้ายในเหตุการณ์สึนามิ ได้เจาะเข้าไปในระบบรักษาความปลอดภัยของเวปไซต์ดังกล่าว โดยอ้างว่าต้องการเพียงทดสอบระบบรักษาความปลอดภัยหลังจากที่ตนได้บริจาคเงินไปแล้วเท่านั้น โดยนาย Cuthbert มีความผิดในการเข้าไปโดยมิชอบและถูกลงโทษปรับ 400 ปอนด์ โดยในการพิจารณานั้นไม่ปรากฏว่า นาย Cuthbert มีความตั้งใจที่จะฉ้อโกงหรือหาเงินจากการเจาะระบบแต่อย่างใด

การตัดสินในคดีนี้ได้มีการตั้งคำถามขึ้นว่าการตัดสินนั้นเหมาะสมหรือไม่ เนื่องจากมีการกล่าวอ้างข้อเท็จจริงว่า[83] นาย Cuthbert ซึ่งมีอาชีพเป็นผู้ดูแลความปลอดภัยของคอมพิวเตอร์ เห็นใจผู้ประสบภัยสึนามิและได้บริจาคเงินให้แก่กับเวปไซต์ที่ก่อตั้งขึ้นเพื่อเป็นกองทุนให้ความช่วยเหลือผู้เคราะห์ร้ายในเหตุการณ์สึนามิ เป็นจำนวน 30 ปอนด์โดยส่งข้อมูลส่วนตัวโดยไม่ได้ปกปิดตนเอง แต่เขาแต่ไม่ได้รับการยืนยันการบริจาคของตน

นาย Cuthbert เริ่มกังวลว่าเขาจะถูกฉ้อโกงบัตรเครดิตที่ใช้ในการบริจาค เขาจึงทำการทดสอบพื้นฐาน ถ้าผลการทดสอบนั้นเป็นว่าเป็นการตั้งเวปไซต์ขึ้นเพื่อฉ้อโกง เขาก็จะแจ้งเจ้าหน้าที่ นาย Cuthbert กล่าวอ้างว่าไม่ได้ทำเพื่อความสนุกและเนื่องจากสงสัยว่าจะเป็นเวปไซต์หลอกลวงจึงได้ทำการทดสอบดังกล่าวและปรากฏว่าเวปไซต์นั้นปลอดภัย

ซึ่งการกระทำนั้นทำให้เขาถูกตัดสินลงโทษ ซึ่งทำให้มีการวิพากษ์วิจารณ์ว่าเป็นการเหมาะสมหรือไม่ ซึ่งหากพิจารณาจากตัวบทกฎหมายของประเทศอังกฤษแล้ว ก็จะเห็นได้ว่า

---

[82] John Oates, “Tsunami hacker convicted,” [Online] Available from : www.theregister.co.uk/2005/10/06/tsunami_hacker_convicted [วันที่ 1 มกราคม 2551]

[83] “Justice versus legality – the case of Daniel Cuthbert,” [Online] Available from : www.samizdata.net/blog/archives/008118.html [วันที่ 1 กุมภาพันธ์ 2551]

มีหลักเกณฑ์ในการกำหนดความรับผิดในการเข้าถึงเหมือนกับของประเทศไทยคือ ไม่ต้องมีเจตนาพิเศษหรือองค์ประกอบอื่น หากมีเจตนาเข้าถึงแล้วการกระทำนั้นก็เป็นความผิด ซึ่งหากข้อเท็จจริงเป็นดังที่กล่าวอ้างกันในเวปไซต์แล้วในความคิดของคนทั่วไปก็มักจะเห็นว่า นาย Cuthbert ไม่ควรจะต้องรับผิดเนื่องจากไม่ได้มีเจตนาร้ายหรือเจตนาที่จะกระทำความผิดแต่อย่างใด แต่อย่างไรก็ตาม ก็อาจมีผู้กล่าวว่าการที่จะพิสูจน์เจตนามุ่งร้ายนั้นเป็นสิ่งที่ทำได้ยากและทำให้ผู้กระทำความผิดกล่าวอ้างเพื่อที่จะให้ตนเองพ้นจากความรับผิดทางอาญาได้

หากกรณีดังกล่าวเกิดขึ้นในประเทศไทย ปัญหาที่จะต้องพิจารณาคือ ศาลควรจะตัดสินอย่างไร เนื่องจากเห็นได้ว่า พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีหลักเกณฑ์ในเรื่องเจตนาว่า เพียงแต่มีเจตนาเข้าถึงก็เป็นความผิดแล้ว และเมื่อการเข้าถึงนั้นเป็นการเข้าถึงโดยไม่มีอำนาจกระทำได้จึงเป็นการเข้าถึงโดยมิชอบ ผู้เขียนจึงเห็นว่าหากคดีดังกล่าวเกิดขึ้นในประเทศไทยแล้ว เมื่อพิจารณาจากความผิดฐานเข้าถึงโดยมิชอบ นาย Cuthbert ก็ต้องถูกลงโทษตามกฎหมายเช่นกัน เนื่องจากกฎหมายไทยเองก็มีองค์ประกอบความรับผิดในส่วนของเจตนาเหมือนของประเทศอังกฤษคือเพียงแค่มีเจตนาเข้าถึงก็เป็นความผิดแล้ว

แต่อย่างไรก็ตาม หากข้อเท็จจริงเป็นดังที่กล่าวอ้างแล้ว นาย Cuthbert ไม่มีเจตนาร้ายใดๆ ที่จะกระทำความผิดและแม้แต่ศาลก็ยอมรับในข้อเท็จจริงนี้เช่นกัน หากแต่ด้วยบทบัญญัติของกฎหมายที่เคร่งครัดทำให้ต้องรับโทษ ทั้งที่การกระทำของนาย Cuthbert ไม่น่าที่จะถูกลงโทษในความผิดอาญา ซึ่งหากพิจารณาดูแล้ว ทางแก้ไขปัญหาดังกล่าวอาจจะทำได้โดยกำหนดให้การกระทำที่จะเป็นความผิดต้องมีเจตนาพิเศษ[84] เช่น ต้องมีเจตนาเพื่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน หรือมีองค์ประกอบอื่น ซึ่งผู้เขียนเห็นว่าจะทำให้ขอบเขตการใช้บังคับกฎหมายมีข้อจำกัดมากขึ้นและเปิดโอกาสให้ศาลได้ใช้ดุลพินิจในการตัดสินคดีที่มีลักษณะคล้ายคดีของนาย Cuthbert ได้กว้างขวางยิ่งขึ้น

5.4 ความผิดสำเร็จ พยายาม ตระเตรียม

---

[84] Judge Stein Schjqlberg and Amanda M. Hubbard, “Background paper harmonizing national and legal approaches on cyber,” [Online]

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะลงโทษผู้กระทำความผิดในการเข้าถึงโดยมิชอบก็ต่อเมื่อการกระทำนั้นเลยขั้นตระเตรียมเข้าขั้นลงมือกระทำความผิดแล้ว ซึ่งถือว่าเป็นการพยายามกระทำความผิดและลงโทษผู้กระทำความผิดสำเร็จ ซึ่งปัญหาที่อาจเกิดขึ้นคือ เมื่อใดที่ถือว่าเป็นการทำความผิดสำเร็จและเมื่อใดถือว่าเป็นการพยายามกระทำความผิดในความผิดเกี่ยวกับการเข้าถึงโดยมิชอบ หรือขั้นตอนใดเป็นเพียงการตระเตรียมในการกระทำความผิด ซึ่งการตระเตรียมกระทำความผิดคือการกระทำที่ห่างไกลมาก เช่น รู้ชื่อและรหัสผ่านของผู้อื่นโดยตั้งใจจะแฮกเข้าไปแต่ยังไม่ได้ทำก็เป็นเพียงแค่การตระเตรียมซึ่งกฎหมายไม่ถือว่าเป็นความผิด

ส่วนการพยายามกระทำความผิดนั้น อาจจะอธิบายได้ง่ายๆ เช่น นายโจกลัวว่านางสาวเจนแฟนสาวของตนหลอกลวงตนและนายโจต้องการเข้าไปดูอีเมล์ของนางสาวเจน โจ log in ไปยัง ISP ของนางสาวเจน ใส่ชื่อของนางสาวเจนและเริ่มเดารหัสผ่าน โจประสบความสำเร็จในความพยายามในครั้งที่ 11 และอ่านข้อความส่วนตัวของนางสาวเจน ซึ่งในกรณีนี้มีปัญหาที่ต้องพิจารณาว่าขั้นตอนใดเป็นการพยายามกระทำความผิด และขั้นตอนใดที่ถือว่าเป็นการกระทำผิดสำเร็จ

ในกรณีที่กล่าวมาข้างต้นนั้น อาจมองได้ 2 แง่มุมว่า การกระทำของโจไม่เป็นความผิดเนื่องจากไม่มีการหวงห้ามในการใส่ชื่อและรหัสผ่านในโปรแกรมผู้ให้บริการการที่นายโจใส่ชื่อและรหัสผ่านย่อมเป็นสิ่งที่ทำได้และไม่มีการหวงห้ามมิให้ทำแต่อย่างใด แต่ก็มีผู้ให้ความเห็นอีกทางหนึ่งว่า[85]การเข้าไปใน ISP และเริ่มเดาชื่อและรหัสผ่านนั้นแม้ไม่เป็นความผิดในการเข้าถึงโดยมิชอบ โดยโจไม่ได้เข้าถึงโดยมิชอบสำเร็จในการกระทำ 10 ครั้งแรก แต่ก็เป็นการพยายามกระทำความผิด โดยกระทำของโจเป็นความผิดสำเร็จในการเข้าถึงโดยมิชอบเมื่อโจใส่รหัสผ่านถูกต้องในการกระทำครั้งที่ 11 ซึ่งการเข้าถึงเกิดขึ้นจากการใช้ ID ปลอมโดยคอมพิวเตอร์เชื่อว่านางสาวเจนเป็นผู้ใส่รหัสผ่านหรือนายโจมีอำนาจกระทำได้ ซึ่งผู้เขียนก็เห็นด้วยกับความเห็นดังกล่าว เพราะการพยายามเดารหัสผ่านเมื่อยังไม่ถูกต้องก็เป็นเพียงความพยายามเข้าถึงเท่านั้น

---

[85] Orin S. Kerr, “Cybercrime's Scope: Interpreting 'Access' and Authorization' in Computer Misuse Statutes,” [Online]

เพราะการกระทำนั้นเป็นการกระทำที่ใกล้ชิดต่อผลแล้ว หากนายโจเดาถูกก็จะเป็นการเข้าถึงโดยมิชอบในทันที

นอกจากนี้ในกรณีพยายามกระทำความผิดที่อาจเกิดขึ้น เช่น นายแดงต้องการเข้าถึงคอมพิวเตอร์ของดำที่ได้กำหนดรหัสผ่านไว้ เมื่อนายแดงพยายาม log in เข้าไปในคอมพิวเตอร์ของดำ พยายามใส่ชื่อผู้ใช้และรหัสผ่านแต่ไม่สำเร็จ นายแดงจึงยกเลิก เป็นการกระทำความผิดหรือไม่ หรือกรณีที่นายแดงพยายาม log in เข้าไปในคอมพิวเตอร์ของดำ ใส่ชื่อผู้ใช้และรหัสผ่านที่ถูกต้องแล้วแต่ยังไม่กด enter ต่อมานายแดงยกเลิกโดยการลบชื่อและรหัสทิ้ง การกระทำของนายแดงเป็นการกระทำความผิดหรือไม่

ในกรณีแรกนั้นผู้เขียนเห็นว่า เป็นกรณีที่นายแดงพยายามกระทำความผิดในการเข้าถึงโดยมิชอบเนื่องจากการนายแดงต้องการเข้าไปในคอมพิวเตอร์ของนายดำโดยพยายามเดารหัสผ่านของนายดำ ซึ่งการกระทำของนายแดงนั้นใกล้ชิดกับผลแล้วเนื่องจากหากนายแดงเดาถูกนายแดงก็สามารถเข้าถึงคอมพิวเตอร์ของนายดำได้เป็นความผิดสำเร็จ แม้นายแดงจะเดาไม่ถูกและล้มเลิกการกระทำความผิดไป แต่การกระทำของนายแดงเป็นการพยายามที่จะเข้าถึงโดยมิชอบแล้ว แต่ปัญหาที่อาจต้องพิจารณาคือ การพยายามกระทำความผิดของนายแดงนั้นเป็นความพยายามที่เป็นไปไม่ได้อย่างแน่แท้ตามมาตรา 81 หรือไม่ ซึ่งในกรณีนี้ผู้เขียนมีความเห็นว่านายแดงพยายามกระทำความผิดตามมาตรา 80 ไม่ใช่การพยายามกระทำความผิดตามมาตรา 81 เนื่องจากเหตุปัจจัยซึ่งใช้ในการกระทำหรือเหตุแห่งวัตถุที่มุ่งหมายกระทำต่อนั้นไม่ใช่ว่าจะไม่สามารถเดารหัสผ่านได้แต่อย่างใด นายแดงมีโอกาสที่จะเดารหัสผ่านได้ถูกต้องเพียงแต่ที่นายแดงเข้าไปในคอมพิวเตอร์ของนายดำไม่สำเร็จเนื่องจากล้มเลิกไปก่อน การกระทำของนายแดงจึงเป็นการกระทำความผิดตามมาตรา 80

ส่วนในกรณีที่สองนั้นอาจจะมองได้ว่าการกระทำของนายแดงใกล้ชิดต่อผลที่จะเกิดขึ้นแล้วขาดเพียงการกด enter เพื่อที่จะเข้าไปในคอมพิวเตอร์ของนายดำได้ซึ่งจะทำให้การกระทำของนายแดงเป็นความผิดสำเร็จ แต่อย่างไรก็หากในกรณีนี้เป็นการที่นายแดงล้มเลิกการกระทำความผิดของตนด้วยความสมัครใจเอง นายแดงก็ไม่ต้องรับผิดแต่อย่างใดเนื่องจากเป็นกรณีที่นายแดงกลับใจไม่กระทำผิดไปโดยตลอดทำให้ไม่ต้องรับโทษสำหรับการพยายามกระทำความผิดนั้น และการตระเตรียมในการกระทำผิดฐานเข้าถึงโดยมิชอบก็ไม่มีกฎหมายกำหนดให้การกระทำนั้นเป็นความผิด นายแดงจึงไม่ต้องรับผิดแต่อย่างใด

5.5 ตัวการ ผู้ใช้ ผู้สนับสนุน

ในการพิจารณาเรื่องตัวการ ผู้ใช้ ผู้สนับสนุน นั้น โดยปกติแล้วย่อมต้องอาศัยหลักเกณฑ์ตามประมวลกฎหมายอาญามาเป็นหลักในการพิจารณาว่าการกระทำใดเป็นตัวการ ผู้ใช้ ผู้สนับสนุน โดยในความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้น ผู้ที่เกี่ยวข้องอาจเป็นได้ทั้งตัวการ ผู้ใช้ หรือผู้สนับสนุนในการกระทำผิดฐานเข้าถึงโดยมิชอบ ซึ่งหากพิจารณาจากฐานความผิดเกี่ยวกับการเข้าถึงโดยมิชอบแล้ว จะเห็นได้ว่าการกระทำความผิดเกี่ยวกับการเข้าถึงโดยมิชอบนั้นอาจแบ่งได้เป็น 2 ส่วน คือ ความผิดในการเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งมีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และความผิดในการล่วงรู้มาตรการการป้องกันแล้วนำไปเผยแพร่โดยมิชอบ

ในความผิดเกี่ยวกับการล่วงรู้มาตรการการป้องกันแล้วนำไปเผยแพร่โดยมิชอบนั้น อาจเป็นได้ทั้งความผิดที่กระทำลงโดยเป็นส่วนหนึ่งของความผิดในการเข้าถึงโดยมิชอบ หรืออาจเป็นความผิดที่เป็นเอกเทศที่ไม่เกี่ยวข้องกับผู้กระทำการเข้าถึงโดยมิชอบก็ได้ เช่น คดี R v Malcolm Farquharson นั้น ศาลอังกฤษตัดสินว่าการใช้โทรศัพท์เพื่อบอกผู้ร่วมกระทำผิดอีกคนหนึ่งให้เข้าถึงข้อมูลโดยปราศจากอำนาจ ทำให้จำเลยเป็นผู้ร่วมกระทำผิดในฐานเจาะระบบ ซึ่งในกรณีเช่นนี้หากเกิดขึ้นในประเทศไทย ผู้ที่โทรศัพท์บอกรหัสให้ผู้อื่นทำการเจาะระบบย่อมต้องมีความผิดในความผิดล่วงรู้มาตรการการป้องกันแล้วนำไปเผยแพร่โดยมิชอบ และย่อมเป็นตัวการร่วมกันในการกระทำความผิดในการเข้าถึงโดยมิชอบด้วย

ซึ่งสิ่งที่อาจจะต้องพิจารณาคือ หากผู้ร่วมกระทำความผิดบอกถึงรหัสผ่านให้แก่ผู้อื่นกระทำความผิดขึ้น ผู้นั้นจะต้องรับผิดทั้งในฐานะตัวการผู้กระทำความผิดในการเข้าถึงโดยมิชอบ และต้องรับผิดในความผิดฐานล่วงรู้มาตรการการป้องกันแล้วนำไปเผยแพร่โดยมิชอบด้วยหรือไม่ หรือหากผู้กระทำความผิดมีฐานะเป็นตัวการในการเข้าถึงโดยมิชอบแล้วย่อมไม่เป็นความผิดในการล่วงรู้มาตรการการป้องกันแล้วนำไปเผยแพร่โดยมิชอบด้วย

ซึ่งในกรณีนี้ ผู้เขียนมีความเห็นว่าหากผู้ร่วมกระทำความผิดบอกถึงรหัสผ่านให้แก่ผู้อื่นกระทำความผิดขึ้น ผู้นั้นจะต้องรับผิดทั้งในฐานะตัวการผู้กระทำความผิดในการเข้าถึงโดยมิชอบ และต้องรับผิดในความผิดฐานล่วงรู้มาตรการการป้องกันแล้วนำไปเผยแพร่โดยมิชอบด้วย เนื่องจากไม่มีการจำกัดว่าผู้ที่ร่วมกระทำความผิดในความผิดฐานเข้าถึงโดยมิชอบแล้วจะไม่ต้องรับผิดในความผิดฐานอื่นอีก

บทที่ 6

บทสรุปและข้อเสนอแนะ

เมื่อคอมพิวเตอร์แพร่หลายทั่วไปในสังคม ไม่จะเต็มใจหรือไม่ก็ตามบุคคลโดยทั่วไปคงไม่สามารถปฏิเสธบทบาทที่เพิ่มมากขึ้นของคอมพิวเตอร์ในชีวิตประจำวันได้ คอมพิวเตอร์ทำให้พฤติกรรมของบุคคลเปลี่ยนแปลงไปทั้งในแง่ชีวิตการทำงาน การพักผ่อน หรือแม้แต่ปฏิสัมพันธ์ในสังคม จึงไม่น่าแปลกใจที่นอกจากการใช้คอมพิวเตอร์ดังที่กล่าวมาแล้ว คอมพิวเตอร์ได้กลายเป็นสิ่งที่ใช้กระทำผิดหรือกลายเป็นเป้าหมายของการกระทำความผิดด้วยเช่นกัน นอกจากนั้นคอมพิวเตอร์ยังก่อให้เกิดการกระทำความผิดในรูปแบบใหม่ๆ ที่ไม่สามารถเกิดขึ้นได้ในสังคมที่ไม่มีคอมพิวเตอร์ใช้

การกระทำความผิดโดยการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์เป็นความผิดที่เกิดขึ้นและเป็นที่รู้จักกันในเวลาไม่กี่สิบปี โดยรูปแบบการกระทำความผิดแตกต่างจากการกระทำความผิดในอดีตทั้งในแง่การกระทำความผิดและการสืบสวนสอบสวน รวมถึงการรวบรวมพยานหลักฐานในการจับกุมและดำเนินคดีกับผู้กระทำความผิด

เมื่อการกระทำความผิดในการเข้าถึงโดยมิชอบมีการกระทำความผิดเกิดขึ้นบ่อยครั้งและเกิดความเสียหายมากขึ้นเนื่องจากความนิยมใช้คอมพิวเตอร์ในด้านต่างๆที่เพิ่มมากขึ้นในสังคม จึงก่อให้เกิดปัญหาในกฎหมายของประเทศต่างๆ ว่ากฎหมายอาญาที่มีอยู่เดิมนั้นสามารถนำตัวผู้กระทำความผิดมาลงโทษได้หรือไม่ ซึ่งในความผิดอาญาดังเดิมที่เพียงแต่อาศัยคอมพิวเตอร์มาช่วยในการกระทำความผิด เช่น หมิ่นประมาท ฉ้อโกง นั้นอาจจะสามารถนำกฎหมายอาญาแบบเดิมมาลงโทษผู้กระทำความผิดได้ แต่ในความผิดที่เป็นความผิดอาชญากรรมคอมพิวเตอร์โดยแท้ที่อาศัยการทำงานของคอมพิวเตอร์ในการกระทำความผิดแล้วองค์กรระหว่างประเทศต่างๆ และนานาประเทศต่างเห็นพ้องต้องกันว่าความผิดอาญาดั้งเดิมไม่สามารถนำตัวผู้กระทำความผิดในการเข้าถึงโดยมิชอบได้ จึงมีการออกกฎหมายมาบังคับใช้สำหรับความผิดฐานเข้าถึงโดยมิชอบ

โดยแนวทางในการออกกฎหมายเกี่ยวกับการเข้าถึงโดยมิชอบนั้น องค์กรระหว่างประเทศ เช่น สหภาพยุโรป ก็ได้มีการกำหนดแนวทางในการกำหนดฐานความผิดในการเข้าถึงโดยมิชอบขึ้น หรือแม้แต่ประเทศต่างๆ ก็มีการกำหนดความผิดเกี่ยวกับการเข้าถึงคอมพิวเตอร์ขึ้นโดยอาจจะกำหนดขึ้นเป็นพระราชบัญญัติแยกต่างหากจากกฎหมายอาญาทั่วไป ดังเช่นในประเทศสหรัฐอเมริกา และประเทศอังกฤษ และบางประเทศก็กำหนดเพิ่มเติมในประมวล

กฎหมายอาญาเดิม เช่น ประเทศเยอรมัน แต่ไม่ว่าจะกำหนดกฎหมายอย่างไรก็ตาม แต่ก็จะเห็นได้ว่าทุกประเทศต่างเล็งเห็นความสำคัญและได้กำหนดกฎเกณฑ์ความรับผิดในการเข้าถึงคอมพิวเตอร์ขึ้น ซึ่งผู้เขียนได้ยกขึ้นมาพิจารณา 3 ประเทศ คือ ประเทศสหรัฐอเมริกา อังกฤษ และเยอรมัน ซึ่งบทบัญญัติของประเทศต่างๆ นั้น อาจมีสิ่งที่คล้ายคลึงและแตกต่างกัน

ประเทศสหรัฐอเมริกา

ในประเทศสหรัฐอเมริกา การกำหนดความผิดในการกระทำความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจ มีอยู่ทั้งในกฎหมายมลรัฐและกฎหมายของรัฐบาลกลาง แต่ที่เป็นกฎหมายหลักที่ถูกหยิบยกขึ้นเพื่อพิจารณาและถือว่าเป็นกฎหมายที่กับการเข้าถึงโดยปราศจากอำนาจโดยตรง คือ The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CFAA) มาตรา 1030 ของรัฐบาลกลาง

กฎหมายเกี่ยวกับการเข้าถึงปราศจากอำนาจนั้นมีรายละเอียดค่อนข้างมาก ผู้เขียนจึงขอสรุปฐานความผิดในมาตรา 1030 ที่เกี่ยวข้องกับการเข้าถึงโดยปราศจากอำนาจดังนี้

1. เอาไปซึ่งข้อมูลเกี่ยวกับความมั่นคงของประเทศสหรัฐอเมริกา
2. เอาไปซึ่งข้อมูลที่เป็นความลับ
3. บุกรุกเข้าไปในคอมพิวเตอร์ของรัฐ
4. เข้าถึงคอมพิวเตอร์เพื่อฉ้อโกงหรือเอาสิ่งที่มีราคา
5. เข้าถึงโดยเจตนาหรือประมาทโดยรู้ตัวทำให้เกิดความเสียหาย

ซึ่งอาจแยกพิจารณาได้ ดังนี้

ฐานความผิด	มาตรา	บทลงโทษอย่างสูง (กรณีจำคุก)
เอาไปซึ่งข้อมูลเกี่ยวกับความมั่นคงของประเทศสหรัฐอเมริกา	(a) (1)	10 ปี (*20 ปี)
เอาไปซึ่งข้อมูลที่เป็นความลับ	(a) (2)	1 ปี หรือ 5 ปี
บุกรุกเข้าไปในคอมพิวเตอร์ของรัฐ	(a) (3)	1 ปี (*10 ปี)
เข้าถึงคอมพิวเตอร์เพื่อฉ้อโกงหรือเอาสิ่งที่มีราคา	(a) (4)	5 ปี (*10 ปี)
เข้าถึงโดยเจตนาหรือประมาทโดยรู้ตัวทำให้	(a) (5) (A) (ii)	5 ปี (*20 ปี)

เกิดความเสียหาย		
เข้าถึงโดยเจตนาและก่อให้เกิดความเสียหาย	(a) (5) (A) (iii)	1 ปี (*10 ปี)

* โทษจำคุกสูงสุดสำหรับกรณีการกระทำผิดตามมาตรานี้ซ้ำอีก

โดยผู้เขียนจะสรุปว่าการกระทำความผิดเนื่องจากการเข้าถึงโดยปราศจากอำนาจหรือเกินขอบอำนาจที่เป็นองค์ประกอบความผิดในของมาตรา 1030 ในอนุมาตราต่างๆ มีดังนี้

การเข้าถึงโดยปราศจากอำนาจที่เป็นองค์ประกอบความผิดในมาตรา 1030 สรุปได้ดังนี้[1]

มาตรา 1030	โดยปราศจากอำนาจ	เกินขอบอำนาจ	ไม่มีองค์ประกอบดังกล่าว
(a) (1) เอาไปซึ่งข้อมูลเกี่ยวกับความมั่นคงของประเทศสหรัฐอเมริกา	/	/	
(a) (2) เอาไปซึ่งข้อมูลที่เป็นความลับ	/	/	
(a) (3) บุกรุกเข้าไปในคอมพิวเตอร์ของรัฐ	/		
(a) (4) เข้าถึงคอมพิวเตอร์เพื่อฉ้อโกงหรือเอาสิ่งที่มีราคา	/	/	
(a) (5) (A) (ii) เข้าถึงโดยเจตนาหรือประมาทโดยรู้ตัวทำให้เกิดความเสียหาย	/		
(a) (5) (A) (iii) เข้าถึงโดยเจตนาและก่อให้เกิดความเสียหาย	/		

เมื่อพิจารณาแล้วจะเห็นได้ว่าไม่ว่ากฎหมาย The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CFAA) มาตรา 1030 ของรัฐบาลกลาง

---

[1] "Prosecuting Computer Crimes : Computer Fraud and Abuse Act"; [PDF; Online] แหล่งที่มา : www.cybercrime.gov (วันที่ 1 กุมภาพันธ์ 2551)

และกฎหมายของมลรัฐ ต่างเริ่มหลักเกณฑ์ความผิดจากการเข้าถึงโดยปราศจากอำนาจ และเพิ่มเติมองค์ประกอบอื่นเข้ามา เช่น การเข้าถึงข้อมูลเกี่ยวกับความมั่นคง ข้อมูลที่เป็นความลับหรือเข้าถึงเพื่อฉ้อโกง จึงเห็นได้ว่าในประเทศสหรัฐอเมริกาได้มีการแบ่งแยกระดับของการเข้าถึงและให้ความสำคัญของระดับชั้นของข้อมูลที่เข้าถึงได้ ทำให้เห็นว่าประเทศสหรัฐอเมริกาให้ความสำคัญในเรื่องของข้อมูลเป็นสำคัญจึงได้ใช้ประเภทของข้อมูลที่ถูกเข้าถึงเป็นหลักในการกำหนดฐานความผิด แต่ไม่มีหลักเกณฑ์ในเรื่องมาตรการป้องกันการเข้าถึงเป็นองค์ประกอบความผิดแต่อย่างใด

โดยประเด็นที่ยังเป็นที่ถกเถียงกันในความผิดฐานเข้าถึงโดยปราศจากอำนาจของสหรัฐอเมริกาคือ เมื่อใดเป็นการเข้าถึง และการเข้าถึงใดเป็นการเข้าถึงโดยปราศจากอำนาจ ซึ่งในประเทศสหรัฐอเมริกาก็ยังมีความขัดแย้งกันในการกำหนดขอบเขตของถ้อยคำในกฎหมาย จะเห็นได้ว่าในการตีความคำว่า “เข้าถึง” และคำว่า “โดยปราศจากอำนาจ” ของศาลสหรัฐอเมริกานั้นมีทั้งการตีความทั้งอย่างกว้างและอย่างแคบ แล้วแต่ศาลนั้นจะพิจารณาตามแต่มุมมองซึ่งมีความแตกต่างกันไป ซึ่งการตีความในขอบเขตที่แตกต่างกันย่อมมีผลถึงความรับผิดทางอาญาของผู้กระทำการนั้น หากศาลตีความอย่างแคบแล้วก็มีแนวโน้มว่าผู้กระทำความผิดจะรอดพ้นจากการลงโทษตามกฎหมายเนื่องจากกล่าวอ้างว่าการกระทำของไม่ใช่การเข้าถึง หรือไม่ใช่การเข้าถึงโดยปราศจากอำนาจ

ประเทศอังกฤษ

ประเทศอังกฤษ ได้กำหนดความผิดฐานเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ (Unauthorized Access) ไว้ใน Computer Misuse Act 1990 มาตรา 1 และมาตรา 2 ซึ่งอาจความรับผิดออกเป็น 2 ส่วน ได้ดังนี้

1. **การเข้าถึงโดยปราศจากอำนาจซึ่งสิ่งที่อยู่ในคอมพิวเตอร์** (เช่น โปรแกรม หรือข้อมูล) ตาม Computer Misuse Act 1990 (CMA) มาตรา 1 ซึ่งถูกแก้ไขเพิ่มเติมโดย Police and Justice Act 2006 (แต่จะมีผลบังคับใช้ประมาณเดือนเมษายน 2008) บุคคลมีความผิด ถ้า

(a) ผู้นั้นได้ทำให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ โดยความจงใจที่จะผ่านสิ่งปกป้องคุ้มครองไม่ให้เข้าสู่ระบบได้ และได้ผ่านสิ่งปกป้องหรือสามารถทำการเข้าถึงใดๆ เช่นว่านั้นเข้าไปยังโปรแกรมใดๆ หรือข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ใดๆ

(b) การผ่านสิ่งปกป้องคุ้มครองหรืออาจถูกปกป้องคุ้มครองเข้าไปสู่ระบบด้วยความจงใจนั้นเป็นการกระทำโดยปราศจากอำนาจ และ

(c) ผู้นั้นได้รู้อยู่ในเวลาที่เขาได้กระทำการอันเป็นเหตุให้คอมพิวเตอร์แสดงผล หรือแสดงการทำงานอันปราศจากอำนาจนั้น

2. **การเข้าถึงโดยปราศจากอำนาจ โดยเจตนาที่จะกระทำหรือให้ความสะดวกแก่การกระทำความผิดอื่น** ตาม Computer Misuse Act 1990 (CMA) มาตรา 2 โดยมาตรา 2 เป็นมาตราที่ใช้บังคับกับกรณีที่เป็นความผิดที่ซับซ้อนขึ้น (Ulterior Hacking Offence) โดยมาตรา 2 กำหนดว่า

(1) บุคคลที่มีความผิดภายใต้บทบัญญัตินี้ ถ้าหากว่าเขาได้กระทำผิดตามมาตรา 1 ด้วยเจตนา (มาตรา 1 บัญญัติว่าการไม่มีอำนาจในการเข้าสู่ระบบเป็นความผิด)

(a) ได้กระทำผิดในสิ่งที่มาตรานี้บังคับให้ หรือ

(b) ให้ความสะดวกในการกระทำผิด (ไม่ว่าโดยตนเองหรือโดยบุคคลใดๆ) และความผิดที่เขาจงใจในการกระทำผิด หรือให้ความสะดวกดังกล่าวต่อไปในมาตรานี้ให้ถือว่าเป็นผู้กระทำผิดเช่นเดียวกับผู้กระทำผิดที่ตนช่วย

(3) เพื่อวัตถุประสงค์ของมาตรานี้ไม่ว่าการกระทำความผิดของผู้กระทำผิดที่อยู่ห่างไกล (Remote hacker) จะได้กระทำลงในโอกาสที่ไม่มีอำนาจในการเข้าสู่ระบบนั้นหรือไม่ หรือโดยอาศัยโอกาสอื่นใดก็ตาม

(4) บุคคลอาจจะมีความผิดตามมาตรานี้ถึงแม้ว่าจะมีข้อเท็จจริงว่าการกระทำความผิดของผู้กระทำความผิดที่อยู่ห่างไกลจะไม่ได้กระทำลงก็ตาม

จากบทบัญญัติของกฎหมายของประเทศอังกฤษจะเห็นได้ว่า ประเทศอังกฤษมีขอบเขตในการกำหนดความรับผิดในการเข้าถึงโดยปราศจากอำนาจที่กว้างมาก และมีบทลงโทษหนักขึ้นสำหรับผู้ที่มีเจตนาร้าย และเพียงแค่เข้าถึงโดยปราศอำนาจก็เป็นความผิดแล้ว โดยไม่จำเป็นต้องพิสูจน์ว่ามีเจตนามุ่งแต่อย่างใด จึงทำให้เกิดปัญหาว่าแม้จะเป็นการเข้าถึงโดยไม่มีเจตนาที่ไม่เหมาะสมแล้ว ก็ยังเป็นความผิดตามกฎหมายและก่อให้เกิดปัญหาทางสังคมเนื่องจากบางครั้งผู้ที่ถูกลงโทษก็ไม่ใช่ผู้ที่เป็นอาชญากรแต่อย่างใด หากแต่เป็นเพียงผู้ใช้คอมพิวเตอร์ตามปกติและทำเกินเลยไปบ้างเท่านั้น

3. ประเทศเยอรมัน

กฎหมายเกี่ยวกับการเข้าถึงโดยไม่มีอำนาจของประเทศเยอรมัน ปรากฏอยู่ในมาตรา 202a (ใหม่) โดยกำหนดว่า "ผู้ใดกระทำการใด ๆ โดยไม่มีอำนาจเข้าถึงข้อมูลที่มิได้มีไว้สำหรับตน และเป็นข้อมูลที่มีมาตรการรักษาความปลอดภัยโดยเฉพาะสำหรับป้องกันมิให้มีการเข้าถึงข้อมูลนั้นได้ ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือมีโทษปรับ"

ดังที่ได้กล่าวมาแล้วว่า กฎหมายของประเทศเยอรมันเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจได้ถูกแก้ไขเพิ่มเติมในประมวลกฎหมายอาญา โดยมีหลักเกณฑ์คล้ายคลึงกับประเทศไทยในเรื่องการเข้าถึงข้อมูลโดยมิชอบ หากแต่มุ่งคุ้มครองเพียงการเข้าถึงข้อมูลในคอมพิวเตอร์เท่านั้น ไม่รวมถึงระบบคอมพิวเตอร์เหมือนในประเทศไทยแต่อย่างใด

4. ประเทศไทย

ในประเทศไทยเองก็มีกฎหมายเกี่ยวกับการเข้าถึงโดยมิชอบด้วยเช่นกัน โดยได้มีการบัญญัติความรับผิดทางอาญาในการเข้าถึงโดยมิชอบไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยได้กำหนดความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ และการล่วงรู้มาตรการการป้องกันโดยมิชอบและนำไปเปิดเผย โดยกำหนดกฎเกณฑ์ที่แตกต่างไปจากกฎหมายต่างประเทศในบางส่วน และเนื่องจากยังเป็นกฎหมายใหม่รวมทั้งมีถ้อยคำที่ไม่ชัดเจนในการตีความจึงอาจก่อให้เกิดปัญหาขึ้นในอนาคตได้ดังที่ได้กล่าวมาแล้วในบทที่ 5

จะเห็นได้ว่ากฎหมายแต่ละประเทศแม้จะมีหลักการเดียวกันคือห้ามการเข้าถึงโดยไม่มีอำนาจ แต่ก็มีองค์ประกอบแตกต่างกันแต่ก็มีแนวทางและการบัญญัติกฎหมายที่แตกต่างกันไปตามแต่จุดประสงค์ของรัฐที่มุ่งจะคุ้มครองสิ่งใดเป็นสำคัญ

ผู้เขียนจะขอเปรียบเทียบความผิดในการเข้าถึงโดยมิชอบกับกฎหมายของประเทศสหรัฐอเมริกา อังกฤษ และเยอรมัน ได้ดังนี้

1. ทั้งประเทศไทย สหรัฐอเมริกา และอังกฤษ ต่างกำหนดให้ความผิดฐานเข้าถึงโดยมิชอบซึ่งเป็นความผิดหนึ่งในความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์เป็นพระราชบัญญัติโดยเฉพาะ ขณะที่ประเทศเยอรมันได้แก้ไขปรับปรุงประมวลกฎหมายอาญาของตนโดยเพิ่มเติมความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจและบทบัญญัติเกี่ยวกับอาชญากรรมคอมพิวเตอร์อื่นๆไว้ในประมวลกฎหมายอาญาเดิม

2. กฎหมายไทยแยกการเข้าถึงระบบคอมพิวเตอร์ออกจากการเข้าถึงข้อมูลคอมพิวเตอร์ ในขณะที่กฎหมายของประเทศสหรัฐอเมริกา อังกฤษ และเยอรมัน ไม่มีการแบ่งแยกระบบข้อมูลคอมพิวเตอร์ออกจากคอมพิวเตอร์อย่างชัดเจน หากแต่จะพิจารณาการเข้าถึงในคอมพิวเตอร์เป็นหลัก และอาจกำหนดรายละเอียดปลีกย่อยว่าเข้าไปเพื่อจุดประสงค์ใด เช่น เพื่อทำการฉ้อโกง เข้าถึงคอมพิวเตอร์ของรัฐ ของประเทศสหรัฐอเมริกา หรือเข้าถึงโดยมีเจตนากระทำความผิดอื่นของประเทศอังกฤษ ในขณะที่ประเทศเยอรมันไม่พูดถึงการเข้าถึงระบบคอมพิวเตอร์หากแต่มุ่งพิจารณาถึงการเข้าถึงข้อมูลในคอมพิวเตอร์เป็นสำคัญ

ผู้เขียนเองเห็นว่าไม่มีความจำเป็นที่จะต้องแยกระบบคอมพิวเตอร์ออกจากข้อมูลคอมพิวเตอร์แต่อย่างใด เนื่องจากการกระทำความผิดในการเข้าถึงนั้นเป็นเรื่องของข้อมูลในคอมพิวเตอร์เป็นหลัก และเมื่อพิจารณาถึงนิยามของกฎหมายแล้ว ก็จะเห็นได้ว่านิยามของคำว่าข้อมูลคอมพิวเตอร์ก็ครอบคลุมถึงระบบคอมพิวเตอร์แล้ว

3. การกำหนดให้การเข้าถึงเป็นความผิดเมื่อต้องล่วงล้ำมาตรการป้องกันเข้าไป ซึ่งเป็นองค์ประกอบของประเทศไทยและประเทศเยอรมัน ซึ่งผู้เขียนเห็นว่าการกำหนดหลักเกณฑ์ดังกล่าวเป็นการผลักภาระให้ประชาชนต้องป้องกันคอมพิวเตอร์ของตนเอง และหากประชาชนไม่ได้ทำการป้องกันดังกล่าว รัฐก็จะเพิกเฉยไม่ดำเนินการเนื่องจากอ้างว่าไม่เป็นความผิดตามกฎหมายฯได้ ดังนั้นผู้เขียนจึงเห็นว่าไม่ควรกำหนดว่าการเข้าถึงนั้นจะเป็นความผิดเมื่อล่วงล้ำมาตรการป้องกันเข้าไป หากแต่ควรกำหนดเหมือนประเทศสหรัฐอเมริกา และอังกฤษที่กำหนดให้การเข้าถึงนั้นเป็นความผิดทันทีที่กระทำโดยปราศจากอำนาจ

เมื่อผู้เขียนได้ศึกษาเนื้อหาตามวิทยานิพนธ์ฉบับนี้อย่างละเอียดแล้ว ผู้เขียนมีข้อเสนอแนะ ดังต่อไปนี้

1. การบัญญัติกฎหมาย

1.1 ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น ไม่ควรที่จะแยกการกระทำความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ออกจากกัน เนื่องจากเป็นการยุ่งยากในการตีความและผู้กระทำความผิดในการเข้าถึงระบบโดยมิชอบก็มีความผิดฐานเข้าถึงข้อมูลโดยมิชอบทันทีตามนิยามที่กฎหมายกำหนดไว้ จึงไม่มีความจำเป็นที่จะต้องแยกฐานความผิดทั้งสองออกจากกันแต่อย่างใด และในต่างประเทศ เช่น สหรัฐอเมริกา อังกฤษ หรือเยอรมัน ก็ไม่มีการแยกฐานความผิดในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ออกจากกันแต่อย่างใด ดังนั้นควร

ที่จะมีการแก้ไขกฎหมายเกี่ยวกับการกำหนดหลักเกณฑ์ความรับผิดในการกระทำความผิดในการเข้าถึงโดยมิชอบ โดยไม่จำเป็นต้องแยกการเข้าถึงระบบคอมพิวเตอร์ออกจากการเข้าถึงข้อมูลคอมพิวเตอร์

1.2 ในการกำหนดองค์ประกอบความผิดนั้น ควรที่จะยกเลิกองค์ประกอบความผิดที่กำหนดว่าต้องเป็นการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีการป้องกันโดยเฉพาะและการป้องกันนั้นไม่ได้มีไว้สำหรับตน โดยกำหนดให้การถึงโดยมิชอบเป็นความผิดในทันที และอาจกำหนดองค์ประกอบอื่นหรือเจตนาพิเศษเป็นองค์ประกอบภายนอกหรือภายในในการกำหนดองค์ประกอบความผิดเพิ่มขึ้น

1.3 การกำหนดเจตนาในการกระทำความผิดเพียงแค่เจตนาทั่วไปนั้นอาจทำให้มีการกำหนดหลักเกณฑ์ขององค์ประกอบภายในมีความเคร่งครัดจนอาจจะไม่เปิดช่องว่างให้ใช้ดุลพินิจได้ ดังนั้นผู้เขียนเห็นว่าควรที่จะเพิ่มเติมองค์ประกอบเกี่ยวกับเจตนา โดยกำหนดเจตนาพิเศษ เช่น เป็นการเข้าถึงโดยมิชอบเพื่อทำให้เกิดความเสียหายแก่ผู้หนึ่งผู้ใดเพื่อที่จะเปิดโอกาสให้ศาลได้ใช้ดุลพินิจในการพิจารณาว่าผู้ที่กระทำความผิดนั้นมีเจตนากระทำความผิดหรือไม่ หรือการกระทำนั้นก่อให้เกิดความเสียหายหรือไม่ ทำให้กฎหมายมีความยืดหยุ่นมากยิ่งขึ้น

1.4 ในความผิดการเข้าถึงโดยมิชอบนั้น ควรที่จะกำหนดการเพิ่มโทษกรณีที่การเข้าถึงนั้นเป็นเรื่องสำคัญ เช่น ข้อมูลความมั่นคง ข้อมูลทางการเงิน โดยกำหนดโทษให้หนักขึ้น ตามระดับความร้ายแรงและความเสียหายที่อาจเกิดขึ้นจากการเข้าถึงนั้น เนื่องจากความร้ายแรงที่เกิดขึ้นนั้นแตกต่างจากการเข้าถึงข้อมูลโดยทั่วไป ตลอดจนกรณีที่เข้าถึงเพื่อที่จะกระทำความผิดอื่นก็เป็นสิ่งที่ร้ายแรงและควรมีการกำหนดโทษให้หนักขึ้น

1.5 เมื่อมีการกำหนดระดับของการเข้าถึงข้อมูลสำคัญและบทลงโทษที่แตกต่างกันไปแล้ว ก็ควรที่จะกำหนดให้การกระทำความผิดในการเข้าถึงโดยมิชอบเพียงอย่างเดียวโดยไม่ได้กระทำความผิดอื่นอีกเป็นความผิดที่ไม่ร้ายแรงและสามารถอันยอมความได้ เนื่องจากในบางกรณีเป็นเพียงการกระทำของเด็กวัยรุ่นที่ไม่มีเจตนาร้ายใดๆ

นอกเหนือจากปัญหาและข้อเสนอแนะในเรื่องการบัญญัติกฎหมายแล้ว สิ่งที่มีความสำคัญอีกส่วนหนึ่งคือปัญหาในการใช้และตีความกฎหมาย โดยผู้เขียนจะขอเสนอแนะในปัญหาการใช้และตีความกฎหมาย ดังต่อไปนี้

2. **การใช้และตีความกฎหมาย**

2.1 ผู้ใช้กฎหมายต้องตีความอย่างระมัดระวัง เนื่องจากความรับผิดในการเข้าถึงโดยมิชอบนี้เป็นกฎหมายใหม่และเกี่ยวข้องกับศาสตร์ทางคอมพิวเตอร์ค่อนข้างมาก โดยผู้ใช้ต้องมีความรู้ความเข้าใจในการพิจารณาหลักเกณฑ์ทางกฎหมายเป็นอย่างมาก รวมตลอดถึงความเข้าใจในศาสตร์ทางคอมพิวเตอร์เพื่อที่จะใช้ดุลพินิจและตีความกฎหมายได้ถูกต้อง

2.2 การตีความคำว่า “เข้าถึง” ในความผิดฐานเข้าถึงโดยมิชอบนั้น ผู้เขียนเห็นว่าศาลต้องตีความคำว่าเข้าถึงอย่างกว้างเพื่อให้ครอบคลุมถึงพฤติกรรมในการกระทำความผิดและเทคโนโลยีใหม่ๆ ที่เกิดขึ้น โดยพิจารณาลักษณะการทำงานของคอมพิวเตอร์เป็นสำคัญ เนื่องจากการเข้าถึงเป็นองค์ประกอบสำคัญในความผิดฐานเข้าถึงโดยมิชอบ หากตีความแคบโดยถือว่าไม่ใช่การเข้าถึงแล้ว ก็จะทำให้มีปัญหาในลงโทษผู้กระทำความผิด

โดยผู้เขียนเห็นว่าแม้ไม่มีการให้คำนิยามคำว่า “เข้าถึง” ไว้ก็ตาม แต่ควรกำหนดเป็นแนวทางหรือบรรทัดฐานของศาลว่าการเข้าไปสื่อสารหรือควบคุมคอมพิวเตอร์ก็เป็นการเข้าถึงแล้ว เพื่อให้ครอบคลุมพฤติกรรมการกระทำความผิดในการเข้าถึงโดยมิชอบ

2.3 การตีความคำว่าการเข้าถึง “โดยมิชอบ” นั้นไม่ควรที่จะกำหนดกฎเกณฑ์ว่าเป็นการมิชอบด้วยกฎหมายหรือปราศจากอำนาจอย่างเดียว เนื่องจากอาจก่อให้เกิดปัญหาในการลงโทษผู้กระทำผิดได้ เช่น หากการเข้าถึงนั้นชอบแล้ว แม้ต่อมาจะไปทำความผิดใดอีก หากไม่มีกฎหมายบัญญัติความผิดไว้ การกระทำนั้นก็ไม่เป็นความผิด เช่น การขโมยข้อมูล เป็นต้น โดยผู้เขียนเห็นว่าควรจะปล่อยให้เป็นหน้าที่ของศาลที่จะตีความให้เหมาะสมกับพฤติกรรมของผู้กระทำผิดว่าเป็นการกระทำที่ไม่ชอบหรือไม่ เพื่อให้เกิดความเป็นธรรมในแต่คดี แต่อย่างไรก็ตามศาลต้องตีความอย่างระมัดระวังเนื่องจากการเข้าถึงโดยมิชอบนี้เป็นความผิดทางอาญาหากไม่ใช้ความระมัดระวังตามสมควรแล้วก็อาจทำให้เกิดผลกระทบทั้งต่อบุคคลและสังคมได้ เนื่องจากกฎหมายอาญาเป็นกฎหมายที่กระทบต่อสิทธิเสรีภาพของบุคคลเป็นอย่างมาก

รายการอ้างอิง

ภาษาไทย

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

กรุง เหลืองมโนธรรม. การศึกษาประเด็นทางกฎหมายเกี่ยวกับการจัดการความไม่มั่นคงของระบบคอมพิวเตอร์ในสังคมไทย : ศึกษาเฉพาะภัยไวรัสคอมพิวเตอร์ แฮกเกอร์ และสแปมเมล์. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2548.

คณิต ณ นคร.รวมบทความทางวิชาการเรื่องข้อสังเกตเกี่ยวกับความผิดฐานลักทรัพย์. กรุงเทพมหานคร : ห้างหุ้นส่วนจำกัดพิมพ์อักษร, 2540.

คณิต ณ นคร. โครงสร้างความรับผิดทางอาญาและข้อถกเถียงทางวิชาการเกี่ยวกับ mens rea. วารสารนิติศาสตร์ ปีที่ 16 ฉบับที่ 3 (กันยายน 2529) : 209.

ฉัทปณัย รัตนพันธ์. อาชญากรรมทางคอมพิวเตอร์ : ศึกษาการกำหนดฐานความผิดและการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์. สารนิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยธรรมศาสตร์, 2547.

เชิดพันธุ์ อุปนิสากร. ความรับผิดทางอาญาของผู้เข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2542

ญาณพล ยั่งยืน. "อาชญากรรมคอมพิวเตอร์" เอกสารประกอบการสัมมนาโครงการเพิ่มศักยภาพข้าราชการฝ่ายตุลาการศาลอุทธรณ์ภาค 9 ประจำปีงบประมาณ พ.ศ. 2550

ทวีเกียรติ มีนะกนิษฐ. กฎหมายอาญา หลักและปัญหา. กรุงเทพมหานคร : สำนักพิมพ์นิติธรรม, 2545.

ทวีเกียรติ มีนะกนิษฐ์. ปัจจัยสำคัญที่ทำให้กฎหมายขาดประสิทธิภาพ : บทบัณฑิตย์ เล่มที่ 60 : 96-103.

ธงชัย โรจน์กังสดาล. เลขานุการภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. สัมภาษณ์, 30 มกราคม 2551.

ธานินทร์ กรัยวิเชียร และวิชา มหาคุณ. การตีความกฎหมาย, พิมพ์ครั้งที่ 3 . กรุงเทพมหานคร : คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2539.

พรทิพย์ ตัณฑวนันท์ . อาชญากรรมเกี่ยวกับข้อมูลอิเล็กทรอนิกส์ . วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยธรรมศาสตร์, 2548.

พรเพชร วิชิตชลชัย.คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550. [Online] แหล่งที่มา : www.doa.go.th/human/other_50/com02_50.pdf

ไพจิตร สวัสดิสาร. การใช้คอมพิวเตอร์ทางกฎหมายและกฎหมายที่เกี่ยวกับคอมพิวเตอร์. กรุงเทพมหานคร : โรงพิมพ์ชวนพิมพ์, 2547

พีรพันธุ์ เปรมภูติ. เอกสารประกอบการสัมมนาเรื่องสภาพปัญหาอาชญากรมทางคอมพิวเตอร์. 10 กันยายน 2539

ภานุ รังสีสหัส. การกระทำความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2533.

นพมาศ ประสิทธิ์มณฑล. อาชญากรรมคอมพิวเตอร์ตามกฎหมายอเมริกา. [Online] แหล่งที่มา : www.geocities.com/elaw007/Article/cybercrime270502.html

ยืน ภู่วรวรรณ และคณะ. โปรแกรมคอมพิวเตอร์ภาษาเบสิค. กรุงเทพมหานคร : ซีเอ็ดยูเคชั่น, 2527.

หยุด แสงอุทัย. กฎหมายอาญา ภาค 2-3. ฉบับพิมพ์ครั้งที่ 9. กรุงเทพมหานคร : สำนักพิมพ์มหาวิทยาธรรมศาสตร์, 2542.

เลิศชาย สุธรรมพร. อาชญากรรมทางคอมพิวเตอร์ : ศึกษาเฉพาะกรณีความปลอดภัยของข้อมูล. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2541.

ศรีศักดิ์ จามรมาน “มีการขโมยข้อมูลส่วนตัวทางอินเทอร์เน็ตในสหรัฐถึง 26 ล้านราย” หนังสือพิมพ์เทเลคอมเจอร์นัล ปีที่ 16 ฉบับที่ 650 หน้า 20 วันที่ 1 - 7 มกราคม 2550. [Online] แหล่งที่มา : www.charm.ksc.au.edu/index_th.htm

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ.คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544. [Online] แหล่งที่มา : www.ecommerce.or.th/ictlaw

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ. แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์ 2546. [Online] แหล่งที่มา : www.etcommission.go.th/books/Cyber_crime.pdf

สันติธร บุญเจือ. คณบดีคณะเทคโนโลยีสารสนเทศและการสื่อสาร วิทยาลัยการศึกษาทางไกลอินเทอร์เน็ต มหาวิทยาลัยอัสสัมชัญ. สัมภาษณ์, วันที่ 24 ธันวาคม 2550.

สาวตรี สุขศรี. ความผิดเกี่ยวกับคอมพิวเตอร์ และอินเตอร์เน็ทตามประมวลกฎหมายอาญาเยอรมัน. แหล่งที่มา www.biolawcom.de

สราวุธ เบญจกุล. .“E-crime” อาชญากรรมทางอิเล็กทรอนิกส์ มหันตภัยในโลกยุคใหม่ [Online] แหล่งที่มา : www.etcommission.go.th/e-crime.html

สุเนติ คงเทพ. การไม่มีอำนาจเข้าสู่ระบบประมวลผล (Hacking). บทบัณฑิตย์ เล่มที่ 55 ตอน 1 (มีนาคม 2542)

สุปรียา อภิวัฒนากร. อาชญากรรมทางคอมพิวเตอร์ : ศึกษากรณีการหลอกลวงทางอินเตอร์เน็ต. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2545.

สรุปสาระสำคัญการประชุมคณะกรรมาธิการวิสามัญ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์. [Online] แหล่งที่มา : http://wiki.nectec.or.th/nectecpedia/index.php

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, กฎหมายธุรกรรมทางอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ กรุงเทพฯ : สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศ แห่งชาติ. 2544

องอาจ เทียนหิรัญ. อาชญากรรมทางคอมพิวเตอร์ : กำหนดฐานความผิดทางอาญาสำหรับการกระทำต่อคอมพิวเตอร์. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขานิติศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยธรรมศาสตร์, 2546.

เอกสารสรุปการสัมมนา "การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และการเตรียมความพร้อมกับกฎหมายใหม่" โครงการสำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอกนิกส์ วันที่ 8 สิงหาคม 2550

ภาษาอังกฤษ

BBC news. Tsunami web hacker found guilty. [Online] Available from : http://news.bbc.co.uk/2/hi/uk_news/england/london/4317008.stm

Computer Misuse Act 1990. [Online] Available from : www.cr-international.com/2008_UK_CPS_Draft_Guiding_Principles_Regarding_Hacking_Tools.pdf

Council of Europe's Explanatory Report on the Convention. [Online] Available from : http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

James T. Tsai. The Misery of Mitra : Considering Criminal Punishment for Computer Crime. [Online] Available from : http://law.bepress.com/expresso/eps/853

J.C.Smith and Brian Hogan. Criminal Law. 4ed. (London, Butterworths, 1978)

Jeffrey Steinberger, Your Right to Employee E-Mail. [Online] Available from : www.entrepreneur.com

John Oates, Tsunami hacker convicted. [Online] Available from : www.theregister.co.uk/2005/10/06/tsunami_hacker_convicted

Judge Stein Schjqlberg and Amanda M. Hubbard. Background paper harmonizing national and legal approaches on cyber. [Online] Available from : www.itu.int

Justice versus legality – the case of Daniel Cuthbert. [Online] Available from : www.samizdata.net/blog/archives/008118.htm

Mcconnell International, Cybercrime...and Punishment?. Archaic Laws Threaten Global Information [Dec., 2000] [Online] Available from : www.mcconnellinternational.com

Michael J L Turner. Computer Misuse Act 1990 cases. [Online] Available from : www.computerevidence.co.uk/Cases/CMA.htm

Orin S. Kerr. Cybercrime's Scope: Interpreting 'Access' and Authorization' in Computer Misuse Statutes. Public Law and Legal Theory Research Paper SeriesResearch Paper No. 65. [Online] Available from : www.law.nyu.edu/journals/lawreview/issues/vol78/no5/NYU502.pdf

The following countries have updated laws to prosecute cyber crime. [Online] Available from : www.mcconnellinternational.com

United Kingdom Parliament. R v Bow Street Magistrates Court and Allison ex parte Government of USA. [Online] Available from : www.parliament.the-stationery-office.co.uk:80/pa/ld199899/ldjudgmt/jd990805/bow.htm

United States Department of Justice. Prosecuting Computer Crimes : Computer Fraud and Abuse Act. [Online] Available from : www.cybercrime.gov

ภาคผนวก

หน้า ๔
เล่ม ๑๒๔ ตอนที่ ๒๗ ก ราชกิจจานุเบกษา ๑๘ มิถุนายน ๒๕๕๐

พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๕๐

เป็นปีที่ ๖๒ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ผู้ให้บริการ” หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑
ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ

จะต้องรับโทษภายในราชอาณาจักร

หมวด ๒
พนักงานเจ้าหน้าที่

มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

มาตรา ๑๙ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๘ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๘ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้วพนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรา ๒๐ ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสอง ลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

มาตรา ๒๑ ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

มาตรา ๒๗ ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา ๑๘ หรือมาตรา ๒๐ หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา ๒๑ ต้องระวางโทษปรับไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

มาตรา ๒๘ การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา ๒๙ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

มาตรา ๓๐ ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง

บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้รับสนองพระบรมราชโองการ
พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวพิญดา เลิศกิตติกุล เกิดเมื่อวันที่ 27 พฤศจิกายน 2524 จังหวัดชลบุรี จบการศึกษาระดับอุดมศึกษาจากคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ปีการศึกษา 2545 สอบไล่ได้ความรู้ชั้นเนติบัณฑิต สมัยที่ 56 ปีการศึกษา 2546 เข้าศึกษาต่อในระดับปริญญาโท ปีการศึกษา 2548 เริ่มรับราชการเมื่อ 3 เมษายน 2549 ในตำแหน่งนิติกร 3 ศาลอุทธรณ์ภาค 9 จนถึงปัจจุบัน